Le Frido 2026
volume 1
Laurent Claessens

Plusieurs extensions et versions de ce livre.

1. La version courante, régulièrement mise à jour et qui deviendra petit à petit le Frido 2027. Téléchargeable sur

   `https://laurent.claessens-donadello.eu/pdf/lefrido.pdf`

2. La version la plus complète, contenant beaucoup de géométrie différentielle

   `https://laurent.claessens-donadello.eu/pdf/giulietta.pdf`

3. Et bien entendu les sources LaTeX

   `https://github.com/LaurentClaessens/mazhe`

Copyright 2011-2026 Laurent Claessens, and many contributors. A complete list could be retrieved from the git log.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the chapter entitled “GNU Free Documentation License”.

(c) 2015-2026 David Revoy pour les illustrations de couverture CC-BY,
https://www.peppercarrot.com/

ISBN : 979-10-97085-46-9

Index thématique

1 : cardinalité
2 : morphismes et compagnie
3 : arithmétique modulo, théorème de Bézout, théorème chinois
4 : divisibilité
5 : équations diophantiennes
6 : types d'anneaux
7 : sous-groupes
8 : groupe symétrique
9 : action de groupe
10 : classification de groupes
11 : fonction indicatrice (totient) d'Euler
12 : produit semi-direct de groupes
13 : théorie des représentations
14 : espaces vectoriels
15 : rang
16 : formes bilinéaires et quadratiques
17 : endomorphismes cycliques
18 : extension de corps et polynômes
19 : polynômes
20 : polynôme d'endomorphismes
21 : dualité
22 : injections
23 : tribu, algèbre de parties, λ-systèmes et co.
24 : théorie de la mesure
25 : normes
26 : inégalités
27 : constructions topologiques
28 : espaces métriques, normés
29 : limite et continuité
30 : intégration
31 : connexité
32 : séparabilité
33 : compacts
34 : densité
35 : application réciproque
36 : applications continues et bornées
37 : suite de Cauchy, espace complet
38 : caractérisations séquentielles
39 : valeurs propres, définie positive
40 : norme matricielle, norme opérateur et rayon spectral
41 : série de matrices
42 : décomposition de matrices
43 : systèmes d'équations linéaires
44 : réduction, diagonalisation
45 : déterminant
46 : espaces de fonctions
47 : fonctions lipschitziennes
48 : suites et séries
49 : suite de fonctions
50 : exponentielle
51 : logarithme
52 : fonction puissance
53 : sommation finie et infinie
54 : polynôme de Taylor
55 : formule des accroissements finis
56 : dérivation
57 : différentielle
58 : équations différentielles
59 : convexité
60 : espaces de Hilbert, base hilbertienne
61 : analyse complexe, fonctions holomorphes
62 : permuter des limites
63 : types de convergence
64 : déduire la nullité d'une fonction depuis son intégrale
65 : inversion locale, fonction implicite
66 : points fixes
67 : changement de variables
68 : techniques de calcul
69 : méthodes de calcul
70 : méthode de Newton
71 : prolongement d'applications
72 : opérations sur les distributions
73 : convolution
74 : séries de Fourier
75 : transformée de Fourier
76 : gaussienne
77 : lemme de transfert
78 : invariants de similitude
79 : isométries
80 : enveloppes
81 : intégration sur des variétés
82 : dénombrements
83 : caractérisation de distributions en probabilités
84 : théorème central limite
85 : indépendance d'événements et de variables aléatoires
86 : probabilités et espérances conditionnelles
87 : chaine de Markov

THEMEooCARDINALITE

Thème 1 : cardinalité Le Frido[1] ne définit pas la notion de nombre cardinal ; ça nous mènerait trop loin. Au lieu de cela, nous allons nous contenter des notions d'équipotence, surpotence et subpotence, et démontrer un certain nombre de résultats en utilisant sans retenue le lemme de Zorn 1.42.

(1) Ensemble infini, définition 1.74.

(2) Ensemble dénombrable, définition 2.34.

(3) Cardinal d'un ensemble fini, définition 2.24.

[1] Ici je mets les références [1, 2, 3, 4] ; pas parce qu'elles sont utiles ici, mais parce que je veux être sûr qu'elles aient les premiers numéros de façon à être facilement reconnaissable. Elle indique les affirmations à propos desquelles le lecteur doit être doublement attentif.

(4) Définition d'équipotence, surpotence et subpotence, notations $A \succ B$ et $A \approx B$, définition 1.71.

(5) Toute partie d'un ensemble fini est finie, lemme 1.76.

(6) Si A est un ensemble fini ou dénombrable, alors il existe une surjection $\mathbb{N} \to A$, lemme 2.44.

(7) Si A est un ensemble infini et si $f\colon A \to B$ est une application injective, alors $f(A)$ est infini, proposition 1.79.

(8) Toute partie infinie de $\mathbb{N}$ est dénombrable, proposition 2.35

(9) Une bijection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, proposition 2.38.

(10) Une décomposition de $\mathbb{N}$ en une infinité de parties équipotentes à $\mathbb{N}$, corolaire 2.40.

(11) Si il existe une surjection $\mathbb{N} \to A$, alors A est fini ou dénombrable, lemme 2.41.

(12) Une union dénombrable d'ensembles finis ou dénombrables est finie ou dénombrable, proposition 2.42

(13) Tout ensemble infini contient une partie en bijection avec $\mathbb{N}$, proposition 2.49.

(14) Toute partie d'un ensemble fini est finie, et toute partie d'un ensemble dénombrable est finie ou dénombrable, proposition 2.50.

(15) Si $A \succeq B$ et $B \succeq A$, alors $A \approx B$, théorème de Cantor-Schröder-Bernstein 1.84

(16) Le théorème de Cantor 1.88 dit qu'il n'existe pas de surjection d'un ensemble vers son ensemble des parties. On en déduit qu'il n'existe pas d'ensemble contenant tous les ensembles (corolaire 1.90).

(17) Si A est infini et si $A \succeq B$, alors $A \approx A \cup B$ par le lemme 2.54.

(18) Si S est un ensemble infini alors il existe une bijection $\varphi\colon \{0,1\} \times S \to S$, proposition 2.56.

(19) Si A est infini, alors $A \times \mathbb{N} \approx A$, proposition 2.59.

(20) Si A est infini et si $B \prec A$, alors $A \setminus B \approx A$, lemme 2.61.

(21) Si A est infini, alors $A \approx A \times A$, théorème 2.66.

Il y a aussi des résultats de cardinalité autour des extensions de corps.

(1) Si $\mathbb{K}$ est un corps infini, alors $\mathbb{K}[X] \approx \mathbb{K}$.

(2) Le théorème de Steinitz 8.134 affirme que tout corps admet une unique clôture algébrique. La preuve utilise pas mal de cardinalité ainsi que le lemme de Zorn 1.42.

THEMEooMorphisme2 THTOC2

Thème 2 : morphismes et compagnie Un morphisme est un concept algébrique. Il s'agit d'une application (pas spécialement inversible) qui préserve la structure. Quand on parle de morphisme, il faut donc préciser la structure. On dit « morphisme de groupe », « morphisme d'espace vectoriel », « morphisme d'anneaux », etc.

(1) Un morphisme de module est la définition 3.94.

(2) Un morphisme de groupes est la définition 1.95.

(3) Un morphisme d'anneaux est la définition 1.106.

(4) Un morphisme de corps est aussi la définition 1.106. Un corps n'a pas plus de structure qu'un anneau.

(5) Un isomorphisme d'espaces topologiques est une application continue, inversible, dont l'inverse est continue, 9.54. On dit aussi un homéomorphisme.

(6) Un difféomorphisme est différentiable d'inverse différentiable, définition 12.321.

(7) Un C^k-difféomorphisme est une application C^k d'inverse C^k. Définition 12.321.

NORMooTXFWooApjnOY

-1.1.
Le mot « homomorphisme » signifie exactement « morphisme », et, sauf incohérence de ma part, il n'est pas utilisé dans le Frido. Si vous tombez sur ce mot quelque part, soyez prudente, vérifiez dans le contexte si le mot attendu est bien « morphisme », et écrivez-moi.

THEMEooNRZHoBMTOO3

Thème 3 : arithmétique modulo, théorème de Bézout, théorème chinois

(1) Pour $\mathbb{Z}^*$ c'est le théorème 3.46.

(2) Existence d'un pgcd et d'un ppcm pour tout partie d'un anneau principal, proposition 3.191.

(3) Théorème de Bézout dans un anneau principal : proposition 3.200 qui dit que si $\delta \in \text{pgcd}(a,b)$ alors il existe u, v tels que $ua + vb = \delta$

(4) Théorème de Bézout dans un anneau de polynômes : théorème 8.47.

(5) En parlant des racines de l'unité et des générateurs du groupe unitaire dans le lemme 21.8. Au passage nous y parlerons de solfège.

(6) La proposition 3.55 qui donne tout entier assez grand comme combinaisons de a et b à coefficients positifs est utilisée en chaines de Markov, voir la définition 40.33 et ce qui suit.

(7) PGCD et PPCM sont dans la définition 1.113.

(8) Calcul effectif du PGCD puis des coefficients de Bézout : sous-sections 3.10.1.1 et 3.10.1.2.

(9) Dans un anneau principal il y a une relation entre idéal engendré et pgcd, ppcm : $(a)+(b) = \text{pgcd}(a,g)$ et $(a) \cap (b) = \text{ppcm}(a,b)$. C'est la proposition 3.203.

(10) Théorème des restes chinois. Il existe beaucoup de théorèmes chinois.

(10a) Dans un anneau principal, si $a = a_1 \dots a_r$ alors on a isomorphisme $A/(a) \simeq A/(a_1) \times \dots \times A/(a_r)$ par le théorème 3.204.

(10b) Version anneaux quotients : théorème 3.134.

(10c) Version congruence. Si les I_i sont des idéaux solutions à l'équation $x \in [a_i]_{I_i}$ sont donnés par la proposition 3.133.

THEMEooDIVTOO4

Thème 4 : divisibilité

(1) Si a divise[2] bc et si a est premier avec c, alors a divise b. Lemme de Gauss 3.58. Pour les anneaux principaux, lemme 3.201.

(2) Si a divise b et b divise a, alors $a = b$, lemme 3.60.

THEMEooDiophTOO5

Thème 5 : équations diophantiennes

(1) Équation $ax + by = c$ dans $\mathbb{N}$, équation (3.273).

(2) Dans 3.10.6, nous résolvons $ax + by = c$ en utilisant Bézout (théorème 3.46).

(3) L'exemple 3.220 donne une application de la pure notion de modulo pour $x^2 = 3y^2 + 8$. Pas de solutions.

(4) L'exemple 3.221 résout l'équation $x^2 + 2 = y^3$ en parlant de l'extension $\mathbb{Z}[i\sqrt{2}]$ et de stathme.

(5) Les propositions 3.225 et 3.227 parlent de triplets pythagoriciens.

(6) Le dénombrement des solutions de l'équation $\alpha_1 n_1 + \dots \alpha_p n_p = n$ utilise des séries entières et des décompositions de fractions en éléments simples, théorème 28.105.

(7) La proposition 2.38 donne une bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ en résolvant dans $\mathbb{N}$ (entre autres) l'équation $k = y^2 + x$ pour k fixé.

[2]Divise, définition 1.109.

THEMEooVIQIooOHTAQS

Thème 6 : types d'anneaux

(1) Définition d'anneau : définition 1.100.

(2) La définition d'anneau principal est 3.37 ; pour un idéal principal, c'est 3.36.

(3) $\mathbb{Z}$ est une anneau intègre[3], lemme 3.34, principal et euclidien (proposition 3.39).

(4) $\mathbb{Z}[X]$ n'est pas principal (voir (5)).

ITEMooNQQMooSnuKvW

(5) Si A est un anneau intègre qui n'est pas un corps, alors $A[X]$ n'est pas principal, lemme 3.135.

(6) L'anneau des fonctions holomorphes sur un compact donné est principal, proposition 28.70.

(7) L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel, exemple 3.199.

(8) L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est ni factoriel ni principal, exemple 3.211.

(9) Tous les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont principaux, mais $\mathbb{Z}/6\mathbb{Z}$ n'est pas principal. Exemple 3.130.

anneau principal

- Définition 3.37.
- Il est intègre, définition 3.37.
- Il est noetherien, lemme 3.207.
- il est factoriel, théorème 3.209.

anneau euclidien

- Définition 3.33.
- Il est principal par 3.38

anneau intègre

- Définition 3.22.

anneau noetherien

- Définition 3.206.

anneau factoriel

- Définition 3.194.
- Il est intègre, définition 3.194.

corps

- Corps, définition 1.213.
- Il est un anneau intègre, lemme 3.23.
- Il est un anneau principal, proposition 3.210.
- Il est un anneau factoriel, proposition 3.210.

Dans un anneau intègre

- Un anneau fini intègre est un corps, proposition 3.192.
- A est intègre si et seulement si $A[X]$ est intègre, théorème 3.260.
- Si un pgcd[4] est inversible, tous les pgcd sont inversibles, lemme 3.26.

Dans un anneau principal

- p est premier si et seulement si il est irréductible si et seulement si l'idéal pA est maximal, proposition 3.93.
- Tous les idéaux sont principaux, définition 3.37.

[3] Définition 3.22.
[4] pgcd, définition 1.113.

- Si $\text{pgcd}(a,b)=1$, $\text{pgcd}(a,c)=1$, alors $\text{pgcd}(a,bc)=1$, lemme 3.202.

Dans un anneau factoriel

- Si p est irréductible et si $p \mid ab$, alors p divise a ou b, lemme 3.195.
- Tout élément irréductible est premier, proposition 3.196.
- Si p est irréductible, pA est un idéal premier, lemme 3.197.
- Si p est irréductible, A/pA est un anneau intègre, lemme 3.197 et proposition 3.90.
- P et Q sont primitifs si et seulement si PQ est primitif, lemme 3.275.
- Formule $c(PQ)=c(P)c(Q)$. Lemme 3.275.
- L'anneau des polynômes $\mathcal{P}(A)=A[X]$ est factoriel, théorème 8.35.

Dans un corps commutatif

- L'anneau $\mathbb{K}[X]$ est factoriel, proposition 8.36, euclidien et principal, lemme 3.266.
- Les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$, lemme 3.5.
- L'anneau $\mathcal{P}(\mathbb{K})$ est euclidien, lemme 3.266.

élément irréductible

- Définition 3.14

élément premier

- Définition 3.13
- Si A est intègre et unitaire, l'élément p est premier si et seulement si l'idéal pA est premier, proposition 3.25.

éléments associés

- Définition 3.184.

Dans un anneau, un idéal est 3.3.

idéal premier

- Définition 3.88.
- Idéal premier si et seulement si A/I est anneau intègre, proposition 3.90.

idéal maximal

- Idéal maximal si et seulement si A/I est un corps, proposition 3.90.

idéal principal

- Définition 3.36.
- Dans un anneau unitaire intègre, p est irréductible si et seulement si il n'y a pas d'idéal principal I tel que $pA \subsetneq I \subsetneq A$, proposition 3.25.

THEMEooSou

Thème 7 : sous-groupes

(1) Théorème de Burnside sur les sous-groupes d'exposant fini de $\text{GL}(n,\mathbb{C})$, théorème 10.314.

(2) Sous-groupes compacts de $\text{GL}(n,\mathbb{R})$, lemme 15.46 ou proposition 15.47.

THEMEooQEEWo

Thème 8 : groupe symétrique

(1) Définition 2.2.

(2) La signature $\epsilon\colon S_n \to \{-1,1\}$ est l'unique morphisme surjectif de S_n sur $\{-1,1\}$, proposition 2.124(1).

(3) La table des caractères du groupe symétrique S_4 est donné dans la section 18.5.

(4) Le groupe symétrique S_4 est le groupe des symétries affines du tétraèdre régulier[5], proposition 20.207.

(5) Le groupe alterné A_5 est l'unique groupe simple d'ordre[6] 60, proposition 7.54.

(6) La proposition 7.44 donne la position du groupe alterné dans le groupe symétrique : A_n est un sous-groupe caractéristique de S_n, et l'unique sous-groupe d'indice 2.

[5] Définition 14.183.
[6] Ordre d'un groupe, définition 2.30.

THEMEooKZHBoo THCOG9

Thème 9 : action de groupe

(1) Définition d'une action de groupe sur un ensemble : 3.236.

(2) Action du groupe modulaire sur le demi-plan de Poincaré, théorème 25.96.

(3) La formule de Burnside (théorème 5.27) parle du nombre d'orbites pour l'action d'un groupe fini sur un ensemble fini.

(4) Des applications de la formule de Burnside : le jeu de la roulette et l'affaire du collier, 20.11.15.1 et 20.11.15.2.

(5) Le groupe symétrique S_n agit sur l'anneau $\mathbb{K}[T_1, \dots, T_n]$, lemme 3.237.

THEMEooTheorieGroupe THCOG10

Thème 10 : classification de groupes

(1) Ordre d'un groupe, définition 2.30.

(2) Structure des groupes d'ordre pq, théorème 7.25.

(3) Le groupe alterné est simple, théorème 7.50.

(4) Définition 7.6 d'un p-groupe.

(5) Théorème de Sylow 7.11.

(6) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 10.314.

(7) $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, corolaire 21.34.

(8) Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, proposition 3.293.

(9) Le premier théorème d'isomorphisme 2.20 dit que si θ est un morphisme de groupes, alors $G/\ker(\theta) = \mathrm{Image}(\theta)$.

(10) Le deuxième théorème d'isomorphisme 2.21 dit que si N est normal dans G, alors $NH/N = H/(H \cap N)$.

(11) Le troisième théorème d'isomorphisme 2.23 dit que, avec des hypothèses de normalité, $(G/M)/(N/M) = G/N$.

À propos d'ordre dans un groupe.

(1) L'ordre d'un groupe est son cardinal. L'ordre d'un élément est le plus petit n tel que $g^n = e$, définition 2.68.

(2) L'ordre d'un élément divise l'ordre du groupe, corolaire 2.74.

(3) Si H est normal dans G, alors $|G/H| = |G|/|H|$, théorème de Lagrange 2.73.

(4) Si G est un groupe cyclique, pour tout diviseur p de $|G|$, le groupe G contient au moins un élément d'ordre p. Théorème de Cauchy 3.164.

THMooUDYMooTHCOG11

Thème 11 : fonction indicatrice (totient) d'Euler

(1) Définition de $\varphi\colon \mathbb{N}^* \to \mathbb{N}^*$ dans 7.29.

(2) Propriétés genre $\varphi(pq) = \varphi(p)\varphi(q)$, corolaire 7.42.

(3) Si p est premier, alors $\varphi(p^k) = p^k - p^{k-1}$, lemme 7.39.

(4) $\varphi(n) = \mathrm{Card}(\Delta_n)$, proposition 21.14.

(5) $n = \sum_{d|n} \varphi(d)$, lemme 7.38.

(6) Le théorème de Euler-Fermat 7.34 donne $a^{\varphi(n)} \in [1]_n$ dès que a et n sont premiers entre eux.

(7) Si A et B sont premiers entre eux, il existe p, m tels que $A^p = mB + 1$, proposition 7.34.

THEMEooProduitSemiDirectTHGT0012

Thème 12 : produit semi-direct de groupes

(1) Définition 2.158.

(2) Le corolaire 2.161 donne un critère pour prouver qu'un produit NH est un produit semi-direct.

(3) L'exemple 20.189 donne le groupe des isométries du carré comme un produit semi-direct.

(4) Le théorème 7.25 classifie les groupes d'ordre pq (p, q premiers distincts) à grands coups de produit semi-directs.

(5) Le théorème 20.85 donne les isométries de $\mathbb{R}^n$ par $\mathrm{Isom}(\mathbb{R}^n) = T(n) \times_\rho O(n)$ où $T(n)$ est le groupe des translations.

(6) La proposition 20.87 donne une décomposition du groupe orthogonal $\mathrm{O}(n) = \mathrm{SO}(n) \times_\rho C_2$ où $C_2 = \{\mathrm{Id}, R\}$ où R est de déterminant -1.

(7) La proposition 13.63 donne $\mathrm{Aff}(\mathbb{R}^n) = T(n) \times_\rho \mathrm{GL}(n, \mathbb{R})$ où $\mathrm{Aff}(\mathbb{R}^n)$ est le groupe des applications affines bijectives de $\mathbb{R}^n$.

THEMEooTheorieRepresentationsTHGT0013

Thème 13 : théorie des représentations

(1) Définition 6.153.

(2) Table des caractères du groupe diédral, section 20.18.

(3) Table des caractères du groupe symétrique S_4, section 18.5.

THEMEooMethodeGauss0014

Thème 14 : espaces vectoriels

(1) Les notations $\mathcal{L}(V, W)$, $\mathcal{L}^0(V, W)$, $\mathrm{GL}(V, W)$ ainsi que les notions de morphismes et d'isomorphismes d'espaces vectoriels normés sont dans la définition 12.331.

(2) Existence d'une base. Pour un espace vectoriel quelconque, proposition 6.27.

(3) Théorème de la base incomplète. Pour un espace vectoriel quelconque, théorème 6.28.

(4) En dimension finie, tout sous-espace vectoriel est fermé, corolaire 9.250.

THEMEooDimensionTHGT0015

Thème 15 : rang

(1) Définition pour une application linéaire : 6.51, pour une matrice : 6.116. L'équivalence est la proposition 6.120.

(2) Le théorème du rang, théorème 6.53

(3) Pour une applicaton linéaire entre deux espaces vectoriels de même dimension finie, il est équivalent d'être injectif, surjectif ou bijectif, c'est le corolaire 6.56.

(4) Pour prouver que des matrices sont équivalentes et pour les mettre sous des formes canoniques, nous avons le lemme 6.127 et son corolaire 6.128.

(5) Tout hyperplan[7] de $\mathbb{M}(n, \mathbb{K})$ coupe $\mathrm{GL}(n, \mathbb{K})$, corolaire 6.128. Cela utilise la forme canonique susmentionnée.

(6) Le lien entre application duale et orthogonal de la proposition 10.193 utilise la notion de rang.

(7) Le lemme 10.303 parle de commutant et utilise la notion de rang. Ce lemme sert à prouver diverses conditions équivalentes à être un endomorphisme cyclique dans le théorème 10.304.

[7] Définition 10.307.

THEMEooOAJKTHEOCV16

Thème 16 : formes bilinéaires et quadratiques

(1) Les formes bilinéaires sont définies en 10.120.

(2) Forme quadratique, définition 10.121.

(3) Équivalence de forme quadratiques, définition 10.253. Deux formes quadratiques sont équivalentes si et seulement si elles ont même signature, proposition 10.254.

(4) Une isométrie d'une forme bilinéaire est affine ou linéaire, théorème 10.153.

(5) Forme bilinéaire dégénérée, définition 10.125.

(6) Une forme bilinéaire est non-dégénérée si et seulement si sa matrice associée est inversible, c'est la proposition 10.230.

(7) Une isométrie d'une forme bilinéaire est linéaire ou affine par le théorème 10.153.

(8) Toute forme quadratique admet des bases orthogonales, théorème 10.246 pour le cas général ; proposition 10.257 pour le cas de $\mathbb{R}^n$, en se basant sur le théorème spectral.

(9) Base q-orthogonale pour une forme quadratique, théorème 10.246.

(10) Le concept de projection orthogonale est la définition 14.151 en dimension finie et la définition 27.6 dans le cas des espaces de Hilbert.

(11) Produit hermitien, définition 10.174. Opérateur hermitien ($A^\dagger = A$), opérateur unitaire ($A^\dagger A = 1$), définition 10.177

matrice

(1) Matrice d'une forme quadratique, définition 10.144.

(2) Théorème de Sylvester à propos de signature (définition 10.159) de forme quadratique réelle : 10.252.

orthogonalité

(1) Il existe une base q-orhogonale, proposition 10.244 et théorème 10.246.

(2) Définition de l'orthogonal $A^\perp$ et du noyau $\ker(b)$, définitions 10.127, 10.128.

(3) Diverses propriétés comme $A^\perp = \mathrm{Span}(A)^\perp$ et $V \cap V^\perp = \ker(b_V)$, propositions 10.129 et 10.130.

(4) En dimension finie, $(V^\perp)^\perp = V$, lemme 10.133.

(5) Nous avons $\dim(V) + \dim(V^\perp) = \dim(E)$, lemme 10.132.

(6) Pour une forme quadratique strictement définie positive ou négative, $E = F \oplus E^\perp$, lemme 10.135.

THEMEooEndoCYCLQU17

Thème 17 : endomorphismes cycliques

(1) Définition 10.101.

(2) Groupe cyclique, définition 2.149.

(3) Son lien avec le commutant donné dans la proposition 10.301 et le théorème 10.304.

(4) Utilisation dans le théorème de Frobenius (invariants de similitude), théorème 10.292.

THEMEooZYKFoEQCOP18

Thème 18 : extension de corps et polynômes

(1) Définition d'une extension de corps 8.59.

(2) Définition de polynôme minimal : 8.64.

(3) Pour l'extension du corps de base d'un espace vectoriel et les propriétés d'extension des applications linéaires, voir la section 10.15.

(4) Extension de corps de base et similitude d'application linéaire (ou de matrices, c'est la même chose), théorème 10.306.

(5) Extension de corps de base et cyclicité des applications linéaires, corolaire 10.305.

(6) À propos d'extensions de $\mathbb{Q}$, le lemme 8.182.

(7) Corps de rupture : définition 8.113 existence par la proposition 8.119. Il n'y a pas unicité.

(8) Corps de décomposition : définition 8.141. Attention : le plus souvent nous parlons de corps de décomposition d'un seul polynôme. Cette définition est un peu surfaite. Existence par la proposition 8.142 qui le donne même comme extension par toutes les racines, et unicité à isomorphisme près par le théorème 8.144, énoncé de façon plus simple (mais pas indépendante !) en la proposition 8.145.

(9) Corps de rupture Vs corps de décomposition. Un corps de rupture est un corps dans lequel le polynôme est cassé en deux ; le corps de décomposition est celui où il se casse en tous ses morceaux. Donc si un polynôme a plein de racines, un corps de rupture doit en contenir une alors que le corps de décomposition doit toutes les contenir.

(10) Si $\mathbb{K}$ est algébrique clos et si $\alpha\colon \mathbb{K} \to \mathbb{L}$ est une extension algébrique, alors $\alpha(\mathbb{K}) = \mathbb{L}$ par le lemme 8.80.

Un trio de résultats qui fait du bon boulot ensemble :

(1) Dans un anneau principal qui n'est pas un corps, un idéal est maximal si et seulement si il est engendré par un irréductible[8] (proposition 3.126).

(2) Dans un anneau, un idéal I est maximal si et seulement si A/I est un corps (proposition 3.86)

(3) Si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est principal (lemme 3.266).

THEMEoo

Thème 19 : polynômes

Définitions Soient un anneau A, un corps $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ et un élément $\alpha \in \mathbb{L}$.

(1) La définition la plus formelle est en tant que module produit $A^{(\mathbb{N})}$, définition 3.228. Le produit et l'évaluation sont définis en 3.231 et la formule $(PQ)(x) = P(x)Q(x)$ dans 3.232.

(2) Si $\mathbb{A}$ est commutatif, alors $\mathbb{A}[X]$ est également commutatif, lemme 3.233.

(3) En ce qui concerne la notation $A[X]$, elle ne devrait pas être utilisée, voir 3.15.2. L'ensemble des polynômes sera noté $\mathcal{P}(A)$ et ceux de degré n (définition 3.230), $\mathcal{P}_n(A)$.

(4) $A[X]$, définition 3.228 ; l'anneau $\mathbb{K}[X]$ a même définition parce que c'est un cas particulier. L'évaluation d'un polynôme en un élément de l'anneau, $P(\alpha)$ est définie en 3.231.

(5) Liens entre $\mathbb{K}[\alpha]$, $\mathbb{K}[X]$, $\mathbb{K}(\alpha)$ et $\mathbb{K}(X)$ lorsque α est transcendant, proposition 8.100.
Et la proposition 8.103 pour le cas où α est algébrique[9].

(6) Si A est un anneau et si α est un élément d'une extension de A (comme anneau), nous écrivons $A[\alpha]$ pour le plus petit sous-anneau de B contenant A et α. C'est la définition 3.258.

(7) $\mathbb{K}(X)$, le corps des fractions de $\mathbb{K}[X]$, définition 8.84. Si $R = P/Q$ dans $\mathbb{K}(X)$, l'évaluation est $R(\alpha) = P(\alpha)Q(\alpha)^{-1}$, définition 8.85.

(8) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est le plus petit corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α, définition 8.86.

(9) À propos de polynômes à plusieurs variables.

- Anneau de polynômes : $A[X_1, \dots, X_n]$ est la définition 3.180.
- Corps engendré : $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ est la définition 8.138.
- Corps des fractions rationnelles : $\mathbb{K}(X_1, \dots, X_n)$ est la définition 8.139.

contenu À propos de $c(P)$.

(1) Définition du contenu $c(P)$, 3.269.

(2) $c(PQ) = c(P)c(Q)$, lemme de Gauss 21.48, et lemme 3.275 pour un anneau factoriel.

(3) Si $c(P) = 1$, on dit que P est primitif au sens des pgcd, définition 3.271.

(4) Si $a \in A$ nous avons $c(aP) = ac(P)$ par le lemme 3.27.

(5) Un polynôme primitif est la définition 3.271.

[8] Irréductibilité, y compris polynôme irréductible, définition 3.14.
[9] Définition 8.71.

Dérivation Plusieurs propriétés du polynôme dérivé P'.

(1) La définition 8.154 donne $P' = \sum_{k=1}^{n} k a_i X^{k-1}$.

(2) Règle de Leibniz, lemme 8.155.

(3) Caractérisation de $P' = 0$ en fonction de la caractéristique de $\mathbb{K}$, lemme 8.156.

Coefficients dans un anneau commutatif (1) Les polynômes à coefficients dans un anneau commutatif sont à la section 3.16.

(2) Un anneau A est intègre si et seulement si $A[X]$ est intègre ; théorème 3.260.

Coefficients dans un corps Les polynômes à coefficients dans un corps sont à la section 8.3.

(1) Si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est euclidien et principal, lemme 3.266.

(2) Nous parlons de l'idéal des polynômes annulateurs dans le théorème 8.43.

(3) Le théorème 8.43 dit que $\mathbb{K}[X]$ est un anneau principal et que tous ses idéaux sont engendrés par un unique polynôme unitaire.

(4) Le polynôme minimal est irréductible, proposition 8.67.

(5) Quelques formules sur le pgcd, lemme 8.57.

Polynôme primitif (1) Un polynôme est irréductible sur A si et seulement si il est irréductible et primitif sur le corps des fractions, corolaire 3.290.

Polynôme d'endomorphisme C'est la section 10.7.

Racines et factorisation (1) Si $\mathbb{A}$ est un anneau, la proposition 3.279 factorise une racine.

(2) Si $\mathbb{A}$ est un anneau, la proposition 3.284 factorise une racine avec sa multiplicité.

(3) Si $\mathbb{A}$ est un anneau, le théorème 3.286 factorise plusieurs racines avec leurs multiplicités.

(4) Le théorème 3.286 nous indique que lorsqu'on a autant de racines (multiplicité comprise) que le degré, alors nous avons toutes les racines.

(5) Si $\mathbb{K}$ est un corps et α une racine dans une extension, le polynôme minimal de α divise tout polynôme annulateur par la proposition 8.101.

(6) Le théorème 8.110 annule un polynôme de degré n ayant $n+1$ racines distinctes.

(7) La proposition 8.185 nous annule un polynôme à plusieurs variables lorsqu'il a trop de racines.

(8) En analyse complexe, le principe des zéros isolés 19.164 annule en gros toute série entière possédant un zéro non isolé.

(9) Polynômes irréductibles sur $\mathbb{F}_q$.

THEMEooPolynomeEndomorphismes THEME20

Thème 20 : polynôme d'endomorphismes

(1) Endomorphismes cycliques et commutant dans le cas diagonalisable, proposition 10.301.

(2) Racine carrée d'une matrice hermitienne positive, proposition 15.33.

(3) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 10.314.

(4) Décomposition de Dunford, théorème 10.265.

(5) Algorithme des facteurs invariants 6.129.

THEMEooULGFDHSOC21

Thème 21 : dualité Ne pas confondre dual algébrique et dual topologique d'un espace vectoriel.

(1) Dual algébrique E^*, définition 6.143.

(2) Dual topologique E', définition 9.338.

(3) Le dual d'un espace de Banach est de Banach, proposition 12.93.

(4) Définition de la base duale 6.144.

(5) $\dim(E) = \dim(E^*)$, lemme 6.144.

(6) Base préduale (existence, unicité) : proposition 6.148.

(7) Théorème de représentation de Riez 29.188 : $L^p = (L^q)'$, et en particulier $L^\infty = (L^1)'$.

(8) Il n'est pas vrai que $(L^\infty)' = L^1$, voir la proposition 29.258.

(9) Dans un espace de Banach[10], $\|x\| = \max_{\substack{\varphi \in E' \\ \|\varphi\|=1}} |\varphi(x)|$, proposition 29.173.

Dual topologique et algébrique Ils sont définis par 6.143. Le dual algébrique est l'ensemble des formes linéaires, et le dual topologique ne considère que les formes linéaires continues (en dimension infinie, les applications linéaires ne sont pas toutes continues).

Topologie Une topologie possible sur le dual d'un espace vectoriel topologique est celle $*$-faible de la définition 9.429.

Nous comparons les topologies faibles et de la norme en la section 12.19.

Théorèmes de dualité Quelques théorèmes établissent des dualités entre des espaces courants.

(1) En dimension finie, $x \mapsto b(x, .)$ est isomorphisme $E \to E^*$ lorsque b est une forme bilinéaire, proposition 10.131.

(2) Le théorème de représentation de Riesz 27.17 pour les espaces de Hilbert.

(3) La proposition 29.186 pour les espaces $L^p\big([0,1]\big)$ avec $1 < p < 2$.

(4) Le théorème de représentation de Riesz 29.188 pour les espaces L^p en général.

Tous ces théorèmes donnent la dualité par l'application $\Phi_x = \langle x, . \rangle$.

THEMEooInjectionsTHEOC22

Thème 22 : injections

(1) L'espace de Sobolev $H^1(I)$ s'injecte de façon compacte dans $C^0(\bar{I})$, proposition 33.6.

(2) L'espace de Sobolev $H^1(I)$ s'injecte de façon continue dans $L^2(I)$, proposition 33.6.

(3) L'espace $L^2(\Omega)$ s'injecte continument dans $\mathscr{D}'(\Omega)$ (les distributions), proposition 32.34.

INTooVDSCoTHXLC23

Thème 23 : tribu, algèbre de parties, λ-systèmes et co. Il existe des centaines de notions de mesures et de classes de parties.

(1) Mesure positive, définition 16.18.

(2) Tribu, définition 16.1.

(3) Une mesure extérieure est la définition 16.10

(4) Une algèbre de partie : définition 16.13. Une mesure sur une algèbre de parties : définition 16.11. L'intérêt est que si on connait une mesure sur une algèbre de parties, elle se prolonge en une mesure sur la tribu engendrée par le théorème de prolongement de Hahn 16.82.

(5) Un λ-système : définition 16.31.

(6) Un π-système : définition 16.34.

(7) Une mesure complexe : définition 16.241.

En théorie de l'intégration, si X est une partie de $\mathbb{R}^n$, la convention est de considérer des fonctions

$$f\colon \big(X, \mathcal{L}\mathrm{eb}(X)\big) \to \big(\mathbb{R}, \mathcal{B}\mathrm{or}(\mathbb{R})\big).$$

Voir les points 16.122 et 16.168 pour les conventions à ce propos.

À propos d'applications mesurables :

(1) Définition d'une application mesurable, définition 16.46.

(2) Une fonction continue est borélienne, théorème 16.58.

(3) Si les f_n sont mesutables (au sens des boréliens), alors $\sup_n f_n$ est mesurable, lemme 16.102.

À propos de tribu induite :

[10] Espace de Banach, définition 9.339.

(1) Définition 16.8.

(2) Les boréliens induits sont bien les boréliens de la topologie induite[11] : $\mathcal{B}\mathrm{or}(Y) = \mathcal{B}\mathrm{or}(X)_Y$, théorème 16.59.

Tribu engendrée.

(1) Tribu engendrée par des parties, définition 16.4.

THEMEooKLVRTHEQCQ4

Thème 24 : théorie de la mesure

Mesure À propos de mesure.

(1) Tribu des boréliens, définition 16.52.
(2) Mesure positive, mesure finie et σ-finie, c'est la définition 16.18.
(3) Le produit de tribus est donné par la définition 16.129,
(4) Une union dénombrable de parties de mesure nulle est de mesure nulle, lemme 16.28.
(5) Produit d'une mesure par une fonction, définition 16.214.
(6) le produit d'espaces mesurés est donné par la définition 16.249.
(7) Mesure de Lebesgue sur $\mathbb{R}$, définition 16.145.
(8) Une partie de $\mathbb{R}$ non mesurable au sens de Lebesgue : l'exemple 16.159.
(9) Mesure de Lebesgue sur $\mathbb{R}^N$, définition 16.251.
(10) Mesure à densité, définition 16.214.

Opérations On peut faire quelques opérations sur les mesures.

(1) Si w est une fonction et μ une mesure, on définit $w \cdot \mu$ par 16.214 : $(w \cdot \mu)(A) = \int_A w d\mu)$.

Théorèmes d'approximation Il est important de pouvoir approcher des fonctions continues ou L^p par des fonctions étagées, sinon on ne parvient pas à faire tourner la machine de l'intégration de Lebesgue.

(1) Si $(S, \mathcal{A}, \mu)$ est un espace mesuré et si $f\colon S \to [0, +\infty]$ est une fonction mesurable, le théorème fondamental d'approximation 16.120 dit qu'il existe une suite croissante de fonctions étagées qui converge vers f.
(2) Les fonctions étagées sont denses dans L^p, proposition 29.59.
(3) Encadrement d'un borélien A par un fermé F et un ouvert V par le lemme 16.88 : $F \subset A \subset V$ avec $\mu(V \setminus F) < \epsilon$.
(4) Approximation L^p de la fonction caractéristique d'un borélien par une fonction continue par le théorème 16.244.

Produit (1) La tribu produit, définition 16.129.
(2) La mesure produit, définition 16.248.

THEMEooUJVXBHZDnG25

Thème 25 : normes

Définitions (1) Espace vectoriel normé : définition 9.232.
(2) Produit scalaire, définition 10.163.
(3) Norme associée à un produit scalaire (cas réel), théorème 12.1.
(4) Norme associée à une forme sesquilinéaire[12] (cas complexe), proposition 12.37.
(5) Identité du parallélogramme $\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2$, proposition 12.37.
(6) Produit scalaire sur $\mathbb{R}^n$, définition 10.168. Norme sur $\mathbb{R}^n$, définition 12.3.
(7) Forme hermitienne sur $\mathbb{C}^n$, définition 10.181. Norme sur $\mathbb{C}^n$, définition 12.38.
(8) La proposition 12.65 donne les normes $\|x\|_1$, $\|x\|_2$ et $\|x\|_\infty$ sur $\mathbb{R}^n$.
(9) Sur $\mathbb{R}^n$, la proposition 19.134 dit que $\|x\|_p$ est une norme.
(10) Norme d'une application n-multilinéaire, définition 12.118.

[11] Topologie induite, définition 9.30.
[12] Définition 10.174.

Topologie (1) Métrique associée à une norme $d(x,y) = \|x-y\|$, définition 9.237.
(2) La topologie d'un espace vectoriel normé est la topologie métrique du théorème 9.158.
(3) Les boules sont les boules métrique définies en (9.172).

Inégalités (1) En général pour les normes $\|.\|_p$, il y a des inégalités dans 19.135 et 19.127.
(2) La proposition 19.140 donne l'inégalité $\|x\|_q \leqslant n^{\frac{1}{q}-\frac{1}{p}}\|x\|_p$ dès que $0 < q < p$.

Équivalence de norme (1) Définition de l'équivalence de norme 12.67.
(2) La proposition 12.68 sur l'équivalence des normes $\|.\|_2$, $\|.\|_1$ et $\|.\|_\infty$ dans $\mathbb{R}^n$.
(3) Toutes les normes sur un espace vectoriel de dimension finie sont équivalentes par le théorème 12.70.

Autres (1) Montrer que le problème $a-b$ est stable dans l'exemple 36.27.
(2) La proposition 14.116 donnant $\rho(A) \leqslant \|A\|$ utilise l'équivalence de toutes les normes sur un espace vectoriel de dimension finie (théorème 12.70.).
(3) La norme $x \mapsto \|x\|$ est une application continue, proposition 9.311.

Norme opérateur et d'algèbre voir le thème 40.

THEMEooInegalitesNormesTHEMA0026

Thème 26 : inégalités Dans $\mathbb{C}$ nous avons $|a+b| \leqslant |a| + |b|$ par la proposition 11.103(1).

Inégalité de Clarkson Pour $f, g \in L^p$ nous avons l'inégalité de Clarkson 29.148 :

$$\|\frac{f+g}{2}\|_p^p + \|\frac{f-g}{2}\|_p^p \leqslant \frac{1}{2}\Big(\|f\|_p^p + \|g\|_p^p\Big). \tag{-1.1}$$

Inégalité de Young Nous avons

$$ab \leqslant \frac{a^p}{p} + \frac{b^q}{q} \tag{-1.2}$$

par la proposition 29.36.

Inégalité de Jensen (1) Une version discrète pour $f\big(\sum_i \lambda_i x_i\big)$, la proposition 19.131.
(2) Une version intégrale pour $f\big(\int \alpha d\mu\big)$, la proposition 29.37.
(3) Une version pour l'espérance conditionnelle, la proposition 38.89.

Inégalité de Hölder Il en existe de nombreuses versions et variations.

(1) Hölder pour L^p : $\|fg\|_1 \leqslant \|f\|_p \|g\|_q$, proposition 29.39.
(2) Hölder pour ℓ^p : $\|x\|_q \leqslant n^{\frac{1}{q}-\frac{1}{p}}\|x\|_p$, proposition 19.140.
(3) $\|x\|_\infty \leqslant \|x\|_p \leqslant n^{1/p}\|x\|_\infty$, théorème 19.135
(4) $\|x\|_p \leqslant n^{1/p}\|x\|_q$, corolaire 19.136.

Inégalité de Minkowsky (1) Pour une forme quadratique[13] q sur $\mathbb{R}^n$ nous avons $\sqrt{q(x+y)} \leqslant \sqrt{q(x)} + \sqrt{q(y)}$. Proposition 12.30.
(2) Si $1 \leqslant p < \infty$ et si $f, g \in L^p(\Omega, \mathcal{A}, \mu)$ alors $\|f+g\|_p \leqslant \|f\|_p + \|g\|_p$. Proposition 29.45.
(3) L'inégalité de Minkowsky sous forme intégrale s'écrit sous forme déballée

$$\left[\int_X \Big(\int_Y |f(x,y)|d\nu(y)\Big)^p d\mu(x)\right]^{1/p} \leqslant \int_Y \Big(\int_X |f(x,y)|^p d\mu(x)\Big)^{1/p} d\nu(y).$$

ou sous forme compacte

$$\left\|x \mapsto \int_Y f(x,y)d\nu(y)\right\|_p \leqslant \int_Y \|f_y\|_p d\nu(y)$$

C'est la proposition 29.50.

Transformée de Fourier Pour tout $f \in L^1(\mathbb{R}^n)$ nous avons $\|\hat{f}\|_\infty \leqslant \|f\|_1$, lemme 31.12.

Inégalité des normes Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leqslant \|f\|_p \|g\|_1$, proposition 29.83.

c_r inégalité La proposition 29.138 donne $\big|f(\omega)+g(\omega)\big|^r \leqslant c_r|f(\omega)|^r + c_r|g(\omega)|^r$.

[13] Définition 10.121.

THEMEooYRIWoBBYZooYRIX

Thème 27 : constructions topologiques

topologie produit Si X et Y sont des espaces topologiques, nous pouvons construire une topologie sur $X \times Y$.

(1) Dans le cas d'un produit infini, c'est la définition 9.65.

(2) La définition de la topologie produit est 9.66.

(3) Pour les espaces vectoriels normés, le produit est donné par la définition 9.305.

(4) L'équivalence entre la topologie de la norme produit et la topologie produit est le lemme 9.305.

(5) Quand V et W sont des espaces métriques, la topologie considérée sur $V \times W$ est celle de la définition 9.305. C'est à la fois la topologie de la norme produit et la topologie produit.

(6) La convergence dans un espace vectoriel est si et seulement si il y a convergence composante par composante, proposition 9.93.

(7) Dans le cas d'espaces normés, la topologie produit est la même que celle de la norme produit, lemme 9.306.

topologie induite Si X est un espace topologique et si A est une partie de X, nous mettons une topologie sur A.

(1) Le topologie induite, définition 9.30.

(2) Si X est un espace vectoriel normé, la topologie induite est celle de la norme restreinte : lemme 9.178.

topologie quotient Si X est topologique et si $\sim$ est une relation d'équivalence[14], nous définissons une topologie sur $X/\sim$.

(1) La topologie quotient est définie en 9.72.

(2) Si X est vectoriel normé, la topologie sur $X/\sim$ est aussi donnée par une norme quotient de la définition 9.426. La proposition 9.428 donne l'équivalence entre la topologie quotient et la norme quotient.

topologie rendant continues des applications Si nous avons une application $f\colon X \to Y$ et si Y est topologique, nous mettons une topologie sur X rendant f continue.

(1) Définition de la plus petite topologie rendant des applications continues, proposition 9.58.

THEMEooEspacesMetriqueHNYooYRIX

Thème 28 : espaces métriques, normés

(1) Un espace métrique est un ensemble muni d'une distance, définition 9.155.

(2) La distance uniforme dans le cas de fonctions à support compact est 9.299.

(3) La distance entre un point et un ensemble est la définition 9.217.

(4) Le théorème-définition 9.158 donne la topologie sur un espace métrique en disant que les boules ouvertes sont une base de la topologie (définition 9.2).

(5) La définition de la convergence d'une suite est la définition 9.14.

(6) Dans un espace vectoriel normé, une application est continue si et seulement si elle est bornée, proposition 12.98.

(7) Un espace vectoriel topologique[15] qui possède en tout point une base dénombrable de topologie accepte une distance, théorème 9.355.

[14] Définition 1.55 pour relation d'équivalence.
[15] Définition 9.239.

THEMEooGVCCoBHBCN20

Thème 29 : limite et continuité

(1) Limite d'une fonction en un point : définition 9.151. Il n'y a pas unicité en général comme le montre l'exemple 9.78 dans un espace non séparé.

(2) Définition de la continuité d'une fonction en un point et sur une partie de l'espace de départ : définition 9.48.

(3) Caractérisation de la limite dans $\mathbb{R}$, proposition 14.1.

(4) Unicité de la limite d'une suite dans un espace séparé : proposition 9.90. Unicité de la limite d'une fonction, toujours dans le cas d'un espace séparé : proposition 9.154.

(5) La proposition 9.432 donne l'unicité de la limite dans le cas des espaces duaux pour la topologie $*$-faible. La proposition 9.154 nous dira qu'il y a unicité dès que l'espace d'arrivée est séparé.

(6) Continuité sur une partie si et seulement si continue en chaque point, c'est le théorème 9.286.

(7) Voir l'exemple 14.55 traité en détail pour la (non) continuité d'une fonction qui fait un saut en un point.

(8) La fonction $(x, y) \mapsto x + y$ est continue, lemme 11.29.

THEMEooHINHoTKEVQW

Thème 30 : intégration À propos d'intégration.

Vocabulaire La différence entre une intégrale qui existe et une fonction intégrable est dans 16.189.

L'ordre dans lequel les choses sont faites

- Nous commençons par considérer des fonctions $f : \Omega \to [0, +\infty]$ dans la définition 16.169.
- Nous donnerons ensuite quelques propriétés restreintes aux fonctions à valeurs positives, par exemple
  (1) La convergence monotone 16.180,
  (2) Lemme de Fatou 16.184.
  (3) (presque) linéarité pour les fonctions positives, théorème 16.185.
- La définition pour les fonctions à valeurs dans $\mathbb{R}$ puis $\mathbb{C}$ est 16.188.
- Pour les fonctions à valeurs dans un espace vectoriel, c'est la définition 16.199.

primitive et intégrale (1) La définition 16.288 donne $\int_a^b f = \int_{]a,b[} f$ lorsque f est intégrable sur $]a, b[$.

(2) Lorsque f n'est pas intégrable sur $]a, b[$ nous pouvons poser $\lim_{x\to b} \int_a^b f$ et dire que c'est une intégrale impropre, définition 16.300.

(3) Si F et G sont primitives de f, alors $F = G + cst$, corolaire 14.225.

Quelque résultats (1) Intégrale associée à une mesure, définition 16.169

(2) L'existence d'une primitive pour toute fonction continue est le théorème 14.465.

(3) La définition d'une primitive est la définition 14.224.

(4) Primitive et intégrale, proposition 16.289.

(5) Intégrale impropre, définition 16.300.

Intégrale et mesure (1) L'intégrale de la fonction 1 donne la mesure : $\int_B 1 d\mu = \mu(B)$, c'est le lemme 16.177.

(2) Le théorème de Radon-Nikodym 16.237 donne une densité pour certaines mesures.

(3) Le produit d'une mesure par une fonction donnée par la définition 16.214 introduit aussi une densité : $(w \cdot \mu)(A) = \int_A w d\mu$.

Limite dans les bornes (1) Si $f : \mathbb{R} \to \mathbb{R}$ est intégrable alors $\lim_{b\to\infty} \int_{[a,b]} f = \int_{[0,\infty[} f$.

(2) Nous avons $\int_{\mathbb{R}} f = \lim_{R\to\infty} \int_{-R}^{R} f$ par la proposition 16.265.

Autre résultats (1) Si $A, B \subset \Omega$ sont des parties disjointes, alors $\int_{A\cup B} f = \int_A f + \int_B f$, proposition 16.196.

(2) La σ-additivité dénombrable, $\int_{\bigcup_i A_i} f d\mu = \sum_{i=0}^{\infty} \int_{A_i} f d\mu$ est dans les propositions 16.212 et 16.213.

THEMEooCHHOOO31

Thème 31 : connexité

(1) Définition 9.118

(2) L'image d'un connexe par une fonction continue est connexe, lemme 9.296.

(3) Un espace topologique est connexe si et seulement si il vérifie les valeurs intermédiaires, proposition 11.58.

(4) Dans un connexe, une partie ouverte et fermée est soit vide soit l'espace entier, proposition 9.121(4).

(5) Connexité par arcs, définition 11.66.

(6) Si U est connexe et si $U \subset S \subset \bar{U}$, alors S est connexe, proposition 9.122.

(7) Une partie de $\mathbb{R}^2$ qui est connexe, mais pas connexe par arcs, proposition 23.56.

(8) Une partie de $\mathbb{R}$ est connexe si et seulement si elle est un intervalle, proposition 11.54.

(9) Le groupe $\mathrm{SL}(n, \mathbb{K})$ est connexe par arcs, proposition 15.24.

(10) Le groupe $\mathrm{GL}(n, \mathbb{C})$ est connexe par arcs, proposition 15.25.

(11) Le groupe $\mathrm{GL}(n, \mathbb{R})$ a exactement deux composantes connexes par arcs, proposition 15.26.

(12) Le groupe $\mathrm{O}(n, \mathbb{R})$ n'est pas connexe, lemme 15.21.

(13) Les groupes $\mathrm{U}(n)$ et $\mathrm{SU}(n)$ sont connexes par arcs, lemme 15.22.

(14) Pour tout $n \geqslant 2$, le groupe $\mathrm{SO}(n)$ est connexe, le groupe $\mathrm{O}(n)$ a deux composantes connexes, proposition 15.8.

(15) Connexité des formes quadratiques de signature donnée, proposition 19.146.

(16) Dans un espace vectoriel normé, les connexes par arcs sont connexes par arcs C^1, proposition 17.6.

THEMEooSEPAOO32

Thème 32 : séparabilité

(1) Espace topologique normal, définition 9.98.

(2) Le dual d'un espace vectoriel normé sépare les points, corolaire 29.174.

(3) Les fermés et les compacts sont séparés dans un espace vectoriel topologique, proposition 9.344.

(4) Le théorème de Hahn-Banach 29.168 parle d'hyperplan qui sépare des parties convexes disjointes (et autres hypothèses).

(5) Les ouverts séparent les points et les compacts, lemme 9.148.

THEMEooQQBHOO33

Thème 33 : compacts

Propriétés générales Quelques propriétés de compacts.

(1) La définition d'un ensemble compact est la définition 9.125.

(2) Ne pas confondre le compactifié d'Alexandrov 9.204 avec la droite réelle achevée 14.26.

(3) Une partie est relativement compacte si sa fermeture est compacte, définition 9.145. Une union finie de relativement compacts est relativement compacte, lemme 9.147.

(4) Si M est un compact de $A \times B$, alors $M \subset K \times L$ où K est compact de A et L de B, proposition 9.143.

(5) Un fermé dans un compact est compact, lemme 9.137. L'intersection entre un compact et un fermé est compacte, proposition 9.138.

(6) Dans un espace Hausdorff[16], les compacts sont fermés, 9.137(2).

(7) Un espace est compact si et seulement si toute intersection finie de fermé est non vide, théorème 9.150.

[16] Hausdorff, définition 9.79.

(8) Un espace est compact si et seulement si toute famille de parties fermées ayant la propriété d'intersection finie a une intersection non vide, théorème 9.150

(9) Tout compact d'un espace topologique séparé est fermé, lemme 9.137(2).

(10) Dans un espace vectoriel réel de dimension finie, les compacts sont les fermés bornés par le théorème 11.23.

(11) Le théorème de Borel-Lebesgue 11.18 dit qu'un intervalle[17] de $\mathbb{R}$ est compact si et seulement si il est de la forme $[a, b]$.

(12) Théorème des fermés emboîtés dans le cas compact, corolaire 9.134. À ne pas confondre avec celui dans le cas des espaces métrique, théorème 9.372.

(13) Théorème des compacts emboîtés, proposition 9.139. Une intersection dénombrable de compacts emboîtés est compacte et non vide.

(14) L'image d'un compact par une fonction continue est un compact, théorème 9.298.

(15) Si $f\colon K \to X$ est une bijection continue, sa réciproque est continue, lemme 9.300.

(16) Suites dans un compact

(16a) Toute suite dans un compact admet une sous-suite convergente, théorème 9.363.

(16b) Dans $\mathbb{R}^n$, toute suite dans un compact admet une sous-suite convergente, théorème 11.59. La démonstration de ce théorème est non seulement plus compliquée que le cas général, mais utilise en plus le cas dans $\mathbb{R}$; lequel cas n'est pas démontré de façon directe dans le Frido.

(16c) Un espace métrique est compact si et seulement si toute suite contient une sous-suite convergente. C'est le théorème de Bolzano-Weierstrass 9.213. La démonstration de ce théorème est indépendante.

(16d) Si une suite de fonctions continues converge simplement vers une fonction continue, alors la convergence est uniforme sur tout compact, proposition 14.403.

(17) Une fonction continue sur un compact est bornée et atteint ses bornes, théorème 9.215.

(18) Une fonction continue sur un compact y est uniformément continue, théorème de Heine 14.80.

(19) Une bijection continue $f\colon K \to X$ entre un compact et un séparé est un isomorphisme, 9.301.

Partition de l'unité sur un compact, théorème 29.89.

Produits de compacts Le théorème de Tychonoff dit que tout produit de compact est compact pour la topologie produit. Nous allons en voir diverses versions.

- $\mathbb{R}$, lemme 11.20.
- Produit fini d'espaces métriques compacts, théorème 9.388.
- Produit dénombrable d'espaces métriques compacts, théorème 9.390.
- En général, théorème 9.381.

Composante connexe À propos de composantes connexes et de compacts.

(1) Si K est compact dans $\mathbb{C}$, alors la partie $\mathbb{C} \setminus K$ possède exactement une composante connexe non bornée. Lemme 28.51.

THEooPUIIoBHDOC34

Thème 34 : densité

(1) Densité de $\mathbb{Q}$ dans $\mathbb{R}$, proposition 11.15.

(2) Densité des polynômes dans $\left(C^0([0,1]), \|.\|_\infty\right)$, théorème de Bernstein 38.193, ou une conséquence de Stone-Weierstrass 14.459.

(3) Densité des polynômes dans $\left(C^0(I), \|.\|_\infty\right)$ lorsque $I = [a, b]$, corolaire 38.194.

(4) Densité de $\mathscr{D}(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$ pour $1 \leqslant p < \infty$, théorème 29.65.

(5) Densité de $\mathscr{S}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 33.15.

(6) Densité de $\mathscr{D}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 33.17.

Cela est utilisé pour le théorème de trace 33.19.

[17] Définition 1.31.

(7) Les applications étagées dans les applications mesurables (qui plus est avec limite croissante), théorème fondamental d'approximation 16.120.

(8) Les fonctions étagées dans les fonctions continues à support compact (pour la norme uniforme), proposition 31.19.

(9) Les fonctions continues à support compact dans $L^2(I)$, théorème 29.68.

(10) Les polynômes trigonométriques sont denses dans $L^p(S^1)$ pour $1 \leqslant p < \infty$. Deux démonstrations indépendantes par le théorème 30.8 et le théorème 29.103.

Les densités sont bien entendu utilisées pour prouver des formules sur un espace en sachant qu'elles sont vraies sur une partie dense. Mais également pour étendre une application définie seulement sur une partie dense. C'est par exemple ce qui est fait pour définir la trace γ_0 sur les espaces de Sobolev $H^s(\mathbb{R}^d)$ en utilisant le théorème d'extension 19.155.

Comme presque tous les théorèmes importants, le théorème de Stone-Weierstrass possède de nombreuses formulations à divers degrés de généralité.

- Le lemme 14.455 le donne pour la racine carré.
- Le théorème 14.461 donne la densité des polynômes dans les fonctions continues sur un compact.
- Le théorème 14.458 est une généralisation qui donne la densité uniforme d'une sous-algèbre de $C(X, \mathbb{R})$ dès que X sépare les points.
- Le théorème 14.459 donne le même résultat pour la densité dans $C(X, \mathbb{C})$.
- Le lemme 30.1 est une version pour les polynômes trigonométriques.
- Le lemme 14.455 est un cas particulier du théorème 14.461, mais nous en donnons une démonstration indépendante afin d'isoler la preuve de la généralisation 14.459. Une version pour les polynômes trigonométriques sera donnée dans le lemme 30.1.

Le théorème de Stone-Weierstrass est utilisé, entre autres nombreuses choses, pour prouver la densité des polynômes trigonométriques dans les fonctions continues sur S^1, voir la proposition 29.120.

THEMEooOXNQodHRCC35

Thème 35 : application réciproque

(1) Définition 1.19.

(2) Dans le cas des réels, des exemples sont donnés en 11.8.

(3) Continuité, théorème de la bijection 14.52.

(4) Continuité de la réciproque pour $f\colon K \to X$, lemme 9.300.

(5) Si f est strictement monotone sur un intervalle, son inverse est continue, théorème de la bijection 14.52.

(6) Théorème de la bijection 14.52 (qui contient aussi de la continuité).

(7) Dérivabilité, proposition 14.203.

(8) Une application continue est injective si et seulement si elle est strictement monotone, lemme 14.49.

THEMEooYCBUodHRC36

Thème 36 : applications continues et bornées

(1) Une application linéaire entre espaces vectoriels topologiques est continue si et seulement si elle est continue en 0. Proposition 9.243.

(2) Application continue, définition 9.48.

(3) Une application linéaire non continue : exemple 12.99 de $e_k \mapsto ke_k$. Les dérivées partielles sont calculées en (27.156).

(4) La dérivation sur les polynômes (exemple 12.100) donne un autre exemple d'application linéaire non continue.

(5) Une application linéaire est bornée si et seulement si elle est continue, proposition 12.98.

(6) Une forme sesquilinéaire est bornée si et seulement si elle est continue, proposition 27.1.

THMooOCXTHMooCXT

Thème 37 : suite de Cauchy, espace complet Nous parlons d'espaces topologiques complets. À ne pas confondre avec un espace mesuré complet, définition 16.70.

Quand nous parlons de suite de Cauchy dans les rationnels, ce sera la définition 3.249(1).

(1) Corps complet : définition 3.249(3), espace métrique complet : définition 9.335.

(2) L'image d'une suite de Cauchy est de Cauchy. Si (x_n) est de Cauchy, alors $\big(f(x_n)\big)$ est de Cauchy quand f est une isométrie, lemme 19.159.

(3) La définition 9.334 donne la notion de suite de Cauchy dans un espace métrique.

(4) La définition 9.332 donne la notion de suite de τ-Cauchy dans un espace vectoriel topologique.

(5) Deux espaces métriques (avec une distance) peuvent être isomorphes en tant qu'espaces topologiques, mais ne pas avoir les mêmes suites de Cauchy, exemple 9.340.

(6) La proposition 9.342 donne l'équivalence entre les suites de Cauchy et les suites τ-Cauchy dans le cas des espaces vectoriels topologiques *normés*.

(7) L'exemple 9.340 est un exemple pire que simplement une suite de Cauchy qui ne converge pas. Le problème de convergence de cette suite n'est pas simplement que la limite n'est pas dans l'espace ; c'est que la suite de Cauchy donnée ne convergerait même pas dans $\mathbb{R}$.

(8) Le théorème 19.163 est un théorème de complétion d'un espace métrique.

(9) Dans $\mathbb{R}$, une suite est convergente si et seulement si elle est de Cauchy, théorème 9.360(2).

(10) Toute suite convergente dans un espace métrique est de Cauchy, proposition 9.343.

Quelques espaces qui sont complets sont listés ci-dessous. Attention : la complétude est bien une propriété de la métrique ; le même ensemble peut être complet pour une distance et pas pour une autre. Souvent, cependant la distance à considérer est donnée par le contexte.

(1) Les réels $\mathbb{R}$, théorème 9.360.

(2) Les complexes $\mathbb{C}$, proposition 9.362.

(3) Un espace vectoriel normé sur un corps complet est complet, proposition 9.366.

(4) La proposition 14.398 donne quelques espaces complets. Soit X un espace topologique métrique, (Y, d) un espace métrique complet. Alors les espaces

  (4a) $\big(C^0_b(X,Y), \|.\|_\infty\big)$

  (4b) $\big(C^0_0(X,Y), \|.\|_\infty\big)$

  (4c) $\big(C^k_0(X,Y), \|.\|_\infty\big)$

  sont complets.

(5) Le lemme 14.399 dit que $\big(C^0(A,B), \|.\|_\infty\big)$ est complet dès que A est compact et B est complet.

(6) L'espace $\mathscr{D}(K)$ est complet tant pour la topologie des seminormes[18] que pour la topologie métrique (qui sont les mêmes). C'est la proposition 32.27.

(7) L'espace $\mathscr{S}(\Omega)$ est complet et métrisable par la proposition 32.78.

(8) L'espace $L^p(\Omega, \mathcal{A}, \mu)$ par le théorème 29.55.

La limite uniforme d'une suite de fonctions dérivables n'est pas spécialement dérivable. Même si les fonctions sont de classe C^∞, la limite n'est pas spécialement mieux que continue. En effet, le théorème de Stone-Weierstrass 14.461 nous dit que les polynômes (qui sont C^∞) sont denses dans les fonctions continues sur un compact pour la norme uniforme. Vous ne pouvez donc pas espérer que $\big(C^p(X,Y), \|.\|_\infty\big)$ soit complet en général.

THEMEooCaractSeq

Thème 38 : caractérisations séquentielles Diverses caractérisations séquentielles.

continuité Des résultats de continuité séquentielle.

(1) Fonction séquentiellement continue, définition 9.166. Dans un espace métrisable séparé, la continuité séquentielle est équivalente à la continuité, proposition 9.173.

(2) Quand une topologie est donnée par un ensemble dénombrable de seminormes, il est métrisable, proposition 9.421.

[18] Seminorme, définition 9.399, et la topologie des seminormes est la définition 9.415.

(3) La continuité implique la continuité séquentielle, proposition 9.162 et corolaire 9.206.

(4) Une version spéciale pour $\mathbb{R}^m$ est donnée par le théorème 14.245.

fermeture Fermeture séquentielle, proposition 9.170.

compacité Un espace topologique séquentiellement compact : toute suite possède une sous-suite convergente, définition 9.130.

THEMEooYEVLoTWTQ039

Thème 39 : valeurs propres, définie positive

À propos de valeurs propres (1) Définition des valeurs propres d'une forme quadratique : définition 10.255.

(2) Définition de valeur propre et vecteur propre pour un endomorphisme $f\colon V \to V$, définition 10.84.

À propos de choses définies positives (1) Une application bilinéaire est définie positive lorsque $g(u,u) \geqslant 0$ et $g(u,u) = 0$ si et seulement si $u = 0$ est la définition 10.122.

(2) Un opérateur ou une matrice est défini positif si toutes ses valeurs propres sont positives, c'est la définition 10.231.

(3) Pour une matrice symétrique, définie positive si et seulement si $\langle Ax, x\rangle > 0$ pour tout x. C'est le lemme 10.235.

(4) Une application linéaire est définie positive si et seulement si sa matrice associée l'est. C'est la proposition 10.236.

Remarque : nous ne définissons pas la notion de matrice définie positive dans le cas d'une matrice non symétrique.

THEMEooOJJFoTWTQ040

Thème 40 : norme matricielle, norme opérateur et rayon spectral Quelques définitions

(1) Définition de la norme opérateur : définition 12.76.

(2) Définition du rayon spectral 12.88.

La norme matricielle n'est rien d'autre que la norme opérateur de l'application linéaire donnée par la matrice.

(1) Lien entre norme matricielle et rayon spectral, le théorème 14.122 assure que $\|A\|_2 = \sqrt{\rho(A^tA)}$.

(2) Lien entre valeurs propres et norme opérateur : le lemme 14.123 pour les matrices symétriques strictement définies positives donne $\|A\|_2 = \lambda_{max}$.

(3) Pour une matrice diagonale, $\|D\|_2 = \max\{|\lambda_i|\}$, lemme 14.124.

(4) Pour toute norme algébrique nous avons $\rho(A) \leqslant \|A\|$, proposition 14.116.

(5) Dans le cadre du conditionnement de matrice. Voir en particulier la proposition 36.110 qui utilise le théorème 14.122.

(6) Rayon spectral et convergence de méthode itérative, proposition 36.148.

Pour la norme opérateur nous avons les résultats suivants.

(1) La majoration $\|Au\| \leqslant \|A\|\|u\|$ est le lemme 12.90.

(2) Définition d'une algèbre : 3.111 et pour une norme d'algèbre : 12.87.

(3) La norme opérateur est une norme d'algèbre : $\|AB\| \leqslant \|A\|\|B\|$, lemme 12.97.

(4) Pour des espaces vectoriels normés, être borné est équivalent à être continu : proposition 12.98.

(5) Le lemme à propos d'exponentielle de matrice 17.173 donne :

$$\|e^{tA}\| \leqslant P\big(|t|\big) \sum_{i=1}^{r} e^{t\,\mathrm{Re}(\lambda_i)}.$$

La norme opérateur est utilisée pour donner une norme sur les produits tensoriels, définition 12.286.

Une norme matricielle donne une topologie. Il y a donc également des liens entre rayon spectral et convergence de série. Dans cette optique, pour les séries de matrices, voir le thème 41.

Notations :

(1) $\mathcal{L}(E,F)$ est l'ensemble des applications linéaires $E \to F$.

(2) $\mathcal{L}^0(E,F)$ est l'ensemble des applications linéaires continues $E \to F$ (par analogie avec C^0). Pour définir $\mathcal{L}^0(E,F)$ il faut que E et F soient des espaces vectoriels topologiques ; le plus souvent ce seront des espaces vectoriels normés.

(3) $\mathrm{End}(E)$ est l'ensemble des applications linéaires $E \to E$.

(4) $\mathrm{End}^0(E)$ est l'ensemble des applications linéaires continues $E \to E$.

THEMEooPQKDoo

Thème 41 : série de matrices

(1) Rayon spectral et norme opérateur : thème 40.

(2) Exponentielle de matrices : thème 50.

(3) Série entière de matrices : section 17.13.

(4) Pour la série $\sum_k A^k = (1-A)^{-1}$.

- Pour un espace de Banach : proposition 12.364.
- Pour les matrices nilpotentes : proposition 10.214.
- En lien avec le rayon spectral (si et seulement si $\rho(A) < 1$) dans la proposition 17.169.
- Le lemme 17.53 parle de la série entière $\sum_{n\in\mathbb{N}} z^{nk} = (1-z^k)^{-1}$.

Cette série est utilisée entre autres dans la proposition 36.168 pour prouver qu'une M-matrice irréductible vérifie $A^{-1} > 0$.

DECooWTAI

Thème 42 : décomposition de matrices

(1) Décomposition de Bruhat, théorème 15.45.

(2) Décomposition de Dunford, théorème 10.265.

(3) Décomposition polaire 15.38 des matrices symétriques et la proposition 19.86 pour la régularité.

THEMEooSyst

Thème 43 : systèmes d'équations linéaires

- Algorithme des facteurs invariants 6.129.
- La méthode du gradient à pas optimal permet de résoudre par itérations $Ax = b$ lorsque A est symétrique strictement définie positive. Il s'agit de minimiser une fonction bien choisie. Propositions 19.142 pour l'existence et 19.143 pour la méthode.

THEMEooDiag

Thème 44 : réduction, diagonalisation Des résultats qui parlent diagonalisation

(1) Définition d'un endomorphisme diagonalisable : 10.215.

(2) Conditions équivalentes au fait d'être diagonalisable en termes de polynôme minimal, y compris la décomposition en espaces propres : théorème 10.220.

(3) Diagonalisation simultanée 10.223, pseudo-diagonalisation simultanée 12.61.

(4) Diagonalisation d'exponentielle 17.151 utilisant la décomposition de Dunford.

(5) Décomposition polaire théorème 15.38. $M = SQ$, S est symétrique, réelle, définie positive, Q est orthogonale.

(6) Décomposition de Dunford 10.265. $u = s + n$ où s est diagonalisable et n est nilpotent, $[s,n] = 0$.

(7) Réduction de Jordan (bloc-diagonale) 10.295.

(8) L'algorithme des facteurs invariants 6.129 donne $U = PDQ$ avec P et Q inversibles, D diagonale, sans hypothèse sur U. De plus les éléments de D forment une chaine d'éléments qui se divisent l'un l'autre.

Le théorème spectral et ses variantes :

(1) Théorème spectral, matrice symétrique, théorème 10.228. Via le lemme de Schur complexe 14.102.

(2) Théorème spectral autoadjoint (c'est le même, mais vu sans matrices), théorème 12.26

(3) Théorème spectral hermitien, lemme 12.41.

(4) Théorème spectral, matrice normales, théorème 14.104.

Pour les résultats de décomposition dont une partie est diagonale, voir le thème 42 sur les décompositions.
Réduction de quadriques :

(1) Réduction de Gauss, théorème 10.242.

Trigonalisation.

(1) Le lemme de Schur complexe 14.102 dit que toute matrice est unitairement équivalente à une matrice triangulaire supérieure.

THMooUXJM

Thème 45 : déterminant

(1) Déterminant d'une matrice : définition 6.89.

(2) Déterminant d'un endomorphisme 10.14.

(3) Déterminant $\det_\varphi$ d'une application linéaire entre espaces différents, proposition 12.104.

(4) Le lemme 12.5 donne la formule $\det(f) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} \langle e_{\sigma(i)}, f(e_i)\rangle$.

(5) Principales propriétés algébriques du déterminant : la proposition 10.15.

(6) La formule $\det(AB) = \det(A)\det(B)$ est la proposition 10.250 pour des matrices et la proposition 10.15(1) pour les applications linéaires.

(7) Déterminant et manipulations de lignes et colonnes, section 6.3.11 et les propositions qui précèdent à partir du lemme 6.91 qui dit que $\det(A) = \det(A^t)$.

(8) Les n-formes alternées forment un espace de dimension 1, proposition 10.8.

(9) Déterminant d'une famille de vecteurs 10.9.

(10) Calcul d'un déterminant de taille 2×2 : équation (6.115).

(11) Interprétations géométriques

(11a) À propos d'orthogonalité, le déterminant est très lié au produit vectoriel en dimension 3. Et il le généralise en dimension supérieure.

(11a.i) Liaison au produit vectoriel (orthogonalité) dans la proposition 12.58.

(11a.ii) En particulier le lemme 12.59 nous dit comment un déterminant donne un vecteur orthogonal à une famille donnée de vecteurs.

(11b) Déterminant et aires, volumes

(11b.i) Déterminant et mesure de Lebesgue : théorème 16.274.

(11b.ii) Aire du parallélogramme : il y a la formule avec le produit vectoriel dans la proposition 20.61, mais l'aire proprement dite, avec une intégrale est dans la proposition 22.26.

(11b.iii) Volume du parallélépipède avec le produit mixte et le déterminant 3×3, 20.62.

Tant que nous en sommes dans les interprétations géométriques, il faut lier déterminant, produit vectoriel, orthogonalité et mesure en notant que l'élément de volume lors de l'intégration en dimension 3 est donné par (22.211) : $dS = \|T_u \times T_v\|$ qui est la norme du produit vectoriel des vecteurs tangents au paramétrage.

Nous voyons dans l'équation (22.208) que l'élément de volume pour une partie de dimension n dans $\mathbb{R}^m$ (à l'occasion d'y intégrer une fonction) est donné par un déterminant mettant en jeu les vecteurs tangents du paramétrage.

(12) Le déterminant de Vandermonde est à la proposition 6.135. Il est utilisé à divers endroits :

(12a) Pour prouver que u est nilpotente si et seulement si $\mathrm{Tr}(u^p) = 0$ pour tout p (lemme 10.212)

(12b) Pour prouver qu'un endomorphisme possédant $\dim(E)$ valeurs propres distinctes est cyclique (proposition 10.301).

(12c) Pour montrer qu'un polynôme ayant $n+1$ racines a tout ses coefficients nuls (proposition 6.136), et donc que les monômes forment une base de l'espace des polynômes (proposition 6.137).

THEMooNMYKo46

Thème 46 : espaces de fonctions En ce qui concerne les densités, voir le thème 34.

(1) $C^\infty(A)$ est l'ensemble des fonctions de classe C^∞ sur A. Les éléments de $C^\infty(A)$ peuvent être à valeurs dans $\mathbb{R}$ ou dans $\mathbb{C}$ selon le contexte.

(2) $\mathscr{D}(A)$ est l'ensemble des fonctions de classe C^∞ dont le support est un compact dans A.

Pour les ensembles $\mathscr{S}(A)$, $\mathscr{D}(A)$ et $L^p(A)$, les fonctions sont à valeurs dans $\mathbb{C}$. La raison est que, de toutes façons, le passage à la transformée de Fourier produit en général des fonctions à valeurs dans $\mathbb{C}$ même si les fonctions de départ sont à valeurs dans $\mathbb{R}$.

Topologie Les espaces de fonctions sont souvent munis de topologies définies par des seminormes[19].

(1) La topologie des seminormes est la définition 9.399.

(2) La définition 32.14 donne les topologies sur $C^\infty(\Omega)$, $\mathscr{D}(K)$ et $\mathscr{D}(\Omega)$.

(3) La topologie $*$-faible sur $\mathscr{D}'(\Omega)$ est donnée par la définition 32.30.

(4) $p_{K,m}(f) = \sum_{|\mu|\leqslant m} \|\partial^\mu f\|_K$ est une seminorme sur $C^\infty(\Omega)$, proposition 32.9.

L'espace $L^2\big([0,2\pi]\big)$ C'est un espace très important, entre autres parce qu'il est de Hilbert et est bien adapté à la transformée de Fourier.

(1) Un rappel de la construction en 29.105.

(2) Le produit scalaire[20] $\langle f, g\rangle$ est donné en (31.188) et la base trigonométrique est (31.189).

(3) La densité des polynômes trigonométriques dans $L^p(S^2)$ est le théorème 29.103 ou le théorème 30.8, au choix.

(4) Une conséquence de cette densité est que le système trigonométrique est une base hilbertienne[21] de L^2 par le lemme 31.48.

L'espace L^2 est discuté en analyse fonctionnelle, dans la section 29.7 et les suivantes parce que l'étude de L^2 utilise entre autres l'inégalité de Hölder 29.39.

Le fait que L^2 soit un espace de Hilbert est utilisé dans la preuve du théorème de représentation de Riesz 29.186.

Si $(\Omega, \mathcal{A}, \mu)$ est un espace mesuré, alors $L^p(\Omega, \mathcal{A}, \mu)$ est un espace de Banach ; c'est le théorème de Riesz-Fischer 29.56.

THEMooFonctionLipschitz47

Thème 47 : fonctions lipschitziennes

(1) Définition : 14.353.

(2) La notion de lipschitzien est utilisée pour définir la stabilité d'un problème, définition 36.26.

(3) Toute fonction lipschitzienne est uniformément continue, proposition 14.358.

[19] Définition 9.399.
[20] Produit scalaire, définition 10.163.
[21] Définition 27.26.

THEMEooSUITESooC48

Thème 48 : suites et séries

Opérations sur les suites (1) Les limites $x_k + y_k \to x + y$ et $\lambda x_k \to \lambda x$ sont la proposition 9.283.

(2) La limite $x_k y_k \to xy$ est la proposition 11.27.

Suites La proposition 11.26 donne une caractérisation de limite de suite dans un espace vectoriel normé.

(1) Les suites adjacentes, c'est la définition 11.40.

(2) Les séries alternées, théorème 12.190. Il s'agit de dire que $\sum_{k=0}^{\infty}(-1)^k a_k$ converge quand a_k est décroissante et tend vers zéro.

(3) Le concept de suite adjacente sert à étudier la série de Taylor de $\ln(x+1)$, voir le lemme 17.113 et ce qui l'entoure.

(4) La définition de la convergence absolue est la définition 12.130.

(5) Une suite réelle croissante et majorée converge, proposition 11.36.

(6) Toute suite dans un compact admet une sous-suite convergente, théorème 9.363.

(7) Pour tout réel, il existe une suite croissante de rationnels qui y converge, proposition 11.16.

Produit de Cauchy (1) Dans une algèbre normée, proposition 12.178,

(2) Dans $\mathbb{C}$, théorème 17.27.

Calcul de suites (1) Somme : $x_n + y_n \to x + y$ est la proposition 11.28.

Série Les séries sont en général dans la section 12.10.

(1) Quelques séries usuelles en 12.13.3 : série harmonique, géométrique, de Riemann, et la mythique arithmético-géométrique.

(1a) La série est associative : $\sum_k (a_k + b_k) = \sum_k a_k + \sum_k b_k$. C'est la proposition 12.173.

(1b) La série harmonique diverge : $\sum_k \frac{1}{k} = \infty$, exemple 12.184.

(1c) La série géométrique : $\sum_{k=0}^{N} q^k = \frac{1-q^{N+1}}{1-q}$, proposition 12.186.

(1d) Une autre cool série : $\sum_{k=1}^{N} \frac{1}{k(k+1)} = \frac{N}{N+1}$, lemme 12.189.

(2) La série de Riemann $\sum_{k=1}^{\infty} 1/k^\alpha$ (définition 17.138) converge ou non selon les valeurs de α. Proposition 16.303 pour $\alpha \in \mathbb{R}$ et 17.140 pour $\alpha \in \mathbb{C}$.

(3) Critère des séries alternées, théorème 12.190.

(4) Convergence d'une série implique convergence vers zéro du terme général, proposition 12.133.

(5) Dans une algèbre normée : $(\sum_{k=0}^{\infty} a_k)b = \sum_{k=0}^{\infty}(a_k b)$, proposition 12.177.

(6) Produit de Cauchy : théorème 17.27 et proposition 12.178.

Sommes infinies En ce qui concerne les sommes finies, la notation $\sum_{i=1}^{N}$ est définie en 2.79. Pour permuter les termes d'une somme avec un élément du groupe symétrique, nous avons la proposition 2.131.

Voici quelques résultats à propos de sommes infinies.

(1) Une somme indexée par un ensemble quelconque est la définition 12.140.

(2) La proposition 12.144 donne une caractérisation pour le sommes de réels positifs.

(3) La définition de la somme d'une infinité de termes est donnée par la définition 12.123.

(4) Une somme de termes positifs indexée par un ensemble indénombrable est toujours infinie par le lemme 12.154.

(5) si la série converge, on peut regrouper ses termes sans modifier la convergence ni la somme (associativité) ; pour les sommes infinies l'associativité et la commutativité dans une série sont perdues. Néanmoins, il subsiste que

(5a) si la série converge absolument, on peut modifier l'ordre des termes sans modifier la convergence ni la somme (commutativité, proposition 12.137).

(6) Permuter une somme infinie avec une application linéaire : $f(\sum_{i\in I} v_i) = \sum_{i\in I} f(v_i)$, c'est la proposition 12.159.

Série entières (1) Rayon de convergence, définition 17.12.

(2) Critère de Hadamard, théorème 17.39. Il donne le rayon de convergence $1/R = \limsup \sqrt[k]{|a_k|}$ ou $1/R = \lim_{k\to\infty} |a_{k+1}/a_k|$.
(3) Convergence absolue à l'intérieur du rayon de convergence, lemme d'Abel 17.18.
(4) La fonction définie par la série entière $z \mapsto \sum_{k=0}^{\infty} a_n z^n$ est holomorphe dans son disque de convergence par la proposition 17.48.
(5) La série entière pour $\frac{1}{1-z^k}$, pour $\frac{1}{\omega - z}$ et pour $\frac{1}{(\omega-z)^k}$ sont dans le lemme 17.53.
(6) Les séries entières se généralisent sur les espaces de Banach en séries de puissances, définition 17.57.

THEMEooSuite

Thème 49 : suite de fonctions

(1) Une limite uniforme de fonctions continues est continue, proposition 14.397.
(2) Sous certaines hypothèses, si $f_i \to f$, alors $f_i' \to f'$, théorème 14.413.
(3) Si les f_k sont continues et si la convergence $\sum_k f_k$ est uniforme, alors la somme est continue, théorème 14.409.

THEMEooKXSG

Thème 50 : exponentielle Toutes les exponentielles sont définies par la série

$$\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!},$$

tant que la somme a un sens.

Réels Voici le plan que nous suivons dans le Frido :

- L'exponentielle est définie par sa série en 17.70.
- Nous démontrons qu'elle vérifie l'équation différentielle $y' = y$, $y(0) = 1$ (théorème 17.88).
- L'équation différentielle $y' = \lambda y$ est dans la proposition 17.92.
- Nous démontrons l'unicité de la solution à cette équation différentielle.
- Nous démontrons qu'elle est égale à $x \mapsto y(1)^x$. Cela donne la définition du nombre e comme valant $y(1)$.
- Nous définissons le logarithme comme l'application réciproque de l'exponentielle (définition 17.95).
- Les fonctions trigonométriques (sinus et cosinus) sont définies par leurs séries. Il est alors montré que $e^{ix} = \cos(x) + i\sin(x)$ (lemme 20.13).

Propriétés

- La formule $a^{-x} = 1/a^x$ est la proposition 14.437(3).
- $\exp(x) = e^x$, proposition 17.91.
- Nous avons l'encadrement $2.5 < e < 3$, lemme 17.93.
- Le nombre e est irrationnel, proposition 17.94.

Complexes (1) La définition de $\exp(a + ib)$ est la définition 17.70.
(2) Les principales propriétés, dont $e^{z+w} = e^z e^w$, sont dans la proposition 20.7.
(3) Nous avons $e^{ix} = e^{iy}$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $y = x + 2k\pi$, corolaire 20.29.
(4) Le fait que $e^{i\theta}$ donne tous les nombres complexes de norme 1 est la proposition 20.66(1).
(5) Le groupe des racines de l'unité est donné par l'équation (21.1).

Algèbre normée commutative Pour la définition c'est la proposition 17.70 et pour la régularité C^∞ c'est la proposition 17.75.

Idem non commutatif Il y a une tentative de théorème 17.76, mais c'est principalement pour les matrices qu'il y a des résultats.

Matrices De nombreux résultats sont disponibles pour les exponentielles de matrices.

(1) $e^{sA}e^{tA} = e^{(s+t)A}$, proposition 17.80.

(2) Si A est une matrice, alors $(e^{tA})'(u) = Ae^{uA}$, proposition 17.82.

(3) Les sections 12.18 et 17.5.3 parlent d'exponentielle de matrices.

(4) L'exponentielle donne lieu à une fonction de classe C^∞, proposition 17.170.

(5) Le lemme à propos d'exponentielle de matrice 17.173 donne :

$$\|e^{tA}\| \leqslant P\big(|t|\big) \sum_{i=1}^{r} e^{t\,\mathrm{Re}(\lambda_i)}.$$

(6) La proposition 17.151 : si $A \in \mathbb{M}(n, \mathbb{R})$ a un polynôme caractéristique scindé, alors A est diagonalisable si et seulement si e^A est diagonalisable.

(7) La section 17.13.3 parle des fonctions exponentielle et logarithme pour les matrices. Entre autres la dérivation et les séries.

(8) Pour résoudre des équations différentielles linéaires : sous-section 34.6.1.

(9) La proposition 17.150 dit que l'exponentielle est surjective sur $\mathrm{GL}(n, \mathbb{C})$.

(10) La proposition 12.367 : si u est un endomorphisme, alors $\exp(u)$ est un polynôme en u.

(11) Calcul effectif : sous-section 17.13.4.

(12) Proposition 15.29 : si $A \in \mathbb{M}(n, \mathbb{C})$ alors $e^{\mathrm{Tr}(A)} = \det(e^A)$.

(13) Les séries entières de matrices sont traitées autour de la proposition 17.167.

Paramétrisation du cercle (1) La proposition 20.66 parle des propriétés de

$$\begin{aligned} \varphi\colon]0, 2\pi[&\to S^1 \\ t &\mapsto e^{it}. \end{aligned} \tag{-1.3}$$

THEMEooLEGENDEnd

Thème 51 : logarithme

(1) Le logarithme pour les réels strictement positifs $\ln\colon]0, \infty[\to \mathbb{R}$ est donné en la définition 17.95 ; c'est l'application réciproque de exp.

(2) Les principales propriétés sont dans la proposition 17.98 : $\ln(xy) = \ln(x) + \ln(y)$ etc.

(3) Dérivée : $\ln'(x) = \frac{1}{x}$, proposition 17.97.

(4) La proposition 17.114 donne la série

$$\ln(1 + x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k. \tag{-1.4}$$

(5) L'exemple 22.132 donne l'encadrement $0.644 \leqslant \ln(2) \leqslant 0.846$.

(6) La proposition 17.150 dit que toute matrice complexe admet un logarithme. En particulier une série explicite est donnée pour le logarithme d'un bloc de Jordan[22].

(7) Sur les complexes, le logarithme $\ln\colon \mathbb{C}^* \to \mathbb{C}$ est la définition 28.31. Attention : ce n'est pas la seule définition possible.

(8) La série harmonique diverge à vitesse logarithmique, et la série des inverses des nombres premiers, c'est encore plus lent : théorème 17.134.

(9) Détermination du logarithme le long d'un chemin dans $\mathbb{C}$, définition 28.47.

(10) Un logarithme continu d'une fonction, définition 28.46.

(11) Théorème de Borsuk 28.49 : il y a toujours un logarithme continu le long d'un chemin homotope à une constante (et il y a même équivalence avec admettre une extension sur $\mathbb{C}^*$).

(12) Si $z \in \mathbb{C}$, nous avons $\int \frac{1}{x+z} dx = \ln(x + z)$, proposition 28.44.

(13) La proposition 28.60 dit qu'une application f a un logarithme continu si et seulement si $\mathrm{Ind}(f \circ \gamma, 0) = 0$.

[22] Jordan, théorème 10.295.

THEMEooBSBLoTWTOQ52

Thème 52 : fonction puissance Il y a beaucoup de choses à dire…

Définition Nous considérons, pour $a > 0$, la fonction $g_a \colon \mathbb{R} \to \mathbb{R}$ donnée par $g_a(x) = a^x$. La définition de cette fonction se fait en de nombreuses étapes.

(1) a^n pour $n \in \mathbb{N}$ en la définition 3.30.

(2) a^n pour $n \in \mathbb{Z}$ en la définition 14.417.

(3) $a^{1/n}$ pour $n \in \mathbb{Z}$ en la définition 14.420.

(4) a^q pour $q \in \mathbb{Q}$ en la définition 14.420.

(5) $\sqrt[n]{x}$ en la définition 14.422.

(6) La fonction g_a est Cauchy-continue sur $\mathbb{Q}$, c'est la proposition 14.434.

(7) a^x pour $a > 0$ et $x \in \mathbb{R}$ en la définition 14.436.

(8) a^z pour $a > 0$ et $z \in \mathbb{C}$ en la définition 20.10.

Quelques propriétés Quelques propriétés.

(1) Si b, m sont des entiers, il existe $n \in \mathbb{N}$ tel que $b^n > m$, proposition 3.32.

(2) Pour tout $q \in \mathbb{Q}$, il y a un $\sqrt{q}$ dans $\mathbb{R}$, proposition 4.99.

(3) Pour $a > 0$ et $x, y \in \mathbb{R}$ nous avons $a^x a^y = a^{x+y}$, proposition 14.437.

(4) Nous avons $(ab)^\alpha = a^\alpha b^\alpha$, proposition 14.448.

(5) Si $a > 0$ et $x, y \in \mathbb{R}$ nous avons $(a^x)^y = (a^y)^x = a^{xy}$ par la proposition 14.447.

(6) Si $\alpha > 0$, alors $x \mapsto x^\alpha$ est strictement croissante pour $x \geqslant 0$, proposition 14.442.

(7) La formule $a^{-x} = 1/a^x$ est la proposition 14.437(3).

(8) La fonction puissance $g_a(x) = a^x$ est continue, proposition 14.437.

Croissance (1) La fonction puissance $f_\alpha(x) = x^\alpha$ est strictement croissante pour les $x > 0$, proposition 14.442

(2) La fonction puissance $g_a(x) = a^x$ est strictement croissante, proposition 14.437.

(3) $\lim_{x\to\infty} x^\alpha = \infty$, proposition 14.449.

Continuité, Dérivation Comme toutes les choses sur la fonction puissance, les preuves sont assez différentes selon que l'on parle de a^x ou de x^a.

(1) La fonction $f_\alpha(x) = x^\alpha$ est continue, proposition 14.446.

(2) La fonction a^x est dérivable et sa dérivée vérifie $g_a'(x) = g_a(x)g_a'(0)$, proposition 14.466.

(3) La formule de dérivation pour $x \mapsto x^q$ avec $q \in \mathbb{Q}$ est la proposition 14.476.

(4) La dérivation de $x \mapsto x^\alpha$ avec $\alpha \in \mathbb{R}$ est la proposition 16.297. Si elle est tellement loin, c'est parce qu'elle nécessite de permuter une limite de fonctions avec une dérivée.

(5) Pour la formule générale de dérivation de $x \mapsto a^x$ demande de savoir les logarithmes (proposition 17.107).

L'équation fonctionnelle L'exponentielle et plus généralement la fonction puissance $g_a(x) = a^x$ peut être introduite au moyen d'une équation fonctionnelle au lieu de l'équation différentielle usuelle. Cette fameuse équation fonctionnelle est

$$f(x+y) = f(x)f(y) \tag{-1.5}$$

en la définition 14.468.

(1) L'équivalence entre l'équation fonctionnelle et l'équation différentielle est donnée par la proposition 14.474.

(2) La fonction $g_a(x) = a^x$ vérifie l'équation fonctionnelle $g_a(x+y) = g_a(x)g_a(y)$ et les conséquences. C'est la définition 14.468 et les choses qui suivent.

(3) L'équation fonctionnelle pour une fonction continue $f \colon \mathbb{R} \to S^1$ est traitée dans la proposition 14.478.

Une définition alternative de la fonction puissance serait de poser directement

$$a^x = e^{x\ln(a)}.$$

De là les propriétés se déduisent facilement. Dans cette approche, les choses se mettent dans l'ordre suivant :

- Définir $\exp(x)$ par sa série pour tout x.
- Démontrer que $\exp(q) = \exp(1)^q$ pour tout rationnel q (première partie de la proposition 17.91).
- Définir $e = \exp(1)$.
- Définir, pour x irrationnel, $a^x = \exp(x\ln(a))$.
- Prouver que $e^x = \exp(x)$ pour tout x.

THEMEooMKLBooTHCOooC53

Thème 53 : sommation finie et infinie La définition du symbole $\sum_{i\in I}$ se fait en trois étapes et deux demi, chacune se basant sur la précédente.

(1) Si $(A, +)$ est un ensemble avec une loi de composition interne, $\sum_{i=0}^{n} a_i$ est en 2.79.

(2) Si I est fini et si est à valeur dans un groupe commutatif, $\sum_{i\in I} f(i)$ est 2.129.

(3) Une somme peut être découpée en parties disjointe : $\sum_{A\cup B} = \sum_A + \sum_B$ par le lemme 2.133.

(4) Enfin si I est un ensemble quelconque, la définition 12.140 introduit la notion de famille sommable dans un espace vectoriel normé.

(5) Si (a_k) est une suite dans un espace vectoriel normé, la somme $\sum_{k=0}^{\infty} a_k$ est avec les sommes partielles dans la définition 12.123.

(6) La somme au sens de Cesàro est la somme des moyennes partielles, définition 12.191.

Notez que $\sum_{k=0}^{\infty} a_k$ n'est pas un cas particulier de $\sum_{k\in\mathbb{N}} a_k$. Une différence de taille entre les deux est que pour que $\sum_{k=0}^{\infty} a_k$ existe, il suffit que les a_k puissent être sommés dans cet ordre. À l'inverse pour que $\sum_{k\in\mathbb{N}} a_k$ existe, il faut que l'ordre de sommation puisse être arbitraire.

Si vous voulez sommer des séries encore moins convergentes, vous pouvez avoir envie d'utiliser la super-somme[5], ou la η-régularisation[6].

THEMEooPolynTHTCooC54

Thème 54 : polynôme de Taylor

Énoncés Il existe de nombreux énoncés du théorème de Taylor, et en particulier beaucoup de formules pour le reste.

(1) Énoncé : théorème 14.486.

(2) Une majoration du reste est dans le théorème 17.63

(3) De classe C^2 sur $\mathbb{R}^n$, proposition 14.493.

(4) Avec un reste donné par un point dans $]x, a[$, proposition 14.505.

(5) Avec reste intégral, théorème 22.129, et théorème 22.127 pour le cas simple $\mathbb{R} \to \mathbb{R}$.

(6) Le polynôme de Taylor généralise à l'utilisation de toutes les dérivées disponibles le résultat de développement limité donné par la proposition 12.311.

(7) Pour les fonctions holomorphes, il y a le théorème 28.79 qui donne une série de Taylor sur un disque de convergence.

Utilisation Des polynômes de Taylor sont utilisés pour démontrer des théorèmes par-ci par-là.

(1) Il est utilisé pour justifier la méthode de Newton autour de l'équation (36.95).

(2) On utilise pas mal de Taylor dans les résultats liant extrémum et différentielle/hessienne. Par exemple la proposition 19.99.

Quelques développements Voici quelques développements limités à savoir. Ils sont calculables en utilisant la formule de Taylor-Young (proposition 14.501).

$$e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + x^n \alpha(x) \qquad \text{ordre } n, \text{proposition } 17.109$$

$$\cos(x) = \sum_{k=0}^{p} \frac{(-1)^k x^{2k}}{(2k)!} + x^{2p+1}\alpha(x) \qquad \text{ordre } 2p+1, \text{proposition } 20.81$$

$$\sin(x) = \sum_{k=0}^{p} \frac{(-1)^k x^{2k+1}}{(2k+1)!} + x^{2p+2}\alpha(x) \qquad \text{ordre } 2p+1, \text{proposition } 20.81$$

$$\ln(1+x) = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k} x^k + \alpha(x)x^n \qquad \text{ordre } n, \text{proposition } 17.112$$

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k \qquad \text{exact proposition } 17.114$$

$$\ln(2) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} \qquad \text{exact proposition } 17.114$$

$$(1+x)^l = \sum_{k=0}^{l} \binom{l}{k} x^k \qquad \text{exact si } l \text{ est entier.}$$

$$(1+x)^l = 1 + \sum_{k=1}^{n} \frac{l(l-1)\dots(l-k+1)}{k!} x^k + x^n\alpha(x) \qquad \text{ordre } n.$$

Dans toutes ces formules, la fonction $\alpha\colon \mathbb{R} \to \mathbb{R}$ vérifie $\lim_{t\to 0} \alpha(t) = 0$.

Le développement limité en 0 d'une fonction paire ne contient que les puissances de x d'exposant pair. Voir comme exemple le développement de la fonction cosinus.

INTERNooXFNTóINTOOZB

Thème 55 : formule des accroissements finis Il en existe plusieurs formes :

(1) Une version adaptée aux espaces normés de dimension finie, avec hypothèse de différentiabilité, est le théorème 14.351. La formule $\|f(b) - f(a)\|_n \leqslant \sup_{x\in[a,b]} \|df_x\|_{\mathcal{L}(\mathbb{R}^m,\mathbb{R}^n)} \|b-a\|_m$.

(2) Une version pour les dérivées partielles est dans le lemme 14.255. Pour rappel, la définition de la dérivation partielle est 12.297.

(3) La formule $f(a+\epsilon e_i) = f(a) + \epsilon(\partial_i f)(a) + \epsilon\alpha(\epsilon)$, proposition 14.256.

(4) L'existence de $c \in]a,b[$ tel que

$$f'(c) = \frac{f(b)-f(a)}{b-a} \tag{-1.7}$$

est le théorème des accroissements finis proprement dit. C'est le théorème 14.217.

(5) Il existe un c entre a et b tel que

$$f(b) = f(a) + (b-a)(\partial_\beta f)(c) \tag{-1.8}$$

où $\beta = b - a$ est la proposition 14.254.

(6) La formule $f(a+h) = f(a) + hf'(a) + \alpha(h)$ pour une fonction $\mathbb{R} \to \mathbb{R}$ en le théorème 12.311.

(7) Une généralisation pour les intervalles non bornés : théorème 14.219.

(8) Espaces vectoriels normés, théorème 12.357

(9) La formule

$$f(a+h) = f(a) + df_a(h) + \alpha(h) \tag{-1.9}$$

est le lemme 12.330.

THEMEooDHTOG56

Thème 56 : dérivation

(1) Définition de la dérivée, définition 12.298.

(2) Dérivée de fonction composée, proposition 14.206 dans le cas réel.

(3) Dérivée partielle de fonction composée, théorème 14.333.

(4) La formule $(f \circ \gamma)'(a) = (\nabla f)\big(\gamma(a)\big) \cdot \gamma'(a)$, corolaire 14.334.

(5) $f(\lambda x)' = \lambda f'(x)$, lemme 14.201.

(6) Toute fonction dérivable est continue, 14.190.

THEMEooDifferentielle

Thème 57 : différentielle

Généralités (1) La différentielle est définie en général pour des espaces vectoriels normés par la proposition 12.296

(2) Différentielle et dérivées partielles continues, théorème 14.325.

(3) Différentielle d'une application linéaire, lemme 12.326.

(4) Nous parlons de différentielle en dimension finie et donnons une interprétation géométrique en 14.25.1.

(5) La recherche d'extrémums d'une fonction sur $\mathbb{R}^n$ passe par la seconde différentielle, proposition 19.99.

(6) Lien entre différentielle seconde (hessienne) et convexité en la proposition 19.126 et le corolaire 19.127.

(7) La différentielle est liée aux dérivées partielles par les formules données au lemme 14.273

$$df_a(u) = \frac{\partial f}{\partial u}(a) = \frac{d}{dt}\Big[f(a+tu)\Big]_{t=0} = \sum_{i=1}^{m} u_i \frac{\partial f}{\partial x_i}(a) = \nabla f(a) \cdot u. \tag{-1.10}$$

(8) La matrice de df en a est $(df_a)_{ij} = df_a(e_j) \cdot e_i = (\partial_j f_i)(a)$, proposition 14.274.

Différentielle et dérivée usuelle Souvent la différentielle est l'opérateur de multiplication par la dérivée : $df_a = f'(a)$.

(1) Pour $f\colon \mathbb{R} \to V$ c'est le lemme 14.279.

(2) Pour les fonctions holomorphes, c'est la proposition 14.346.

(3) Pour $f\colon \mathbb{R} \to \mathbb{C}$ c'est le lemme 14.347.

(4) Dans le même ordre d'idée la dérivée complexe est liée à la dérivée usuelle par la formule de la proposition 14.348 : $(f \circ \gamma)'(t) = (f' \circ \gamma)(t)\gamma'(t)$.

Différentielle et dérivées partielles À propos de fonctions de classe C^k, définition 12.317.

(1) Une fonction est de classe C^1 si et seulement si ses dérivées partielles sont continues, théorème 14.325.

(2) Une fonction est C^n si et seulement si ses dérivées partielles sont C^{n-1}, c'est le théorème 14.367.

(3) Différentiabilité en un seul point si les dérivées partielles sont continues en ce point : proposition 14.323.

Fonctions composées À propos de la formule $d(f \circ g)_a = dg_{f(a)} \circ df_a$, il y a deux théorèmes très semblables.

(1) Le théorème 12.335 insiste sur des hypothèses locales.

(2) Le théorème 12.336 fait des hypothèses plus globales pour s'alléger l'esprit, mais fait une récurrence pour dire que $f \circ g$ est de classe C^r si f et g le sont.

(3) Dans le cas d'espaces vectoriels normés de dimension finie, proposition 12.339.

(4) Composée avec une application linéaire, propositions 12.338 et 12.337.

Fonctions à valeurs avec plusieurs variables La proposition 14.303 donne $\phi\big(a(x), b(x)\big)' = (\partial_1 \phi)a' + (\partial_2 \phi)b'$.

Applications à valeurs dans les endomorphismes (1) $A\colon U \to \mathrm{End}(V, W)$ est C^p si ses composantes le sont, proposition 14.372.

(2) $A\colon U \to \mathrm{End}(V, W)$ est C^p si $s \mapsto A(s)v$ est C^p pour tout v, proposition 14.372

Thème 58 : équations différentielles L'utilisation des théorèmes de point fixe pour l'existence de solutions à des équations différentielles est fait dans le chapitre sur les points fixes.

(1) Le théorème de Cauchy-Lipschitz $y'(t,\lambda) = f\big(y(t,\lambda),\lambda\big)$ existe en plusieurs versions :

  (1a) Avec f continue et lipschitzienne, théorème 19.65. Il est utilisé dans

    (1a.i) Pour calculer la transformée de Fourier de $e^{-x^2/2}$ dans le lemme 31.24.

  (1b) Cauchy-Lipschitz holomorphe : théorème 28.128.

  (1c) Cauchy-Lipschitz analytique : théorème 28.130.

(2) Le théorème de Schauder a pour conséquence le théorème de Cauchy-Arzela 22.34 pour les équations différentielles.

(3) Le théorème de Schauder 22.33 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 19.65) sans la condition de Lipschitz.

(4) Théorème de stabilité de Lyapunov 34.46.

(5) Le système proie-prédateur de Lotka-Volterra 34.47.

(6) Équation de Schrödinger, théorème 34.55.

(7) L'équation $(x-x_0)^\alpha u = 0$ pour $u \in \mathscr{D}'(\mathbb{R})$, théorème 32.50.

(8) La proposition 34.50 donne un résultat sur $y'' + qy = 0$ à partir d'une hypothèse de croissance.

(9) Équation de Hill $y'' + qy = 0$, proposition 34.52.

Thème 59 : convexité

Fonctions convexes L'essentiel des résultats sur les fonctions convexes sont dans la section 19.16. On a surtout :

(1) Définition des fonctions convexes : 19.105 et 19.123 en dimension supérieure.

(2) En termes de différentielles, 19.124 pour la différentielle première et 19.127 pour la hessienne.

(3) Une courbe paramétrée convexe est la définition 23.90.

(4) L'enveloppe convexe d'une courbe fermée simple et convexe : 23.92.

(5) Courbure et convexité d'une courbe paramétrée : section 23.13.4.

(6) Une courbe paramétrée convexe est localement le graphe d'une fonction convexe par le lemme 23.91.

(7) La convexité est utilisée dans la méthode du gradient à pas optimal de la proposition 19.143.

(8) La fonction $t \mapsto t^p$ est strictement convexe sur les positifs dans le lemme 19.116.

(9) Une inégalité sympa : $a^r + b^r \leqslant (a+b)^r \leqslant 2^{r-1}(a^r + b^r)$ pour $a, b > 0$ et $r > 1$, lemme 29.135.

En termes de parties convexes, on a :

Parties convexes (1) Définition 9.228 d'une partie convexe d'un espace vectoriel.

(2) Une boule est convexe, proposition 9.276.

(3) Un polygone convexe est défini en 20.180, et les racines de l'unité forment un polygone convexe par la proposition 20.181.

Thème 60 : espaces de Hilbert, base hilbertienne Beaucoup de choses concernant les espaces L^2, et en particulier la base trigonométrique sont dans le thème 46.

(1) Toute partie orthonormale d'un espace de Hilbert est libre, proposition 27.23.

(2) Tout espace de Hilbert possède une base hilbertienne, proposition 27.36.

(3) Unicité de la décomposition dans une base hilbertienne, proposition 27.37.

THEMEooAnalyseCHEQOOAA

Thème 61 : analyse complexe, fonctions holomorphes

(1) Application holomorphe, définition 14.339.

(2) Le lien entre différentielle et dérivée complexe est donné par les équations

$$df_{z_0}(z) = f'(z_0)z = (\partial_z f)(z_0)z \tag{-1.11}$$

par (14.949) et la proposition 28.5. Cela se résume par la formulation lapidaire $f' = \partial_z f$.

(3) Série de Laurent $f(z) = \sum_{n\in\mathbb{Z}} a_n z^n$, théorème 31.59.

(4) Théorème fondamental du calcul intégral version holomorphe, théorème 28.9.

THEMEooJGEHoTNZQOOBB

Thème 62 : permuter des limites

Permuter des dérivées partielles Pour permuter les dérivées partielles, la clef est d'être C^k.

(1) Si une fonction est de classe C^2, le théorème de Schwarz 14.381 dit que

$$\partial_k\partial_l f = \partial_l\partial_k f. \tag{-1.12}$$

(2) Pour une fonction de classe C^m, on peut permuter m dérivées partielles avec la proposition 14.394.

Fonctions définies par une intégrale Les théorèmes sur les fonctions définies par une intégrale, section 19.7. Nous avons entre autres

(1) $\partial_i \int_B f = \int_B \partial_i f$, avec B compact, proposition 19.47.

(2) Si f est majorée par une fonction ne dépendant pas de x, nous avons le théorème 19.38 pour la continuité de $x \mapsto \int_\Omega f(x,\omega)d\mu(\omega)$.

(3) Pour la fonction $F(x) = \int_\Omega f(x,\omega)d\mu(\omega)$, nous avons la dérivation sous l'intégrale par la formule de Leibniz

$$F'(a) = \int_\Omega \frac{\partial f}{\partial x}(a,\omega)d\mu(\omega) \tag{-1.13}$$

démontrée en le théorème 19.42 ou 19.46.

Des variations avec des dérivées partielles et des différentielles sont dans 19.47 et dans 19.48.

(4) Si $f\colon \mathbb{C}\times\Omega \to \mathbb{C}$ est holomorphe (pour $\mathbb{C}$), alors F est holomorphe et

$$F'(z) = \int_\Omega \frac{\partial f}{\partial z}(z,\omega)d\mu(\omega). \tag{-1.14}$$

(5) Pour des dérivées partielles multiples, nous avons la formule

$$(\partial^\alpha F)(x) = \int_\Omega (\partial^\alpha f_\omega)(a)d\mu(\omega) \tag{-1.15}$$

dans la proposition 19.44.

(6) Si l'intégrale est uniformément convergente, nous avons le théorème 19.39 qui donne la continuité de $F(x) = \int_\Omega f(x,\omega)d\mu(\omega)$.

(7) Pour dériver $\int_B g(t,z)dt$ avec B compact dans $\mathbb{R}$ et $g\colon \mathbb{R}\times\mathbb{C}\to\mathbb{C}$, il faut aller voir la proposition 28.66.

(8) En ce qui concerne le x dans la borne, le théorème 16.289 lie primitive et intégrale en montrant que $F(x) = \int_a^x f(t)dt$ est une primitive de f (sous certaines conditions). Le théorème fondamental de l'analyse 16.290 en est une conséquence.

(9) Si T est une **distribution**, alors nous avons

$$T\big(x\mapsto(\partial_y^\alpha\phi)(x,y_0)\big) = \partial_y^\alpha\Big(T\big(x\mapsto\phi(x,y)\big)\Big)_{y=y_0}. \tag{-1.16}$$

C'est la proposition 32.54.

Dérivée et intégrale (1) Dériver $\int_\Omega f(x,\omega)d\omega$, théorème 19.46.

Série et intégrale (1) L'application $\int_0^t f(t,\lambda)dt$ est analytique[23] si f est analytique, proposition 17.210.

Série et limite (1) $\lim_k \sum_n a_{n,k} = \sum_n \lim_k a_{n,k}$, lemme 17.219.

Limite et intégrale (1) Théorème de la convergence monotone, théorème 16.180.

(2) $\int \sum_n f_n = \sum_n \int f_n$ dans le corolaire 16.183.

Fubini Le théorème de Fubini permet non seulement de permuter des intégrales, mais également des sommes parce que ces dernières peuvent être vues comme des intégrales sur $\mathbb{N}$ muni de la tribu des parties et de la mesure de comptage[24]. Nous utilisons cette technique pour permuter une somme et une intégrale dans l'équation (28.319).

L'utilisation de Fubini pour permuter des intégrales (sur deux variables différentes) ou deux sommes est expliquée dans 16.308.

C'est par exemple utilisé pour permuter deux sommes dans le cadre des chaines de Markov en 40.8.

- le théorème de Fubini-Tonelli 16.304 demande que la fonction soit mesurable et positive ;
- le théorème de Fubini 16.307 demande que la fonction soit intégrable (mais pas spécialement positive) ;
- le corolaire 16.306 demande l'intégrabilité de la valeur absolue des intégrales partielles pour déduire que la fonction elle-même est intégrable.

Limite et dérivées, différentielle (1) Permuter limite et dérivée dans le cas $\mathbb{R} \to \mathbb{R}$, théorème 14.413.

(2) Permuter limite et dérivées partielles, théorème 14.416.

(3) Permuter limite et différentielle, théorème 17.9.

Quelques remarques sur les techniques de démonstration.

(1) Le résultat fondamental 14.413 est démontré sans recourir à des intégrales. Une preuve alternative, plus courte, avec des intégrales est donnée en 16.327.

(2) Permuter limite et dérivée partielle, théorème 14.416.

(3) Permuter série et différentielle, théorème 17.9.

Somme et dérivée Permuter somme et différentielle, théorème 17.9.

Limite et mesure Une mesure n'est pas toujours une limite, mais la définition d'une mesure positive sur un espace mesurable parle de permuter limite et mesure : définition 16.18(2).

Norme et intégrale L'inégalité de Minkowski (29.183) permute la norme L^p et l'intégrale. Il n'y a cependant pas vraiment permutation, mais inégalité. C'est déjà mieux que rien.

Distribution et intégrale C'est le théorème 32.55.

Pour les fonctions holomorphes (1) Une série convergent uniformément de fonctions holomorphes est holomorphe, proposition 28.87.

Régularité dans les bornes.

- Le corolaire 29.61 dit que $\lim_{h\to 0} \int_a^{a+h} f = 0$.
- La proposition 29.62 dit que $x \mapsto \int_a^x f$ est continue.

THTOC63

Thème 63 : types de convergence Il y a plein de types de convergence.

Pour les séries Types de convergence pour les séries.

(1) convergence absolue, définition 12.130,

(2) convergence normale, définition 12.131,

(3) Convergence uniforme, définition 12.132

Pour les intégrals Types de convergence pour les intégrales.

(1) Convergence uniforme, définition 19.10.

[23] Définition 17.190.

[24] Mesure de comptage, définition 16.266.

THEMEooDASVolWZOO64

Thème 64 : déduire la nullité d'une fonction depuis son intégrale Des résultats qui disent que si $\int f = 0$ c'est que $f = 0$ dans un sens ou dans un autre.

(1) Il y a le lemme 16.201 qui dit ça.

(2) Un lemme du genre dans L^2 existe aussi pour $\int f\varphi = 0$ pour tout φ. C'est le lemme 29.90.

(3) En utilisant le théorème de représentation de Riesz, on peut prouver que $\int_\Omega f\chi = 0$ implique $f = 0$ pour tout $f \in L^p$, proposition 29.191.

(4) Si $\int f\chi = 0$ pour tout χ à support compact alors $f = 0$ presque partout, proposition 31.29.

(5) Si $\int_a^x f = 0$ pour tout x, alors $f = 0$, proposition 31.30.

(6) La proposition 29.26 donne $f = 0$ dans L^p lorsque $\int fg = 0$ pour tout $g \in L^q$.

(7) Une fonction $h \in C_c^\infty(I)$ admet une primitive dans $C_c^\infty(I)$ si et seulement si $\int_I h = 0$. Théorème 19.2.

Dans le même ordre d'idées, si $f > 0$ et si $\mu(X) > 0$ alors $\int_X f > 0$ par le lemme 16.203.

THEMEooInverseWZOO65

Thème 65 : inversion locale, fonction implicite

(1) Théorème d'inversion locale dans un Banach : théorème 19.76.

(2) Inversion locale version analytique : théorème 17.216.

(3) Fonction implicite dans un Banach : théorème 19.77.

(4) Utilisé pour montrer que le flot d'une équation différentielle est un C^p-difféomorphisme local, voir 34.39.

(5) Pour le théorème de Von Neumann 19.90.

THEMEooWAYJoiWZOO66

Thème 66 : points fixes

(1) Il y a plusieurs théorèmes de points fixes.

Théorème de Picard 19.60 donne un point fixe comme limite d'itérés d'une fonction lipschitzienne. Il aura pour conséquence le théorème de Cauchy-Lipschitz 19.65, l'équation de Fredholm, théorème 19.64 et le théorème d'inversion locale dans le cas des espaces de Banach 19.76.

Théorème de Brouwer qui donne un point fixe pour une application d'une boule vers elle-même. Nous allons donner plusieurs versions et preuves.

(1a) Dans $\mathbb{R}^n$ en version C^∞ via le théorème de Stokes, proposition 22.30.

(1b) Dans $\mathbb{R}^n$ en version continue, en s'appuyant sur le cas C^∞ et en faisant un passage à la limite, théorème 22.32.

(1c) Dans $\mathbb{R}^2$ via l'homotopie, théorème 28.68. Oui, c'est très loin. Et c'est normal parce que ça va utiliser la formule de l'indice qui est de l'analyse complexe[25].

Théorème de Markov-Kakutani 22.36 qui donne un point fixe à une application affine continue d'un convexe fermé borné dans lui-même.

Théorème de Schauder C'est une version valable en dimension infinie du théorème de Brouwer. Théorème 22.33

(2) Pour les équations différentielles

(2a) Le théorème de Schauder a pour conséquence le théorème de Cauchy-Arzela 22.34 pour les équations différentielles.

(2b) Le théorème de Schauder 22.33 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 19.65) sans la condition de Lipschitz, mais alors sans unicité de la solution. Notons que de ce point de vue nous sommes dans la même situation que la différence entre le théorème de Brouwer et celui de Picard : hors hypothèse de type « contraction », point d'unicité.

(3) En calcul numérique

- La convergence d'une méthode de point fixe est donnée par la proposition 36.48.

[25] On aime bien parce que ça ne demande pas Stokes, mais quand même hein, c'est pas gratos non plus.

- La convergence quadratique de la méthode de Newton est donnée par le théorème 36.54.
- En calcul numérique, section 36.5
- Méthode de Newton comme méthode de point fixe, sous-section 36.6.2.

(4) D'autres utilisations de points fixes.

- Processus de Galton-Watson, théorème 40.59.
- Dans le théorème de Max-Milgram 27.60, le théorème de Picard est utilisé.

THEMEooChangementDeVariables THEO067

Thème 67 : changement de variables Il n'existe rien en mathématique qui s'appelle « changement de variables » : il n'existe que des compositions de fonctions. Ce snobisme terminologique étant, voici un certain nombre de résultats de changement de variables.

(1) Dans des intégrales, théorème 16.284.

(2) Dans des limites, le lemme 9.251 donne $\lim_{x\to a} f(x) = \lim_{x\to b} f(x+a-b)$ si la limite existe.

(3) Dans les limites, la proposition 9.252 dit que $\lim_{x\to b} f(x+a) = \lim_{x\to a+b} f(x)$.

(4) Dans une équation aux dérivées partielles, exemple 35.132.

(5) Limite de fonction composée $\lim_{x\to a}(f\circ g)$, proposition 9.253.

THEMEooLTCIdeCalcul THEO068

Thème 68 : techniques de calcul Il y en a pour tous les gouts.

Primitives et intégrales Toute la section 20.2 donne des trucs et astuces pour trouver des primitives et des intégrales.

Limite à deux variables Les exemples de limites à plusieurs variables font souvent intervenir des coordonnées polaires (du théorème 20.239) ou autres fonctions trigonométriques. Ils sont donc placés beaucoup plus bas que la théorie.

- Méthode du développement asymptotique, sous-section 20.15.2.
- Méthode des coordonnées polaires, sous-section 20.15.1.
- Utilisation du théorème de la fonction implicite, dans l'exemple 20.241.

THEMEooMethodesCalcul THEO069

Thème 69 : méthodes de calcul

(1) Théorème de Rothstein-Trager 22.97.

(2) Algorithme des facteurs invariants 6.129.

(3) Méthode de Newton, théorème 36.63

(4) Calcul d'intégrale par suite équirépartie 30.10.

THEMEooMethodeNewton THEO070

Thème 70 : méthode de Newton

(1) Nous parlons un petit peu de méthode de Newton en dimension 1 dans 36.6.

(2) La méthode de Newton fonctionne bien avec les fonctions convexes par la proposition 36.56.

(3) La méthode de Newton en dimension n est le théorème 36.63.

(4) Un intervalle de convergence autour de α s'obtient par majoration de $|g'|$, proposition 36.48.

(5) Un intervalle de convergence quadratique s'obtient par majoration de $|g''|$, théorème 36.54.

(6) En calcul numérique, section 36.6.

(7) Méthode de Newton pour calculer $\sqrt{A}$, exemple 36.57.

THEMEooProlongeTHEMOo71

Thème 71 : prolongement d'applications

(1) Prolongement de fonction définie sur une partie dense, théorème 19.156

(2) Lemme de Borel 17.187.

(3) Prolongement méromorphe de la fonction Γ d'Euler.

(4) Le théorème de Tietze prolonge des fonctions continues définies sur un fermé. Prolongement continu dans le cas métrique, théorème 29.177. Dans le cas d'un espace normal, théorème 28.23.

THEMEooDistributionsTHEMOo72

Thème 72 : opérations sur les distributions

(1) Convolution d'une distribution par une fonction, définition par l'équation (32.221).

(2) Dérivation d'une distribution, proposition-définition 32.36.

(3) Produit d'une distribution par une fonction, définition 32.35.

THEMEooConvolution

Thème 73 : convolution

(1) Définition 29.78, et principales propriétés sur $L^1(\mathbb{R})$ dans le théorème 29.79.

(2) Le produit de convolution est commutatif : pour tout $f, g \in L^1(\mathbb{R}^d)$ nous avons $f * g = g * f$, lemme 29.80.

(3) Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leqslant \|f\|_p \|g\|_1$, proposition 29.83.

(4) $\varphi \in L^1(\mathbb{R})$ et $\psi \in \mathscr{S}(\mathbb{R})$, alors $\varphi * \psi \in \mathscr{S}(\mathbb{R})$, proposition 29.271.

(5) Les suites régularisantes : $\lim_{n\to\infty} \rho_n * f = f$ dans la proposition 31.18.

(6) Convolution d'une distribution par une fonction, définition par l'équation (32.221).

(7) Nous avons $(f * g)' = f * g'$, proposition 29.84.

(8) Si $f \in L^1(\mathbb{R}^d)$ et $g \in C^\infty(\mathbb{R}^d)$, alors $f * g \in C^\infty$, corolaire 29.85.

(9) Somme de variables aléatoires : $f_{x+Y} = f_X * f_Y$, proposition 38.44.

THMooHWEBTHMOo74

Thème 74 : séries de Fourier

- Le système trigonométrique est donné en la définition 29.98.
- Les coefficients de Fourier de $c_n(f)$ sont donnés par 29.100.
- Formule sommatoire de Poisson, proposition 31.15.
- Inégalité isopérimétrique, théorème 31.62.
- Fonction continue et périodique dont la série de Fourier ne converge pas, proposition 31.57.
- Nous allons montrer la convergence de $\sum_{k\in\mathbb{Z}} c_k(f)e^{inx}$ vers $f(x)$ dans divers cas :

  (1) Si f est continue et périodique, convergence au sens de Cesàro, théorème de Fejér 30.7.

  (2) Convergence au sens $L^2\Big([0, 2\pi]\Big)$ dans le théorème 31.49.

  (3) Si f est continue, périodique et si sa série de Fourier converge uniformément, théorème 30.15.

  (4) Si f est périodique et la série des coefficients converge absolument pour tout x, proposition 30.16.

  (5) Si f est périodique et de classe C^1, théorème 30.17.

  (6) Unicité des coefficients de Fourier, corolaire 31.52.

  Il est cependant faux de croire que la continuité et la périodicité suffisent à obtenir une convergence, comme le montre la proposition 31.57.

THEMEooTransfoFHTOOG75

Thème 75 : transformée de Fourier

(1) Définition sur L^1, définition 31.1.

(2) La transformée de Fourier d'une fonction $L^1(\mathbb{R}^d)$ est continue, proposition 31.11.

(3) L'espace de Schwartz[26] est stable par transformée de Fourier. L'application $\mathcal{F}\colon \mathscr{S}(\mathbb{R}^d) \to \mathscr{S}(\mathbb{R}^d)$ est continue. Proposition 31.22

(4) L'application $\mathcal{F}\colon \mathscr{S}(\mathbb{R}^d) \to \mathscr{S}(\mathbb{R}^d)$ est une bijection. Formule d'inversion, proposition 31.63.

THEMEooGaussienneFHTOOG76

Thème 76 : gaussienne

(1) Le calcul de l'intégrale

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$$

est fait de deux façons dans l'exemple 16.310. Dans les deux cas, le théorème de Fubini 16.307 est utilisé.

(2) Le lemme 31.24 calcule la transformée de Fourier de $g_\epsilon(x) = e^{-\epsilon\|x\|^2}$ qui donne $\hat{g}_\epsilon(\xi) = \left(\frac{\pi}{\epsilon}\right)^{d/2} e^{-\|\xi\|^2/4\epsilon}$.

(3) Le lemme 31.25 donne une suite régularisante à base de gaussienne.

(4) Elle est utilisée pour régulariser une intégrale dans la preuve de la formule d'inversion de Fourier 31.63

THEMEooJREIσFHTOOG77

Thème 77 : lemme de transfert Il y a deux résultats qui portent ce nom. Le premier est dans la théorie de Fourier, le résultat $\hat{f}' = i\xi\hat{f}$.

(1) Lemme 31.21 sur $\mathscr{S}(\mathbb{R}^d)$

(2) Lemme 33.10 pour L^2.

L'autre lemme de transfert est en théorie des tribus, le résultat $\sigma\big(f^{-1}(\mathcal{C})\big) = f^{-1}\big(\sigma(\mathcal{C})\big)$ du lemme 16.50. Celui-ci est d'ailleurs plutôt nommé « lemme de transport ».

Il existe aussi un théorème de transfert 38.99 qui parle de variables aléatoires :

$$E(f \circ X) = \int_\Omega f\big(X(\omega)\big) dP(\omega) = \int_{\mathbb{R}^d} f(x) dP_X(x) \tag{-1.17}$$

THEMEooInvariantsFHTOOG78

Thème 78 : invariants de similitude

(1) Théorème 10.292.

(2) Pour prouver que la similitude d'applications linéaires résiste à l'extension du corps de base, théorème 10.306.

(3) Pour prouver que la dimension du commutant d'un endomorphisme de E est de dimension au moins $\dim(E)$, lemme 10.303.

(4) Nous verrons dans la remarque 10.293 à propos des invariants de similitude que toute matrice est semblable[27] à la matrice bloc-diagonale constituées des matrices compagnon (définition 10.287) de la suite des polynômes minimaux.

THMooVUCLFHTOOG79

Thème 79 : isométries Il y a $(\mathbb{R}^n, \|.\|)$ et $(\mathbb{R}^n, d)$.

Les isométries de $\|.\|$ sont linéaires, tandis que les isométries de la distance contiennent aussi les translations et les rotations de centre différent de l'origine.

Ne pas confondre une isométrie d'un espace affine avec une isométrie d'un espace euclidien[28]. Les isométries d'un espace euclidien préservent le produit scalaire et fixent donc l'origine (lemme 12.35). Les isométries des espaces affines par contre conservent les distances (définition 13.64) et peuvent donc déplacer l'origine de l'espace vectoriel sur lequel il est modelé ; typiquement les translations sont des isométries de l'espace affine mais pas de l'espace euclidien.

Parfois, lorsqu'on coupe les cheveux en quatre, il faut faire attention en parlant de $\mathbb{R}^n$: soit on en parle comme d'un espace métrique (muni de la distance), soit on en parle comme d'un espace normé (muni de la norme ou du produit scalaire).

[26] Définition 29.259.
[27] Définition 6.126.
[28] Définition 10.167.

Général Quelques résultats généraux et en vrac à propos d'isométries.

(1) Définition d'une isométrie pour une forme bilinéaire, 10.151. Pour une forme quadratique : définition 10.150.

(2) Définition du groupe orthogonal 10.42, et le spécial orthogonal $\mathrm{SO}(n)$ en la définition 10.45. Le groupe $\mathrm{SO}(2)$ est le groupe des rotations, par corolaire 20.150.

(3) La rotation $R_A(\theta)$ d'un angle θ autour du point $A \in \mathbb{R}^2$ est donnée par la définition 20.139.

(4) La proposition 20.151 donne à toute rotation $R_0(\theta)$ une matrice de la forme connue. C'est autour de cela que nous définissons les angles, définition 20.169.

(5) Le groupe orthogonal est le groupe des isométries de $\mathbb{R}^n$, proposition 10.44.

(6) Les isométries de l'espace euclidien sont affines, 10.153.

(7) Les isométries de l'espace euclidien comme produit semi-direct : $\mathrm{Isom}(\mathbb{R}^n) \simeq T(n) \times_\rho \mathrm{O}(n)$, théorème 20.85.

(8) Isométries du cube, section 7.7.

(9) Nous parlons des isométries affines du tétraèdre régulier dans la proposition 20.207.

Groupe diédral Le groupe diédral est un peu central dans la théorie des isométries de $(\mathbb{R}^2, d)$ parce que beaucoup de sous-groupes finis des isométries de $(\mathbb{R}^2, d)$ sont en fait isomorphes au groupe diédral.

(1) Générateurs du groupe diédral, proposition 20.187.

(2) Un sous-groupe fini des isométries de $(\mathbb{R}^2, d)$ contenant au moins une réflexion est isomorphe au groupe diédral par le théorème 20.212.

(3) Le théorème 20.214 dit que le groupe des isométries propres d'une partie quelconque de $(\mathbb{R}^2, d)$ est soit cyclique soit isomorphe au groupe diédral.

Isométries et réflexions Dans un espace euclidien, toute isométrie peut être décomposée en réflexions autour d'hyperplans. Voici quelques énoncés à ce propos.

(1) Définition d'une rotation dans $\mathbb{R}^2$ 20.132.

(2) Définition d'une réflexion par rapport à un hyperplan : 20.89.

(3) Définition d'une réflexion par rapport à un point : 20.204.

(4) La caractérisation en termes de projection orthogonale est le lemme 20.117 ; en termes de médiatrice c'est le lemme 20.121.

(5) Définition d'un hyperplan 10.307.

(6) En dimension 2, une rotation est définie comme composée de deux réflexions en la définition 20.129.

(7) En dimension 2, les réflexions ont un déterminant -1 par le lemme 20.143.

(8) Les isométries du plan $(\mathbb{R}^2, d)$ sont données dans le théorème 20.203, et sont au plus 3 réflexions par le théorème 20.201.

(9) Décomposition des isométries de $\mathbb{R}^n$ en réflexions par le lemme 20.94.

(10) En particulier, les éléments de $\mathrm{SO}(3)$ sont des compositions de deux réflexions par le corolaire 20.97.

(11) Une isométrie de $\mathbb{R}^n$ préserve l'orientation si et seulement si elle est la composition d'un nombre pair de réflexions. C'est le théorème 20.103.

(12) Une isométrie de $(\mathbb{R}^2, d)$ laissant un point fixe est soit une rotation soit une réflexion, lemme 9.88.

Sous-groupe fini (1) Les sous-groupes finis des isométries de $(\mathbb{R}^2, d)$ sont cycliques, théorème 20.212.

(2) Les sous-groupes finis de $\mathrm{SO}(3)$ sont listés dans 20.236.

(3) Les sous-groupes finis de $\mathrm{SO}(2)$ sont cycliques, lemme 20.154.

THEMEooEnveloppes

Thème 80 : enveloppes

(1) L'ellipse de John-Loewner donne un ellipsoïde de volume minimum autour d'un compact dans $\mathbb{R}^n$, théorème 19.151.

(2) Le cercle circonscrit à une courbe donne un cercle de rayon minimal contenant une courbe fermée simple, proposition 23.89.

(3) Enveloppe convexe du groupe orthogonal 15.44.

(4) Enveloppe convexe d'une courbe fermée plane comme intersection des demi-plans tangents, proposition 23.95.

THEMEooIntegrationVarietes

Thème 81 : intégration sur des variétés Définition d'une variété : 22.1.

orientation La notion d'orientation commence avec l'orientation des bases d'un espace vectoriel et continue jusqu'à orienter des variétés à partir de ses cartes.

(1) Classe d'orientation sur les bases d'un espace vectoriel, définition 10.27.

(2) Orientation sur une surface, définition 22.60.

(3) Variété orientable, définition 22.17.

Intégrale Nous définissons d'abord l'intégrale sur une carte, et ensuite sur une variété. En ce qui concerne les formes différentielles, nous n'intégrons que des n-formes sur des variétés de dimension n.

(1) Intégrale d'une fonction sur une carte, définition 22.9.

théorème de Stokes, théorème de Green et compagnie Tous ces théorèmes sont des conséquences plus ou moins directes de celui de Stokes, et des généralisations du théorème fondamental de l'analyse.

(1) Forme générale, théorème 22.71.

(2) Rotationnel et circulation, théorème 26.8.

Le théorème de Stokes peut être utilisé pour montrer le théorème de Brouwer, proposition 22.30.

THEMEooDenombrements

Thème 82 : dénombrements

- Le nombre de parties de taille k dans un ensemble de taille n est $\binom{n}{k}$, proposition 3.70.
- Coloriage de roulette (20.11.15.1) et composition de colliers (20.11.15.2).
- Nombres de Bell, théorème 17.189.
- Le dénombrement des solutions de l'équation $\alpha_1 n_1 + \dots \alpha_p n_p = n$ utilise des séries entières et des décompositions de fractions en éléments simples[29], théorème 28.105.

THEMEooProbabilites

Thème 83 : caractérisation de distributions en probabilités

(1) La probabilité conjointe est la définition 38.26.

(2) La fonction de répartition est la définition 38.90.

(3) La fonction caractéristique est la définition 38.93.

THEMEooTheoremeCentralLimite

Thème 84 : théorème central limite

(1) Pour les processus de Poisson[30], théorème 42.22.

[29] Éléments simples, lemme 21.15.
[30] Définition 42.5.

THEMEooProbaIndTHEOO085

Thème 85 : indépendance d'événements et de variables aléatoires

(1) Événements indépendants, définition 38.8.

(2) Variables aléatoires indépendantes, définition 38.13.

(3) Espérance de variables aléatoires indépendantes : $E(X_1 \cdots X_n) = E(X_1) \dots E(X_n)$, proposition 38.39.

(4) Densité de variables aléatoires indépendantes : $f_X(x_1, \dots, x_n) = f_{X_1}(x_1) \dots f_{X_n}(x_n)$, proposition 38.29.

THEMEooProbaCondTHEOO086

Thème 86 : probabilités et espérances conditionnelles Les deux définitions de base, sur lesquelles se basent toutes les choses conditionnelles sont :

- L'espérance conditionnelle d'une variable aléatoire sachant une tribu : $E(X|\mathcal{F})$ de la définition 38.66.

Les autres sont listées ci-dessous.

Probabilité conditionnelle .

Plusieurs probabilités conditionnelles.

- D'un événement en sachant un autre : la définition 38.58 donne
$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$
Cela est la définition de base. L'autre est une définition dérivée.
- D'un événement vis-à-vis d'une variable aléatoire discrète. C'est par la définition 38.84 qui définit la variable aléatoire
$$P(A|X)(\omega) = P(A|X = X(\omega)).$$
Dans le cas continu, c'est la définition 38.85 :
$$P(A|X) = P(A|\sigma(X)) = E(\mathbb{1}_A|\sigma(X)).$$
- D'un événement par rapport à une tribu. C'est la variable aléatoire
$$P(A|\mathcal{F}) = E(\mathbb{1}_A|\mathcal{F}).$$

Espérances conditionnelles Plusieurs espérances conditionnelles.

- D'une variable aléatoire par rapport à un événement, définition 38.78 :
$$E(X|A) = \frac{E(X\mathbb{1}_A)}{P(A)}. \tag{-1.18}$$
- d'une variable aléatoire par rapport à une tribu. La variable aléatoire $E(X|\mathcal{F})$ est la variable aléatoire $\mathcal{F}$-mesurable telle que
$$\int_B E(X|\mathcal{F}) = \int_B X$$
pour tout $X \in \mathcal{F}$. Si $X \in L^2(\Omega, \mathcal{A}, P)$ alors $E(X|\mathcal{F}) = \texttt{proj}_K(X)$ où K est le sous-ensemble de $L^2(\Omega, \mathcal{A}, P)$ des fonctions $\mathcal{F}$-mesurables (théorème 38.66). Cela au sens des projections orthogonales.
- d'une variable aléatoire par rapport à une autre. La définition 38.68 est une variation sur le même thème :
$$E(X|Y) = E(X|\sigma(Y)),$$

Notons que partout, si X est une variable aléatoire, la notation « sachant X » est un raccourci pour dire « sachant la tribu engendrée par X ».

Quelque formules.

(1) Pour l'espérance conditionnelle d'une variable aléatoire prenant seulement une quantité dénombrable de valeurs : $E(X|A) = \sum_{k=0}^{\infty} y_k P(X = y_k|A)$ par le lemme 38.79.

(2) La probabilité conditionnelle se factorise par rapport à l'union disjointe par le lemme 38.62 : $P\left(\bigcup_{i=0}^{\infty} A_i|B\right) = \sum_{i=0}^{\infty} P(A_i|B)$.

THEMEEHMoC87

Thème 87 : chaine de Markov

(1) Construction d'une chaine de Markov dont la matrice de transition est donnée, lemme 40.42.

(2) Principales propriétés d'une chaine de Markov homogène, proposition 40.39.

(3) Si la chaine de Markov est irréductible, alors il y a unicité de l'état stationnaire, proposition 40.16. Mais attention : cela ne veut pas encore dire que la chaine converge effectivement vers cet état.

(4) Si la chaine est irréductible et apériodique, alors il y a convergence en loi vers l'unique loi invariante, théorème 40.37.

(5) État absorbant, définition 40.44.

-1.1 Conventions sur les matrices et changement de bases

SECooBTTTooZZABWA

-1.1.1 Matrices et applications linéaires

SUBSECooAFPDooOzXdGz

Le lien entre matrice et application linéaire est donné par la définition 6.78. L'application d'une matrice à un vecteur est (6.95). Le lien le plus simple entre l'application linéaire et les éléments de matrice est donné par la proposition 6.81. Voici les relations :

$$T_{\alpha i} = T(e_i)_\alpha \tag{-1.19a}$$

$$T(e_i) = \sum_\alpha T_{\alpha i} f_\alpha \tag{-1.19b}$$

$$T(x) = \sum_{i\alpha} T_{\alpha i} x_i f_\alpha \tag{-1.19c}$$

$$T(x)_\alpha = \sum_i T_{\alpha i} x_i. \tag{-1.19d}$$

De la même manière nous utiliserons (rarement) la notation suivante (définition 11.110) si $x \in \mathbb{R}^n$ et $T \in \mathbb{M}(n \times n)$:

$$xT = \sum_{ij} x_i T_{ij} e_j. \tag{-1.20}$$

À partir de là, il est possible de parler de vecteur propre à gauche lorsque $xT = \lambda x$.

Cela définit une application $\psi\colon \mathbb{M}(n \times m, \mathbb{K}) \to \mathcal{L}(E, F)$ qui a plein de propriétés.

(1) C'est une bijection, proposition 6.81(4).

(2) C'est un isomorphisme d'algèbre, proposition 6.84.

(3) C'est un isomorphisme d'espaces vectoriels, proposition 6.82.

(4) Isomorphisme d'algèbres et d'anneaux, proposition 6.84.

(5) Isomorphisme d'espaces topologiques, proposition 6.84.

Lorsque nous avons une base orthonormée[31] nous avons aussi les propositions 10.182 et 10.182 qui donnent des formules avec produit scalaire :

(1) $T_{\alpha i} = e_\alpha \cdot T(e_i)$

(2) $x \cdot Ay = \sum_{kl} A_{kl} x_k y_l$.

où le point est le produit scalaire usuel de $\mathbb{R}^n$.

[31] Définition 10.165.

-1.1.2 Le changement de base

Soit un espace vectoriel V muni de deux bases $(e_i)_{i=1,\dots,n}$ et $(f_\alpha)_{\alpha=1,\dots,n}$. Le lemme 6.130 donne le lien entre les vecteurs de base :

(1) $f_\alpha = \sum_i Q_{i\alpha} e_i$

(2) $e_i = \sum_\alpha Q^{-1}_{\alpha i} f_\alpha$

La proposition 6.131 donne un certain nombre de formules pour les coordonnées des vecteurs :

(1) $y_\alpha = \sum_i Q^{-1}_{\alpha i} x_i$

(2) $x_i = \sum_\alpha Q_{i\alpha} y_\alpha$.

(3) $x_i = (Qy)_i$

(4) $x = Qy$

La transformation de la matrice d'une application linéaire lors d'un changement de base est la proposition 6.134. Soit une application linéaire $T\colon V \to V$ de matrices A et B dans les bases $\{e_i\}$ et $\{f_\alpha\}$. Si les bases sont liées par $f_\alpha = \sum_i Q_{i\alpha} e_i$, alors les matrices A et B sont liées par

$$B = Q^{-1} A Q. \tag{-1.21}$$

En ce qui concerne la base duale, si $e'_j = \sum_i A_{ij} e_i$, alors

$$\alpha'_j = \sum_j A^{-1}_{jk} \alpha_k, \tag{-1.22}$$

proposition 6.150.

-1.1.3 Changement de base : matrice d'une forme bilinéaire

La proposition 10.147 fait le changement de matrice d'une forme bilinéaire lors d'un changement de base. Si la matrice de q dans la base $\{e_i\}$ est A et celle dans la base $\{f_\alpha\}$ est B, alors

$$B = Q^t A Q. \tag{-1.23}$$

Pour comparaison avec la loi de transformation des matrices des applications linéaires, voir la remarque 10.148.

Plus généralement, si ϕ est une application linéaire, la matrice de $q \circ \phi$ est $\phi^t q \phi$, proposition 10.146.

-1.2 Multiindice et liste d'indices

NORMooRRZCooMOKAzY

-1.2.
Je crois qu'il y a quelques incohérences de notations/dénominations dans le texte. En principe quand on parle de $\mathbb{R}^n$, un **multiindice** [7] est une vecteur d'entiers positifs à n composantes. Si $\alpha = (2, 1)$ alors nous avons la notation

$$\partial^\alpha f = \frac{\partial^2}{\partial x_1} \frac{\partial}{\partial x_2} f \tag{-1.24}$$

Cette notation pose problème lorsque, par exemple, $\partial_1^2 \partial_2 f \neq \partial_1 \partial_2 \partial_1 f$. La notation en multiindice permet aussi d'écrire, pour $x \in \mathbb{R}^n$:

$$x^\alpha = \prod_{i=1}^n x_i^{\alpha_i} \tag{-1.25}$$

Elle pose également problème lorsque l'on veut faire une récurrence sur l'ordre de dérivation en ajoutant une seule dérivation à la fois.

C'est pourquoi nous introduisons le concept de **liste d'indices**. En parlant de $\mathbb{R}^n$, une liste d'indices est un vecteur arbitrairement long (mais fini) d'entiers dans $\{1, \dots, n\}$. Si, dans $\mathbb{R}^7$, $\alpha = (1, 3, 1, 5)$, alors

$$\partial^\alpha f = \partial_1 \partial_3 \partial_1 \partial_5 f. \tag{-1.26}$$

Si α est une liste d'indices de longueur p, une **queue de** α est une liste d'indices de longueur $0 < k \leqslant p$ de la forme $(\alpha_{p-k+1}, \alpha_{p-k+2}, \dots, \alpha_p)$.

Voir aussi la définition 3.177 pour $\alpha!$.

-1.3 Anglicismes

SECooPBZVooCVInFT

Voici quelques anglicismes dont je ne me souviens jamais.

(1) Une σ-algèbre est une tribu, définition 16.1.

(2) Le « uniform boundedness principle » est le théorème de Banach-Steinhaus 12.201.

(3) Un anneau est ce qu'on appelle « *ring* » en anglais. Un corps est en anglais « *field* ». De plus le mot « *field* » comprend la commutativité. Donc certains utilisent le mot « corps » pour dire « corps commutatif » et parlent alors d'anneau *à division* pour parler de corps non commutatifs.

(4) Le théorème de Cauchy-Lipschitz est nommé « Picard–Lindelöf » en anglais.

Table des matières

Thématique **1**
-1.1 Conventions sur les matrices et changement de bases . . . 41
-1.1.1 Matrices et applications linéaires . . . 41
-1.1.2 Le changement de base . . . 42
-1.1.3 Changement de base : matrice d'une forme bilinéaire . . . 42
-1.2 Multiindice et liste d'indices . . . 42
-1.3 Anglicismes . . . 43

Table des matières **44**

Index **76**

Liste des notations **98**

I Le Frido **103**

0 Introduction **105**
0.1 Auteurs, contributeurs, sources et remerciements . . . 105
0.1.1 Ceux qui ont travaillé sur le Frido . . . 105
0.1.2 Aide directe, mais pas volontairement sur le Frido . . . 106
0.1.3 Des gens qui ont fait un travail qui m'a bien servi . . . 107
0.2 Originalité . . . 107
0.3 Les choses qui doivent vous faire tiquer . . . 108
0.4 Quelques choix qui peuvent provoquer des quiproquos . . . 108
0.5 Autres choix pas spécialement standards . . . 108
0.5.1 Mathématique intéressante . . . 109
0.6 Sage est là pour vous aider . . . 109
0.6.1 Lancez-vous dans Sage . . . 109
0.6.2 Exemples de ce que Sage peut faire pour vous . . . 109
0.7 Comment contribuer et aider ? . . . 111
0.7.1 Orthographe . . . 111
0.7.2 Contributions IA . . . 111
0.7.3 Des preuves qui manquent . . . 111
0.7.4 Du texte qui manque . . . 111
0.7.5 Des exemples qui manquent . . . 111
0.7.6 Des choses qui n'aident pas . . . 111
0.7.7 Trucs de programmation et de LaTeX . . . 112
0.8 Les politiques éditoriales . . . 112
0.8.1 Licence libre . . . 112
0.8.2 pdflatex . . . 112
0.8.3 utf8 . . . 112
0.8.4 Notations . . . 112
0.8.5 De la bibliographie . . . 112
0.8.6 Faire des références à tout . . . 112
0.8.7 Des listes de liens internes . . . 112
0.8.8 Pas de références vers le futur . . . 113

1 Les naturels et les entiers **115**
1.1 Les bases . . . 115
1.1.1 Axiomatique et grammaire . . . 115

1.1.2 Les théorèmes encapsulants . . . 115
1.2 Ensembles, relations, fonctions . . . 116
1.2.1 Opérations ensemblistes . . . 116
1.2.2 Des relations aux bijections . . . 117
1.2.3 Ensemble ordonné . . . 119
1.2.4 Intervalle . . . 120
1.2.5 Minimum, maximum, minimal, maximal, etc. . . . 120
1.2.6 Lemme de Zorn . . . 121
1.2.7 Quelques relations ensemblistes . . . 122
1.2.8 Relations d'équivalence . . . 127
1.2.9 Applications bien définies . . . 128
1.2.10 Relations ternaires, opérations . . . 129
1.3 Cardinalité . . . 130
1.3.1 Équipotence, surpotence, subpotence . . . 130
1.3.2 Un peu d'infinité . . . 131
1.3.3 Théorème de Cantor-Schröder-Bernstein . . . 136
1.3.4 Comparabilité cardinale . . . 139
1.3.5 Théorème de Cantor, ensemble des ensembles . . . 140
1.4 Quelques structures algébriques . . . 141
1.4.1 Positivité . . . 144
1.4.2 Diviseurs, pgcd et ppcm . . . 145
1.4.3 Règle des signes dans un anneau totalement ordonné . . . 146
1.4.4 Valeur absolue, corps valué . . . 147
1.5 Les entiers naturels . . . 149
1.5.1 Importance des naturels dans les ensemble . . . 149
1.5.2 Triplet naturel . . . 149
1.5.3 Applications définies par récurrence . . . 150
1.5.4 Addition sur les naturels . . . 153
1.5.5 Ordre sur les naturels . . . 156
1.5.6 Multiplication dans les naturels . . . 163
1.5.7 Presque unicité des triplets naturels . . . 165
1.5.8 Cardinalité dans $\mathbb{N}$ . . . 167
1.5.9 Division euclidienne . . . 168
1.6 Ensembles finis . . . 169
1.7 Les entiers relatifs . . . 171
1.7.1 Opposé . . . 172
1.7.2 Ordre sur $\mathbb{Z}$ . . . 174
1.8 Corps . . . 177
1.8.1 Définitions, morphismes . . . 177

2 Théorie des groupes (début) 179
2.1 Groupes . . . 179
2.1.1 Définition, unicité du neutre . . . 179
2.1.2 Morphisme de corps . . . 180
2.1.3 Groupe ordonné . . . 180
2.1.4 Classes de conjugaison . . . 181
2.2 Sous-groupe normal . . . 181
2.3 Théorèmes d'isomorphismes . . . 184
2.4 Quelques résultats de cardinalité . . . 186
2.4.1 Ordre d'un groupe . . . 189
2.4.2 Minimum, maximum . . . 189
2.4.3 Dénombrabilité et ensemble des naturels . . . 190
2.4.4 Ajouter ou soustraire des cardinalités . . . 195
2.5 Indice d'un sous-groupe et ordre des éléments . . . 200
2.5.1 Ordre d'un élément . . . 200
2.6 Groupe simple . . . 201
2.7 Symbole de sommation . . . 202
2.7.1 Sommation . . . 202
2.7.2 Écriture d'un naturel dans une base . . . 205
2.7.3 Symbole de produit . . . 209
2.8 Permutations, groupe symétrique . . . 209

2.8.1 Décomposition en cycles . . . 210
2.8.2 Parité d'une permutation, signature . . . 217
2.8.3 Permutations un peu ordonnées . . . 219
2.9 Somme à valeurs dans un groupe commutatif . . . 220
2.9.1 Cardinalité d'ensembles finis . . . 225
2.10 Groupes . . . 226
2.10.1 Sous-groupe engendré . . . 226
2.11 Groupe dérivé . . . 228
2.12 Produit semi-direct de groupes . . . 229
2.13 Groupe de torsion . . . 231
2.14 Famille presque nulle . . . 231

3 Anneaux **233**
3.1 Anneaux . . . 233
3.1.1 Idéal dans un anneau . . . 233
3.1.2 Idéal engendré . . . 234
3.1.3 Autres trucs sur les idéaux . . . 236
3.1.4 Élément irréductible et premier . . . 237
3.1.5 Anneau intègre . . . 237
3.1.6 Fonction puissance . . . 241
3.1.7 Anneau euclidien . . . 241
3.1.8 Anneau principal et idéal premier . . . 242
3.2 Le groupe et anneau des entiers . . . 243
3.2.1 Division euclidienne . . . 243
3.2.2 Sous-groupes de $(\mathbb{Z}, +)$ . . . 245
3.2.3 Théorème de Bézout . . . 245
3.2.4 PGCD, PPCM . . . 247
3.2.5 Décomposition en facteurs premiers . . . 248
3.2.6 Double comptage . . . 250
3.2.7 Binôme de Newton . . . 251
3.2.8 Divisibilité des coefficients binomiaux . . . 254
3.2.9 Coefficients binomiaux et polynômes . . . 255
3.3 Idéal dans un anneau . . . 256
3.4 Module sur un anneau . . . 260
3.4.1 Module produit . . . 261
3.4.2 Sous-module . . . 263
3.5 Caractéristique d'un anneau . . . 265
3.5.1 Endomorphisme de Frobenius . . . 266
3.5.2 Caractéristique deux . . . 266
3.6 Anneau intègre . . . 267
3.7 Théorèmes chinois et idéaux . . . 269
3.8 Sous-groupe normal . . . 272
3.9 Inversibles et nilpotents . . . 275
3.10 PGCD, PPCM et éléments inversibles . . . 276
3.10.1 Calcul effectif du PGCD et théorème de Bézout . . . 276
3.10.2 Générateurs . . . 278
3.10.3 pgcd, ppcm dans $\mathbb{N}$ . . . 279
3.10.4 Ordre d'un élément dans un groupe fini . . . 282
3.10.5 Écriture des fractions . . . 283
3.10.6 Équation diophantienne linéaire à deux inconnues . . . 285
3.10.7 Quotients . . . 286
3.11 Coefficients multinomiaux . . . 286
3.11.1 Théorème multinomial . . . 286
3.12 Polynômes de plusieurs variables . . . 288
3.12.1 Divisibilité et classes d'association . . . 289
3.12.2 PGCD et PPCM . . . 289
3.12.3 pgcd, ppcm dans un anneau principal . . . 290
3.12.4 Anneaux intègres et corps . . . 290
3.13 Anneau factoriel . . . 291
3.13.1 Autour du théorème de Bézout . . . 292
3.13.2 Théorème chinois . . . 294

3.13.3 Idéal premier . . . 295
3.13.4 Anneau noethérien . . . 296
3.14 Anneau $\mathbb{Z}/6\mathbb{Z}$ . . . 298
3.14.1 Équations diophantiennes . . . 300
3.14.2 Triplets pythagoriciens et équation de Fermat pour $n = 4$ . . . 301
3.15 Polynômes . . . 304
3.15.1 Polynômes d'une variable . . . 304
3.15.2 La notation $A[X]$ . . . 306
3.15.3 Action du groupe symétrique . . . 307
3.15.4 Corps des fractions . . . 308
3.15.5 Corps totalement ordonné . . . 313
3.16 Polynômes à coefficients dans un anneau commutatif . . . 314
3.16.1 Monômes . . . 314
3.16.2 Évaluation . . . 314
3.16.3 Polynômes sur un anneau intègre . . . 315
3.16.4 Division euclidienne . . . 315
3.16.5 Polynôme primitif . . . 316
3.16.6 Racines des polynômes . . . 318
3.16.7 Quelques identités . . . 321
3.16.8 Générateurs pour le groupe multiplicatif . . . 322

4 Les rationnels et les réels **323**
4.1 Les rationnels . . . 323
4.1.1 Relation d'ordre . . . 323
4.1.2 Caractéristique . . . 325
4.1.3 Infini dénombrable . . . 325
4.2 Suite de Cauchy dans un corps totalement ordonné . . . 326
4.2.1 Suites de Cauchy dans les rationnels . . . 328
4.3 Insuffisance des rationnels . . . 329
4.3.1 Série géométrique . . . 330
4.4 Les réels . . . 333
4.4.1 L'ensemble . . . 333
4.4.2 Relation d'ordre . . . 336
4.4.3 $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ . . . 342
4.4.4 Complétude . . . 343
4.4.5 Intervalles . . . 346
4.4.6 Maximum, supremum et compagnie . . . 346
4.4.7 Racines . . . 353
4.4.8 Partie entière, partie fractionnaire . . . 354
4.4.9 Le tore . . . 354
4.5 Les complexes . . . 356
4.5.1 Conjugaison complexe . . . 357
4.5.2 Norme, topologie, etc. . . . 358

5 Théorie des groupes (suite) **359**
5.1 Suite de composition . . . 359
5.2 Groupes résolubles . . . 362
5.3 Action de groupes . . . 364

6 Espaces vectoriels (début) **371**
6.1 Parties libres, génératrices, bases et dimension . . . 371
6.1.1 Et en dimension infinie . . . 377
6.1.2 Espace librement engendré . . . 379
6.2 Applications linéaires . . . 380
6.2.1 Définition . . . 380
6.2.2 Linéarité et bases . . . 383
6.2.3 Rang . . . 384
6.3 Matrices . . . 389
6.3.1 Définitions . . . 389
6.3.2 Identifier matrices et applications linéaires . . . 391
6.3.3 Ensemble des applications linéaires . . . 394

6.3.4 Déterminant . . . 395
6.3.5 Déterminant en petite dimension . . . 395
6.3.6 Manipulations de lignes et de colonnes . . . 395
6.3.7 Réduction de Gauss . . . 401
6.3.8 Matrices inversibles . . . 402
6.3.9 Inversibilité et déterminant . . . 404
6.3.10 Quelques ensembles de matrices particuliers . . . 404
6.3.11 Déterminant et combinaisons de lignes et colonnes . . . 404
6.3.12 Transvections . . . 405
6.3.13 Mineur, rang . . . 406
6.3.14 Matrices équivalentes et semblables . . . 408
6.3.15 Algorithme des facteurs invariants . . . 409
6.4 Changement de base . . . 411
6.4.1 Changement de base : vecteurs de base . . . 411
6.4.2 Changement de base : coordonnées . . . 411
6.4.3 Changement de base : matrice d'une application linéaire . . . 412
6.4.4 Déterminant de Vandermonde . . . 413
6.5 Espaces de polynômes . . . 414
6.6 Projection et orthogonalité . . . 416
6.7 Dualité . . . 416
6.7.1 Changement de base duale . . . 418
6.7.2 Orthogonal . . . 419
6.8 Représentation de groupe . . . 419
6.9 Somme directe d'espaces vectoriels . . . 420
6.9.1 Structure réelle . . . 422

7 Classification de certains groupes 425
7.1 Théorèmes de Sylow . . . 425
7.2 Groupe monogène . . . 428
7.3 Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$ . . . 430
7.4 Groupes abéliens finis . . . 431
7.5 Groupes d'ordre pq . . . 433
7.5.1 Fonction indicatrice d'Euler . . . 436
7.5.2 Générateurs . . . 439
7.5.3 Fonction indicatrice d'Euler (propriétés) . . . 439
7.6 Groupe symétrique, groupe alterné . . . 440
7.6.1 Le groupe alterné . . . 440
7.6.2 Sous-groupes normaux . . . 444
7.6.3 Indice . . . 446
7.7 Isométries du cube . . . 447

8 Corps 451
8.1 Généralités . . . 451
8.1.1 Corps ordonnés . . . 451
8.1.2 Automorphismes de $\mathbb{R}$ et $\mathbb{C}$ . . . 451
8.1.3 Corps premier . . . 453
8.1.4 Petit théorème de Fermat . . . 454
8.1.5 Nombres de Sophie Germain . . . 455
8.2 Théorème des deux carrés . . . 457
8.2.1 Un peu de structure dans $\mathbb{Z}[i]$ . . . 457
8.2.2 Résultats chinois . . . 460
8.3 Polynômes à coefficients dans un corps . . . 463
8.3.1 Irréductibilité . . . 467
8.3.2 Idéaux . . . 468
8.3.3 Identité de Bézout . . . 470
8.3.4 Lemme et théorème de Gauss . . . 470
8.3.5 Polynômes sur un corps et pgcd . . . 471
8.4 Extension de corps . . . 473
8.4.1 Extension et polynôme minimal . . . 474
8.4.2 Extensions algébriques et éléments transcendants . . . 476
8.4.3 Extension algébrique et polynôme minimal . . . 478

8.4.4 Extensions et polynômes . . . 479
8.4.5 Racines de polynômes . . . 488
8.4.6 Corps de rupture . . . 489
8.4.7 Pile d'extensions . . . 492
8.4.8 Clôture algébrique . . . 492
8.4.9 Polynômes à plusieurs variables . . . 498
8.4.10 Corps de décomposition . . . 499
8.4.11 Non irréductible ou pas corps ? . . . 502
8.4.12 Clôture algébrique . . . 503
8.4.13 Dérivée de polynômes . . . 504
8.4.14 Extensions séparables . . . 504
8.5 Idéal maximum . . . 510
8.5.1 Idéal maximum . . . 510
8.6 Polynômes symétriques et alternés . . . 511
8.6.1 Polynômes symétriques, alternés ou semi-symétriques . . . 511
8.6.2 Polynôme symétrique élémentaire . . . 511
8.6.3 Relations coefficients racines . . . 513
8.7 Minuscule morceau sur la théorie de Galois . . . 514

9 Topologie générale 517
9.1 Éléments généraux de topologie . . . 517
9.1.1 Définitions et propriétés de base . . . 517
9.1.2 Base de topologie . . . 517
9.1.3 Fermés . . . 518
9.1.4 Quelques exemples . . . 519
9.1.5 Adhérence, fermeture, intérieur, point d'accumulation et point isolé . . . 520
9.1.6 Topologie sur $\mathbb{Q}$ . . . 527
9.1.7 Applications continues . . . 528
9.2 Topologies rendant continue . . . 529
9.2.1 Topologie initiale . . . 529
9.2.2 Topologie produit . . . 533
9.2.3 Topologie de la convergence simple . . . 534
9.2.4 Topologie finale . . . 534
9.2.5 Topologie quotient . . . 535
9.3 Espace séparable . . . 536
9.4 Suites et convergence . . . 536
9.4.1 Convergence dans un fermé . . . 537
9.4.2 Pour des limites uniques : séparabilité . . . 538
9.4.3 Topologie induite . . . 539
9.4.4 Fonctions équivalentes . . . 539
9.5 Espace topologique normal et complètement normal . . . 541
9.6 Connexité . . . 544
9.7 Compacité . . . 547
9.7.1 Définition et notions connexes . . . 548
9.7.2 Autres compacité . . . 549
9.7.3 Quelques propriétés . . . 550
9.7.4 Espace relativement compact . . . 553
9.7.5 Propriété d'intersection finie . . . 553
9.8 Limite de fonction . . . 554
9.9 Topologie, distances et normes . . . 555
9.9.1 Distance et topologie métrique . . . 556
9.9.2 Précompact . . . 557
9.9.3 Caractérisations séquentielles . . . 558
9.9.4 Suites et espaces métriques . . . 558
9.9.5 Continuité de la distance . . . 560
9.9.6 Topologie métrique et induite . . . 560
9.9.7 Intérieur, adhérence et frontière . . . 560
9.9.8 Boules ouvertes, fermées, sphères . . . 563
9.9.9 Espace localement compact . . . 564
9.9.10 Compactifié d'Alexandrov . . . 566
9.9.11 Continuité séquentielle . . . 568

9.9.12 Continuité et compacité . . . 569
9.9.13 Distance à un ensemble . . . 571
9.9.14 Espace métrisable . . . 573
9.9.15 Connexité . . . 573
9.9.16 Convexité . . . 574
9.9.17 Norme . . . 574
9.9.18 Topologie . . . 577
9.10 Espaces vectoriels topologiques . . . 577
9.10.1 De complexe à réel . . . 578
9.10.2 Base de topologie . . . 578
9.10.3 Corps topologique . . . 580
9.10.4 Les applications linéaires sont continues . . . 581
9.10.5 Voisinage symétrique et équilibré . . . 581
9.10.6 Espace topologique localement convexe . . . 584
9.10.7 Limite de suites . . . 586
9.11 Applications continues . . . 588
9.11.1 Continuité . . . 588
9.11.2 Continuité et topologie induite . . . 589
9.11.3 Continuité et connexité . . . 590
9.11.4 Continuité et compacité . . . 592
9.11.5 Distance uniforme . . . 592
9.11.6 Continuité de la réciproque sur un compact . . . 592
9.11.7 Espace vectoriel topologique . . . 593
9.12 Produit fini d'espaces vectoriels normés . . . 593
9.12.1 Distance et norme produit . . . 593
9.13 Topologie réelle en dimension n . . . 597
9.13.1 Ouverts et fermés . . . 597
9.13.2 Point d'accumulation, point isolé . . . 597
9.13.3 Limite de suite . . . 598
9.14 Topologie et distance . . . 598
9.15 Suites de Cauchy, métrique et espaces complets . . . 600
9.15.1 Généralités . . . 600
9.15.2 Espace de Banach . . . 601
9.15.3 Espace topologique métrique . . . 602
9.15.4 Compacts, fermés . . . 603
9.15.5 Équivalence entre Cauchy et $\tau-$Cauchy . . . 611
9.16 Norme, espace vectoriel normé . . . 612
9.17 Espaces métriques . . . 614
9.17.1 Espaces métrisables . . . 614
9.17.2 Fonctions continues . . . 615
9.17.3 Théorème de Tykhonov . . . 621
9.17.4 Ensembles enchainés . . . 621
9.17.5 Produit fini d'espaces métriques . . . 622
9.17.6 Équicontinuité . . . 623
9.17.7 Continuité uniforme . . . 624
9.18 Partie maigre et nulle part dense . . . 624
9.19 Seminormes . . . 625
9.19.1 Seminorme . . . 625
9.19.2 Fonctionnelle de Minkowski . . . 626
9.20 Topologie des seminormes . . . 630
9.20.1 Topologie initiale des seminormes . . . 630
9.20.2 Topologie avec des boules . . . 631
9.20.3 Seminorme et métrisable . . . 637
9.20.4 Boules et topologie . . . 637
9.20.5 Espace dual . . . 640
9.20.6 Espace $C^k(\mathbb{R}, E')$ . . . 641
9.21 Espaces de Baire . . . 642

10 Espaces vectoriels (encore) 645
10.1 Déterminants . . . 645
10.2 Applications multilinéaires . . . 645

10.2.1 Formes multilinéaires alternées . . . 646
10.2.2 Déterminant d'une famille de vecteurs . . . 647
10.2.3 Déterminant d'un endomorphisme . . . 650
10.2.4 Déterminant de Gram . . . 653
10.2.5 Déterminant de Cauchy . . . 653
10.2.6 Matrice de Sylvester . . . 653
10.2.7 Théorème de Kronecker . . . 656
10.3 Orientation . . . 657
10.3.1 Cas vectoriel . . . 657
10.3.2 Cas affine . . . 659
10.4 Hermitien, orthogonal, adjoint . . . 659
10.4.1 Opérateur orthogonal, matrice orthogonale . . . 661
10.5 Topologie . . . 662
10.5.1 Boules et sphères . . . 662
10.5.2 Ouverts, fermés, intérieur et adhérence . . . 663
10.5.3 Point isolé, point d'accumulation . . . 669
10.5.4 Des exemples . . . 670
10.6 Valeur propre et vecteur propre . . . 673
10.6.1 Généralités . . . 673
10.6.2 Dans le vif du sujet . . . 673
10.7 Polynômes d'endomorphismes . . . 675
10.7.1 Polynômes d'endomorphismes . . . 675
10.7.2 Polynôme minimal et minimal ponctuel . . . 678
10.7.3 Polynôme caractéristique . . . 683
10.8 Formes bilinéaires et quadratiques . . . 687
10.8.1 Dégénérescence d'une forme bilinéaire . . . 688
10.8.2 Orthogonal pour une forme bilinéaire . . . 688
10.8.3 Formes quadratiques . . . 691
10.8.4 Isotropie . . . 693
10.9 Formes bilinéaires et quadratiques . . . 693
10.9.1 Matrice associée à une forme bilinéaire . . . 694
10.9.2 Changement de base : matrice d'une forme bilinéaire . . . 694
10.9.3 Isométrie, forme quadratique et bilinéaire . . . 695
10.9.4 Isométries . . . 696
10.10 Signature, théorème de Sylvester . . . 698
10.11 Produit scalaire, produit hermitien . . . 699
10.11.1 Autoadjoint . . . 701
10.11.2 Hermitien, unitaire, etc. . . . 701
10.11.3 Éléments de matrice . . . 702
10.11.4 Transposée : pas d'approche naïve . . . 703
10.11.5 Transposée : la bonne approche . . . 704
10.11.6 Polynômes de Lagrange . . . 706
10.11.7 Dual de $\mathbb{M}(n, \mathbb{K})$ . . . 707
10.12 Diagonalisation et trigonalisation . . . 708
10.12.1 Matrices semblables . . . 708
10.12.2 Trace de matrices semblables . . . 709
10.12.3 Endomorphismes nilpotents . . . 710
10.12.4 Endomorphismes diagonalisables . . . 712
10.12.5 Diagonalisation : cas complexe, pas toujours . . . 715
10.12.6 Diagonalisation : cas réel . . . 716
10.12.7 Matrice définie positive . . . 717
10.12.8 Réduction de Gauss . . . 720
10.12.9 Orthogonalité pour une forme bilinéaire . . . 723
10.12.10 Équivalence de formes quadratiques . . . 727
10.12.11 Diagonalisation . . . 727
10.13 Fonctions . . . 729
10.14 Sous-espaces caractéristiques . . . 729
10.14.1 Théorèmes de décomposition . . . 731
10.14.2 Valeurs singulières . . . 733
10.15 Extension du corps de base . . . 734
10.15.1 Extension des applications linéaires . . . 734

10.15.2 Projections . . . 736
10.15.3 Rang, polynôme minimal, polynôme caractéristique . . . 738
10.16 Frobenius et Jordan . . . 740
10.16.1 Matrice compagnon . . . 740
10.16.2 Réduction de Frobenius . . . 741
10.16.3 Forme normale de Jordan . . . 743
10.17 Commutant et endomorphismes cycliques . . . 745
10.17.1 Endomorphisme cyclique . . . 745
10.17.2 Commutant : cas diagonalisable . . . 745
10.17.3 Commutant : cas général . . . 748
10.18 Hyperplans et formes linéaires . . . 750
10.18.1 Hyperplan dans un espace euclidien . . . 751
10.19 Trouver la matrice d'une symétrie donnée . . . 752
10.20 Théorème de Burnside . . . 754
10.21 Ellipsoïde . . . 755
10.22 Système d'équations linéaires : méthode de Gauss . . . 756

11 Analyse réelle : topologie et continuité **759**
11.1 Intervalles . . . 759
11.2 Application réciproque . . . 760
11.2.1 Définitions . . . 760
11.2.2 Graphe de la fonction réciproque . . . 761
11.3 Topologie sur l'ensemble des réels . . . 762
11.3.1 Compacité pour les réels . . . 763
11.3.2 Conséquence : les fermés bornés sont compacts . . . 765
11.3.3 Suites et limites dans les réels . . . 766
11.3.4 Opérations sur les limites . . . 766
11.3.5 Exemples . . . 767
11.3.6 Limites infinies . . . 768
11.3.7 Topologie et matrices . . . 768
11.3.8 Suites croissantes et bornées . . . 769
11.3.9 Suites adjacentes . . . 770
11.3.10 Limite supérieure et inférieure . . . 771
11.3.11 Ouverts, voisinage, topologie . . . 773
11.3.12 Intervalles et connexité . . . 774
11.3.13 Théorème de Bolzano-Weierstrass . . . 777
11.3.14 Recouvrement par des intervalles ouverts . . . 778
11.4 Connexité par arcs . . . 780
11.4.1 Composition d'arcs . . . 780
11.4.2 Connexité par arcs . . . 780
11.4.3 Des exemples . . . 781
11.4.4 Quelques mots à propos de la droite réelle achevée . . . 783
11.5 Continuité . . . 784
11.5.1 Opération sur la continuité . . . 785
11.5.2 La fonction la moins continue du monde . . . 786
11.5.3 Approche topologique . . . 787
11.5.4 Limite sur des chemins . . . 788
11.5.5 Racine carrée . . . 788
11.5.6 Module sur les nombres complexes . . . 789
11.5.7 Théorème de Perron-Frobenius . . . 793
11.5.8 Limite à gauche et à droite . . . 796
11.5.9 Continuité de la racine carrée, invitation à la topologie induite . . . 796
11.5.10 Second degré (parabole) . . . 798

12 Espaces vectoriels normés **801**
12.0.1 Norme, produit scalaire et Cauchy-Schwarz (cas réel) . . . 801
12.0.2 Topologie . . . 804
12.0.3 Le tore . . . 805
12.0.4 Le tore . . . 807
12.0.5 La sphère . . . 810
12.1 Théorème spectral autoadjoint . . . 812

12.2 Norme euclidienne . . . 813
12.2.1 Inégalité de Minkowski . . . 814
12.2.2 Cauchy-Schwarz etc. cas complexe . . . 815
12.3 Norme à partir d'un produit scalaire . . . 816
12.3.1 Diagonalisation : cas complexe, ce qu'on a . . . 817
12.3.2 Projection et orthogonalité . . . 817
12.3.3 Théorème de Pythagore . . . 819
12.3.4 Produit vectoriel . . . 819
12.3.5 Produit mixte . . . 822
12.3.6 Complétion de bases, procédé de Gram-Schmidt . . . 823
12.3.7 Pseudo-réduction simultanée . . . 824
12.4 Approximations . . . 825
12.4.1 Quelques exemples de normes sur $\mathbb{R}^n$ . . . 826
12.5 Équivalence des normes . . . 827
12.5.1 En dimension finie . . . 827
12.5.2 Contre-exemple en dimension infinie . . . 831
12.6 Norme opérateur . . . 831
12.6.1 Matrice bloc-diagonale . . . 833
12.6.2 Norme d'algèbre . . . 834
12.6.3 Applications linéaires dans un espace de Banach . . . 835
12.7 Application linéaire continue et bornée . . . 836
12.7.1 Déterminant entre espaces différents . . . 838
12.7.2 Suites . . . 840
12.7.3 Continuité du produit de matrices . . . 842
12.8 Applications multilinéaires . . . 843
12.8.1 Norme . . . 843
12.8.2 Continuité . . . 845
12.8.3 Continuité de la composition . . . 847
12.8.4 Norme . . . 847
12.9 Applications multilinéaires . . . 849
12.10 Séries . . . 850
12.11 Sommes de familles infinies . . . 851
12.11.1 Suites . . . 851
12.11.2 Séries . . . 852
12.11.3 Terme général . . . 852
12.11.4 Convergence commutative . . . 853
12.11.5 Famille sommable . . . 857
12.11.6 Sommation associative . . . 861
12.11.7 Somme non dénombrables . . . 862
12.11.8 Sommes dénombrables . . . 862
12.12 Liens entre différents types de sommabilité . . . 865
12.12.1 Séries entières . . . 870
12.12.2 Somme téléscopique . . . 871
12.12.3 Distributivité . . . 871
12.12.4 Produit de Cauchy . . . 872
12.13 Série réelle . . . 872
12.13.1 Critères de convergence absolue . . . 872
12.13.2 Critères de convergence simple . . . 874
12.13.3 Quelques séries usuelles . . . 875
12.13.4 Séries alternées . . . 877
12.13.5 Moyenne de Cesàro . . . 878
12.13.6 Écriture décimale d'un réel . . . 878
12.13.7 Théorème de Banach-Steinhaus . . . 881
12.13.8 Convergence forte . . . 884
12.14 Application ouverte . . . 885
12.15 Produit tensoriel d'espaces vectoriels . . . 887
12.16 Produit tensoriel . . . 890
12.16.1 Définition générale . . . 891
12.16.2 Constructions du produit tensoriel . . . 892
12.16.3 Construction abstraite . . . 893
12.16.4 Bases . . . 896

12.16.5 Construction par les formes multilinéaires . . . 898
12.16.6 Décomposabilité . . . 900
12.16.7 Produit tensoriel d'applications linéaires . . . 901
12.16.8 Contraction . . . 902
12.16.9 Tenseurs symétriques et alternés . . . 903
12.16.10 Décomposition . . . 908
12.16.11 Règle de Leibniz pour le produit extérieur . . . 910
12.16.12 Produit intérieur . . . 917
12.16.13 Pull back . . . 920
12.16.14 Norme . . . 920
12.16.15 Applications bilinéaires, matrices et produit tensoriel . . . 921
12.16.16 Application d'opérateurs . . . 922
12.16.17 Convergence en norme et par composante . . . 922
12.17 Calcul différentiel dans un espace vectoriel normé . . . 923
12.17.1 Limite de fonctions . . . 923
12.17.2 Définition de la différentielle . . . 923
12.17.3 Pas en dimension infinie . . . 924
12.17.4 Dérivée directionnelle . . . 924
12.17.5 Théorème des accroissements finis . . . 927
12.17.6 Différentielle d'ordre 2 . . . 929
12.17.7 Quelques mots à propos des différentielles d'ordre supérieur . . . 930
12.17.8 Topologie et norme induite . . . 931
12.17.9 Différentielle d'applications linéaires . . . 932
12.17.10 Différentielle d'applications multilinéaires . . . 933
12.17.11 Accroissements finis . . . 934
12.17.12 Notations pour les applications linéaires . . . 935
12.17.13 (non ?) Différentiabilité des applications linéaires . . . 935
12.17.14 Dérivation en chaine et formule de Leibniz . . . 935
12.17.15 Composition . . . 937
12.17.16 Règle de Leibniz . . . 940
12.17.17 Inverse . . . 941
12.17.18 Différentiation de produit tensoriel . . . 941
12.17.19 Produit cartésien . . . 944
12.17.20 Formule des accroissements finis . . . 946
12.17.21 Applications multilinéaires . . . 949
12.17.22 Différentielle partielle . . . 950
12.17.23 L'inverse, sa différentielle . . . 951
12.18 Exponentielle de matrice . . . 953
12.19 Espace dual . . . 954
12.19.1 Topologies . . . 955
12.19.2 Module de continuité . . . 956
12.20 Mini introduction aux nombres p-adiques . . . 957
12.20.1 La flèche d'Achille . . . 957
12.20.2 La tortue et Achille . . . 958
12.20.3 Dans les nombres p-adiques, c'est vrai . . . 958

13 Espaces affines **961**
13.1 Vecteurs agissant sur un espace . . . 961
13.2 Repères cartésiens affines . . . 962
13.3 Classification affine des coniques . . . 962
13.4 Applications affines . . . 966
13.4.1 Autres propriétés . . . 967
13.5 Isomorphismes . . . 969
13.6 Sous-espaces affines . . . 969
13.7 Barycentre . . . 970
13.7.1 Sous-espaces affines . . . 971
13.7.2 Enveloppe convexe . . . 973
13.7.3 Applications affines et barycentre . . . 975
13.8 Repères, coordonnées cartésiennes et barycentriques . . . 976
13.8.1 Équation de droite . . . 980
13.8.2 Associativité, coordonnées barycentriques dans un triangle . . . 980

13.9 Applications affines sur $\mathbb{R}^n$ . . . 981
13.9.1 Structure de groupe pour les applications affines . . . 982
13.10 Isométries . . . 983

14 Analyse réelle : limites et dérivation 985
14.1 Limite de fonctions . . . 985
14.1.1 Définition . . . 985
14.1.2 Quelques règles de calcul . . . 987
14.2 Limites pointées et épointées . . . 990
14.2.1 Théorèmes de composition de limites . . . 992
14.2.2 Discussion pointée Vs épointée . . . 995
14.3 Limites en l'infini . . . 998
14.3.1 Droite réelle achevée . . . 998
14.3.2 Limites en l'infini . . . 999
14.3.3 Limite en des nombres . . . 1000
14.3.4 Limites quand tout va bien . . . 1001
14.3.5 Limites de fonctions . . . 1001
14.3.6 Limite à gauche et à droite . . . 1002
14.4 Limite en compactifié d'Alexandrov . . . 1003
14.4.1 Prolongement par continuité . . . 1003
14.4.2 Prolongement par continuité . . . 1005
14.4.3 Théorème de la bijection . . . 1005
14.5 Limite et continuité . . . 1008
14.5.1 Prolongement des rationnels vers les réels . . . 1010
14.6 Espace des fonctions continues . . . 1013
14.7 Uniforme continuité . . . 1017
14.8 Fonctions sur un compact . . . 1020
14.9 Polynômes, théorème de d'Alembert . . . 1020
14.9.1 Polynômes sur les réels . . . 1020
14.9.2 Polynômes sur les complexes . . . 1021
14.10 Trigonalisation . . . 1026
14.10.1 Trigonalisation : généralités . . . 1026
14.10.2 Trigonalisation : cas complexe . . . 1027
14.11 Matrices, spectre et norme . . . 1033
14.11.1 Rayon spectral . . . 1033
14.11.2 Normes de matrices et d'applications linéaires . . . 1037
14.12 Droites dans un espace vectoriel . . . 1042
14.12.1 Parallélisme et perpendicularité . . . 1043
14.12.2 Droites et applications linéaires . . . 1044
14.12.3 Projection orthogonale . . . 1046
14.13 Géométrie dans le plan . . . 1048
14.13.1 Segment, médiatrice et équidistance . . . 1050
14.13.2 Cercles . . . 1056
14.14 Géométrie dans l'espace . . . 1057
14.14.1 Droites et plans dans l'espace . . . 1057
14.14.2 Plan médiateur . . . 1059
14.14.3 Tétraèdre . . . 1060
14.15 Plan médiateur dans l'espace . . . 1061
14.16 Dérivée : exemples introductifs . . . 1061
14.16.1 La vitesse . . . 1061
14.16.2 La tangente à une courbe . . . 1061
14.16.3 L'aire en dessous d'une courbe . . . 1062
14.17 Dérivation de fonctions réelles . . . 1063
14.17.1 Exemples . . . 1064
14.17.2 Interprétation géométrique : tangente . . . 1065
14.17.3 Interprétation géométrique : approximation affine . . . 1066
14.18 Règles de calcul . . . 1067
14.18.1 Dérivée de la réciproque . . . 1071
14.18.2 Dérivée de fonction composée . . . 1073
14.18.3 Dérivée de fonction périodique . . . 1074
14.19 Dérivation et croissance . . . 1074

14.19.1 Théorèmes de Rolle . . . 1074
14.19.2 Théorème des accroissements finis . . . 1077
14.19.3 Règle de L'Hôpital . . . 1078
14.19.4 Dérivée et primitive . . . 1080
14.20 Fonctions de plusieurs variables . . . 1081
14.20.1 Graphes de fonctions à plusieurs variables . . . 1083
14.20.2 Courbes de niveau . . . 1084
14.21 Limites à plusieurs variables . . . 1088
14.21.1 Caractérisation de la limite par les suites . . . 1090
14.21.2 Règle de l'étau . . . 1091
14.21.3 Méthode des chemins . . . 1092
14.22 Dérivée directionnelle . . . 1094
14.23 Accroissements finis et dérivées partielles . . . 1094
14.24 Formes différentielles . . . 1095
14.24.1 Décomposition dans la base duale . . . 1095
14.24.2 L'isomorphisme musical . . . 1096
14.25 Différentielle . . . 1097
14.25.1 Exemples introductifs . . . 1097
14.25.2 Différentielle . . . 1098
14.25.3 Matrice de la différentielle . . . 1098
14.25.4 Différentielle, dual et forme différentielle . . . 1100
14.25.5 Ce n'est pas la différentielle extérieure . . . 1100
14.25.6 Continuité, dérivabilité et différentiabilité . . . 1101
14.25.7 Calcul de valeurs approchées . . . 1104
14.25.8 Différentielle et tangente . . . 1105
14.25.9 Prouver qu'une fonction n'est pas différentiable . . . 1106
14.25.10 Gradient . . . 1110
14.25.11 Linéarité . . . 1110
14.26 Produit . . . 1110
14.26.1 Difficulté d'ordre supérieur . . . 1112
14.26.2 Solution : produit tensoriel . . . 1112
14.26.3 Formes bilinéaires . . . 1113
14.27 Différentielle de fonction composée . . . 1113
14.27.1 Fonctions composées . . . 1116
14.28 Différentielle de fonctions à plusieurs variables . . . 1117
14.29 Autres trucs sur la différentielle . . . 1119
14.29.1 Dérivée partielle et directionnelles . . . 1119
14.29.2 Gradient : direction de plus grande pente . . . 1120
14.29.3 Gradient : orthogonal au plan tangent . . . 1120
14.29.4 Mise en bouche en dimension 2 . . . 1121
14.29.5 Différentielle et dérivées partielles . . . 1122
14.29.6 Plan tangent . . . 1122
14.29.7 Notes idéologiques quant au concept de plan tangent . . . 1122
14.29.8 Gradient et recherche du plan tangent . . . 1123
14.30 Jacobienne . . . 1125
14.30.1 Rappels et définitions . . . 1125
14.31 Fonctions de classe C^1 . . . 1126
14.32 Différentielle et dérivée complexe . . . 1134
14.32.1 Quelques règles de calcul . . . 1138
14.33 Théorèmes des accroissements finis . . . 1138
14.34 Fonctions lipschitziennes . . . 1139
14.35 Différentielles d'ordre supérieur . . . 1141
14.35.1 Différentielle et dérivées partielles . . . 1141
14.35.2 Application à valeurs dans les opérateurs . . . 1145
14.35.3 Espaces d'applications multilinéaires et identifications . . . 1145
14.35.4 Fonctions différentiables plusieurs fois . . . 1149
14.35.5 Différentielle seconde, fonction de classe C^2 . . . 1150
14.35.6 Ordre supérieur . . . 1153
14.35.7 Différentielle et dérivées partielles multiples . . . 1153
14.36 Suites et séries : généralités . . . 1156
14.36.1 Norme supremum . . . 1156

14.36.2 Convergence uniforme . . . 1156
14.36.3 Série de fonctions . . . 1159
14.37 Permuter limite et dérivée . . . 1160
14.38 La fonction puissance . . . 1166
14.38.1 Sur les naturels . . . 1167
14.38.2 Sur les rationnels, racines . . . 1168
14.39 Densité des polynômes . . . 1183
14.39.1 Théorème de Stone-Weierstrass . . . 1183
14.40 Primitive de fonction continue . . . 1186
14.40.1 Dérivation de la fonction puissance (première) . . . 1187
14.40.2 Équation fonctionnelle . . . 1189
14.40.3 Dérivation de la fonction puissance (seconde) . . . 1193
14.40.4 Vers les complexes . . . 1194
14.41 Polynômes de Taylor . . . 1195
14.41.1 Fonctions « petit o » . . . 1199
14.41.2 Autres formulations . . . 1200
14.41.3 Formule et reste . . . 1200
14.41.4 Reste intégral . . . 1201
14.42 Développement limité autour de zéro . . . 1201
14.42.1 Généralités . . . 1201
14.42.2 Formule de Taylor-Young . . . 1202
14.42.3 Règles de calcul . . . 1203
14.43 Développement ailleurs qu'à l'origine . . . 1205
14.44 Développement au voisinage de l'infini . . . 1206
14.44.1 La fonction puissance : remarques pour la suite . . . 1206
14.45 Fonctions réelles de deux variables réelles . . . 1206
14.45.1 Limites de fonctions à deux variables . . . 1206
14.45.2 Dérivées partielles . . . 1207
14.45.3 Différentielle et accroissement . . . 1207
14.46 Les fonctions à valeurs vectorielles . . . 1208
14.47 Fonctions vectorielles de plusieurs variables . . . 1208
14.48 Limites à plusieurs variables . . . 1209
14.49 Champs de vecteurs . . . 1212
14.49.1 Matrice jacobienne . . . 1212
14.50 Divergence, rotationnel et l'opérateur nabla . . . 1213
14.51 Interprétation de la divergence . . . 1215
14.52 Quelques formules de Leibniz . . . 1216

15 Analyse sur des groupes 1219
15.0.1 Groupe topologique . . . 1219
15.1 Action de groupe et connexité . . . 1220
15.2 Espaces de matrices . . . 1223
15.2.1 Dilatations et transvections . . . 1223
15.2.2 Connexité de certains groupes . . . 1229
15.2.3 Densité . . . 1231
15.2.4 Racine carrée d'une matrice hermitienne positive . . . 1233
15.2.5 Racine carrée d'une matrice symétrique positive . . . 1234
15.2.6 Décomposition polaires : cas réel . . . 1234
15.2.7 Enveloppe convexe . . . 1237
15.2.8 Décomposition de Bruhat . . . 1239
15.3 Sous-groupes du groupe linéaire . . . 1241

16 Tribus, théorie de la mesure, intégration 1245
16.1 Tribus . . . 1245
16.1.1 Généralités . . . 1245
16.1.2 Tribu engendrée . . . 1246
16.1.3 Tribu induite . . . 1247
16.2 Théorie de la mesure . . . 1247
16.2.1 Mesure sur un ensemble de parties . . . 1247
16.2.2 Mesure sur une algèbre de parties . . . 1248
16.2.3 Mesure sur une tribu, espace mesuré . . . 1250

16.2.4 Mesures sigma-finies . . . 1250
16.2.5 Suite du texte . . . 1251
16.2.6 λ-système . . . 1254
16.2.7 π-système . . . 1255
16.2.8 Unicité des mesures . . . 1255
16.2.9 Mesure extérieure . . . 1256
16.3 Applications mesurables . . . 1259
16.3.1 Propriétés . . . 1259
16.3.2 D'une tribu à l'autre . . . 1259
16.4 Tribu borélienne . . . 1260
16.4.1 Applications continues et boréliennes . . . 1261
16.4.2 Tribu de Baire . . . 1263
16.5 Espace mesuré complet . . . 1265
16.5.1 Partie négligeable . . . 1265
16.5.2 Prolongement . . . 1273
16.5.3 Mesure image . . . 1275
16.5.4 Régularité d'une mesure . . . 1276
16.5.5 Théorème de récurrence . . . 1283
16.6 Mesurabilité des fonctions à valeurs réelles . . . 1283
16.6.1 Fonctions à valeurs réelles sur un espace mesurable . . . 1284
16.6.2 Fonction étagée . . . 1289
16.6.3 Fonctions réelles à variables réelles . . . 1292
16.7 Tribu produit . . . 1293
16.7.1 Produit d'espaces mesurables . . . 1293
16.7.2 Le cas des boréliens . . . 1295
16.8 Mesure de Lebesgue sur $\mathbb{R}$ . . . 1296
16.8.1 Mesure et tribu de Lebesgue . . . 1300
16.8.2 Propriétés de la mesure de Lebesgue . . . 1301
16.8.3 Fonctions mesurables . . . 1305
16.8.4 Ensemble de Vitali (non mesurable) . . . 1306
16.8.5 Ensemble de Cantor . . . 1306
16.8.6 Mesure positive sans intervalle . . . 1308
16.9 Intégrale par rapport à une mesure . . . 1309
16.9.1 Définition pour les fonctions à valeurs positives . . . 1309
16.9.2 Premières propriétés . . . 1311
16.9.3 Propriétés plus avancées . . . 1314
16.9.4 Fonctions à valeurs réelles . . . 1317
16.9.5 Additivité de l'intégrale . . . 1319
16.9.6 Fonctions à valeurs vectorielles (dimension finie) . . . 1320
16.9.7 Quelques propriétés . . . 1322
16.9.8 Permuter limite et intégrale . . . 1323
16.9.9 Additivité de l'intégrale de Lebesgue . . . 1326
16.9.10 Produit d'une mesure par une fonction (mesure à densité) . . . 1327
16.9.11 Mesure et topologie . . . 1329
16.10 Mesure à densité . . . 1332
16.10.1 Théorème de Radon-Nikodym . . . 1332
16.10.2 Mesure complexe . . . 1346
16.10.3 Théorème d'approximation . . . 1346
16.11 Produit de mesures . . . 1347
16.12 Tribu et mesure de Lebesgue sur $\mathbb{R}^d$ . . . 1352
16.12.1 Propriétés d'unicité . . . 1353
16.12.2 Régularité . . . 1354
16.13 Propriétés de l'intégrale de Lebesgue . . . 1355
16.13.1 Quelques limites dans les bornes . . . 1356
16.13.2 Mesure de comptage et série . . . 1358
16.13.3 Théorème de la moyenne . . . 1360
16.14 Changement de variables dans une intégrale multiple . . . 1361
16.14.1 Des lemmes . . . 1361
16.14.2 Déterminant et mesure de Lebesgue . . . 1361
16.14.3 Ensembles négligeables . . . 1363
16.14.4 Parties et fonctions mesurables . . . 1364

16.14.5 Le théorème et sa démonstration . . . 1364
16.14.6 Exemples . . . 1369
16.15 Changement d'espace mesuré . . . 1369
16.16 Primitives et intégrales . . . 1370
16.16.1 Théorème fondamental du calcul intégral . . . 1371
16.16.2 Exemples et applications . . . 1372
16.16.3 Intégrales impropres . . . 1373
16.17 Théorème de Fubini-Tonelli et de Fubini . . . 1375
16.17.1 Utiliser Fubini sur $\mathbb{R}^n$ . . . 1383
16.17.2 Absolue continuité et variation bornée . . . 1384
16.17.3 Nouveau titre . . . 1385
16.17.4 Permuter limite et dérivée . . . 1385

17 Suites et séries de fonctions **1387**
17.1 Séries de fonctions . . . 1387
17.1.1 Intégration de séries de fonctions . . . 1387
17.1.2 Différentiabilité . . . 1389
17.2 Séries entières . . . 1393
17.2.1 Disque de convergence . . . 1394
17.2.2 Somme et produit de séries . . . 1396
17.2.3 Séries entières et polynômes . . . 1401
17.2.4 Critère de comparaison . . . 1407
17.2.5 Convergence normale . . . 1407
17.2.6 Unicité . . . 1409
17.2.7 Dérivation . . . 1410
17.2.8 Intégration . . . 1412
17.3 Séries de Taylor . . . 1413
17.3.1 Série de puissance . . . 1413
17.3.2 Polynôme de Taylor d'une série entière . . . 1414
17.3.3 Une majoration pour le reste . . . 1414
17.3.4 Fonctions analytiques . . . 1415
17.4 Algèbre engendrée par une matrice . . . 1417
17.5 Exponentielle sur une algèbre normée . . . 1417
17.5.1 Définition . . . 1417
17.5.2 Différentielles . . . 1419
17.5.3 Exponentielle de matrice . . . 1422
17.6 Exponentielle et logarithme dans les réels . . . 1425
17.6.1 L'équation différentielle . . . 1425
17.6.2 Existence . . . 1426
17.6.3 Le nombre de Neper e . . . 1426
17.6.4 Application réciproque : logarithme . . . 1428
17.6.5 Approximations numériques de e . . . 1430
17.6.6 Résumé des propriétés de l'exponentielle . . . 1431
17.6.7 Dérivée de la fonction puissance . . . 1433
17.6.8 Dérivée du logarithme . . . 1434
17.6.9 Taylor pour l'exponentielle . . . 1434
17.6.10 Analycité . . . 1434
17.6.11 Autres propriétés et petits calculs . . . 1434
17.6.12 Taylor pour le logarithme . . . 1435
17.6.13 Développements et calcul de limites . . . 1438
17.6.14 Une petite intégrale . . . 1438
17.7 Vitesses des puissances, de l'exponentielle et du logarithme . . . 1439
17.7.1 Un peu de théorie . . . 1439
17.7.2 Fonction de Riemann . . . 1441
17.7.3 Nombres premiers . . . 1444
17.7.4 Quelques limites . . . 1445
17.8 Trigonométrie hyperbolique . . . 1449
17.9 Séries entières de matrices . . . 1451
17.9.1 Différentiabilité . . . 1451
17.10 Exponentielle de matrices . . . 1453
17.10.1 Diagonalisabilité d'exponentielle . . . 1454

17.11 Étude d'asymptote . . . 1455
17.12 Développement en série . . . 1456
17.12.1 Série génératrice d'une suite . . . 1456
17.12.2 Développement en série et Taylor . . . 1456
17.12.3 Resommer une série . . . 1458
17.13 Séries entières de matrices . . . 1462
17.13.1 Rayon de convergence . . . 1463
17.13.2 Convergence et rayon spectral . . . 1463
17.13.3 Exponentielle et logarithme de matrice . . . 1465
17.13.4 Calcul effectif de l'exponentielle d'une matrice . . . 1467
17.14 Lemme de Borel . . . 1468
17.14.1 Fonctions plateaux, Urysohn, partition de l'unité . . . 1468
17.14.2 Lemme de Urysohn . . . 1472
17.14.3 Le lemme de Borel . . . 1473
17.15 Nombres de Bell . . . 1474
17.16 Applications analytique entre espaces de Banach . . . 1477
17.16.1 Applications analytiques . . . 1477
17.16.2 Opérateur d'inversion . . . 1482
17.16.3 Famille sommable . . . 1482
17.16.4 Intégrale par rapport à une des variables . . . 1486
17.16.5 Différentielle . . . 1489
17.16.6 Polynômes . . . 1490
17.16.7 Weierstrass et Cauchy-Lipschitz analytique . . . 1491
17.16.8 Série de puissance sur $\mathbb{C}$ . . . 1494
17.16.9 L'opérateur d'inversion est analytique . . . 1494

18 Représentations et caractères **1499**
18.1 Représentations et caractères . . . 1499
18.1.1 Crochet de dualité et transformée de Fourier . . . 1500
18.1.2 Groupes non abéliens . . . 1501
18.1.3 Représentations linéaires des groupes finis . . . 1502
18.1.4 Module . . . 1503
18.1.5 Structure hermitienne . . . 1505
18.1.6 Caractères . . . 1505
18.2 Équivalence de représentations et caractères . . . 1506
18.2.1 Représentation régulière . . . 1508
18.2.2 Caractères et représentations : suite et fin . . . 1509
18.3 Représentation produit tensoriel . . . 1511
18.4 Exemple sur le groupe symétrique . . . 1511
18.5 Table des caractères du groupe symétrique S_4 . . . 1512
18.5.1 Calculs à partir de rien ou presque . . . 1512
18.5.2 À propos de la représentation ρ_s . . . 1514
18.5.3 À propos de la représentation ρ_u . . . 1514

19 Encore de l'analyse (et c'est pas fini) **1517**
19.1 Densité des polynômes . . . 1517
19.2 Primitive et intégrale . . . 1517
19.2.1 Théorème taubérien de Hardy-Littlewood . . . 1517
19.2.2 Théorème de Müntz . . . 1521
19.3 Intégrales convergeant uniformément . . . 1523
19.3.1 Définition et propriété . . . 1523
19.4 L'aire en dessous d'une courbe . . . 1524
19.5 Propriétés des intégrales . . . 1525
19.6 Techniques d'intégration . . . 1526
19.6.1 Intégration par parties . . . 1526
19.6.2 Changement de variables – pour trouver des primitives . . . 1528
19.6.3 Changement de variables – pour calculer des intégrales . . . 1529
19.6.4 Intégrations des fractions rationnelles réduites . . . 1531
19.6.5 Quelques formules à connaitre . . . 1531
19.6.6 Critères de convergence uniforme . . . 1532
19.7 Fonctions définies par une intégrale . . . 1535

19.7.1 Continuité sous l'intégrale . . . 1535
19.7.2 Le coup du compact . . . 1537
19.7.3 Dérivabilité sous l'intégrale . . . 1537
19.7.4 Dérivation et intégrale . . . 1539
19.7.5 Différentiabilité sous l'intégrale . . . 1540
19.7.6 Dérivation dans les bornes . . . 1542
19.8 Théorème d'Hadamard . . . 1545
19.9 Deux théorèmes de point fixe . . . 1546
19.9.1 Points fixes attractifs et répulsifs . . . 1546
19.9.2 Picard . . . 1547
19.10 Théorèmes de point fixes et équations différentielles . . . 1549
19.10.1 Théorème de Cauchy-Lipschitz réel . . . 1549
19.10.2 Théorème de Caucy-Lipschitz analytique (tentative) . . . 1556
19.11 Flot . . . 1559
19.12 Théorèmes d'inversion locale et de la fonction implicite . . . 1560
19.12.1 Mise en situation . . . 1560
19.12.2 Théorème d'inversion locale . . . 1560
19.12.3 Théorème de la fonction implicite . . . 1563
19.12.4 Exemple . . . 1565
19.13 Décomposition polaire (régularité) . . . 1566
19.14 Théorème de Von Neumann . . . 1568
19.15 Recherche d'extrémums . . . 1570
19.15.1 Extrema à une variable . . . 1570
19.15.2 Extrema libre . . . 1571
19.15.3 Extremums et hessienne . . . 1572
19.15.4 Un peu de recettes de cuisine . . . 1574
19.15.5 Extrema liés . . . 1575
19.16 Fonctions convexes . . . 1577
19.16.1 Inégalité des pentes . . . 1577
19.16.2 Convexité et régularité . . . 1578
19.16.3 Dérivées d'une fonction convexe . . . 1579
19.16.4 Graphe d'une fonction convexe . . . 1580
19.16.5 Convexité et hessienne . . . 1585
19.16.6 Quelques inégalités . . . 1591
19.16.7 Norme l^p . . . 1592
19.16.8 Hölder . . . 1593
19.17 Algorithme du gradient à pas optimal . . . 1597
19.18 Formes quadratiques, signature, et lemme de Morse . . . 1601
19.19 Ellipsoïde de John-Loewner . . . 1605
19.20 Prolongement de fonctions . . . 1610
19.20.1 Encore du prolongement . . . 1612
19.21 Complétion d'un espace métrique . . . 1614
19.21.1 Principe des zéros isolés . . . 1618
19.22 Un petit extra . . . 1619

20 Trigonométrie, isométries 1621
20.1 Trigonométrie . . . 1621
20.1.1 Définitions, périodicité et quelques valeurs remarquables . . . 1621
20.1.2 Exponentielle avec « e » . . . 1623
20.1.3 Formules de trigonométrie . . . 1624
20.2 Trucs et astuces de calcul d'intégrales . . . 1636
20.2.1 Quelques intégrales « usuelles » . . . 1636
20.2.2 Reformer un carré au dénominateur . . . 1638
20.2.3 Décomposition en fractions simples . . . 1639
20.3 Très modeste approximation de π . . . 1639
20.3.1 Les fonctions tangente et arc tangente . . . 1640
20.3.2 La fonction arc sinus . . . 1642
20.3.3 La fonction arc cosinus . . . 1644
20.3.4 Une meilleure approximation de π . . . 1645
20.3.5 Angle entre deux vecteurs . . . 1646
20.3.6 Aire du parallélogramme . . . 1647

20.4 Paramétrisation du cercle . . . 1648
20.5 Cercle trigonométriques . . . 1649
20.5.1 Bijection continue . . . 1649
20.5.2 Inverse . . . 1652
20.5.3 Cercle trigonométrique . . . 1652
20.5.4 Du point de vue de la tribu, mesure et co. . . . 1653
20.6 Exemples trigonométriques . . . 1656
20.6.1 Quelques équations trigonométriques . . . 1657
20.6.2 Développements en série . . . 1657
20.7 Isométries de l'espace euclidien . . . 1658
20.7.1 Structure du groupe Isom($\mathbb{R}^n$) . . . 1659
20.8 Réflexion par rapport à un hyperplan . . . 1662
20.9 Isométries dans $\mathbb{R}^n$ . . . 1663
20.9.1 Préserver l'orientation . . . 1667
20.10 Groupes finis d'isométries . . . 1668
20.10.1 Points fixés par une affinité . . . 1670
20.11 Classification des isométries dans $\mathbb{R}^2$ . . . 1671
20.11.1 Projection orthogonale . . . 1671
20.11.2 Réflexions . . . 1673
20.11.3 Points fixés par une isométrie . . . 1676
20.11.4 Translations et réflexions . . . 1677
20.11.5 Rotations . . . 1677
20.11.6 Rotation d'un angle donné . . . 1680
20.11.7 Rotations vectorielles . . . 1682
20.11.8 Matrice des transformations orthogonales . . . 1684
20.11.9 Rotations, SO(2) et matrice de rotation . . . 1686
20.11.10 Rotation et application affine . . . 1686
20.11.11 Angle orienté . . . 1688
20.11.12 Angles et nombres complexes . . . 1691
20.11.13 Polygone convexe . . . 1695
20.11.14 Groupe diédral . . . 1696
20.11.15 Applications : du dénombrement . . . 1703
20.11.16 Classification . . . 1704
20.11.17 Classification des isométries de $\mathbb{R}$ . . . 1706
20.11.18 Isométries du tétraèdre régulier . . . 1707
20.11.19 Représentation de S_4 via les isométries du tétraèdre . . . 1708
20.12 Transformations de Lorentz . . . 1710
20.12.1 Sous-groupe fini d'isométries du plan . . . 1712
20.12.2 Relations trigonométriques dans un triangle rectangle . . . 1716
20.12.3 Pavages du plan . . . 1717
20.13 Un peu de structure de O(n) . . . 1731
20.13.1 Valeurs propres dans O(n) . . . 1731
20.13.2 Sous-groupes finis de SO(3) . . . 1734
20.14 Systèmes de coordonnées . . . 1742
20.14.1 Coordonnées polaires . . . 1742
20.14.2 Coordonnées cylindriques . . . 1749
20.14.3 Coordonnées sphériques . . . 1750
20.15 Calcul de limites . . . 1751
20.15.1 Méthode des coordonnées polaires . . . 1752
20.15.2 Méthode du développement asymptotique . . . 1754
20.16 Quelques intégrales avec de la trigonométrie . . . 1756
20.16.1 Changement de variables . . . 1756
20.16.2 Coordonnées polaires . . . 1756
20.16.3 Coordonnées cylindriques . . . 1757
20.16.4 Un autre système utile . . . 1758
20.17 Aire d'une surface de révolution . . . 1759
20.18 Table de caractères du groupe diédral . . . 1761
20.18.1 Représentations de dimension un . . . 1761
20.18.2 Représentations de dimension deux . . . 1762
20.18.3 Le compte pour n pair . . . 1764
20.18.4 Le compte pour n impair . . . 1764

21 Corps finis, racines de l'unité **1765**
21.1 Le groupe des racines de l'unité dans les nombres complexes . . . 1765
21.1.1 Le groupe . . . 1765
21.1.2 Fonction indicatrice d'Euler . . . 1768
21.1.3 Décomposition en éléments simples . . . 1769
21.2 Chiffrement RSA . . . 1770
21.2.1 Mise en place par Bob . . . 1770
21.2.2 Chiffrement . . . 1771
21.2.3 Déchiffrement . . . 1771
21.2.4 Une imprudence à ne pas commettre . . . 1771
21.2.5 Problèmes calculatoires . . . 1772
21.2.6 La solidité de RSA . . . 1772
21.2.7 Note non mathématique pour doucher l'enthousiasme . . . 1772
21.3 Polynômes cyclotomiques . . . 1772
21.3.1 Définitions et propriétés . . . 1772
21.3.2 Nombres premiers . . . 1776
21.4 Corps finis . . . 1777
21.4.1 Théorème de Wedderburn . . . 1778
21.4.2 Existence, unicité . . . 1779
21.4.3 Symboles de Legendre et carrés . . . 1781
21.4.4 Théorème de Chevalley-Warning . . . 1786
21.4.5 Contenu d'un polynôme . . . 1788
21.4.6 Théorème de l'élément primitif . . . 1789
21.4.7 Construction de $\mathbb{F}_{p^n}$ . . . 1793
21.4.8 Exemple : étude de $\mathbb{F}_{16}$ . . . 1795
21.4.9 Fonction de Möbius . . . 1797
21.4.10 Polynômes irréductibles sur $\mathbb{F}_q$ . . . 1799
21.4.11 Matrices . . . 1801
21.5 Constructions à la règle et au compas . . . 1802
21.5.1 Quelques constructions . . . 1802
21.5.2 Nombres constructibles . . . 1804
21.5.3 Polygones constructibles . . . 1806

22 Intégration sur des variétés **1811**
22.1 Variétés . . . 1811
22.1.1 Introduction . . . 1811
22.1.2 Définition, carte . . . 1811
22.1.3 Ancienne définition . . . 1812
22.1.4 Espace tangent . . . 1813
22.2 Intégration . . . 1814
22.2.1 Le problème pour une intégration globale . . . 1814
22.2.2 Intégrale sur une carte . . . 1814
22.2.3 Quelques expressions pour l'élément de volume . . . 1816
22.3 Intégrale sur une variété . . . 1817
22.3.1 Mesure sur une carte . . . 1817
22.3.2 Intégrale sur une carte . . . 1818
22.3.3 Exemples . . . 1819
22.3.4 Orientation . . . 1819
22.4 Longueur, aire, volumes etc. . . . 1821
22.4.1 Quelques aires faciles . . . 1821
22.5 Autres théorèmes de points fixes . . . 1823
22.5.1 Brouwer . . . 1823
22.5.2 Théorème de Schauder . . . 1827
22.5.3 Théorème de Cauchy-Arzella . . . 1828
22.5.4 Théorème de Markov-Kakutani . . . 1829
22.6 Intégrales curvilignes . . . 1830
22.6.1 Chemins de classe C^1 . . . 1830
22.6.2 Intégrer une fonction . . . 1831
22.6.3 Intégrer un champ de vecteurs . . . 1832
22.6.4 Intégrer une forme différentielle sur un chemin . . . 1832
22.6.5 Intégration d'une forme différentielle sur un chemin . . . 1833

22.6.6 Interprétation physique : travail . . . 1834
22.6.7 Intégrer un champ de vecteurs sur un bord en 2D . . . 1835
22.6.8 Intégrer une forme différentielle sur un bord en 2D . . . 1835
22.6.9 Intégrer une forme différentielle sur un bord en 3D . . . 1835
22.6.10 Intégrer un champ de vecteurs sur un bord en 3D . . . 1835
22.6.11 Dérivées croisées et forme différentielle exacte . . . 1836
22.7 Surfaces paramétrées . . . 1837
22.7.1 Graphe d'une fonction . . . 1838
22.7.2 Intégrale sur une partie de $\mathbb{R}^m$ . . . 1839
22.8 Intégrales de surface . . . 1839
22.8.1 Intégrale d'un champ de vecteurs . . . 1839
22.9 Aires et intégrales . . . 1840
22.9.1 Aire d'une surface paramétrée . . . 1840
22.9.2 Intégrale d'une fonction sur une surface . . . 1841
22.9.3 Intégrale d'une 2-forme . . . 1842
22.10 Flux d'un champ de vecteurs à travers une surface . . . 1842
22.11 Divergence, Green, Stokes . . . 1845
22.11.1 Théorème de la divergence . . . 1845
22.11.2 Lacets et homotopie . . . 1846
22.11.3 Formule de Green . . . 1847
22.11.4 Formule de Stokes . . . 1848
22.12 Résumé des intégrales vues . . . 1849
22.12.1 L'intégrale d'une fonction sur les réels . . . 1849
22.12.2 Intégrale d'une fonction sur un chemin . . . 1849
22.12.3 Intégrale d'une fonction sur une surface . . . 1850
22.12.4 Intégrale d'une fonction sur un volume . . . 1850
22.12.5 Conclusion pour les fonctions . . . 1851
22.12.6 Circulation d'un champ de vecteurs . . . 1851
22.12.7 Flux d'un champ de vecteurs . . . 1851
22.12.8 Conclusion pour les champs de vecteurs . . . 1851
22.12.9 Attention pour les surfaces fermées ! . . . 1852
22.13 Formes différentielles exactes et fermées . . . 1853
22.14 Théorème d'Abel angulaire . . . 1855
22.15 Passage à la limite sous le signe intégral . . . 1858
22.15.1 Intégrale en dimension un . . . 1858
22.15.2 Intégrales convergentes . . . 1859
22.15.3 La méthode de Rothstein-Trager . . . 1859
22.16 Rappel sur les intégrales usuelles . . . 1864
22.17 Intégrales le long de chemins . . . 1865
22.17.1 Circulation d'un champ de vecteur . . . 1865
22.18 Circulation d'un champ conservatif . . . 1866
22.19 Intégration de fonction à deux variables . . . 1868
22.19.1 Intégration sur un domaine rectangulaire . . . 1868
22.19.2 Intégration sur un domaine non rectangulaire . . . 1869
22.19.3 Changement de variables . . . 1871
22.20 Les intégrales triples . . . 1871
22.20.1 Volume . . . 1872
22.21 Un petit peu plus formel . . . 1874
22.21.1 Intégration sur un domaine non rectangulaire . . . 1874
22.22 Aire et primitive . . . 1875
22.22.1 Longueur d'arc de courbe . . . 1876
22.22.2 Aire de révolution . . . 1877
22.22.3 Taylor avec reste intégral . . . 1877
22.22.4 Approximation de ln(2) . . . 1880
22.23 Constructions plus naïves de l'intégrale dans le cas réel . . . 1882
22.23.1 Mesure de Lebesgue, version rapide . . . 1882
22.23.2 Pavés et subdivisions . . . 1882
22.23.3 Intégrale d'une fonction en escalier . . . 1885
22.23.4 Intégrales partielles . . . 1885
22.23.5 Réduction d'une intégrale multiple . . . 1886
22.23.6 Propriétés de l'intégrale . . . 1887

22.23.7 Intégrales multiples, cas général . . . 1888
22.23.8 Réduction d'une intégrale multiple . . . 1888
22.23.9 Intégrales sur des parties de $\mathbb{R}^2$ . . . 1890
22.23.10 Intégrales sur des parties de $\mathbb{R}^3$ . . . 1892
22.23.11 Fonctions et ensembles non bornés . . . 1894
22.23.12 Lemme de Morse . . . 1895
22.24 Autres intégrales sympathiques . . . 1897
22.24.1 Intégrale de Wallis . . . 1897
22.24.2 Formule de Stirling . . . 1900
22.24.3 La fonction sinus cardinal, intégrale de Dirichlet . . . 1903

23 Arcs paramétrés **1913**
23.1 Définitions . . . 1913
23.2 Longueur d'arc . . . 1913
23.3 Abscisse curviligne . . . 1915
23.3.1 Formule intégrale de la longueur . . . 1917
23.4 Suite du chapitre . . . 1922
23.5 Autres exemples . . . 1922
23.6 Élément de longueur . . . 1923
23.6.1 Élément de longueur : cartésiennes . . . 1923
23.6.2 Élément de longueur : polaires (1) . . . 1924
23.6.3 Élément de longueur : polaires (2) . . . 1924
23.6.4 Approximation de la longueur par des cordes . . . 1926
23.7 Arc géométrique . . . 1927
23.7.1 Abscisse curviligne et paramétrage normal . . . 1929
23.7.2 Tangente à une courbe paramétrée . . . 1933
23.8 Un peu de topologie . . . 1935
23.9 Repère de Frenet . . . 1937
23.9.1 Torsion . . . 1939
23.10 Hors des coordonnées normales . . . 1940
23.11 Tracer des courbes paramétriques dans $\mathbb{R}^2$ . . . 1942
23.12 Courbes planes . . . 1943
23.12.1 Angle . . . 1943
23.12.2 Courbure signée . . . 1944
23.12.3 Degré, indice et homotopie . . . 1947
23.13 Courbes fermées planes . . . 1953
23.13.1 Cercle circonscrit . . . 1953
23.13.2 Description locale . . . 1955
23.13.3 Enveloppe convexe . . . 1956
23.13.4 Courbure et convexité . . . 1959
23.13.5 Théorème des quatre sommets . . . 1960
23.13.6 Théorème d'Urysohn . . . 1962

24 Géométrie hyperbolique **1965**
24.1 Inversion . . . 1965
24.1.1 Cercles perpendiculaires . . . 1965
24.1.2 Inversion . . . 1966

25 Espaces projectifs **1971**
25.1 Sous-espaces projectifs . . . 1971
25.2 Espace projectifs comme « complétés » d'espaces affines . . . 1973
25.3 Théorème de Pappus . . . 1975
25.4 Homographies . . . 1976
25.4.1 Homographies . . . 1976
25.4.2 Le groupe projectif . . . 1977
25.4.3 Repères projectifs . . . 1978
25.4.4 Identifications $P(\mathbb{K}^2)$ vers $\mathbb{K} \cup \{\infty\}$ . . . 1982
25.4.5 Birapport . . . 1983
25.5 Coordonnées homogènes . . . 1988
25.5.1 Curiosité : matrice de translation . . . 1989
25.5.2 Dualité . . . 1989

25.5.3 Polynômes . . . 1991
25.6 La sphère de Riemann $P_1(\mathbb{C})$ . . . 1992
25.6.1 Éléments de géométrie dans $P_1(\mathbb{C})$ . . . 1992
25.6.2 Homographies . . . 1995
25.6.3 Birapport . . . 2001
25.6.4 Division harmonique . . . 2004
25.6.5 Groupe circulaire . . . 2007
25.6.6 Action du groupe modulaire . . . 2009

26 Analyse vectorielle **2015**
26.1 Le théorème de Green . . . 2015
26.2 Théorème de la divergence dans le plan . . . 2018
26.2.1 La convention de sens de parcours . . . 2018
26.2.2 Théorème de la divergence . . . 2019
26.3 Théorème de Stokes . . . 2020
26.4 Théorème de Gauss . . . 2021
26.5 Coordonnées curvilignes . . . 2022
26.5.1 Base locale . . . 2022
26.5.2 Importance de l'orthogonalité . . . 2023
26.5.3 Coordonnées polaires . . . 2024
26.5.4 Coordonnées cylindriques . . . 2025
26.5.5 Coordonnées sphériques . . . 2025
26.5.6 Gradient en coordonnées curvilignes . . . 2025
26.5.7 Divergence en coordonnées curvilignes . . . 2027
26.5.8 Laplacien en coordonnées curvilignes orthogonales . . . 2029
26.5.9 Rotationnel en coordonnées curvilignes orthogonales . . . 2029
26.6 Les formules . . . 2030
26.6.1 Coordonnées polaires . . . 2030
26.6.2 Coordonnées cylindriques . . . 2030
26.6.3 Coordonnées sphériques . . . 2031

27 Espaces de Hilbert **2033**
27.1 Espaces de Hilbert . . . 2033
27.1.1 Sous-espace vectoriel fermé ??? . . . 2036
27.2 Théorème de la projection . . . 2036
27.3 Systèmes orthogonaux et bases . . . 2039
27.3.1 Orthogonal d'une partie . . . 2039
27.3.2 Dual, théorème de représentation de Riesz . . . 2040
27.3.3 Séparabilité . . . 2041
27.3.4 Base hilbertienne . . . 2043
27.3.5 Décomposition dans une base hilbertienne . . . 2048
27.3.6 Digression sur les normes opérateurs . . . 2052
27.3.7 Applications linéaires et continuité . . . 2053
27.4 Théorème de Kochen-Specker . . . 2055
27.5 Théorème de Lax-Milgram . . . 2056

28 Analyse complexe **2061**
28.1 Fonctions holomorphes . . . 2061
28.1.1 Équations de Cauchy-Riemann . . . 2061
28.1.2 Intégrale sur un chemin dans $\mathbb{C}$ . . . 2064
28.1.3 Intégrales sur des chemins fermés . . . 2065
28.1.4 Homotopie entre applications . . . 2067
28.1.5 Intégrale et homotopie . . . 2068
28.1.6 Théorème de Tietze (espace normal) . . . 2070
28.2 Logarithme complexe . . . 2072
28.2.1 La fonction argument . . . 2072
28.2.2 Une définition possible du logarithme . . . 2075
28.2.3 Pas plus de continuité . . . 2077
28.2.4 Pas d'unicité : autres déterminations de l'argument . . . 2078
28.2.5 Pas d'unicité : développement en série . . . 2079
28.2.6 Pas d'unicité : laquelle choisir ? . . . 2079

28.2.7 Logarithme comme primitive . . . 2080
28.2.8 Logarithme sur un chemin . . . 2081
28.2.9 Lacets, indice et homotopie . . . 2083
28.2.10 Théorème de Cauchy et analycité . . . 2089
28.2.11 Théorème de Brouwer en dimension 2 . . . 2093
28.2.12 Principe des zéros isolés . . . 2093
28.2.13 Prolongement de fonctions holomorphes . . . 2095
28.2.14 Théorème de Runge . . . 2096
28.3 Intégrales de fonctions holomorphes . . . 2098
28.3.1 Holomorphie sous l'intégrale . . . 2098
28.3.2 Mesure de Radon . . . 2102
28.4 Conditions équivalentes à l'holomorphie . . . 2104
28.5 Limites, séries et dérivée . . . 2104
28.6 Singularités, pôles et méromorphe . . . 2105
28.7 Dénombrement des solutions d'une équation diophantienne . . . 2109
28.8 Fonctions d'Euler . . . 2115
28.8.1 Euler et factorielle . . . 2118
28.9 Exponentielle et logarithme complexe . . . 2118
28.9.1 Propriétés de l'exponentielle . . . 2118
28.9.2 Intégrale de Fresnel . . . 2119
28.10 Théorème de Weierstrass . . . 2121
28.11 Analyse complexe en plusieurs variables . . . 2122
28.11.1 Série . . . 2123
28.11.2 Inversion locale . . . 2123
28.11.3 Extension d'analytique vers holomorphe . . . 2124
28.11.4 Espace de fonctions holomorphes . . . 2126
28.11.5 Cauchy-Lipschitz holomorphe . . . 2126
28.11.6 Cauchy-Lipschitz analytique . . . 2129

29 Analyse fonctionnelle 2133
29.1 Théorème d'isomorphisme de Banach . . . 2133
29.2 Théorème d'Ascoli . . . 2133
29.3 Espaces de Lebesgue L^p . . . 2140
29.3.1 Généralités . . . 2140
29.3.2 Un peu de convergence de suites . . . 2144
29.3.3 L'espace L^∞ . . . 2145
29.3.4 Quelques identifications . . . 2147
29.3.5 Inégalité de Young, Jensen, Hölder et de Minkowski . . . 2148
29.3.6 Inégalité de Minkowski . . . 2152
29.3.7 Ni inclusions ni inégalités . . . 2164
29.3.8 Complétude . . . 2166
29.3.9 Théorèmes d'approximation . . . 2171
29.3.10 Densité des fonctions infiniment dérivables à support compact . . . 2172
29.3.11 Approximation . . . 2175
29.3.12 Partie uniformément intégrable . . . 2175
29.4 Autres résultats de convergence . . . 2176
29.5 Convolution . . . 2178
29.5.1 Fonction plateau, lemme d'Urysohn . . . 2181
29.5.2 Partition de l'unité . . . 2183
29.5.3 Approximation de l'unité . . . 2184
29.6 Intégrale sur des variétés . . . 2186
29.6.1 Formes différentielles . . . 2186
29.6.2 Intégrale d'une fonction sur une sous-variété . . . 2187
29.6.3 Densité des polynômes trigonométriques . . . 2187
29.7 Espaces L^2, généralités . . . 2189
29.8 L'espace $L^2(\mathbb{R}^d)$ . . . 2191
29.9 L'espace $L^2(S^1)$ . . . 2191
29.9.1 Espace mesuré . . . 2191
29.9.2 Topologie . . . 2193
29.9.3 Système trigonométrique . . . 2198
29.9.4 Convolution . . . 2199

29.9.5 Approximation de l'unité . . . 2201
29.9.6 Base hilbertienne (suite des polynômes trigonométriques) . . . 2205
29.9.7 Convolution, bis . . . 2206
29.10 Sur $[0, 2\pi[$ . . . 2206
29.11 Des inégalités . . . 2207
29.11.1 c-r inégalité . . . 2207
29.11.2 Inégalité de Hanner . . . 2209
29.11.3 Inégalités de Clarkson . . . 2214
29.12 Théorème de la projection normale . . . 2218
29.12.1 Espace uniformément convexe . . . 2218
29.12.2 Uniforme convexité des espaces de Lebesgue . . . 2220
29.12.3 Théorème de la projection normale . . . 2221
29.13 Jauge . . . 2222
29.14 Théorèmes de Hahn-Banach . . . 2224
29.14.1 Applications $\mathbb{R}$-linéaires et $\mathbb{C}$-linéaires . . . 2224
29.14.2 Hahn-Banach, théorème d'extension dominée . . . 2226
29.14.3 Hyperplan séparateur . . . 2228
29.14.4 Prolongement de fonctionnelles (dimension finie) . . . 2231
29.14.5 Prolongement de fonctionnelles (dimension infinie) . . . 2233
29.15 Théorème de Tietze . . . 2235
29.15.1 Pas de bijections bicontinues entre dimensions différentes . . . 2238
29.16 Dualité, réflexivité et théorème de représentation de Riesz . . . 2240
29.16.1 Le théorème de Jordan . . . 2255
29.16.2 Lemmes pour la parties composantes connexe . . . 2255
29.16.3 Lemmes pout la partie frontière . . . 2267
29.16.4 Théorème de Jordan . . . 2275
29.17 Topologie faible . . . 2275
29.17.1 Bases de topologie . . . 2276
29.17.2 Convergence . . . 2277
29.17.3 Helly et Goldstine . . . 2281
29.17.4 Banach-Alaoglu . . . 2283
29.17.5 Espace de Banach réflexif, Kakutani . . . 2286
29.17.6 Espaces L^∞ . . . 2287
29.18 Espace de Schwartz . . . 2288
29.18.1 Topologie . . . 2289
29.18.2 Produit de convolution . . . 2291
29.19 Théorème de Montel . . . 2292
29.20 Espaces de Bergman . . . 2293

30 Séries de Fourier **2297**
30.1 Densité des polynômes trigonométriques . . . 2297
30.1.1 Convergence pour les fonctions continues (via Weierstrass) . . . 2297
30.1.2 Convergence pour les fonctions continues (via Fejér) . . . 2297
30.1.3 Densité dans L^p . . . 2300
30.1.4 Suite équirépartie, critère de Weyl . . . 2301
30.2 Fonctions de Dirichlet . . . 2303
30.3 Coefficients et série de Fourier . . . 2304

31 Transformation de Fourier **2307**
31.1 Transformée de Fourier sur $L^1(\mathbb{R}^d)$ . . . 2307
31.1.1 Formule sommatoire de Poisson . . . 2311
31.2 Suite régularisante . . . 2313
31.3 Dérivation dans les bornes . . . 2314
31.4 Transformée de Fourier dans l'espace de Schwartz . . . 2315
31.4.1 Quelques transformées de Fourier . . . 2317
31.5 Intégrales et fonctions nulles . . . 2320
31.6 L'espace de Lebesgues $L^2\big([a, b]\big)$ . . . 2323
31.7 Sur $[-T, T[$ . . . 2329
31.7.1 Le cas dans $[0, 2\pi]$ . . . 2330
31.7.2 À propos des coefficients . . . 2333
31.7.3 Le contre-exemple que nous attendions tous . . . 2334

31.8 Série de Laurent . . . 2337
31.8.1 Inégalité isopérimétrique . . . 2341
31.8.2 Formule d'inversion . . . 2343
31.9 Transformée de Fourier sur $L^2(\mathbb{R}^d)$ . . . 2346
31.9.1 Le problème . . . 2346
31.9.2 Extension de $L^1 \cap L^2$ vers L^2 . . . 2347

32 Distributions **2349**
32.1 Dérivée faible . . . 2349
32.1.1 Dérivée partielle au sens faible . . . 2349
32.1.2 Dérivée faible partielle . . . 2351
32.1.3 Formules de Leibniz . . . 2352
32.2 Topologie et convergence sur des espaces de fonctions . . . 2353
32.2.1 Limite inductive . . . 2353
32.2.2 Les espaces classiques . . . 2353
32.2.3 Espaces de fonctions et topologie inductive . . . 2359
32.2.4 Convergence dans les fonctions test . . . 2359
32.3 Distributions . . . 2361
32.3.1 Multiplication d'une distribution par une fonction . . . 2364
32.3.2 Dérivée de distribution . . . 2364
32.3.3 Ordre et support d'une distribution . . . 2365
32.4 L'espace $C^\infty(\mathbb{R}, \mathscr{D}'(\mathbb{R}^d))$ . . . 2368
32.4.1 Dérivation . . . 2370
32.5 Une équation de distribution . . . 2370
32.6 Localisation, principe de recollement . . . 2371
32.7 Permuter distributions, dérivées et intégrales . . . 2375
32.8 Distributions tempérées . . . 2379
32.8.1 Topologie . . . 2381
32.8.2 Distributions associées à des fonctions . . . 2381
32.8.3 Composition avec une fonction . . . 2382
32.8.4 Transformée de Fourier d'une distribution tempérée . . . 2382
32.8.5 Convolution d'une distribution par une fonction . . . 2382
32.8.6 Approximation de la distribution de Dirac . . . 2383
32.8.7 Peigne de Dirac . . . 2385
32.9 L'espace $C^\infty(\mathbb{R}, \mathscr{S}'(\mathbb{R}^d))$ . . . 2386
32.9.1 Propriétés générales . . . 2386
32.9.2 Dérivation . . . 2388

33 Espaces de Sobolev, équations elliptiques **2391**
33.1 Espaces de Sobolev . . . 2391
33.1.1 Sur un intervalle de $\mathbb{R}$ . . . 2391
33.1.2 Sur un ouvert de $\mathbb{R}^n$ . . . 2396
33.1.3 Espace de Sobolev fractionnaire . . . 2397
33.2 Trace . . . 2400
33.3 Théorème de plongement . . . 2402

34 Équations différentielles ordinaires **2407**
34.1 Équation homogène, solution particulière . . . 2408
34.2 Que faire avec $f(z)dz = g(t)dt$? . . . 2408
34.3 Équations linéaires du premier ordre . . . 2409
34.3.1 Pourquoi la variation des constantes fonctionne toujours ? . . . 2412
34.4 Équations à variables séparées . . . 2413
34.4.1 La méthode rapide . . . 2413
34.4.2 La méthode plus propre . . . 2413
34.4.3 Les théorèmes . . . 2413
34.5 Équations linéaires d'ordre supérieur . . . 2416
34.5.1 Équations et systèmes linéaires à coefficients constants . . . 2416
34.5.2 Si les coefficients ne sont pas constants ? . . . 2417
34.6 Système d'équations linéaires . . . 2417
34.6.1 La magie de l'exponentielle... . . . 2417
34.6.2 ... mais la difficulté . . . 2418

34.6.3 La recette . . . 2418
34.6.4 Système d'équations linéaires avec matrice constante . . . 2419
34.6.5 Système d'équations linéaires avec matrice non constante . . . 2419
34.7 Réduction de l'ordre . . . 2419
34.8 Autour de Cauchy-Lipschitz . . . 2421
34.8.1 Fuite des compacts et explosion en temps fini . . . 2421
34.8.2 Écart entre deux conditions initiales . . . 2423
34.8.3 Flot d'un champ de vecteurs . . . 2424
34.8.4 Stabilité de Lyapunov . . . 2436
34.8.5 Système proies-prédateurs de Lotka-Volterra . . . 2440
34.9 Équation du second ordre . . . 2443
34.9.1 Wronskien . . . 2443
34.9.2 Avec second membre . . . 2444
34.9.3 Équation $y'' + q(t)y = 0$ . . . 2444
34.9.4 Équation de Hill . . . 2445
34.10 Différents types d'équations différentielles . . . 2448
34.10.1 Équation homogène . . . 2448
34.10.2 Équation de Bernoulli . . . 2449
34.10.3 Équation de Riccati . . . 2449
34.10.4 Équation différentielle exacte . . . 2449
34.11 Distributions pour les équations différentielles . . . 2450
34.11.1 Équation de Schrödinger . . . 2450
34.12 Équations différentielles du premier ordre . . . 2453
34.13 Premier ordre, variables séparables . . . 2455
34.14 Équations différentielles linéaires du premier ordre . . . 2458
34.14.1 Méthode de variation de la constante . . . 2459
34.15 Équations différentielles linéaires du second ordre . . . 2460
34.15.1 Équations différentielles linéaires du second ordre homogènes à coefficients constants . . . 2460
34.15.2 Linéaires du second ordre à coefficients constants, non homogènes . . . 2462
34.16 Fonction de Green . . . 2463

35 Équations aux dérivées partielles **2465**
35.1 Symbole principal, équation des caractéristiques . . . 2465
35.2 Méthode des caractéristiques pour l'ordre 1 . . . 2465
35.2.1 Un exemple complet un peu minimal . . . 2466
35.2.2 Un théorème d'existence et d'unicité . . . 2468
35.3 Méthode des caractéristiques pour l'ordre 2 . . . 2471
35.3.1 Principe général . . . 2471
35.3.2 Exemple : l'équation d'onde . . . 2472
35.4 Classification des équations du second ordre . . . 2473
35.4.1 Problème au limite . . . 2474
35.5 Principe du maximum . . . 2475
35.6 Quelques exemples . . . 2478
35.6.1 Un changement de variables . . . 2478

36 Numérique **2481**
36.1 Introduction . . . 2481
36.2 Représentations numériques . . . 2481
36.2.1 Entier relatif en complément à deux (binaire) . . . 2481
36.2.2 Représentation en virgule flottante . . . 2483
36.2.3 Simple précision, IEEE-754 . . . 2483
36.3 Problèmes pour écrire des nombres . . . 2485
36.3.1 Troncature : la base . . . 2486
36.3.2 Troncature : le drift . . . 2486
36.3.3 Quelques bonnes règles . . . 2487
36.3.4 Erreur de "cancellation" . . . 2487
36.3.5 Calcul d'une dérivée . . . 2489
36.3.6 Erreur d'absorption . . . 2490
36.4 Conditionnement et stabilité . . . 2490
36.4.1 Comment choisir et penser le K ? . . . 2493
36.5 Un peu de points fixes . . . 2493

36.5.1 Choix de la fonction à point fixe . . . 2493
36.5.2 Convergence quadratique . . . 2495
36.5.3 Convergence . . . 2496
36.6 Méthode de Newton . . . 2497
36.6.1 « Justification » par la formule de Taylor . . . 2498
36.6.2 « Justification » par points fixes . . . 2498
36.6.3 Convergence de la méthode de Newton . . . 2499
36.6.4 Racine carrée par la méthode de Newton . . . 2500
36.6.5 Formalisation de l'algorithme . . . 2500
36.6.6 Caractéristiques . . . 2501
36.6.7 Exemple de la racine carrée . . . 2502
36.6.8 Si multiplicité . . . 2502
36.6.9 Et la dérivée ? . . . 2503
36.6.10 Méthode de Newton : le cas général . . . 2503
36.7 Estimation de l'ordre de convergence . . . 2504
36.8 Autres méthodes . . . 2505
36.8.1 Méthode de Schröder . . . 2505
36.8.2 Halley . . . 2505
36.9 Méthode des sécantes variables . . . 2505
36.9.1 Aitken . . . 2506
36.10 Équations algébrique . . . 2507
36.10.1 Résoudre un système linéaire . . . 2507
36.10.2 Caractéristiques . . . 2507
36.10.3 Définitions . . . 2508
36.11 Équations non linéaires . . . 2508
36.11.1 Méthode de bissection . . . 2509
36.12 Efficacité . . . 2511
36.13 Exemples sous forme d'exercices . . . 2512
36.14 Approximations de fonctions . . . 2515
36.14.1 Critère d'interpolation . . . 2515
36.14.2 Base de Newton . . . 2516
36.14.3 Méthode des minimums quadratiques . . . 2518
36.14.4 Notre espace de Hilbert . . . 2518
36.14.5 Droite de régression . . . 2520
36.15 Conditionnement d'une matrice . . . 2520
36.15.1 Perturbation du vecteur . . . 2522
36.15.2 Perturbation de la matrice . . . 2523
36.16 Système linéaires (généralités) . . . 2524
36.16.1 Les méthodes directes . . . 2525
36.16.2 Méthodes itératives . . . 2525
36.17 Système linéaires (méthodes directes) . . . 2526
36.17.1 Inversion de matrice triangulaire . . . 2526
36.17.2 Transformation gaussienne . . . 2526
36.17.3 Méthode de Gauss pour résoudre des systèmes d'équations linéaires . . . 2527
36.17.4 Méthode de Gauss sans pivot (décomposition LU) . . . 2528
36.17.5 Matrice de permutation élémentaire . . . 2531
36.18 Méthode de Gauss avec pivot partiel (décomposition PLU) . . . 2532
36.18.1 L'idée . . . 2532
36.18.2 Le théorème . . . 2533
36.18.3 D'un point de vue algorithmique . . . 2536
36.18.4 Exemples . . . 2538
36.19 Résolution de systèmes linéaires (suite) . . . 2540
36.19.1 Déterminant . . . 2540
36.19.2 Plusieurs termes indépendants . . . 2541
36.19.3 Cholesky . . . 2541
36.20 Système linéaire (méthodes itératives) . . . 2544
36.20.1 La méthode générale . . . 2545
36.20.2 Jacobi . . . 2545
36.20.3 Gauss-Seidel . . . 2545
36.20.4 Autres . . . 2545
36.21 Indices connectés, matrice irréductible . . . 2546

36.22 Localisation des valeurs propres . . . 2547
36.22.1 Matrices à diagonale dominante . . . 2549
36.22.2 M-matrice . . . 2552

37 Méthode des différences finies 2555
37.1 Problèmes de dimension un . . . 2555
37.1.1 Un schéma à cinq points . . . 2556
37.1.2 Exemple . . . 2560
37.2 Problèmes de dimension deux . . . 2561
37.2.1 Discrétisation en croix . . . 2561
37.2.2 Discrétisation en carré . . . 2562
37.2.3 Résolution de la discrétisation en croix . . . 2563
37.3 Consistance, convergence . . . 2565
37.3.1 Définitions, mise en place . . . 2565
37.3.2 Exemple . . . 2566
37.3.3 Consistance, stabilité et convergence . . . 2567
37.3.4 Exemple : schéma à cinq points, laplacien en croix . . . 2568
37.4 Autres laplaciens . . . 2569
37.4.1 Travail avec le laplacien à 9 points . . . 2572

38 Variables aléatoires et théorie des probabilités 2573
38.1 Espace de probabilité . . . 2573
38.2 Variables aléatoires . . . 2574
38.2.1 Loi d'une variable aléatoire . . . 2574
38.2.2 Indépendance . . . 2574
38.2.3 Lois conjointes et indépendance . . . 2579
38.2.4 Densité jointe . . . 2583
38.2.5 Espérance . . . 2585
38.2.6 Moment . . . 2587
38.2.7 Somme et produit de variables aléatoires indépendantes . . . 2587
38.2.8 Variance . . . 2589
38.2.9 Covariance . . . 2590
38.2.10 Probabilité conditionnelle : événements . . . 2591
38.2.11 Espérance conditionnelle . . . 2593
38.2.12 Probabilité conditionnelle : tribu . . . 2600
38.2.13 Variables de Rademacher indépendantes . . . 2602
38.2.14 Un petit paradoxe . . . 2603
38.2.15 Inégalité de Jensen . . . 2609
38.2.16 Fonction de répartition . . . 2609
38.2.17 Fonction caractéristique . . . 2610
38.2.18 Fonction génératrice des moments, transformée de Laplace . . . 2611
38.2.19 Théorème de transfert . . . 2612
38.2.20 Changement de variables . . . 2614
38.3 Convergence . . . 2615
38.3.1 Convergence et fonction caractéristique . . . 2619
38.4 Loi des grands nombres, théorème central limite . . . 2623
38.4.1 Loi des grands nombres . . . 2623
38.4.2 Théorème central limite . . . 2625
38.4.3 Marche aléatoire . . . 2628
38.5 Les lois usuelles : du blabla . . . 2629
38.5.1 Loi de Bernoulli . . . 2629
38.5.2 Loi binomiale . . . 2629
38.6 Les lois usuelles . . . 2630
38.6.1 Loi de Bernoulli . . . 2630
38.6.2 Loi binomiale . . . 2631
38.6.3 Loi multinomiale . . . 2632
38.6.4 Loi géométrique . . . 2632
38.6.5 Loi de Poisson . . . 2633
38.6.6 Loi exponentielle . . . 2633
38.6.7 Approximation de la binomiale par une Poisson . . . 2637
38.6.8 Loi de Poisson et loi exponentielle . . . 2637

38.6.9 Loi normale . . . 2639
38.6.10 Vecteurs gaussiens . . . 2640
38.6.11 Variable aléatoire de Rademacher . . . 2644
38.6.12 Loi de Student . . . 2645
38.6.13 Indépendance, covariance et variance de somme . . . 2645
38.7 Estimation des grands écarts . . . 2646
38.8 Simulations de réalisations de variables aléatoires . . . 2649
38.8.1 Générateur uniforme . . . 2649
38.8.2 Simulation par inversion . . . 2650
38.8.3 Algorithme de Box-Muller . . . 2651
38.8.4 Méthode du rejet . . . 2652
38.8.5 Simuler une loi géométrique à l'ordinateur . . . 2653
38.8.6 Simuler une loi exponentielle à l'ordinateur . . . 2653
38.8.7 Simuler une loi de Poisson à l'ordinateur . . . 2653
38.9 Sage . . . 2654
38.9.1 Loi exponentielle . . . 2654
38.9.2 Inverser des lois . . . 2654
38.10 Monte-Carlo . . . 2655
38.10.1 Intervalle de confiance . . . 2656
38.11 Résultats qui se démontrent avec des variables aléatoires . . . 2657
38.11.1 Nombres normaux . . . 2657
38.11.2 Théorème de Bernstein . . . 2659

39 Statistiques **2663**
39.1 Notations et hypothèses . . . 2663
39.2 Modèle statistique . . . 2663
39.3 Modèles d'échantillonnages . . . 2666
39.4 Estimation ponctuelle . . . 2669
39.5 Statistiques et estimateurs . . . 2670
39.5.1 Qualité des estimateurs . . . 2670
39.5.2 Méthode des moments . . . 2671
39.5.3 Méthode de substitution . . . 2672
39.5.4 Méthode du maximum de vraisemblance . . . 2673
39.5.5 Exemples sous forme d'exercices . . . 2673
39.5.6 Estimation d'une fonction de répartition . . . 2675
39.5.7 Exemples sous forme d'exercices . . . 2675
39.5.8 Espérance et variance d'un estimateur . . . 2677
39.6 Estimation par intervalle de confiance . . . 2678
39.6.1 Région de confiance . . . 2680
39.6.2 Fonction pivotale . . . 2681
39.6.3 Sondage de proportion . . . 2683
39.7 Estimer une densité lorsqu'on ne sait rien . . . 2684
39.7.1 Distance entre des mesures . . . 2684
39.7.2 Estimateur par fenêtres glissantes . . . 2685
39.8 Test d'hypothèses, prise de décision . . . 2687
39.8.1 Exemple : qualité des pièces d'usine . . . 2687
39.8.2 Exemple : la résistance d'un fil . . . 2688
39.8.3 Vocabulaire et théorie . . . 2688
39.8.4 Risque de première et seconde espèce . . . 2689
39.8.5 Modèle paramétrique de loi gaussienne . . . 2690
39.9 Tests paramétriques . . . 2691
39.10 Tests d'adéquation . . . 2692

40 Chaînes de Markov à temps discret **2697**
40.1 Généralités . . . 2697
40.1.1 Matrice stochastique . . . 2699
40.2 Chaînes de Markov sur un ensemble fini . . . 2699
40.2.1 Graphe de transition . . . 2701
40.2.2 Nombre de visites . . . 2702
40.2.3 Récurrent et transient . . . 2703
40.2.4 Chaînes irréductibles . . . 2705

40.2.5 Périodique et irréductible . . . 2709
40.3 Marche aléatoire sur $\mathbb{Z}$ . . . 2710
40.3.1 Chaînes de Markov homogènes . . . 2712
40.3.2 Chaîne de Markov définie par récurrence . . . 2714
40.4 Classification des états . . . 2717
40.5 Mesure invariante . . . 2719
40.6 Convergence vers l'équilibre . . . 2721
40.7 Processus de Galton-Watson . . . 2722

41 Martingales **2727**
41.1 Convergence de martingales . . . 2727
41.2 Temps d'arrêt et martingale terminée . . . 2729
41.2.1 Nombre de montées . . . 2730
41.2.2 Théorèmes d'arrêt . . . 2733
41.3 Décomposition de martingales . . . 2736
41.4 Problème de la ruine du joueur . . . 2737
41.4.1 Le cas où la pièce est truquée . . . 2738
41.4.2 Le cas où la pièce est non truquée . . . 2741
41.4.3 Un petit complément . . . 2743

42 Processus de Poisson **2745**
42.1 Processus de Poisson . . . 2745
42.1.1 Processus a-Poisson . . . 2745
42.1.2 Processus c-Poisson . . . 2745
42.1.3 Processus n-Poisson . . . 2746
42.1.4 Processus o-Poisson . . . 2746
42.1.5 Équivalence de définitions . . . 2759
42.1.6 Estimateurs . . . 2759
42.2 Quelques trucs sur la simulation . . . 2761
42.2.1 Le théorème central limite pour Markov . . . 2761
42.2.2 Feuille 5 . . . 2762
42.2.3 Feuille 6 . . . 2762
42.2.4 Feuille 7 . . . 2762
42.2.5 Simuler des lois conditionnelles . . . 2762

43 Langages **2765**
43.1 Alphabets et mots . . . 2765
43.2 Langages . . . 2766

44 Utilisation dans les autres sciences **2769**
44.1 Démystification du MRUA . . . 2769
44.1.1 Preuve de la formule . . . 2769
44.1.2 Interprétation graphique . . . 2770
44.2 Relativité en mécanique newtonienne . . . 2770
44.2.1 Relativité du mouvement . . . 2770
44.2.2 Bob et Alice . . . 2770
44.3 Invariance de la vitesse de la lumière . . . 2770
44.3.1 Champ de gravitation et électrique . . . 2770
44.3.2 Support du champ : pas d'éther . . . 2771
44.3.3 Le problème . . . 2771
44.4 Conséquences . . . 2772
44.4.1 Ligne d'univers . . . 2772
44.4.2 Transformations de Lorentz . . . 2772
44.4.3 Conditions d'existence . . . 2775
44.4.4 La notion d'intervalle . . . 2776
44.4.5 Le cône de lumière d'un point . . . 2776
44.4.6 Contraction des longueurs . . . 2776
44.4.7 Dilatation des intervalles de temps . . . 2777
44.4.8 Invariance de l'intervalle . . . 2778
44.4.9 Vitesse limite . . . 2781
44.5 Applications . . . 2782

44.5.1 Le GPS . . . 2782
44.5.2 Les ondes électromagnétiques . . . 2782
44.6 Mécanique relativiste . . . 2782
44.6.1 Des problèmes, toujours des problèmes . . . 2782
44.6.2 Loi d'addition des vitesses . . . 2783
44.6.3 L'action d'une force . . . 2783
44.6.4 Équivalence entre la masse et l'énergie . . . 2785
44.7 Principe de correspondance . . . 2785

45 Exemples avec Sage **2787**
45.1 Graphiques . . . 2787
45.1.1 Autres . . . 2787

46 Épilogue : la constante de Weiner **2805**
46.0.1 Résultats prouvés dans le Frido . . . 2805
46.0.2 Autres résultats . . . 2805
46.0.3 Conjectures . . . 2806

47 Développements possibles **2807**
47.1 Algèbre et géométrie . . . 2807
47.2 Analyse . . . 2811
47.3 Anciennes leçons . . . 2814

48 GNU Free Documentation License **2823**

Bibliographie **2829**

Index

λ-système, 1254
π-système, 1255
σ-compact, 549
k-forme différentielle, 1095
p-groupe, 425
p-Sylow, 425
q-orthogonal, 694

Abel
    angulaire, 1855
    convergence radiale, 1407
Abel
    angulaire, 1855
    convergence radiale, 1407
abélianisé, 229
abscisse
    curviligne, 1929
absolument continue, 1384
absorbant, 2717
accélération d'un chemin, 1913
accroissement, 1207
accroissements finie
    dérivée partielle, 928
action, 307
    adjointe, 364
    de groupe
        Wedderburn, 1778
    domaine fondamental, 366
    fidèle, 364
    libre, 370
    transitive, 370
action continue, 1220
action de groupe, 652
    sur des matrices, 1895
action fidèle, 364
action transitive, 370
adjoint, 659, 701
affine
    application, 966
    espace, 961
    sous-espace, 969
aire, 1891
aire dans $\mathbb{R}^2$, 1821
algèbre, 264
    de parties, 1248
    engendrée, 264
algèbre de Banach, 601
algèbre engendrée, 1417
algébrique, 476
algébriquement
    indépendant, 515
algorithme, 2508
    consistant, 2508
    facteurs invariants, 409
    fortement consistant, 2508
    stable, 2508
algorithme convergent, 2508
alignement
    dans un espace projectif, 1972
alphabet, 2765
alterné
    groupe, 440
    polynôme, 511
analytique entre espaces de Banach, 1477
angle
    d'une courbe, 1946
    entre deux droites, 1693
    orienté de vecteurs, 1688
angle entre deux vecteurs, 1646
anneau, 142
    $\mathbb{Z}/n\mathbb{Z}$, 434, 1770, 1777, 1781
    à division, 451
    de séries formelles, 1474
    élément régulier, 145
    euclidien
        facteurs invariants, 409
    factoriel, 291
    noethérien, 296
    principal, 458, 682
        utilisation, 459
    quotient par un idéal, 236
Anneau
    $\mathbb{Z}/n\mathbb{Z}$
        polynôme cyclotomique, 1774
anneau commutatif, 142
anneau intègre, 238
anneau principal
    Bézout, 292
anneau topologique, 580
anneau valué, 147
apériodique
    état d'une chaine de Markov, 2709
application, 117
    de classe C^k, 930
    définie positive, 687
    différentiable, 923, 930, 1101, 1139, 1561, 1895
        extrémums lié, 1575
    en escalier, 1884
    linéaire
        théorème de Banach-Steinhaus, 883

mesurable, 1252
ouverte, 595
semi-définie positive, 687
tangente, 1105
application k-linéaire, 645
application k-multilinéaire, 645
application affine, 697
application bilinéaire, 687
application bloc-diagonale, 833
application multilinéaire
décomposable, 900
application ouverte, 885
application quotient, 535
application réciproque, 118
applications homotopes, 2067
applications linéaires semblables, 708
approximation
de fonctions
par des polynômes, 2660
de l'unité, 2184
par polynômes, 1519
polynomiale, 2096
arc
géométriques, 1928
paramétré, 1913
arc cosinus, 1644
arc sinus, 1643
arc tangente, 1641
archimédien, 163
$\mathbb{N}$, 167
$\mathbb{Q}$, 325
$\mathbb{R}$, 340
associée
subdivision, 1884
associés
éléments d'un anneau, 289
asymptotiquement pivotale, 2681
attractif
point fixe, 1546
automorphisme, 529
d'espace vectoriel, 382
automorphisme de groupes, 141
axiome
du choix, 117

Baire
tribu, 1263
Baire
tribu, 1263
barycentre
cas affine, 970
cas vectoriel, 1668
enveloppe convexe, 974
base, 372
d'un module, 263
de Newton, 2517
de topologie
dénombrable, 568
espace métrique, 568
duale, 416
espace préhilbertien, 2043
hilbertienne, 2043
utilisation, 2341
locale, 2023
base associée à un repère cartésien, 962
base canonique de $\mathbb{R}^m$, 376
base de topologie, 517
base de topologie et continuité, 528
base de voisinages, 518
base orthonormée, 699
base préduale, 418
Bergman (espace), 2293
Bernoulli, 2629
somme, 2647
Berry-Esséen (borne), 2627
Bessel
inégalité, 2043
Bézout
calcul effectif, 278
polynômes, 470
biais
d'estimateur, 2671
bien
conditionné, 2491
enchainé, 621
biholomorphe, 2123
bijection, 117
bilinéaire, 645
binormale, 1938
birapport, 1983
birapport dans $\mathbb{C} \cup \{\infty\}$, 2001
birégulier
point sur une courbe, 1926
Bolzano-Weierstrass
espaces métriques, 569
bon
ordre, 121
bonne seminorme, 2354
bord, 560
borélienne
fonction, 1261
tribu, 1260
boréliens, 1260
borné, 568
partie de V, 662
temps d'arrêt, 2729
bornée
différentielle, 1126
partie de $\mathbb{R}^m$, 1017
suite, 769
boule
ouverte, 556
boule dans un corps, 313
boule fermée, 563
Bruhat (décomposition), 1239
Burnisde
formule, 367

canonique
base, 376
décomposition, 129
espace affine, 962

canonique
base, 376
décomposition, 129
espace affine, 962
Cantor
ensemble, 1306
caractère, 1505
abélien, 1499
de S_4, 1512
groupe diédral, 1761
irréductible, 1505
caractéristique
d'un anneau, 265
d'une équation différentielle, 2465
polynôme, 683
sous-groupe, 181
cardinal, 186
cardioïde, 1925
carré
dans un corps fini, 1781
carrée
matrice, 389
carte, 1812
Cauchy
critère
uniforme, 866
déterminant, 653
formule, 2089
suite, 611
théorème, 425
Cauchy-continue, 1011
Cauchy-Riemann, 2062
Cauchy-Schwarz, 801, 2035
Cayley
théorème, 425
cellule d'un pavage, 1884
centrale (application), 1505
centralisateur, 181, 233
centre
d'un anneau, 233
d'un groupe, 181
d'une rotation, 1678
cercle
circonscrit à une courbe, 1953
dans la sphère de Riemann, 1993
cercle-droite, 1994
cercles
perpendiculaires, 1965
cercles tangents, 1056
Cesàro
moyenne, 878
chaine, 621
de Markov, 2697
convergence, 2721
finie, 2699
homogène, 2697
irréductible, 2700
récurrente positive, 2707
chaine de Markov apériodique, 2710
chaine de Markov régulière, 2700
champ
conservatif, 1866
de vecteurs, 1832
champ de vecteur conservatif, 1834
champ dérivant d'un potentiel, 1866
changement de variable, 1928
Chasles, 961
chemin, 1846
dans $\mathbb{R}^p$, 1913
chemin C^1 par morceaux, 1830
chemin de Jordan, 1846
chemin régulier, 1846
circulation, 1865
classe
d'association, 289
de conjugaison, 181
classe d'association, 289
classe de conjugaison
dans S_4 , 216
clôture algébrique, 477
codimension, 377
coefficient binomial, 251
coefficients
de Fourier, 2188
coefficients binomiaux, 251
coefficients de Fourier, 2199
coercion, 2056
coercive, 1597
colinéarité, 1971
combinaison
convexe, 970
combinatoire, 1703
commutant, 745
commutateur
dans un groupe, 228
commutativement sommable, 853
compacité, 569, 617, 621, 2100, 2121
sous-groupes du groupe linéaire, 1241
théorème de Dini, 1157
utilisation, 1606
théorème de Montel, 2292
compact, 548, 664
arc paramétré, 1913
boule unité, 766
et fonction continue, 570, 777
fermé et borné, 765
intervalle $[a, b]$, 764
le coup du, 1537
localement, 564
opérateur, 2133
produit dénombrable, 623
produit fini, 622
quasi, 548
séquentiellement, 549
suite exhaustive, 619
compacts et fermés, 550
complément
à deux, 2481
complémentaire, 116
complet
$\mathbb{R}$
corps, 345

espace métrique, 611
corps, 313
espace mesuré, 1265
espace topologique, 600
métrique, 600
complété
d'un espace métrique, 1616
complète
famille de projecteurs, 263
complétion
projective, 1974
complétion d'espace métrique, 1615
complétude, 1612, 1616, 2166
espaces L^p, 2167
complexe conjugué, 357
composante, 1208
composante connexe, 546
composition, loi interne, 129
composition
suite de, 359
concaténation
de langages, 2766
de mots, 2765
concave, 1577
log-concave, 1583
condition initiale, 2454
conditionnement
absolu, 2491
d'une matrice inversible, 2521
relatif asymptotique, 2508
Cône de lumière, 2776
conjugué hermitien, 701
conjugués
éléments d'une extension, 476
connectés
indices d'une matrice, 2546
connexe par arc, 780
connexe par arcs
sphère, 810
connexité, 621
définition, 545
et intervalles, 774
fonction holomorphe, 1618
indice d'une courbe, 2083
le groupe $\mathrm{GL}^+(n,\mathbb{R})$, 1230
par arc
fonction différentiable, 1139
points d'accumulation, 617
prolongement analytique, 1618
signature d'une forme quadratique, 1602
théorème de Runge, 2096
théorème des valeurs intermédiaires, 788
utilisation
Brouwer, 2093
consistance
estimateur, 2670
ordre, 2565
constructible
angle, 1806
point, 1802
réel, 1802
construction
des réels, 334
contenu, 316
continue
fonction entre espaces métriques, 615
fonction entre espaces topologiques, 528
forme différentielle, 1096
continuité
fonction définie par une intégrale, 1535
séquentielle, 558
contraction, 903, 1547
convergence
commutative, 853
dans un espace vectoriel normé, 766
de martingales, 2735
en loi, 2615
en probabilité, 2615
ordre, 2504
presque surement, 2615
quadratique, 2495
rapidité, 1444, 2311, 2312, 2503, 2647
suite
dans un corps, 313
suite dans $\mathbb{R}^m$, 598
suite numérique, 766, 1519, 2301
Abel angulaire, 1855
uniforme, 851
intégrale, 1523
théorème de Dini, 1157
convergence absolue, 852
convergence de suite, 520
convergence forte, 884
convergence normale, 852
convexe
courbe plane, 1955
fonction sur $\mathbb{R}^n$, 1585
convexité
barycentre, 973
enveloppe de $O(n)$, 1238
fonction, 1577
inégalité de Jensen, 1591
locale, 584
méthode de Newton, 2500
utilisation, 1606
convolution, 2587, 2723
convolution sur S^1, 2199
coordonnées
cartésiennes
dans un espace affine, 977
curvilignes, 2022
cylindrique, 1749
dans un espace affine, 962
homogène, 1988
sphériques, 1750
coordonnées barycentrique, 979
coordonnées polaires, 1744
corps, 177
complet, 313
de décomposition, 499
de rupture, 489
polynôme cyclotomique, 1774

des fractions, 308
extension, 505, 513
fini, 1781, 1784, 1787
Wedderburn, 1778
formellement réel, 451
ordonné, 146
premier, 453
corps algébriquement clos, 477
corps valué, 147
cosinus, 1621
hyperbolique, 1449
courbe, 1913
efficacité, 2689
étude métrique, 2341
fermée, 1943
simple, 1943
courbe de Jordan, 1846
courbe de niveau, 1082, 1084
courbe simple, 1846
courbes tangentes, 1056
courbure, 1938
signée, 1944
totale, 1945
covariance, 2590
critère
Abel, 1395
Cauchy
uniforme, 866
de Cauchy, 345, 611
Weierstrass, 1532
série de fonctions, 1160
critère du quotient, 873
critique
Galton-Watson, 2723
point, 1571
point d'un arc, 1926
région, 2688
valeur, 2689
cycle, 210
cyclique
endomorphisme, 680
matrice, 680
cycloïde
coordonnées normales, 1931
longueur, 1925

décalage, 2483
décalage, 2483
décomposition
Bruhat, 1239
canonique, 129
corps, 499
Dunford, 732
application, 1454
exponentielle de matrice, 1181
Jordan
et exponentielle de matrice, 1453
polaire, 1235
primaire, 731
sous-espaces caractéristiques, 731
spectrale, 731
décomposition de Hahn, 1336
décomposition de Jordan, 1338
décomposition décimale, 881
degré
application $S^1 \to S^1$, 1947
d'une représentation, 420
extension de corps, 474
degré d'un polynôme, 304
demi-plan, 1051
dénombrable, 190
dénombrable à l'infini, 549
dénombrement, 1703
partitions de $\{1, \dots, n\}$, 1474
dense, 523
densité, 1616
d'une variable aléatoire, 2574
dans un espace de fonction
critère de Weyl, 2301
de $\mathbb{Q}$ dans $\mathbb{R}$, 762
utilisation, 1583
de $\mathrm{GL}(n, \mathbb{R})$ dans $\mathbb{M}(n, \mathbb{R})$, 1231
de $\mathscr{D}(\mathbb{R}^n)$ dans $L^1(\mathbb{R}^n)$, 2290
de $C_c^\infty(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$, 2173
de $L^2\big([0,1]\big)$ dans $L^p\big([0,1]\big)$, 2174
de $S^+(n, \mathbb{R})$ dans $S^{++}(n, \mathbb{R})$, 1235
des fonctions étagées dans L^p, 2173
des polynômes
dans $C_c^0[0,1]$, 2660
matrices diagonalisables dans $\mathbb{M}(n, \mathbb{C})$, 1231
mesure, 1327
points extrémaux dans $\mathcal{L}$, 1237
prolongement, 1612
densité conjointe, 2581
densité d'une mesure, 1328
densité jointe, 2583
déplacement, 1717
dérivabilité
fonction définie par une intégrale, 1537
lemme de Borel, 1473
dérivable
au sens complexe, 1134
fonction, 2407
dérivation
au sens des distribution
Sobolev, 2394
dérivé
groupe, 228
dérivée, 924
dans Sobolev $H^1(I)$, 2391
distributionnelle, 2364
faible, 2351
fonction à valeurs dans E', 641
partielle, 1094, 1207
seconde, 1064
dérivée directionnelle, 924
dérivée faible, 2349
dérivée partielle, 924
déterminant, 646
Cauchy, 1522
d'un endomorphisme, 650
d'une famille de vecteurs, 647

de Cauchy, 653
et inversibilité, 650
forme linéaire alternée, 646
Gram, 653, 1521
interprétation géométrique, 1361
matrice, 395
résultant, 655, 1859
utilisation, 1606
Vandermonde, 413
détermination
logarithme, 2078
principale, 2078
détermination du logarithme, 2081
développable
en série entière, 1456
développement
asymptotique, 1206
limité
en zéro, 1201
fonction holomorphe, 2061
premier ordre, 928
Taylor, 1895
diagonale
dominante, 2549
fortement dominante, 2549
strictement dominante, 2549
diagonalisable, 712
et polynôme minimum scindé, 713
exponentielle, 1454
diagonalisation
cas complexe, 1028
cas réel, 716
endomorphisme autoadjoint, 812
simultanée, 715
diamètre, 1017
diédral, 1703
difféomorphisme, 931
de classe C^k, 1149
différence
centrée, 2555
divisée, 2517
progressive, 2555
régressive, 2555
différentiabilité, 1139
différentielle, 923
de $u \mapsto u^{-1}$, 952
partielle, 950
totale, 1207
dilatation, 1223
dilatation (matrice), 405
dimension, 376
n-formes multilinéaires alternées, 646
définition, 376
sous-espace affine, 969
utilisation, 974
direction, 924, 1933
sous-espace affine, 969
Dirichlet
noyau, 2297
théorème, 2298
théorème (sur les nombres premiers), 1777
disque de convergence, 1394
distance, 556
associée à une norme, 576
compatible, 604
entre deux mesures de probabilités, 2684
invariante, 604
point et ensemble, 600
distance discrète, 599
distance produit, 593
distingué
sous-groupe, 181
distribution, 2361
de Dirac, 2380
équation de Schrödinger, 2450
produit par une fonction, 2364
tempérée, 2380
divergence, 1213
divise, 145
diviseur
dans un anneau, 145
de zéro, 237
de zéro à droite, 237
polynôme, 316
diviseur de zéro, 237
division
euclidienne, 243, 315
harmonique, 2004
division euclidienne
quotient dans $\mathbb{N}$, 169
reste dans $\mathbb{N}$, 169
domaine, 760
de définition d'une fonction, 117
fondamental d'une action, 366
dominé
modèle statistique, 2669
dominée
convergence (Lebesgue), 1324
mesure, 1332
dominée par le dessus, 626
dominée par une seminorme, 626
droite
dans la sphère de Riemann, 1993
projective, 1971
droite affine, 980, 1042
droite réelle achevée, 783
droite vectorielle, 1042
droites parallèles, 1043
droites perpendiculaires, 1043
dual
d'un espace de Hilbert, 2040
de $\mathbb{M}(n, \mathbb{K})$, 707
de $L^p(\Omega)$, 2251
de L^p, 2246
dual algébrique, 416
dual topologique, 601, 954
Dunford
décomposition, 732
dyadique, 1352
développement, 341
écart-type, 2589
échantillon, 2664, 2666

effectif
empirique, 2692
effectif
empirique, 2692
efficacité
courbe, 2689
d'une méthode itérative, 2511
élément
de surface, 1842
de torsion, 231
élément
inversible
dans un anneau, 237
élément de surface, 1817
élément maximal, 120
élément minimal, 120
élément premier, 237
élément régulier, 130
à droite, 130
à gauche, 130
ellipsoïde, 755
elliptique
équation aux dérivées partielles, 2473
endomorphisme, 382
cyclique, 680
décomposition
polaire, 1235
diagonalisable, 754, 1233, 2447
Dunford, 732
diagonalisation, 716
nilpotent
Dunford, 732
préservant une forme quadratique, 1243
sous-espace stable, 732, 2447
endomorphisme direct, 659
endomorphisme préserve l'orientation, 659
engendré
λ-système, 1254
corps, extension, 482
sous-espace affine, 969
sous-groupe, 226
ensemble
archimédien, 163
de Cantor, 1306
différence symétrique, 126
infini, 131
ensemble connexe, 545
ensemble des mots, 2765
ensemble fini, 131
ensemble ordonné, 119
totalement ordonné, 119
ensemble quotient, 127
ensembles
disjoints, 116
entier, 171
entier relatif
négatif, 174
positif, 174
strictement négatif, 174
strictement positif, 174
entiers relatifs
négatifs, 174
positifs, 174
entrelacement, 1506
enveloppe
convexe, 973
équation
aux variations, 2429
de Riccati, 2449
des classes, 367
des orbites, 366
différentielle
étude qualitative, 2447
Hill, 2445
homogène, 2448
système, 2447
diophantienne, 285, 301, 303
Fredholm, 1549
orbite-stabilisateur, 365
équation
différentielle
linéaire, 2409
ordinaire d'ordre 1, 2407
variables séparées, 2413
générale de degré n, 515
équation de droite, 1048
équation différentielle
linéaire du premier ordre, 2458
linéaire du premier ordre, homogène, 2458
linéaire du second ordre, 2460
linéaire du second ordre, homogène, 2460
premier ordre, 2453
second ordre, 2454
variables séparables, 2456
équation exponentielle, 1189
équation fonctionnelle, 1188
équation homogène associée, 2458
équicontinu, 623
équipotent, 130
équivalence
arcs paramétrés, 1927
chemin, 1921
classe de fonctions, 2140
de représentations, 1506
de suites, 768
homotopie, 2086
suite de composition, 361
équivalence de forme quadratiques, 727
équivalence de normes, 827
erreur, 2518, 2544
assignation, 2486
de consistance, 2565
discrétisation, 2565
quadratique, 2520
troncature, 2486
erreur relative, 2485
escalier, 1289
espace
L^2
Sobolev, 2394
L^p, 2144
de Bergman, 2293

de fonctions
L^p, 2167
Sobolev H^1, 2394
de Hilbert
espace de Sobolev H^1, 2394
de probabilité, 2573
de Schwartz, 2288, 2379
de Sobolev, 2391, 2397
euclidien, 824
mesurable, 1245
mesuré, 1250
complété, 1267
métrique, 556
base de topologie, 568
projectif, 1971
séparé, 536
topologique
métrisable, 614
vectoriel, 261
dimension, 646
vectoriel topologique
métrisable, 556
espace complètement normal, 541
espace connexe, 544
espace de Baire, 642
espace de Banach, 601
espace de Sobolev, 2396
espace propre, 673
espace tangent, 1813
espace topologique, 517
espace topologique normal, 541
espace vectoriel
topologique, 577
espace vectoriel normé, 575
espérance, 2585
conditionnelle, 2594, 2595
événement, 2595
variable aléatoire, 2599
estimateur, 2670
biais, 2671
consistant, 2670
de fonction de répartition, 2675
maximum de vraisemblance, 2673
estimateur convergeant, 2670
estimation
des grands écarts, 2647
étagée
fonction, 1289
état
apériodique, 2709
récurrent, 2703
récurrent positif, 2703
transitoire, 2703
Éther, 2771
étoile de Kleene, 2767
étranger
dans leur ensemble, 316
étrangers
polynômes, 316
Euclide
algorithme étendu, 276
lemme, 249
euclidien
anneau, 241
espace, 699
évaluation
polynôme plusieurs variables, 288
événement, 2573
Événement, 2776
exact
intervalle de confiance, 2678
excès
intervalle de confiance, 2678
exhaustive (suite de compacts), 619
exponentielle, 1432
convergence, 876
de matrice, 953, 1453, 1454, 1465
utilisation, 1569
existence, 1426
rapide, 1772
unicité, 1189
exposant, 431, 754
d'un groupe, 274
extension
corps de base, 734
de corps, 474, 513
algébrique, 485
finie, 1789
simple, 482
utilisation, 1806
isométrie, 1613
séparable, 508
extension algébrique, 477
extension algébriquement clos, 477
extrapolation, 2516
extrémité
d'un intervalle, 774
extrémum, 1895
lié, 1575
local
relatif, 1575
extrémum local, 1570
extrémums, 1573
volume d'un ellipsoïde, 1606

facteur
intégrant, 2450
facteur
intégrant, 2450
factoriel
anneau, 291
factorisation
de polynôme, 320, 488
faisceau de droites, 1990
famille
sommable, 857
famille trigonométrique
sur S^1, 2198
Fatou, 1315
Fejér
noyau, 2298
fermé, 518, 664

fermeture séquentielle, 559
filtration, 2727
filtration naturelle, 2727
fine
subdivision, 1913
fixateur, 364
flot, 2424, 2465
flux
d'un champ de vecteur, 1845
flux d'un champ de vecteurs, 1843
fonction, 117, 760
Γ d'Euler, 2115
à décroissance rapide, 2288
bijective, 117
borélienne, 1261
caractéristique, 1886
d'une variable aléatoire, 2610
composée de fonctions, 118
continue
égales, 559
convexe, 1577, 1583
croissante, 119
de Dirichlet, 2303
de Möbius, 1797
de répartition, 2609
définie par une intégrale, 1471, 1535, 1540, 2121, 2323
Γ d'Euler, 2115
utilisation, 2636
domaine de définition, 117
en escalier intégrable, 1885
ensemble de définition, 117
étagée, 2172
génératrice, 2611
holomorphe, 2121
théorème de Montel, 2292
image, 760
injective, 117
méromorphe
Γ d'Euler, 2115
monotone, 119
surjective, 117
valeurs vectorielles, 1208
fonction analytique, 1195
fonction continue en un point, 528
fonction dérivée, 924
fonction intégrable, 1318
fonction périodique, 1074
fonctionnelle
énergie, 2059
fonctionnelle de Minkowski, 627
fonctions équivalentes, 539
fondamental
domaine d'une action, 366
forme
bilinéaire, 687
non dégénérée, 688
différentielle, 1095
exacte, 1853
fermée, 1853
linéaire
différentielle, 1575
quadratique, 1602, 1604, 1895
groupe orthogonal, 1243
forme bilinéaire symétrique, 687
forme canonique
fonction simple, 1290
matrice de transition, 2718
forme linéaire, 416, 646
forme multilinéaire alternée, 646
forme quadratique, 687
formle multilinéaire antisymétrique, 645
formule
Bayes, 2591
Burnside, 367
d'expulsion (produit vectoriel), 822
de Cauchy, 2089
Hadamard, 1404
inversion Möbius, 1799
probabilité totales, 2591
sommatoire de Poisson, 2311
Taylor
utilisation, 2503
formule binomiale, 255
Formule de Leibniz, 2352
formule de Stirling, 1901
formule de Taylor
reste intégral, 1878
formule des classes, 365
Fourier, 2311
série
utilisation, 2341
transformée
groupe abélien fini, 1501
fraction
rationnelle
intégration, 1859
fraction dyadique, 342, 1964
fraction rationnelle, 1531
fractions
rationnelles, 310
fractions (corps), 308
Fredholm
équation, 1549
Frenet
formules, 1939
fréquence
empirique, 2692, 2702
Fresnel
intégrale, 2119
Frobenius
morphisme, 266
frontière, 560, 668
Fubini
théorème
dans $\mathbb{R}^n$, 1382

Galton-Watson
sous-critique, 2723
sur-critique, 2723
Galton-Watson
sous-critique, 2723

sur-critique, 2723
Gauss
lemme
polynômes, 470
somme de, 1782
générateur, 228
génératrice
partie d'un module, 263
géométrie
avec des groupes, 1697, 2010
avec nombres complexes, 1697, 2010
géométrique
avec des nombres complexes, 2341
Gershgorin
disque, 2547
gradient, 926, 1103, 1110, 1125
Gram (déterminant), 653
Gram-Schmidt, 824
graphe, 760, 1065
de transition (chaine de Markov), 2701
fonction, 1081
fonction de deux variables, 1083
Grönwall (lemme), 2407
groupe, 141
$\mathrm{GL}(n,\mathbb{R})$, 1604
p-groupe, 425
action, 2010
utilisation, 1243
agissant sur un ensemble
diédral, 1696
alterné, 440
circulaire, 2007
de Galois, 515
de permutation, 1761
de permutations, 1703
caractères de S_4, 1512
de torsion, 231
dérivé, 228
de $\mathrm{GL}(n,\mathbb{K})$, 1229
de $\mathrm{SL}(n,\mathbb{K})$, 1229
du groupe alterné, 442
du groupe symétrique, 441
des isométries
espace métrique, 599
des symétries, 1714
diédral, 1696, 1703
générateurs (preuve), 1697
générateurs (utilisation), 1761
en géométrie, 1696
et géométrie, 646, 1703, 2010
isométries du cube, 447
fini, 427, 434, 1703, 1770, 1778, 1781
alterné, 441
diédral, 1696
Wedderburn, 1778
linéaire, 1239
décomposition polaire, 1235
enveloppe convexe de $\Omega(n)$, 1238
hyperplan, 708
sous-groupes compacts, 1241
modulaire, 2009
orthogonal, 661
d'une forme quadratique, 1243
partie génératrice, 441, 1770, 2010
permutation, 646, 652, 1239, 1770
diédral, 1696
projectif, 1977
quotient, 359
simple, 201
sous-groupe, 141
spécial orthogonal, 662
symétrique, 179
action sur un triangle, 1502
groupe abélien, 141
groupe commutatif, 141
groupe cyclique, 228
groupe de pavage, 1717
groupe dérivé
de $\mathrm{GL}(n,\mathbb{C})$, 1223
groupe ordonné, 180
groupe résoluble, 362
groupe simple, 201
groupe topologique, 1219

Hadamard
conditions, 2475
formule, 1404
Hadamard
conditions, 2475
formule, 1404
Hardy-Littlewood (théorème), 1519
Hausdorff, 536
Heine (théorème), 1018
hermitienne, 701
hessienne, 1151
Hilbert
espace, 2035
holomorphe, 1135
sur un compact, 1135
homéomorphisme, 529
homogène
chaine de Markov, 2697
homographie, 1976, 2010
sur $\mathbb{C}\cup\{\infty\}$, 1997
homothétie, 1055
homotopie, 1846
homotopie à extrémité fixées, 1847
hyperbolique
équation aux dérivées partielles, 2474
hyperplan, 750
de $\mathbb{M}(n,\mathbb{K})$, 708
sépare
au sens strict, 2229
séparer
au sens large, 2228
hyperplan vectoriel, 750
hypothèse
alternative, 2688
composite, 2688
multiple, 2688
nulle, 2688
simple, 2688

idéal
bilatère, 233
dans un anneau, 233
principal
à droite, 242
à gauche, 242
idéal
bilatère, 233
dans un anneau, 233
principal
à droite, 242
à gauche, 242
idéal à droite, 233
idéal engendré, 234
idéal maximal, 258
idéaux premiers dans leur ensemble, 233
idéaux premiers entre eux, 233
identifiable, 2669
identité de polarisation, 692
image, 760
par une fonction, cas général, 117
incompressible
champ de vecteur, 1215
indécomposable
module, 264
indépendance, 2574
affine, 976
algébrique, 515
évènements, 2574
événements
utilisation, 2658, 2737
familles d'ensembles mesurables, 2574
projective, 1978
variables aléatoires, 2576
indicatrice d'Euler, 436
indice, 200
d'une courbe dans $\mathbb{C}$, 2083
de rotation, 1947
indice d'inertie, 698
inductif, 121
induite
topologie, 665
tribu, 1247
inégalité
arithmético-géométrique, 1591
Bessel, 2043
Cauchy-Schwarz, 801, 2035
de Khintchine, 2644
de la moyenne, 1139
des pentes, 1577
Hölder, 2149
utilisation, 2589, 2660
isopérimétrique, 2341
Jensen, 1591
espérance conditionnelle, 2609
pour une somme, 1591
version intégrale, 2148
Kantorovitch, 1591
Markov, 2623
Minkowski, 2152
triangulaire, 556, 575
inférence statistique, 2663
infimum, 347
injection, 117
intégrable
fonction à valeurs vectorielles, 1321
fonction non en escalier, 1891
fonction positive, 1894
intégrale
calcul, 2301
convergente, 1374, 1859
d'une fonction sur une carte, 1818
d'une fonction sur une variété, 2187
d'une forme différentielle, 1833
fonction en escalier, 1885
Fresnel, 2119
impropre, 1373, 1374
sur un chemin, 1831
intégrale d'une fonction, 1310
intégrale d'une forme différentielle, 1832
intégrale de Dirichlet, 1911
intégrale existe, 1318
intégrale sur une carte, 1814
intégration
fraction rationnelle, 1859
intéressante, 109
intérieur, 520
d'un ensemble, 663
point, 663
interpolation, 2516
intervalle, 779
d'un ensemble ordonné, 120
longueur, 1297
Intervalle, 2776
intervalle de confiance
asymptotique, 2682
invariance cyclique
trace, 391
invariant
de similitude, 742
invariante
mesure
pour une chaine de Markov, 2719
inverse
dans un groupe, 179
inverse généralisé, 2650
inversion, 1966
dans le groupe symétrique, 218
inversion dans $\mathbb{C} \cup \{\infty\}$, 1995
involution, 715
irrationalité
$\sqrt{2}$, 330
irréductible
chaine de Markov, 2700
dans un anneau, 237
module, 264
représentation, 1503
isobarycentre, 971
isométrie
de forme quadratique, 695
de l'espace euclidien $\mathbb{R}^2$, 1697
espace euclidien

isométries du cube, 447
groupe, 599
isométrie (forme bilinéaire), 695
isométrie d'espaces métriques, 599
isométrie positive, 1667
isomorphisme, 891
$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, 1781
d'anneaux, 233
de corps, 180
espace affine, 969
espace vectoriel normé, 935
espaces vectoriels, 382
isomorphisme d'ensembles ordonnés, 119
isomorphisme d'espace topologique, 529
isotrope
cône, 693
sous-espace, 693
totalement, 693
vecteur, 693

jacobien, 1125, 1212
jacobien, 1125, 1212
jauge, 2222
Jordan
réduction, 744
Jordan-Hölder, 359

Kronecker
symbole, 376
Kronecker
symbole, 376

l, 174
l, 174
lacet, 1846
lacet de Jordan, 1846
Lagrange
multiplicateur, 1575
polynôme, 706
théorème, 201
lagrangien, 1575
langage, 2766
itéré, 2767
itéré strict, 2767
unité, 2766
vide, 2766
Laplace
transformée, 2611
laplacien, 2029
Legendre
symbole, 1781
Leibnitz, 1067
Leibniz
applications entre espaces vectoriels normés, 949
lemme
Borel, 1473
d'Euclide, 249
de Borel-Cantelli, 2621
de Gauss
contenu de polynôme, 1788
pour des entiers, 248
de Morse, 1895
de Schreider, 361
de Slutsky, 2620
de transport, 1259
de Zorn, 121
des noyaux, 675
Fatou, 1315
Gauss
dans un anneau principal, 293
polynômes, 470
Grönwall, 2407
Hadamard, 1545
Schur complexe, 1027
Schur réel, 716
lemme de regroupement, 2578
lettres, 2765
Levi-Civita, 2024
libre
action, 370
partie, 371
partie d'un module, 263
librement engendré, 379
Ligne d'univers, 2772
limite, 729
d'ensembles, 1253
d'une fonction, 554
de fonctions holomorphes, 2121
de suite
espace topologique, 520
inférieure, 772
inversion, 1474, 1519, 2121, 2144
permutation
utilisation, 2611
suite dans $\mathbb{R}^m$, 598
suite numérique, 766
supérieure, 771, 772
unicité, 555
limite à droite, 796, 1002
limite à gauche, 796
limite de suite, 520
limite épointée, 991
limite inductive, 2353
limite inférieure, 771
limite pointée, 990
linéaire
application, 380
linéairement indépendant
module, 261
lipschitzienne, 1139, 1547
localement, 1140
liste d'indices, 42
localement
intégrable, 1373
localement fini, 542
log-concave, 1583
logarithme
complexe, 2075
dans $\mathbb{C}$, 2072
de matrice, 1465
sur les réels positifs, 1428
logarithme d'une application, 2081

loi
χ^2, 2645
binomiale
comportement asymptotique, 2647
conjointe, 2579
de Poisson, 2633
des grands nombres
forte, 2623
pour les chaines de Markov, 2721
processus de Poisson, 2758
utilisation, 2647, 2658
marginale, 2579
normale
vecteur gaussien, 2640
parente, 2663, 2664
parente d'un échantillon, 2666
réciprocité quadratique, 1784
sans mémoire, 2635
Student, 2645
loi binomiale, 2631
loi d'une variable aléatoire, 2574
loi exponentielle, 2633
loi stationnaire, 2700
longueur
arc géométrique, 1928
d'un arc paramétré compact, 1914
d'un intervalle, 1297
d'une arrête, 1883
élément de, 1923
longueur d'arc, 1915
Lotka-Volterra, 2440

M-matrice, 2552
M-matrice, 2552
magma, 129
commutatif, 130
élément neutre, 130
à droite, 129
à gauche, 129
élément régulier, 130
unifère, 130
maigre, 1263
majorant, 120, 347
essentiel, 2145
manipulation de lignes, 401
Markov
inégalité, 2623, 2668
martingale, 2727
bornée dans $L^2(\Omega)$, 2728
matrice, 389, 1239, 2010
compagnon, 740
creuse, 2525
cyclique, 680
d'une application linéaire, 392
de dilatation, 405
de permutation, 405
de similitude, 1135
de Sylvester, 653
de transvection, 405
dense, 2525
équivalence, 408
dans le groupe linéaire, 1243
hermitienne
racine carrée, 1233
jacobienne, 1110, 1125
normale, 1027
orthogonale, 404, 661
permutation
élémentaire, 2531
racine carrée, 1233
réductible, 2546
semblable, 1233
semblables, 1604
symétrique, 1604
réelle, 1602
trigonalisable, 1026
matrice bloc-diagonale, 833
matrice d'une forme bilinéaire, 694
matrice de transition, 2697
matrice diagonale, 712
matrice positive, 793
matrice primitive, 793
matrice stochastique, 2699
matrice-colonne, 389
matrice-ligne, 389
matrices
similitude, 408
matrices équivalentes, 708
matrices semblables, 708
maximale
partie orthonormale, 2044
maximum, 120, 189
global, 1570
local, 1570
maximum local, 1570
médiatrice, 1050
méromorphe, 2107
mesurable
application, 1252
au sens de m^*, 1258
ensemble, 1251
fonction, 1259
Lebesgue, 1882
mesure
σ-finie, 1250
angle entre vecteurs, 1689
complexe, 1346
dans une carte, 1817
de Borel, 1281
de comptage, 1358, 1382
de Lebesgue, 1300
de Radon, 1281, 2102
extérieure, 1247
externe, 1882
finie, 1250
image, 1275
positive, 1250
probabilité, 2573
produit, 1350
régulière, 1281
extérieure, 1281
intérieure, 1281

sur un ensemble de parties, 1247
mesure σ-finie, 1248
mesure à densité, 1328
mesure absolument continue, 1328, 1332
mesure finie, 1248
mesure signée, 1250
mesures mutuellement singulières, 1332
méthode
des chemins, 1092
Newton, 2503
cas convexe, 2500
Méthode
de Newton, 2498
métrisable
espace vectoriel topologique, 556
minimum, 189
ensemble ordonné, 120
minimum local, 1570
minorant, 120, 347
modèle
échantillonnage, 2664, 2666
paramétrique, 2664
modèle statistique, 2663
modulaire (groupe), 2009
module
à gauche, 260
de continuité, 956
indécomposable, 264
irréductible, 264
simple, 264
module d'un nombre complexe, 789
module produit, 261
moment, 2587
fonction génératrice, 2611
monogène, 228
extension de corps, 482
monoïde, 458
monôme, 314
monotone par morceaux, 1293
monotonie, 2445
morphisme
d'algèbres, 264
d'anneaux, 144
de corps, 180
espace vectoriel normé, 935
Frobenius, 266
morphisme de groupes, 141
morphisme de modules, 260
morphisme de produits tensoriels, 891
mot, 2765
longueur d'un mot, 2765
mot vide, 2765
nombre d'occurrences, 2765
mot non vide, 2765
moyenne
de Cesàro, 878
empirique, 2589
empirique d'un échantillon, 2666
quadratique, 2589
multiindice, 42, 286
multiplicateur
de Lagrange, 1575
multiplication, 163
multiplicité
racine d'un polynôme, 319
racine de $f(x) = 0$, 2497
valeur propre
algébrique, 1026
géométrique, 1026

nabla, 1123
nabla, 1123
négatif, 338
négligeable
partie d'un espace mesuré, 1265
neutre
dans un groupe, 179
Newton
méthode, 2503
nilpotent, 237
niveau de confiance, 2678
nombre
complexe
norme 1, 1778
de Fermat, 1806
dénormalisé, 2484
normal, 2658
normalisé, 2484
premier, 434, 458, 1444, 1770, 1777, 1781
dans leur ensemble, 247
théorème des deux carrés, 459
tours d'une courbe plane, 1945
nombre de montées, 2730
nombre entier
divisible, 169
impair, 169
pair, 169
nombre premier
décomposition, 249
polynôme cyclotomique, 1774
nombres complexes, 356
non dénombrable, 190
normal
arc paramétré, 1929
endomorphisme, 1027
nombre, 2658
sous-groupe, 181
normal extérieur
vecteur, 1845
normale
loi réduite, 2639
principale, 1938
normalisateur, 181
norme, 574
d'algèbre, 834
d'application linéaire, 831
d'une application linéaire, 832
euclidienne
dans $\mathbb{R}^m$, 813
supremum, 826
sur $\mathbb{Z}[i\sqrt{5}]$, 298
normé

espace vectoriel, 576
norme maximum, 769
norme quotient, 639
norme supremum, 851
normes équivalentes, 827
noyau
application vers un groupe, 184
d'une forme bilinéaire, 693
Dirichlet, 2297
Fejér, 2298
vers un espace vectoriel, 382
noyau d'une forme bilinéaire, 688
nulle part dense, 624

o-connexe, 544
o-connexe, 544
observation, 2573
opérateur
défini positif, 717
opérateur autoadjoint, 701
opérateur hermitien, 701
opérateur unitaire, 701
opérateurs
compatibles, 2055
opération sur un ensemble, 129
opposés
chemins, 1921
orbite
d'un point sous une action, 364
orbite d'un élément sous une permutation, 210
ordre, 119
bon ordre, 121
d'un élément, 200
d'un polynôme, 318
d'une matrice carrée, 389
dans un anneau, 146
de convergence d'un schéma, 2566
distribution, 2365
partiel, 119
sur un anneau factoriel, 292
total, 119
ordre d'un groupe, 189
orientation, 658, 1819, 1839
origine
abscisse curviligne, 1929
repère affine, 977
orthogonal, 699, 2039
coordonnées curviligne, 2023
famille de projecteurs, 263
matrice, 661
opérateur, 661
sous-espace, 419
orthogonal pour une forme bilinéaire, 688
orthonormé, 813
système, 2042
oscillation
d'une fonction, 1013
d'une fonction en un point, 1013
osculateur (cercle), 1942
ouvert, 517, 664

parabolique
équation aux dérivées partielles, 2474
parabolique
équation aux dérivées partielles, 2474
paracompact, 543
parallèle
sous-espaces affines, 969
parallélogramme, 1822
paramétrage, 1921
normale, 1929
paramétrages
admissible, 1928
Parseval, 2048
partie
génératrice, 228, 371
régulière, 1201
totale, 2041
partie absolument convexe, 581
partie absorbante, 581
partie connexe, 544
partie convexe, 574
partie discrète, 523
partie entière, 354
partie équilibrée, 581
partie fractionnaire, 354
partie inductive, 764
partie libre
module, 261
partie linéaire, 966
partie maigre, 624
partie négative, 1333
partie nulle, 1333
partie positive, 1333
partie symétrique, 581
partition
dénombrable mesurable, 1286
partition d'ensembles, 116
partition de l'unité, 2183
passage aux classes, 535
pavable, 1883
pavage du plan, 1717
pavé, 1882
Pearson
théorème, 2692
peigne de Dirac, 2385
période, 1074
permutation, 179
matrice, 405
permutation impaire, 218
permutation paire, 218
permuter
dérivée et intégrale
$\mathbb{R}^n$, 1540
dans $\mathbb{R}$, 1537
dans $\mathbb{R}$ avec les bornes, 1542
dérivée et limite, 1163
différentielle et intégrale
$\mathbb{R}^n$, 1541
intégrale
et série, 1382
limite et intégrale

convergence dominée, 1324
convergence monotone, 1314
espace mesuré, 1535, 1536
série entière et dérivation, 1410
série entière et intégration, 1413
somme et intégrale, 1315, 1387
permuter limite et intégrale, 1535
petit théorème de Fermat, 454
pgcd
calcul effectif, 277
dans un anneau intègre, 145
polynômes, 472
pivotale, 2681
plan
projectif, 1971
tangent, 1125, 1208
plan affine, 1042
plan médiateur, 1059
plan vectoriel, 1042
Plancherel, 2048
plongement, 1612
Poincaré (demi-plan), 2009
point
d'équilibre
stable, 2436
pondéré, 970
point accessible de ∂A, 2267
point adhérent, 521
point critique
définition, 1896
point d'accumulation, 527
point d'équilibre, 2436
point extrémal dans un convexe, 1237
point fixe, 2723
attractif, 1546
Brouwer, 1825
Picard, 1547
Schauder, 1827
point intérieur, 520
point isolé, 527
Poisson
formule sommatoire, 2311
processus, 2746
polaire
nombre complexes, 1651
pôle, 1734, 2105
polydisque, 2122
polygone, 1695
polygone convexe, 1695
polynôme
à plusieurs indéterminées, 656, 1787
alterné, 511
annulateur, 675, 679
caractéristique, 683, 1032
contenu, 316
cyclotomique, 1772
irréductibilité, 1774
propriétés, 1773
d'endomorphisme, 1233
décomposition de Dunford, 732
de Bernstein, 2660
irréductible
sur $\mathbb{F}_q$, 1799
minimal, 478
d'un élément d'une extension, 475
ponctuel, 679
racines, 513
semi-symétrique, 511
symétrique, 511, 513, 652, 656, 1787
élémentaire, 514
trigonométrique, 2188
polynôme de Lagrange, 706
polynôme de plusieurs variables, 288
polynôme de Taylor, 1195
polynôme dérivé, 504
polynôme irréductible, 237
polynôme primitif, 316
polynôme scindé, 467
polynôme séparable, 507
polynôme sur espace de Banach, 1490
polynôme sur un espace de Banach, 1413
polynôme symétrique élémentaire, 511
polynôme trigonométrique, 2198
polynômes, 304
portée
mesure, 1333
positif, 338
positivement liés, 791
positivité, 144
potentiel, 1837, 1866
ppcm
dans un anneau intègre, 145
prébase, 519
précision
simple, 2483, 2484
précompact, 557
préhilbertien, 2035
premier
corps, 453
deux éléments d'un anneau principal, 247
deux polynômes entre eux, 316
idéal, 258
premier type
région solide, 1892
préserve l'orientation, 659, 1667
presque
nulle, 231
partout, 1252
surjective, 2235
primitif
élément d'un corps, 1781
élément d'une extension de corps, 482
racine, 1792
triplet pythagoricien, 301
primitive, 1062, 1864
de fonction continue, 1187
et intégrale, 1375
fonction, 1080
primitive et intégrale, 1371
principal
anneau, 242
idéal, 242

principe
prolongement analytique, 1618
zéros isolés, 1618
Principe de correspondance, 2785
probabilité
conditionnelle, 2591
problème
aux limites d'évolution, 2474
aux limites stationnaires, 2474
bien posé, 2474
limite de Dirichlet, 2474
limite de Von Neumann, 2474
problème de Cauchy, 2454
processus
adapté à une filtration, 2727
arrêté, 2735
croissant prévisible, 2736
Galton-Watson, 2722
Poisson, 2746
sans mémoire, 2635
processus arrêté, 2736
processus de comptage, 2745
processus de Poisson, 2745
produit, 163
d'une mesure par une fonction, 1327
de convolution, 2178
et Fourier, 2309
de langages, 2766
de mots, 2765
distribution et fonction, 2364
espaces mesurés, 1352
mixte, 820, 822
scalaire
en général, 699
sur $\mathbb{M}(n,\mathbb{R})$, 1039
semi-direct, 229
tensoriel
de représentations, 1511
vectoriel, 819
produit de Cauchy, 1397, 1398, 1400
produit extérieur, 907
produit hermitien, 701
produit intérieur, 917
produit pseudo-scalaire, 699
produit remarquable, 2097
produit scalaire sur $\mathbb{R}^n$, 700
produit tensoriel, 891, 893
projecteur
dans un module, 263
projecteur parallèlement, 422
projectif
complétion, 1974
droite, 1971, 1972
espace, 1971
groupe, 1977
hyperplan, 1972
plan, 1971
repère, 1978
sous-espace, 1971
projection
orthogonale, 2038
projection normale, 2218
projection orthogonale, 1672
prolongement
analytique, 1618
utilisation, 2292
de fonctions, 1612
lemme de Borel, 1473
méromorphe de la fonction Γ, 2115
par continuité, 1004, 1005
dans $H^1(I)$, 2394
par densité, 1612
théorème de Hahn, 1273
prolongement de fonctionnelle linéaire, 2233
propriété d'intersection finie, 553
propriété d'intersection non vide, 549
propriété des valeurs intermédiaires, 777
propriété universelle, 891
pseudo-dimension, 2265
puissance
d'un langage, 2766
d'un mot, 2766
d'un point, 1965
d'un test, 2689
d'une inversion, 1995
pull back, 920

quasi-compact, 548
quasi-compact, 548
quaternion, 510
queue de liste d'indices, 42
quotient, 243, 316
dans une suite de composition, 359
de groupe, 359
de groupes, 433
quotient d'un chemin, 2255
quotient d'un espace vectoriel, 887

racine
carré
de matrice hermitienne, 1233
carré de matrice
hermitienne positive, 1233
d'un polynôme, 318
de l'unité, 754, 1697, 1774, 1777, 2010
primitive, 1768
utilisation, 1773
de polynôme, 488
multiple, 2497
primitive, 1792
simple, 2497
racine
carré
de matrice hermitienne, 1233
carré de matrice
hermitienne positive, 1233
d'un polynôme, 318
de l'unité, 754, 1697, 1774, 1777, 2010
primitive, 1768
utilisation, 1773
de polynôme, 488
multiple, 2497

primitive, 1792
simple, 2497
racine carrée, 788
racine de l'unité, 1765
racine multiple, 319
racine simple, 319
raffinement, 1913
subdivision d'un pavé, 1884
rang, 384, 646, 726
classe d'équivalence, 408
diagonalisation, 716
différentielle, 1575
utilisation, 2040
rang d'une forme quadratique, 698
rang d'une matrice, 406
rare, 1263
rationnels, 323
rayon
de courbure, 1938
de torsion, 1939
spectral, 834, 1181
rayon de convergence, 1394, 1413
réciproque
dérivabilité, 1077
recouvrement, 548
rectangle
produit de tribus, 1294
rectifiable, 1914
arc géométrique, 1928
récurrent
état, 2703
nul, 2703
point d'un système dynamique, 1283
positif, 2703
réduction
d'endomorphisme, 732
Jordan, 744
réduction de Frobenius, 742
réel, 334
réflexif, 2241
réflexion, 1706
dans $\mathbb{R}^2$, 1674
glissée, 1704
par rapport à un hyperplan, 1662
réflexion par rapport à un point, 1706
région
critique, 2689
de confiance exacte, 2680
de rejet, 2689
règle du produit nul, 238
régularité
d'une mesure, 1281
extérieure de la mesure de Lebesgue, 1303
intérieure de la mesure de Lebesgue, 1305
régulier
arc, 1926
point d'un arc, 1926
régulière
surface, 1837
rejet
région dans une prise de décision, 2688
relation
d'ordre, 119
relation anormale, 2512
relation binaire, 117
relation d'équivalence, 127
relation ternaire, 117
relation unaire, 117
relations
coefficient-racines, 514
de Chasles, 961, 1525
relativement compact, 553
relèvement, 1947
repère
affine, 977
cartésien
espace affine, 962
de Frenet, 1938
projectif, 1978
représentation, 419
de groupe fini
caractères de S_4, 1512
fidèle, 420
groupe diédral, 1761
irréductible, 1503, 1504
produit tensoriel, 1511
régulière gauche, 1508
virgule fixe, 2483
Représentation
virgule flottante normalisée, 2483
répulsif
point fixe, 1546
résidu
méthode itérative, 2544
résolvante, 2419
reste, 243, 316
d'un développement limité, 1201
restriction d'une distribution, 2371
résultant, 654
utilisation, 656, 1859
Riemann
fonction, 1441
risque
première espèce, 2689
quadratique, 2671
seconde espèce, 2689
rotation
en dimension 2, 1677
rotation d'angle θ, 1681
rotation-homothétie, 1995
rupture
corps, 489

schéma
consistant, 2565
schéma
consistant, 2565
schéma discret convergent, 2566
schéma numérique, 2565
Schrödinger, 2450
Schur (théorème), 1506
section

de graphe, 1082
propriété des, 1347
segment
dans $\mathbb{R}^p$, 774
dans un espace affine, 971
semi-défini positif, 717
semi-simple
endomorphisme, 681
semi-symétrique
polynôme, 511
seminorme, 625
seminorme quotient, 639
seminormes séparantes, 637
séparable, 2041
élément d'une extension, 508
espace topologique, 536
extension de corps, 508
polynôme non constant, 507
séparation stricte, 2229
sépare
les points, 1183
séquentiellement fermé, 558, 559
série
dans un espace vectoriel normé, 850
de Fourier, 2304, 2311
utilisation, 2341
de puissance, 1394
donnant $(1-A)^{-1}$, 951
entière, 1394, 1474, 2311
Abel angulaire, 1855
processus de Markov, 2723
utilisation, 2611
fonctions, 1519, 2311
génératrice d'une suite, 1456
géométrique, 875
nombres, 1519
numérique, 1444, 1474
Riemann, 1447
Taylor, 1457
série convergente, 850
série de Laurent, 2337
série de puissance, 1413
série de Taylor, 1195
série divergente, 850
série entière
fonctions holomorphes, 2089
série harmonique, 875
sesquilinéaire, 701
signature
forme quadratique, 698
signature d'une permutation, 217
similitude, 1135
simple
extension de corps, 482
fonction, 1289
module, 264
singularité, 2105
singularité effaçable, 2105
singularité isolée, 2105
sinus, 1621
hyperbolique, 1449
sinus cardinal, 1638, 1903
solfège, 1767
solution
générale, 2453
particulière, 2453
somme
inférieure, 1888
partielle, 850
supérieure, 1888
somme directe, 420
somme directe (de représentations), 1503
somme directe topologique, 579
somme partielles
Abel angulaire, 1855
sommet, 1960
Sophie Germain, 455
sous arc, 1913
sous-additivité
sur algèbre de parties, 1248
sous-anneau, 256
sous-corps premier, 453
sous-espace
affine engendré par une partie, 969
caractéristique, 729
sous-espace topologique, 524
sous-groupe
caractéristique, 181
distingué, 434
dans le groupe alterné, 441
engendré, 226
normal, 359, 433
sous-groupe distingué, 181
sous-groupe normal maximal, 201
sous-martingale, 2727
sous-module, 263
sous-module engendré, 261
spectre
matrice hermitienne, 817
matrice symétrique réelle, 716
spectre d'un endomorphisme, 674
sphère, 563
de Riemann, 1992
stabilisateur, 364
stabilité
d'un point d'équilibre, 2436
Lyapunov, 2437
stable, 2490
schéma numérique, 2568
stathme
sur $\mathbb{Z}[i]$, 457
stathme euclidien, 241
stationnaire
chaine de Markov, 2720
statistique, 2670
statistiques
descriptives, 2663
strictement
convexe
sur $\mathbb{R}^n$, 1585
strictement convexe, 1577
strictement croissante, 119

structure
complexe, 1944
structure d'anneau canonique, 233
structure réelle, 422
Student, 2645, 2682
subdivision, 1883
associée à une fonction, 1884
d'un intervalle, 1913
subordonnée
norme, 831
subpotent, 130
suite, 231
arithmético-géométrique, 876
de Cauchy, 600
dans un corps, 313
de fonctions, 2144
théorème de Montel, 2292
de fonctions intégrables, 1535, 2121
de Jordan-Hölder, 359
définie par itération, 2503
équirépartie, 2301
critère de Weyl, 2301
exacte, 229
régularisante, 2313
suite de composition, 359
suite de variables aléatoires de Bernoulli, 2722
suites adjacentes, 770
supplémentaire, 377
support, 1885
d'une permutation, 210
distribution, 2365
famille d'éléments, 231
supremum, 347
d'une suite d'ensembles, 1245
supremum essentiel, 2145
sur-martingale, 2727
surface paramétrée, 1837
surjection, 117
surpotent, 130
Sylow
p-Sylow, 425
Sylvester (matrice), 653
symbole
de Legendre, 1781
symbole principal, 2465
symétrique
polynôme, 511
système
fondamental, 2416
orthonormé, 2042
trigonométrique, 2042, 2187
système trigonométrique, 2325

tangent
vecteur unitaire, 1938
tangent
vecteur unitaire, 1938
tangente, 1640, 1933
Tangente hyperbolique, 2779
tangente hyperbolique, 1451
taubérien, 1517
taux d'accroissement, 1577
Taylor
série entière, 1457
temps d'arrêt, 2729
temps de première atteinte, 2703
temps de retour, 2703
tenseur, 897
tenseur alterné, 904
tenseur symétrique, 904
terminée
martingale, 2734
test, 2688
bilatéral, 2689
unilatéral, 2689
tétraèdre régulier, 1060
théorème
accroissements finis, 947
dans $\mathbb{R}$, 1077
forme générale, 1139
Ascoli, 2135
Banach-Steinhaus, 883
avec seminormes, 2136
base incomplète, 375
Beppo-Levi, 1314
Bézout
polynômes, 470
utilisation, 654
Bolzano-Weierstrass, 569
Borel-Cantelli, 2573
Borel-Lebesgue, 765
Brouwer
dimension 2, 2093
Carathéodory, 974
Cauchy
groupe, 282
Cauchy-Arzela, 1828
Cauchy-Lipschitz, 1549
Cayley-Hamilton, 686, 1232
central limite, 2625
processus de Poisson, 2760
Chevalley-Warning, 1787
chinois, 462
anneau principal, 294
Cochran, 2668
Cochrane, 2668
convergence
dominée de Lebesgue, 1324
monotone, 1314
de Jordan, 2275
de représentation de Riesz, 2040
décomposition des noyaux
et exponentielle de matrice, 1467
des deux carrés, 459
version faible, 458
Dini, 1157
Dirichlet, 2298
forme faible, 1777
Doob, 2735
du rang, 385
élément primitif, 1789
élément primitif, 509, 1790

extension d'isométrie, 1613
Fejér, 2299
fonction implicite dans $\mathbb{R}^n$, 1564
fonction implicite dans Banach, 1563
Fubini
dans $\mathbb{R}^n$, 1382
espace mesuré, 1378
version compacte dans $\mathbb{R}^2$, 1868
Fubini-Tonelli, 1376
fuite des compacts, 2421
Gauss
polynômes, 470
Gauss-Wantzel, 1806
Glivenko-Cantelli, 2675
Hahn-Banach, 2226
Hardy-Littlewood, 1519
Heine, 1018
incidence, 1972
inversion locale, 1561
utilisation, 1575, 1895
isomorphisme
second, 184
troisième, 186
isomorphisme de Banach, 2133
Kronecker, 656
Lagrange, 201
Lie-Kolchin, 1030
Lotka-Volterra, 2441
Markov-Takutani, 1829
Montel, 2292
Pappus
affine, 1975
projectif, 1976
Pearson, 2692
petit de Fermat, 454
Picard, 1547
point fixe
Brouwer, 2093
projection
cas vectoriel, 2038
partie fermée convexe, 2036
prolongement de Hahn, 1273
prolongement de Riemann, 2106
Radon-Nikodym, 1339
complexe, 1346
Rolle, 1074
Rothstein-Trager, 1859
Runge, 2096
Schauder, 1827
Schur, 1506
spectral, 731
autoadjoint, 812
matrice symétrique, 716
matrices normales, 1028
stabilité de Lyapunov, 2437
Stone-Weierstrass, 1183, 1186
Sylvester, 726
taubérien, 1517
taubérien faible, 1857
transfert, 2613
Tykhonov
dénombrable, 623
fini, 622
valeurs intermédiaires, 788
Von Neumann, 1569
Wedderburn, 1778
Weierstrass, 570
théorème de Baire, 625, 643
théorème de Brouwer, 1826
théorème de Cartan-Dieudonné, 1664
théorème de correspondance, 182
théorème de Tykhonov, 621
théorème des extrémums liés, 1575
théorème fondamental du calcul intégral, 1371
topologie, 517, 665
$*$-faible, 640, 2363
p-adique, 958
discrète, 519
engendrée par une famille, 519
forte, 834
grossière, 519
métrique, 556
sur $\mathscr{D}(\Omega)$, 2354
sur $\mathscr{D}(K)$, 2354
sur $C^\infty(\Omega)$, 2353
sur dual topologique, 640
usuelle sur $\mathbb{R}^n$, 666
topologie d'une norme, 804
topologie de la convergence simple, 534
topologie des seminormes, 632
topologie faible, 2276
topologie finale, 534
topologie induite, 523
topologie initiale, 530
topologie produit, 533
topologie quotient, 535
tore, 354
torsion, 1939
d'un groupe, 231
totale, 2041
trace, 2400
dual de $\mathbb{M}(n,\mathbb{K})$, 707
matrice, 710
produit scalaire sur $\mathbb{M}(n,\mathbb{R})$, 1039
unicité pour la propriété de trace, 707
trace d'endomorphisme, 710
transcendant, 476
transformation
Fourier, 2311
gaussienne, 2526
transformée
de Cauchy, 2102
de Fourier, 2307, 2610
continuité, 2309
groupe abélien fini, 1501
Fourier
distribution tempérée, 2382
Laplace, 2611
transient
état, 2703
transition
probabilité, 2697

transitoire
état, 2703
transposé, 660
transposée, 704
transposition, 216
transvection, 1223
transvection (matrice), 405
transversale, 366
tribu, 1245
borélienne, 1260
de Baire, 1263
de Lebesgue, 1300
induite, 1247
produit, 1293
tribu de Lebesgue sur S^1, 1655
tribu engendrée, 1246
tribu engendrée par une application, 1246
trigonalisation
et polynôme caractéristique, 1026
simultanée, 1029, 1030
triplet
pythagoricien, 301
triplet naturel, 149
type
fini
en algèbre, 510
espace vectoriel, 374

unicité
des mesures, 1255
unicité
des mesures, 1255
uniformément continue, 624
uniformément convexe, 2218
uniformément intégrable, 2175
unipotent, 237
unitaire
normale principale, 1938

valeur
principale (distribution), 2380
propre, 673
valeur
principale (distribution), 2380
propre, 673
valeur absolue, 147
p-adique, 958
valeur principale, 2073
valeur propre
d'une forme quadratique, 728
forme quadratique, 727
valeur singulière, 733
valuation
p-adique, 958
valuation d'un polynôme, 304
Vandermonde (déterminant), 413
variable
de décision, 2689
variable aléatoire, 2574
absolument continue, 2574
Bernoulli
marche aléatoire, 2710
utilisation, 2660
binomiale
utilisation, 2737
centrée, 2588
de Bernoulli
utilisation, 2737
de Rademacher, 2644
variable aléatoire de Bernoulli, 2630
variance, 2589
empirique, 2590, 2667
empirique corrigée, 2667
vecteur gaussien, 2640
variation bornée, 1384
variation des constantes, 2410, 2417
variation totale, 1384
variété, 1575, 1811
variété
orientée, 1820
variété orientable, 1820
vecteur
cyclique, 680
gaussien, 2640
propre, 673
unitaire normal, 1938
unitaire tangent, 1934
vecteur propre à gauche, 793
vers l'intérieur de D, 2267
Vitali (ensemble), 1306
vitesse d'un chemin, 1913
vitesse de convergence de suites, 1443
voisinage, 518, 665
volume
d'une région solide, 1893
région bornée dans $\mathbb{R}^3$, 1891
volume dans $\mathbb{R}^3$, 1821
vraisemblance, 2673

Weiner
constante, 2805
Weiner
constante, 2805
wronskien, 2443

Liste des notations

Algèbre

$[\mathbb{L} : \mathbb{K}]$ degré d'une extension de corps, page 474

(S) idéal engendré par S, page 234

$\mathcal{L}(E, F)$ Ensemble des applications linéaires de E dans F, page 380

$\mathbb{F}_p$ lorsque p est premier, page 453

$\mathbb{F}_{p^n}$ corps fini à p^n éléments, page 1779

$\mathbb{K}(A)$ corps contenant $\mathbb{K}$ et A, page 482

$\mathbb{K}[A]$ anneau contenant $\mathbb{K}$ et A, page 482

$\mathrm{Fun}(X, Y)$ les applications de X vers Y, page 233

$\mathrm{S}(E)$ Les opérateurs autoadjoints de E, page 702

∇f gradient de la fonction f, page 1110

$\mathtt{proj}_V$ projection de $V \times W$ sur V, page 595

$\mathrm{res}(P, Q)$ résultant des polynômes P et Q, page 654

$\mathrm{Span}(A)$ l'ensemble des combinaisons linéaires finies d'éléments de A, page 371

$\sqrt{A}$ racine d'une matrice hermitienne positive, page 1233

$\theta_\alpha(P)$ la multiplicité de α par rapport à P, page 319

$A[X]$ tous les polynômes de degré fini à coefficients dans A, page 306

$A_n[X]$ les polynômes à coefficients dans A et de degré inférieur ou égal à n, page 314

$C(P)$ matrice compagnon, page 740

$D \mid P$ D divise P, page 316

$df_a(u)$ Application de la différentielle de f sur le vecteur u, page 1098

$E_\lambda(T)$ Espace propre de T, page 674

$f^{(n)}$ La n-ième dérivée de la fonction f, page 1197

$mat_{\mathcal{B}}(q)$ matrice de q dans la base $\mathcal{B}$, page 1605

$o(x)$ fonction tendant rapidement vers zéro, page 1199

$U(A)$ ensemble des inversibles, page 237

U_n Le groupe des racines n^{e} de l'unité, page 1765

Ensembles de matrices

$S^+(n, \mathbb{R})$ matrices symétriques définies positives, page 718

$S^{++}(n, \mathbb{R})$ matrices symétriques strictement définies positives, page 718

$\mathrm{Aut}(E)$ automorphisme de l'espace vectoriel E, page 382

$\mathcal{L}^0(E,F)$ applications linéaires bornées (continues), page 935

$\mathrm{End}(E)$ les endomorphismes de E, page 382

$\mathrm{O}(n,\mathbb{R})$ le groupe des matrices orthogonales, page 661

$\Omega(E)$ formes quadratiques non dégénérées, page 1601

$Q(E)$ formes quadratiques réelles sur E, page 687

$Q^+(E)$ formes quadratiques positives, page 1601

$Q^{++}(E)$ formes quadratiques strictement définies positives, page 1601

$S_n^{p,q}(\mathbb{R})$ matrices symétriques réelles de signature (p,q), page 1602

$\beta(s)$ Vecteur unitaire de la binormale, page 1938

$\gamma \sim g$ Équivalence d'arcs paramétrés, page 1927

$\nu(s)$ Vecteur unitaire de la normale principale, page 1938

$c(s)$ rayon de courbure, page 1938

$t(s)$ Torsion, page 1939

Géométrie

$P(E)$ l'espace projectif de E, page 1971

$(x_0 : \ldots : x_n)$ coordonnées homogènes dans un espace projectif, page 1988

$\mathcal{C}\mathrm{onv}(A)$ enveloppe convexe, page 973

$\mathrm{PGL}(E)$ groupe projectif, page 1977

B^o orthogonal dans le dual, page 419

$G[\mathbb{C}]$ combinaisons d'éléments de G à coefficients dans $\mathbb{C}$, page 1503

$P_1(\mathbb{C})$ sphère de Riemann, page 1992

Chaînes de Markov

$\pi(x)$ lié au temps de retour, page 2705

Probabilités et statistique

$\sigma(f)$ La tribu engendrée par une variable aléatoire ou une application, page 1246

$a \wedge b$ $\min(a,b)$, page 2733

K_X matrice de covariance d'un vecteur gaussien, page 2640

$m(\mathcal{A})$ Ensemble des fonctions $\mathcal{A}$-mesurables, page 1261

Théorie des groupes

$(G/H)_g$ classes à gauche, page 364

$[a]_p$ ensemble des $a + kp$, page 286

$[G,G]$ groupe dérivé, page 228

$[g,h]$ commutateur dans un groupe, page 228

$\mathrm{Aff}(\mathbb{R}^n)$ Le groupe des applications affines bijectives de $\mathbb{R}^n$., page 982

gr_G groupe engendré, page 226

$\hat{G}$ groupe des caractères de G, page 1499

σ_x réflexion par rapport à x, page 1706

A_n groupe alterné, page 440

$D(G)$ groupe dérivé, page 228

D_n groupe diédral, page 1696

G^{ab} groupe abélianisé de G, page 229

$N \times_\phi H$ produit semi-direct, page 229

S_n le groupe symétrique, page 179

$N \lhd G$ Le sous-groupe N est normal dans G, page 181

Topologie et théorie des ensembles

$\mathrm{Adh}(A)$ adhérence de A, page 521

$\complement A$ Le complémentaire de l'ensemble A, page 116

$\mathrm{Diam}(A)$ Diamètre de la partie A, page 1017

∂A La frontière de l'ensemble A, page 668

$A \Delta B$ différence symétrique, page 126

A^c complémentaire de A, page 116

Analyse

$C^\infty(I, \mathscr{D}'(\mathbb{R}^d))$ fonctions à valeurs dans les distributions, page 2368

$(S, \hat{\mathcal{F}}, \hat{\mu})$ complété de l'espace mesuré $(S, \hat{\mathcal{F}}, \hat{\mu})$, page 1267

$\mathcal{L}(E, F)$ Les applications linéaires de E vers F, page 935

$\arg(z)$ La valeur principale de l'argument de $z \in \mathbb{C}$, page 2073

$\mathbb{D}_b$ l'ensemble des écritures décimales en base b, page 878

$\mathbb{R}$ l'ensemble des réels, page 334

$\mathbb{R}^+$ les réels positifs ou nuls, page 337

exp exponentielle, page 1432

$\mathscr{H}'$ dual, page 2040

$\mathrm{Isom}(X)$ Le groupe des isométries de X, page 599

$\liminf a_n$ limite inférieure, page 772

$\limsup a_n$ limite supérieure, page 772

$\mathcal{L}^p$ espace de Lebesgue, sans les classes, page 2140

$\mu \ll \nu$ La mesure μ est absolument continue par rapport à la mesure ν, page 1332

$\mu \perp \nu$ mesures mutuellement singulières, page 1332

μ^* La mesure extérieure associée à la mesure μ, page 1257

∂_z,$\partial_{\bar{z}}$ dérivées partielles d'une fonction complexe, page 2061

$\mathtt{proj}_K(x)$ projection orthogonale de x sur y, page 2038

$\sigma(\mathcal{D})$ tribu engendrée par $\mathcal{D}$, page 1246

$\mathscr{D}(\Omega)$ Les fonctions C^∞ à support compact sur Ω, page 2361

$\mathscr{S}'(\mathbb{R}^d)$ espace des distributions tempérées, page 2380

$A^2(\Omega)$ espace de Bergman, page 2293

$A^\perp$ orthogonal d'une partie., page 2039

$C^\infty\big(\mathbb{R}, \mathscr{S}'(\mathbb{R}^d)\big)$ Fonctions à valeurs dans les distributions., page 2450

$C_c(I)$ fonctions continues à support compact dans I, page 2175

$f \sim g$ fonctions ayant des limites équivalentes, page 1092

$H^1(\Omega)$ espace de Sobolev sur Ω, page 2396

$H^1(I)$ espace de Sobolev, page 2391

$H^m(M)$ espace de Sobolev, page 2397

$L^1_{loc}(I)$ fonctions intégrables sur les compacts de I, page 2391

L^p espace de Lebesgue avec les classes, page 2142

$M_i\varphi$ La fonction $x \mapsto x_i\varphi(x)$, page 2288

$S_n f$ somme partielle de série de Fourier, page 2330

Première partie

Le Frido

Chapitre 0

Introduction

0.1 Auteurs, contributeurs, sources et remerciements

SECooINTROremerciements

Les remerciements, dans chaque catégorie, sont mis dans l'ordre chronologique approximatif.

0.1.1 Ceux qui ont travaillé sur le Frido

SUBooINTROremerciementsFrido

(1) Carlotta Donadello pour l'ensemble du cours de CTU de géométrie analytique 2010-2011. Une grosse partie de « analyse réelle » vient de là.

(2) Les étudiants de géométrie analytique en CTU 2010-2011 ont détecté d'innombrables coquilles. Les étudiants du cours présentiel de géométrie analytique 2011-2012 ont signalé un certain nombre d'incorrections dans les exercices et les corrigés. Les agrégatifs de Besançon 2011-2012 pour leurs plans et leurs développements.

(3) Lilian Besson pour m'avoir signalé un paquet de fautes, et quelques points pas clairs en statistiques.

(4) Plouf qui m'a signalé une coquille dans le fil la-selection-scientifique-de-la-semaine-numero-106.

(5) Benjamin de Block pour des coquilles et une mise au point sur les conventions à propos de $\mathbb{R}^+$ et $(\mathbb{R}^+)^*$.

(6) Olivier Garet pour avoir répondu à plein de questions de probabilités.

(7) François Gannaz pour de la relecture et une version plus claire de la preuve (et de l'énoncé) de la proposition 21.10.

(8) Danarmk pour des réponses à des questions dans les commentaires (allongement pour éviter un Overfull hbox) http://linuxfr.org/nodes/110155/comments/1675589. Et aussi pour une discussion à propos de la topologie sur $\mathscr{D}(\Omega)$.

(9) Cédric Boutilier pour des réponses à des questions de probabilité statistique. https://github.com/LaurentClaessens/mazhe/issues/16

(10) Remsirems pour des réponses à des questions d'analyse[1]

(11) Bertrand Desmons pour plusieurs patchs rendant plus clairs de nombreux passages sur les suites de Cauchy dans $\mathbb{Q}$.

(12) Anthony Ollivier pour m'avoir fait remarquer qu'il n'est pas vrai que $A[X]$ est euclidien lorsque A est intègre (contre-exemple : $A = \mathbb{Z}$). Ça fait une faute de moins dans le Frido.

(13) ybailly pour avoir détecté un bon nombre de coquilles dans la partie sur les ensembles de nombres.

(14) Éric Guirbal pour le remplacement de `frenchb` par `french`.

(15) cdrcprds pour une réponse à une question d'algèbre, démonstration à l'appui à propos de pgcd. Également pour sa relecture sans pitié de la partie sur la cardinalité (en particulier $A \approx A \setminus B$) et pour avoir pointé l'utilité du théorème de comparabilité cardinale.

[1] http://linuxfr.org/nodes/110155/comments/1675813

(16) Antoine Bensalah pour avoir répondu à une question sur Lax-Milgram tout en même temps que pointé une erreur dans la démonstration et fourni l'exemple 27.61 sur l'optimalité de l'inégalité.

(17) Guillaume Deschamps pour ses remarques à propos du fait que le chapitre « constructions des ensembles » est très ardu.

(18) Guillaume Barriere pour sa relecture attentive jusqu'aux corps.

(19) Samy Clementz pour avoir découvert une faute dans la définition de mesure positive sur un espace mesurable.

(20) Sylvain Rousseau pour avoir clarifié une construction dans le théorème de Bower version C^∞.

(21) Maxmax pour des typos dans l'index thématique.

(22) Laurent Choulette pour une typo dans les propriétés du neutre d'un groupe.

(23) Pierre Lairez pour la démonstration du théorème d'inversion de limite et de dérivée 14.413 sans passer par les intégrales (et les lemmes correspondants à propos du module de continuité).

(24) Gregory Berhuy pour des réponses d'algèbres dans les catégories facile, moyen et difficile.

(25) Benoît Tran pour avoir signalé un paquet de typos dans la démonstration de l'ellipsoïde de John-Loewner et ses dépendances.

(26) Provatiscus pour avoir signalé un paquet de choses pas claires, et surtout pour avoir trouvé une faute dans la démonstration du fait qu'une fonction continue sur $\mathbb{Q}$ se prolonge en une fonction continue sur $\mathbb{R}$. Et pour cause : cet énoncé est faux. https://github.com/LaurentClaessens/mazhe/issues/124

(27) William pour l'environnement `example` qui gère correctement le triangle.

(28) Colin Pitrat pour de nombreuses remarques, typos et relecture de théorèmes.

(29) Bruno Turgeon pour une très belle moisson de fautes de frappe (euphémisme pour dire « mon ignorance crasse de l'orthographe »).

(30) Sacha Dhénin pour une belle quantité de fautes de frappes et pour avoir soulevé quelques points pas clairs (par exemple la définition du sous-groupe engendré dans le cas de la partie vide).

(31) Patrice Goyer pour m'avoir signalé quelques fautes et pas mal de points pas clairs dans les polynômes et dans la théorie généraliste des ensembles. Et pour m'avoir fait remarquer (deux fois) que mon script de déploiement ne marchait pas.

(32) Alain Vigne pour une quantité (presque) indénombrable de fautes d'orthographe et de mauvaises tournures de phrase dans les espaces vectoriels, la construction de nombres, la théorie des groupes et les anneaux. Il m'a également pointé quelques fautes et points vraiment pas clairs dans des démonstrations dont la correction a permis de bien améliorer la qualité du texte.

(33) Quentin Guyot pour une quantité de typos proche du nombre de Graham dont beaucoup me semblent impossible à détecter sans une lecture attentive ; (au moins) huit entrées dans l'erratum lui sont dues (au sens où c'est lui qui les a trouvées, pas qu'il les a causées).

(34) Jean Abou Samra pour la démonstration de la connextité par arcs C^1.

(35) jperon pour le classement de l'index en comptant les é comme des é. Voir [8].

0.1.2 Aide directe, mais pas volontairement sur le Frido

SUBooINTROremerciementsDirecte

(1) Plein de monde pour diverses contributions à des énoncés d'exercices. Pierre Bieliavsky pour les énoncés d'analyse numérique (MAT1151 à Louvain la Neuve 2009-2010). Jonathan Di Cosmo pour certaines corrections de MAT1151. François Lemeux, exercices sur les normes de matrices et correction de coquilles. Martin Meyer et Mustapha Mokhtar-Kharroubi pour certains exercices du cours *Outils mathématiques* (surtout ceux des DS et examens).

(2) Nicolas Richard et Ivik Swan pour les parties des exercices et rappels de calcul différentiel et intégral (Université libre de Bruxelles, 2003-2004) qui leurs reviennent.

(3) Carlotta Donadello pour la partie géométrie analytique : topologie dans $\mathbb{R}^n$, courbes, intégrales, limites. (Université de Franche-Comté 2010-2012)

(4) Le forum usenet de math, en particulier pour la construction des corps fini dans le fil « Vérifier qu'un polynôme est primitif » initié le 20 décembre 2011.

(5) Mihai Bostan nous a donné ses notes manuscrites de son cours présentiel de géométrie analytique 2009-2010. (Presque) Toute la structure du cours de géométrie analytique lui est due (qui est maintenant fondue un peu partout dans les chapitres d'analyse).

0.1.3 Des gens qui ont fait un travail qui m'a bien servi

SUBooINTROremerciementsAutres

(1) Arnaud Girand pour avoir mis ses développements bien faits en ligne. Une bonne vingtaine de résultats un peu partout dans ces notes viennent de lui.

(2) Le site http://www.les-mathematiques.net m'a donné les preuves de nombreux résultats.

(3) Pierre Monmarché pour son document en ligne tout plein de développements, et des réponses à des questions.

(4) Tous les contributeurs du Wikipédia francophone (et aussi un peu l'anglophone) doivent être remerciés. J'en ai pompé des quantités astronomiques ; des articles utilisés sont cités à divers endroits du texte, mais ce n'est absolument pas exhaustif.

(5) Les intervenants du fil « Antisymétrisation, alterné, déterminant et caractéristique » sur `les-mathematiques.net` m'ont bien aidé pour la section sur les déterminants 10.1 (bien qu'ils ne le savent pas).

(6) Xavier Mauquoy pour l'énoncé et la preuve du théorème 4.26.

(7) David Revoy pour les dessins de Pepper&Carrot de la couverture.

J'ai souvent donné entre parenthèses à côté des mots « théorème », « lemme » ou « proposition » une ou plusieurs références vers les sources de la preuve que je donne. Ce sont parfois des liens vers la bibliographie ; parfois aussi des liens hypertextes vers des sites, des blogs, etc. Tous ces gens ont fait du bon boulot. Sans toute cette « communauté », l'internet serait mort[2].

0.2 Originalité

SECooINTROoriginalite

Ces notes ne sont pas originales par leur contenu : ce sont toutes des choses qu'on trouve facilement sur internet ; je crois que la bibliographie est éloquente à ce sujet. Ce cours se distingue des autres sur les points suivants.

La longueur J'ai décidé de ne pas me soucier de la taille du fichier. Il fera cinq mille pages s'il le faut, mais il restera en un bloc. Étant donné qu'il n'existe qu'une seule mathématique, il ne m'a pas semblé intéressant de produire une division artificielle entre l'analyse, la géométrie ou l'algèbre. Tous les résultats d'une branche peuvent (et sont) être utilisés dans toutes les autres branches.

Dans cette optique, je me suis évertué à ne créer que des références « vers le haut ». À moins d'oubli de ma part[3], il n'y a aucun endroit du texte qui dépend d'un lemme démontré plus bas. Le fait qu'un théorème B soit plus bas qu'un théorème A signifie qu'on peut démontrer A sans savoir B.

La licence Ce document est publié sous une licence libre. Elle vous donne explicitement le droit de copier, modifier et redistribuer.

Les mises à jour Ce document est régulièrement mis à jour. Des fautes d'orthographe sont corrigées (presque) chaque jour. Si vous me signalez une faute de mathématique, elle sera corrigée.

Transparence Je ne fais pas semblant que ces notes soient parfaites. Les points sur lesquels je ne suis pas sûr, les preuves que j'ai inventées moi-même sont clairement indiqués pour inciter le lecteur à redoubler de prudence. Une liste de questions à résoudre est incluse en la section 0.7. Voir 0.3 pour plus de détails.

[2] Cette dernière phrase doit être comprise comme un appel à ne pas utiliser Moodle et autres iCampus pour diffuser vos cours de math, ou en tout cas pas comme moyen exclusif.

[3] Par exemple pour les théorèmes pour lesquels je n'ai pas lu ni a fortiori écrit de preuves.

0.3 Les choses qui doivent vous faire tiquer

SECooWVHBooCaYoXP

Un cours de math doit toujours être lu attentivement, surtout si vous avez l'intention de resservir à un jury le fruit de vos lectures. Dans ce livre, trois éléments doivent vous faire redoubler de prudence.

La référence [1] D'abord les références à [1] indiquent qu'une bonne partie de ce qui suit est de l'invention personnelle de l'auteur. Cela ne veut évidemment pas dire que c'est moi qui ai découvert le résultat. Ça veut dire que je n'ai pas trouvé le résultat ou certaines parties de la preuve.

Les notes en bas de page Certaines notes en bas de page sont écrites dans une fonte spéciale[4]. Elles indiquent des points sur lesquels je doute ou des étapes de calculs que je ne parviens pas à reproduire en suivant mes sources. Lorsque vous voyez une telle note, redoublez de prudence, allez voir la source, et écrivez-moi si vous pouvez résoudre le problème.

Les environnements dédiés Et enfin certains problèmes sont indiqués plus longuement dans un environnement dédié en petits caractères comme ceci :

¡¡ Avertissement/question au lecteur !! 0.1
Les choses écrites comme ceci sont des questions ou des éléments sur lesquels j'ai un doute. Lisez-les attentivement. Ces notes mentionnent des points que personnellement je n'oserais pas affirmer plein d'aplomb à un jury d'agrégation.

0.4 Quelques choix qui peuvent provoquer des quiproquos

SECooINTROquiproquos

Comme tout cours de mathématique, ce cours fait des choix qui sont parfois discutables. Voici quelques points sur lesquels les choix faits ici ne sont peut-être pas ceux fait par tout le monde. Ce sont donc des points sur lesquels vous devez faire attention pour éviter les quiproquos lors par exemple d'un oral dans un concours.

(1) Nous utilisons la définition « épointée » de limite d'une fonction en un point. Elle diffère de celle donnée par le ministère de l'enseignement en France. Si votre but est de passer un concours d'enseignement en France, vous devriez lire 14.2 ; dans tous les autres cas, la définition prise ici est celle qu'il vous faut.

(2) Un compact est une partie d'un espace topologique pour lequel tout recouvrement par des ouverts admet un sous-recouvrement fini. Le fait d'être séparable n'est pas inclus dans la définition de compact. De nombreux textes français incluent la séparabilité dans la compacité.

(3) Le logarithme sur $\mathbb{C}$ est une application $\ln : \mathbb{C}^* \to \mathbb{C}$ définie partout sauf en zéro. Elle n'est donc pas continue sur la fameuse demi-droite. À ne pas confondre avec une *détermination* du logarithme qui est par définition continue et donc non définie sur la demi-droite.

Cela est un choix très discutable. La raison de donner à la notation « ln » cette signification est simplement de suivre l'usage de Sage. Pour Sage, $\ln(-1)$ existe et vaut $i\pi$.

Voir les remarques 28.43.

(4) Le mot « corps » n'implique pas la commutativité bien que tous les corps du Frido soient commutatifs, et nous n'utilisons pas la terminologie « anneau à division ». Voir la section -1.3 et la discussion 8.1.

0.5 Autres choix pas spécialement standards

SECooINTROchoixPasStandards

Nous listons ici quelques choix qui n'induisent pas de différences ou d'incompatibilité avec les autres cours, mais qui doivent être compris et justifiés.

(1) Nous n'utilisons pas les notations $o(x)$ ou autres $O(N^2)$. D'abord parce que je n'ai jamais très bien compris comment elles fonctionnent, et ensuite (surtout) parce que ces notations induisent en erreur. Ce sont des notations qui cachent, sous des notations a peu près intuitive, l'utilisation de théorèmes pas simples.

Écrire

$$f(x) = P(x) + o(x^2), \tag{0.1}$$

[4] Les notes comme celle-ci signifient qu'il y a certaines choses dont je ne suis pas sûr.

c'est un peu comme quand on écrit (horreur !)

$$F(x) = \int f(x)dx + C. \tag{0.2}$$

Où est le x à droite ? Quel est le statut de C ?

Même chose pour la notation $f(x) = P(x) + o(x^2)$. Le x de $o(x^2)$ est-il le x qu'on a à gauche ? Si $g(x) = Q(x) + o(x^2)$, est-ce le même o que celui de f ?

(2) Nous allons être plus calme avec la notation $A[X]$ pour les polynômes sur l'anneau A, et encore moins $A[X_1, \dots, X_n]$ pour les polynômes de n variables. Au lieu de cela nous utilisons $\mathcal{P}(A)$ et $\mathcal{P}_n(A)$.

Est-ce que vous diriez que $A[X] = A[Y]$? Quelle est exactement la nature de X dans $P = X^2 + 1$ ou dans $P(X) = X^2 + 1$? Si $P \in A[X]$ vaut $P(X) = X^2$ et si $Q \in A[Y]$ vaut $Q(Y) = Y^2$, est-ce que vous oseriez écrire $P = Q$?

0.5.1 Mathématique intéressante

SUBooINTROmathInteressante

Définition 0.2.
Une notion mathématique est ***intéressante*** *si elle permet de répondre à une question que l'on peut se poser sans connaitre la notion.*

EXEooINTROmathInteressantes1

Exemple 0.3.
Étant donné un segment dans le plan, quels sont les triangles rectangles dont ce segment est l'hypoténuse ?

Nous n'avons pas besoin de cercles pour poser cette question. Mais nous avons besoin de connaissances sur les cercles pour y répondre. Donc l'étude des cercles est intéressante. △

EXEooINTROmathInteressantes2

Exemple 0.4.
Comment fonctionne la gravitation ?

Cette question peut être posée sans connaitre de calcul tensoriel, d'équations différentielles ou d'intégrales. Et pourtant, tous ces concepts sont utiles pour y répondre. △

0.6 Sage est là pour vous aider

SECooINTROsage

Il existe de nombreux logiciels de mathématique. Notre préféré est Sage pour une raison très précise : Sage est (en simplifiant) un module pour Python. Donc quand on travaille en Sage, on dispose de tout Python. La syntaxe et la structure de Sage ne sont pas *ad hoc* pour faire des maths, et ce qu'on apprend en Sage peut être recyclé pour faire n'importe quoi : navigateur web, script de manipulation de texte, traitement d'image, réseau neuronaux, …

Sage est un logiciel disponible pour l'épreuve de modélisation de l'agrégation de mathématique ; il y a donc de bonnes chances que vous en ayez l'usage.

0.6.1 Lancez-vous dans Sage

SUBooINTROsageLancezVous

(1) Aller sur `http://www.sagemath.org`,

(2) créer un compte,

(3) créer des feuilles de calcul et s'amuser !!

Il y a beaucoup de documentation sur le site officiel[5], et nous vous conseillons particulièrement le livre [9].

Si vous comptez utiliser régulièrement ce logiciel, je vous recommande *chaudement* de l'installer sur votre ordinateur.

0.6.2 Exemples de ce que Sage peut faire pour vous

SUBooINTROsageExemples

Ce livre est émaillé de petits bouts de code en Sage montrant ses différentes fonctionnalités là où nous en avons besoin[6]. Voici une liste (non exhaustive) de ce que Sage peut faire pour vous.

(1) Calculer des limites de fonctions, exemples 45.1 et 45.2.

[5] http://www.sagemath.org
[6] Soit un vrai besoin comme tracer un graphique en 3D, soit de la paresse comme calculer une grosse dérivée.

(2) Tracer des graphes de fonctions, exemple 45.2.

(3) Tracer des courbes en trois dimensions, voir exemple 14.233. Notez que pour cela vous devez installer aussi le logiciel Jmol. Pour Ubuntu, c'est dans le paquet `icedtea6-plugin`.

(4) Calculer des dérivées partielles de fonctions à plusieurs variables, voir exemple 45.3.

(5) Résoudre des systèmes d'équations linéaires. Voir les exemples 45.4 et 45.5. Lire aussi la documentation.

(6) Tout savoir d'une forme quadratique, voir exemple 45.6.

(7) Calculer la matrice hessienne de fonctions de deux variables, déterminer les points critiques, déterminer le genre de la matrice hessienne aux points critiques et écrire les extrémums de la fonctions (sous réserve d'être capable de résoudre certaines équations), voir les exemples 45.7 et 45.8.

(8) Indiquer une infinité de solutions à une équation en utilisant des paramètres. L'exemple 45.9 montre ça avec une équation algébrique. Un exemple concernant des fonctions trigonométriques :

```
sage: solve(sin(x)/cos(x)==1,x,to_poly_solve=True)
[x == 1/4*pi + pi*z1]
sage: solve(sin(x)**2==cos(x)**2,x,to_poly_solve=True)
[sin(x) == cos(x), x == -1/4*pi + 2*pi*z86, x == 3/4*pi + 2*pi*z84]
```

Notez l'option `to_poly_solve=True` dans `solve`.

(9) Calculer des dérivées symboliquement, voir exemple 45.10.

(10) Calculer des approximations numériques comme dans l'exemple 45.11.

(11) Calculer dans un corps de polynômes modulo comme $\mathbb{F}_p[X]/P$ où P est un polynôme à coefficients dans $\mathbb{F}_p$. Voir l'exemple 21.64.

Sage peut en général faire tout ce que vous êtes capable de faire à l'entrée en master et probablement bien plus, à la notable exception des limites à deux variables.

REMooINTROsageAttention

Remarque 0.5.
Sage peut toutefois vous induire en erreur si vous n'y prenez pas garde parce qu'il sait des choses en mathématique que vous ne savez pas. Par conséquent il peut parfois vous donner des réponses (mathématiquement exactes) auxquelles vous ne vous attendez pas. Voir par exemple 17.165 pour le logarithme de nombres négatifs. Et aussi ceci :

```
1
2
3  SageMath version 7.3, Release Date: 2016-08-04
4  Type "notebook()" for the browser-based notebook interface.
5  Type "help()" for help.
6
7  sage: limit(1/x,x=0)
8  Infinity
9  sage: limit(1/x**2,x=0)
10 +Infinity
```

tex/sage/sageSnip017.sage

Sage fait une différence entre `Infinity` et `+Infinity` et donne

$$\lim_{x\to 0} \frac{1}{x} = \infty \tag{0.3}$$

ainsi que

$$\lim_{x\to 0} \frac{1}{x^2} = +\infty. \tag{0.4}$$

Voir aussi la compactification en un point d'Alexandroff 9.204.

0.7 Comment contribuer et aider ?

SecooCKWWooBFgnea

0.7.1 Orthographe

Quelques règles.

(1) Le Frido utilise l'orthographe rectifiée. Le plus visible est « corolaire » au lieu de « corollaire » et quelques accents circonflexes qui sautent. Par exemple : « convergence presque sure » au lieu de « presque sûre ».

(2) Le Frido écrit « à priori » et non « a priori » parce que si au bout de seulement quelques décennies on a le droit d'écrire « des pizzas » ou comme si ce n'était pas un mot italien, au bout de 1000 ans il faut se calmer en prétendant que « à priori » est du latin.

(3) En termes de féminisation, on n'écrit pas « la.e lectrice.teur » mais on utilise

```
\randomGender{le lecteur}{la lectrice}
```

et une des deux formes sera choisie au hasard durant la compilation. Comme ça le Frido est neutre en moyenne. La macro est bien faite : elle choisira la même forme si on l'appelle deux fois dans le même paragraphe.

0.7.2 Contributions IA

Je n'ai à priori rien contre le fait d'utiliser une IA pour faire de math. MAIS MAIS MAIS MAIS !

Ne me faites pas une contribution qui consiste à balancer un énoncé dans ChatGPT pour juste me donner la sortie. Ça, je peux le faire moi-même.

(1) Relisez la preuve pour vous assurer qu'elle est correcte.

(2) Assurez-vous que les résultats utilisés dans la preuve soient déjà dans le Frido. Sinon, donnez un énoncé précis. Pas besoin de preuve pour le résultat intermédiaire. Sauf si c'est l'IA qui vous l'a donné. En effet il arrive encore (2026) que l'IA fasse une faute et, quand on lui demande comment il justifie telle ligne, qu'il balance « c'est un résultat connu que <et bam, un énoncé faux> ».

Plus généralement, ne me faites pas de contributions que vous ne comprenez pas vous-même. Si vous les faites, vous utiliseriez mieux votre temps à contribuer à un autre projet.

0.7.3 Des preuves qui manquent

SUBooINTROhowtoContribProofs

Vous trouverez un peu partout des énoncés sans preuves. Certaines sont surement très faciles, et d'autres probablement assez compliquées. N'hésitez pas à rédiger une preuve et me l'envoyer.

Vous pouvez m'envoyer vos preuves sous forme de « c'est bien fait dans tel cours », avec une URL.

Ne me dites juste pas « c'est bien fait dans tel *livre* ». Je ne travaille pas à l'université, et je n'ai pas accès à une bibliothèque universitaire ; je n'ai donc pas réellement accès à ces fameux « livres » dont tout le monde parle.

0.7.4 Du texte qui manque

SUBooINTROhowtoContribText

Vous remarquerez que de nombreuses pages du Frido sont des enchainements de théorèmes et démonstrations sans articulations. Autrement dit, il manque ce qu'à l'agrégation on dirait à l'oral quand on présente le plan. Si vous avez des idées de choses à ajouter ici ou là, faites-le moi savoir.

0.7.5 Des exemples qui manquent

SUBooINTROhowtoContribExamples

Si vous connaissez de bons exemples, faites-le moi savoir.

0.7.6 Des choses qui n'aident pas

Il y a toutefois un type de contribution qui n'est pas très utile : les modifications de style ou de notations. Ne me faites pas un commit changeant 50 fichiers pour modifier « strictement définie positive » en « définie positive » ou pour améliorer le d dans $\int f(x)dx$.

0.7.7 Trucs de programmation et de LaTeX

SUBooINTROhowtoContribProg

(1) Comment faire en sorte que les mots commençant par « é » soient avec les « e » dans l'index, et non avant les « a » ? Il me faudrait un mécanisme plus automatique que faire `machin@truc`.

Une fonction en Python qui prend en entrée le fichier bbl sous forme de string et qui ressort sous forme de string le fichier bbl modifié me convient.

(2) Écrire un script (en Python ou autre) qui prend en argument deux numéros ou noms de chapitres et qui retourne l'ensemble des lignes du premier qui contient des `ref` ou `eqref` dont le label correspondant est dans le second.

Attention : il faut tenir compte de `input` de façon récursive.

Bonus : calculer le hash sha1 de chaque ligne du résultat et ne pas l'afficher si il se trouve dans la liste du fichier `commons.py`.

0.8 Les politiques éditoriales

SECooINTROpolitics

Certaines parties de ce texte ne respectent pas les politiques éditoriales. Ce sont des erreurs de jeunesse, et j'en suis le premier triste.

0.8.1 Licence libre

SUBooINTROpoliticsFreelic

Je crois que c'est clair.

0.8.2 pdflatex

SUBooINTROpoliticsPdflatex

Tout est compilable avec pdfLaTeX. Pas de pstricks, de psfrag ou de ps<quoiquecesoit>.

0.8.3 utf8

SUBooINTROpoliticsUTF8

Je crois que c'est clair.

0.8.4 Notations

SUBooINTROpoliticsNotations

On essaie d'être cohérent dans les notations et les conventions. Pour la transformée de Fourier par exemple, je crois que la définition du produit scalaire dans L^2, des coefficients de Fourier, de la transformation et de la transformation inverse sont cohérents. Cela demande, lorsqu'on suit un livre qui ne suit pas les conventions utilisées ici, de convertir parfois massivement.

0.8.5 De la bibliographie

SUBooINTROpoliticsBiblio

On évite d'écrire en haut de chapitre « les références pour ce chapitre sont … ». Il est mieux d'écrire au niveau des théorèmes, entre parenthèses, les références.

Lorsqu'on écrit l'énoncé d'un théorème sans retranscrire la démonstration, il faut mettre une référence vers un document *en ligne* qui en contient la preuve. Il est vraiment fastidieux de chercher une preuve sur internet et de tomber sur des dizaines de documents qui donnent l'énoncé mais pas la preuve.

0.8.6 Faire des références à tout

SUBooINTROpoliticsInternalRefs

Lorsqu'un utilise le théorème des accroissements finis, il ne faut pas écrire « d'après le théorème des accroissements finis, blablabla ». Il faut écrire un `\ref` explicite vers le résultat. Cela alourdit un peu le texte, mais lorsqu'on joue avec un texte de plus de 2000 pages, il est parfois laborieux de trouver le résultat qu'on cherche (surtout si il existe plusieurs versions d'un résultat et que l'on veut faire référence à une version particulière).

0.8.7 Des listes de liens internes

SUBooINTROpoliticsInternalLinks

Le début du Frido contient une espèce d'index thématique. Il serait bon de l'étoffer.

0.8.8 Pas de références vers le futur

SUBooINTROpoliticsNoFutureRef

Dans le Frido, *aucune* preuve ne peut faire une référence vers un résultat prouvé plus bas. On n'utilise pas le théorème 10 dans la démonstration du théorème 7. Cela est une contrainte forte sur le découpage en chapitres et sur l'ordre de présentation des matières.

Il est bien entendu accepté et même encouragé de mettre des notes du type « Nous verrons plus loin un théorème qui … ». Tant que ce théorème n'est pas *utilisé*, ça va.

Chapitre 1

Les naturels et les entiers

1.1 Les bases

SECooIntroBases

1.1.1 Axiomatique et grammaire

SUBooNaturelsEntiers

1.1.
Le Frido n'est pas supposé être lu dans l'ordre de la première à la dernière page ; les matières y sont présentées dans l'ordre logique mathématique, et non dans l'ordre logique pédagogique, et encore moins par ordre de difficulté croissante.

En mathématique, si on lit une démonstration et que l'on veut vraiment tout justifier, et justifier toutes les étapes de tous les résultats utilisés, on tombe forcément un jour sur les axiomes.

Or l'axiomatique est un sujet particulièrement difficile. Nous n'allons donc pas « tout justifier » jusque là. Nous n'allons même pas préciser quel système d'axiome est utilisé. En particulier nous n'allons pas donner l'axiomatique des ensembles : nous allons supposer connus les ensembles et leurs principales propriétés.

NorooFridoGrammaire

1.2.
Nous n'allons pas non plus formaliser la grammaire des expressions mathématiques[1]. Nous supposons que vous êtes capables de lire des expressions comme

$$x \in \mathbb{N} \Rightarrow \{a \geqslant x\} \text{ est infini.} \tag{1.1}$$

1.1.2 Les théorèmes encapsulants

SUBooThmEncapsulants

1.3.
Je propose d'introduire le concept de « théorème encapsulant ». Un théorème est encapsulant lorsque les techniques et concepts utiles à sa démonstration ne sont pas utiles pour énoncer et utiliser le théorème.

Sauter la démonstration d'un théorème encapsulant permet donc de sauter des parties entières de la mathématique.

Un exemple typique d'un théorème qui n'est pas encapsulant est le théorème de Rolle 14.210. Les ingrédients de la démonstration (topologie, dérivée) sont présents dans l'énoncé[2]. D'habitude, quand on utilise le théorème de Rolle on est dans un contexte où on est en train de parler de dérivée, de topologie, et de théorème des valeurs intermédiaires.

Notez que le théorème de Stokes (théorème 26.8, plus généralement théorème 22.71) n'est pas non plus encapsulant parce que pour énoncer le théorème, il faut quand même définir les intégrales, les différentielles, les bords, etc. La démonstration de Stokes ne fait pas intervenir de concepts réellement nouveaux par rapport à ce qu'il faut savoir pour énoncer Stokes.

Le Frido va accepter sans démonstrations deux théorèmes encapsulants qui évitent de devoir parler de pans entiers de la théorie des ensembles.

(1) Le lemme de Zorn 1.42. Il cachera toute la complexité de l'axiome du choix et la moitié de ce qu'apporte cet axiome par rapport à ZF.

(2) L'existence d'un ensemble des naturels (théorème 1.127). Même si nous proposerons un moyen d'en construire un, cela cachera toute la complexité d'axiomatisation, des différentes définitions d'ensembles finis, d'existence de maximum, etc. Voir [10, 11].

[1] J'utilise ici des mots que je ne comprends pas, juste pour me donner l'air malin.

[2] C'est-à-dire que pour énoncer le théorème de Rolle, il faut déjà connaître pratiquement toutes les notions nécessaires pour le démontrer.

Notez que les énoncés de ces théorèmes ne demandent pas grand chose : relation d'ordre sur un ensemble pour le lemme de Zorn ; ensemble et application injective pour les naturels.

Je me demande d'ailleurs si il existe beaucoup d'autres théorèmes encapsulants.

1.2 Ensembles, relations, fonctions

NORMSEGridEMathsEnsembles

1.4.
Tout cela pour dire que le Frido ne traitera que de la partie facile de la mathématique.

1.2.1 Opérations ensemblistes

SUBooOperationsEnsemblistes2

1.5.
Nous supposons avoir une théorie des ensembles qui tient la route. En particulier nous supposons que les notions suivantes sont connues :

(1) ensemble vide,

(2) ensemble des parties.

(3) ensemble, appartenance, intersection, union.

(4) produit cartésien de plusieurs ensembles[3].

Si I est un ensemble et si pour chaque $i \in I$ nous avons un ensemble A_i, alors nous ne définissons pas ce qu'est

$$\bigcup_{i\in I} A_i. \tag{1.2}$$

Et si J est un ensemble et qu'on a une bijection $\varphi\colon I \to J$ nous ne démontrons pas que

$$\bigcup_{i\in I} A_i = \bigcup_{j\in J} A_j. \tag{1.3}$$

Ce sont toutes des choses dont la construction à partir des axiomes n'est en aucun cas évidente. En particulier, des « définitions » comme « l'intersection de deux ensembles est l'ensemble contenant exactement les éléments communs aux deux ensembles » ne sont pas correctes parce qu'elles passent à côté de l'existence et de l'unicité d'un tel ensemble.

DEFooJLBVooMyCQMO

Définition 1.6.
Soit E, un ensemble et A, une partie de E (c'est-à-dire un sous-ensemble de E). Le ***complémentaire*** *de l'ensemble A, dans E, noté $\complement A$ est l'ensemble des éléments de E qui ne font pas partie de A :*

$$\complement A = E \setminus A = \{x \in E \text{ tel que } x \notin A\}. \tag{1.4}$$

Nous allons aussi régulièrement noter le complémentaire de A par A^c.

DefEnsemblesDisjoints

Définition 1.7.
Deux ensembles A et B sont ***disjoints*** *si leur intersection est vide*[4] *; en d'autres termes, si il n'existe aucun élément commun à A et B.*

DefPartitionEnsembles

Définition 1.8.
Soit E un ensemble, et E_α des parties de E indexées sur un ensemble A. Les E_α forment une ***partition*** *si :*

- *pour tous $\alpha, \beta \in A$, on a soit $E_\alpha = E_\beta$, soit $E_\alpha \cap E_\beta = \varnothing$;*
- *la réunion des E_α est E.*

On dit aussi que E est partitionné par les E_α.

NorooDepartTheoEns

1.9.
Remarquez par exemple que la première phrase de l'article de Wikipédia sur la construction de $\mathbb{N}$ est « Partant de la théorie des ensembles, on identifie 0 à l'ensemble vide, puis on construit … ». Il est bien précisé que l'on part d'une théorie des ensembles.

La suite de ce chapitre sera essentiellement sans exemple parce qu'avant d'avoir construit les ensembles de nombres, je ne sais pas très bien quels exemples on peut donner de quoi que ce soit.

[3] Nous en proposons une définition dans un cadre général – définition 1.22 –, dont les fondements devraient être analysés de très près.

[4] Remarquez que les mots « intersection » et « vide » sont de ceux que nous avons décidé de ne pas définir.

1.2.2 Des relations aux bijections

DEFmRelFtBijectFns

Définition 1.10 ([12]).
*Une **relation binaire** d'un ensemble E vers un ensemble F est une partie de $E \times F$.*

Si G est une relation binaire entre E et F, et si $(x; y) \in G$, nous notons $x\mathcal{R}_G y$ et nous disons que x est en relation avec y.

*On définit aussi une **relation unaire** d'un ensemble E comme une partie de E, et une **relation ternaire** de trois ensembles E_1, E_2 et E_3 comme une partie de $E_1 \times E_2 \times E_3$.*

DefooApplicFct

Définition 1.11.
*Soit G une relation binaire entre deux ensembles E et F. Si, pour tout $x \in E$, et tous y, $y' \in F$, les relations $x\mathcal{R}_G y$ et $x\mathcal{R}_G y'$ entraînent $y = y'$, alors on peut associer à chaque $x \in E$ apparaissant comme première composante dans G, l'élément unique $y \in F$ qui est en relation avec x dans G. Cette association définit une **fonction** de E dans F.*

Le plus souvent, les fonctions entre deux ensembles sont désignées par f, ou selon le contexte, par une autre lettre, souvent minuscule. On notera presque toujours les ensembles concernés par la fonction, et on adopte alors la notation $f : E \to F$.

*Pour marquer l'association, à $x \in E$, du $y \in F$ correspondant à travers f, on note cet élément $f(x)$: ainsi, $f(x) \in F$, et il est appelé **image de x par f**.*

L'ensemble des $x \in E$ pour lesquels il existe $y \in F$ tel que $x\mathcal{R}_G y$ est noté D_f, ou bien Domaine f *; on l'appelle **domaine de définition de f** , ou encore **ensemble de définition de f**. Lorsque* Domaine$(f) = E$*, on dit que f est une **application**.*

RemLienFctRelation

Remarque 1.12 (Lien entre fonction et relation).
Si $f : E \to F$ est une fonction de relation sous-jacente G, alors :

- Domaine $f = \{x \in E$ tel que $\exists y \in F : (x, y) \in G\}$;
- $\Im f = \{y \in F$ tel que $\exists x \in E : (x, y) \in G\}$;
- Graph $f = G$.

REMooFonctionDomaineEntier

Remarque 1.13.
Dans le Frido, on prend comme convention que, quand on écrit $f : E \to F$, alors Domaine $f = E$. C'est un choix qui n'est peut-être pas standard, mais qui évite des complications sur ce qu'est réellement le domaine de définition. En particulier, dans le Frido, on ne verra que très rarement f « tout seul ».

En revanche, on ne sait rien sur $\Im f$ a priori. Il ne faut pas déduire de la notation que l'ensemble image $\Im f$ serait F tout entier.

NORooLMBYooYjUoju

1.14.
L'**axiome du choix** que nous acceptons peut s'énoncer comme ceci[13] : Étant donné un ensemble X d'ensembles non vides, il existe une fonction définie sur X, appelée fonction de choix, qui à chacun d'entre eux associe un de ses éléments.

DefooInjSurjBij

Définition 1.15.
Soient deux ensembles E et F. Une fonction $f : E \to F$ est

*(1) **surjective** si pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$;*

*(2) **injective** si pour tout $y \in F$, il existe au plus un $x \in E$ tel que $y = f(x)$;*

*(3) **bijective** si elle est à la fois injective et surjective.*

NORMooMethodePreuveInj

1.16.
La méthode la plus courante pour démontrer qu'une application $f : E \to F$ est injective est de considérer $x, y \in E$ tels que $f(x) = f(y)$, et de prouver à partir de là que $x = y$. Ou alors de supposer $x \neq y$ et d'obtenir une contradiction.

La technique de la contradiction est évidemment la plus courante lorsque l'égalité $f(x) = f(x)$ implique une équation faisant intervenir $1/(x - y)$.

La surjection et l'injection sont des propriétés bien différentes qu'il convient de prouver séparément. De plus une même « formule » peut définir une application injective, surjective, bijective ou non selon les ensembles sur lesquels nous la considérons.

DEFcomposeeFonctions

Définition 1.17.
Soit $f : X \to Y$ et $g : Y \to Z$ deux fonctions définies respectivement sur les ensembles X et Y. On

définit alors la ***composée*** *de f avec g comme la fonction $g \circ f$ de l'ensemble X vers l'ensemble Z telle que $(g \circ f)(x) = g\big(f(x)\big)$.*

On remarquera que le domaine de définition de $g \circ f$ est l'ensemble $\{x \in \text{Domaine}\, f$ tel que $f(x) \in \text{Domaine}\, g\}$, sous-ensemble de Domaine f.

LEMooWBYSooFqyqQP

Lemme 1.18.
Soient deux ensembles A et B ainsi qu'une application $f\colon A \to B$. Nous supposons qu'il existe une application $g\colon B \to A$ telle que $f \circ g = \mathrm{Id}_B$ et $g \circ f = \mathrm{Id}_A$.

Alors f est une bijection.

Démonstration. En deux parties.

(1) **Injection** Supposons que $f(a) = f(b)$. Alors en appliquant g des deux côtés, et en utilisant le fait que $g \circ f = \mathrm{Id}_A$, nous trouvons $a = b$.

(2) **Surjection** Soit $x \in B$. Posons $a = g(x)$. Alors, en utilisant le fait que $f \circ g = \mathrm{Id}_B$ nous avons

$$f(a) = (f \circ g)(x) = x. \tag{1.5}$$

Donc x est dans l'image de f et f est surjective.

□

DEFooTRGYooRxORpY

Définition 1.19.
*Soit $f\colon A \to B$ une bijection. L'****application réciproque*** *de f est la fonction*

$$\begin{aligned} f^{-1}\colon B &\to A \\ y &\mapsto \text{le } x \in A \text{ tel que } f(x) = y. \end{aligned} \tag{1.6}$$

Plus généralement si $f\colon X \to Y$ est une fonction quelconque et si $S \subset Y$, nous notons

$$f^{-1}(S) = \{x \in \text{Domaine}\, f \text{ tel que } f(x) \in S\}, \tag{1.7}$$

et dans le cas où S est réduit à un unique élément y, nous notons $f^{-1}(y)$ au lieu de $f^{-1}\big(\{y\}\big)$. Si de plus $f^{-1}(S)$ est un singleton x, nous noterons $f^{-1}(S) = x$ et non $f^{-1}(S) = \{x\}$.

REMooDifferenceElementSingleton

Remarque 1.20.
Les plus acharnés parmi les lecteurs se rendront compte de la différence ontologique fondamentale entre x et $\{x\}$, et donc des abus de notations explicitées dans la définition précédente.

PROPooBXVSooZXmwKC

Proposition 1.21 ([1])**.**
Soit $f\colon A \to B$ une fonction. Si X et Y sont des parties de A, alors :

ITEMooFctInclusionInter

(1) on a l'inclusion $f(X \cap Y) \subseteq f(X) \cap f(Y)$;

ITEMooFctInjEgaliteInter

(2) si de plus, f est injective[5]*, alors $f(X \cap Y) = f(X) \cap f(Y)$;*

ITEMooFctInjDisjonction

(3) si enfin, f est injective et X et Y sont disjoints, alors $f(X) \cap f(Y) = \varnothing$ (autrement dit : $f(X)$ et $f(Y)$ sont disjoints aussi).

Démonstration. Prouvons d'abord $f(X \cap Y) \subseteq f(X) \cap f(Y)$, ensuite $f(X) \cap f(Y) \subseteq f(X \cap Y)$ dans le cas où f est une injection, et enfin le cas d'ensembles disjoints.

(1) **Première inclusion** Si $\xi \in f(X \cap Y)$, alors il existe $s \in X \cap Y$ tel que $\xi = f(s)$. Étant donné que $s \in X$, nous avons $\xi = f(s) \in f(X)$. Et comme $s \in Y$ nous avons aussi $\xi = f(s) \in f(Y)$. Au final $\xi = f(x) \in f(X) \cap f(Y)$.

(2) **Seconde inclusion** Si $\xi \in f(X) \cap f(Y)$, il existe $x \in X$ et $y \in Y$ tels que $\xi = f(x)$ et $\xi = f(y)$. Par injectivité de f, nous avons $x = y$ et donc $\xi \in f(X \cap Y)$.

(3) **Ensembles disjoints** Si f est injective, et si $X \cap Y = \varnothing$, alors il n'y a aucun élément dans $f(X \cap Y) = f(X) \cap f(Y)$.

□

[5] Définition 1.15.

DEFooTYIMooZUsYJw

Définition 1.22 (Produit cartésien infini[14])**.**
Soit un ensemble I ainsi qu'une collection d'ensembles $\{A_i\}_{i\in I}$. Nous notons $\prod_{i\in I} A_i$ l'ensemble des applications $f\colon I\to\bigcup A_i$ telles que $f(i)\in A_i$.

Avec cette notation nous avons aussi

$$\mathrm{Fun}(X,Y)=\prod_{x\in X} Y. \tag{1.8}$$

1.2.3 Ensemble ordonné

DefooFLYOooRaGYRk

Définition 1.23.
*Une **relation d'ordre** sur un ensemble E est une relation binaire[6] (notée $\leqslant$) sur E telle que pour tous $x,y,z\in E$,*

ITEMooQTXOooTZXEnu

(1) Réflexivité : $x\leqslant x$

(2) Antisymétrie : $x\leqslant y$ et $y\leqslant x$ implique $x=y$

(3) Transitivité : $x\leqslant y$ et $y\leqslant z$ implique $x\leqslant z$.

Pour suivre les notations de la définition 1.10, la partie G de $E\times E$ est une relation d'ordre lorsque

(1) $(x,x)\in G$ pour tout $x\in G$,

(2) Si $(x,y)\in G$ et $(y,x)\in G$, alors $x=y$,

(3) Si $(x,y)\in G$ et $(y,z)\in G$, alors $(x,z)\in G$.

Dans la suite nous n'allons plus écrire de relations binaires en détaillant l'ensemble sous-jacent.

*Lorsque nous avons un ensemble E et une relation d'ordre $\leqslant$ sur E, nous disons que le couple $(E,\leqslant)$ est un **ensemble ordonné**.*

DEFooFTZAooLrtNEo

Définition 1.24 (Application croissante, décroissante et monotone)**.**
Soient des ensembles ordonnés E et F. Soit une application $f\colon E\to F$.

*(1) L'application f est **croissante** si pour tout $x\leqslant y$ dans E nous avons $f(x)\leqslant f(y)$ dans F. Elle est **strictement croissante** $x<y\Rightarrow f(x)<f(y)$.*

*(2) La fonction f est dite **monotone** sur I si elle est, soit croissante, soit décroissante, sur I.*

DEFooQEIAooGzzdiu

Définition 1.25 ([1])**.**
*Un **isomorphisme** d'ensembles ordonnés est une bijection croissante[7] dont la réciproque est croissante.*

DEFooVGYQooUhUZGr

Définition 1.26.
*Un ensemble ordonné est **totalement ordonné** si deux éléments quelconques si deux éléments sont toujours comparables : si $x,y\in E$ alors nous avons soit $x\leqslant y$ soit $y\leqslant x$. Si les éléments ne sont pas tous comparables, nous disons que l'ordre est **partiel**.*

LEMooZUAZooFlziuO

Lemme 1.27 ([1])**.**
Si E est un ensemble alors l'ensemble des parties muni de l'inclusion $(\mathcal{P}(E),\subset)$ est un ensemble partiellement ordonné.

Démonstration. Il suffit de vérifier les conditions.

(1) $A\subset A$, ok.

(2) Si $A\subset B$ et $B\subset A$ alors $A=B$, ok.

(3) $A\subset B$ $B\subset C$ implique $A\subset C$, ok.

□

PROPooNPLNooTqXVYz

Proposition 1.28 ([1])**.**
Si $(E,\leqslant)$ est un ensemble ordonné, alors $(E,\geqslant)$ est également un ensemble ordonné.

[6] Définition 1.10.
[7] Application croissante, définition 1.24.

Démonstration. Il faut vérifier.

(1) Nous avons $x \geqslant x$ sans problèmes.

(2) Si $x \geqslant y$ et $y \geqslant z$, alors $y \leqslant x$ et $z \leqslant y$. Cela donne $z \leqslant x$, c'est-à-dire $x \geqslant z$.

(3) Si $x \geqslant y$ et $y \geqslant x$, on a $y \leqslant x$ et $x \leqslant y$ et donc $x = y$.

□

ExeooOrdreInclusion

Exemple 1.29.
Si E est un ensemble, l'inclusion est un ordre sur l'ensemble des parties de E, mais pas un ordre total parce que si X, Y sont des parties de E, alors nous n'avons pas automatiquement soit $X \subset Y$ soit $Y \subset X$. △

NORMooIntroIntervalleOrdonne

1.30.
On convient assez naturellement de la notation suivante : écrire $x \leqslant y \leqslant z$ revient à écrire $(x \leqslant y)$ et $(y \leqslant z)$. Cela s'étend à un nombre (fini) quelconque d'éléments, et le lecteur saura interpréter correctement, nous l'espérons, des inégalités du genre $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_n$ dans les prochains développements.

1.2.4 Intervalle

La notion d'ordre permet d'introduire la notion d'intervalle, qui s'écrit assez simplement une fois la convention prise.

DefEYAooMYYTz

Définition 1.31.
Soit un ensemble totalement ordonné $(E, \leqslant)$. Un ***intervalle*** *de E est une partie I telle que tout élément compris entre deux éléments de I soit dans I. La partie I de E est un intervalle si*

$$\forall a, b \in I,\ \forall x \in E, (a \leqslant x \leqslant b \Rightarrow x \in I).$$

1.2.5 Minimum, maximum, minimal, maximal, etc.

DEFooDNWRooTiMAzK

Définition 1.32.
Soit un ensemble ordonné $(E, \leqslant)$ et une partie A de E. Un élément $p \in E$ est un ***minorant*** *de A si pour tout $a \in A$, les éléments p et a sont comparables et $p \leqslant a$. Si de plus, $p \in A$, on dira que p est un* ***minimum*** *de A.*

Les notions de ***maximum*** *et de* ***majorant*** *sont définies de façon analogue (en remplaçant $p \leqslant a$ par $a \leqslant p$).*

DEFooBZNRooYRPGme

Définition 1.33 ([15])**.**
Soient un ensemble ordonné $(E, \leqslant)$, et une partie $A \subset E$. Un élément $M \in A$ est un ***élément maximal*** *de A si pour tout $x \in E$ si $M \leqslant x$ alors $x = M$.*

De même, nous disons que $m \in A$ est un ***élément minimal*** *de A si pour tout $x \in A$, nous avons $x \leqslant m \Rightarrow x = m$.*

PROPooUniciteMinMax

Proposition 1.34.
Soit $(E, \leqslant)$ un ensemble ordonné, et A un sous-ensemble de E admettant un minimum. Alors ce minimum est unique.

Démonstration. Soit m le premier élément minimum de A. Quel que soit $x \in A$, on sait que x et m sont comparables, et que $m \leqslant x$.

Supposons que $p \in A$ soit un (autre) élément minimum de A. Alors, par ce fait, on a $p \leqslant m$; mais par définition de m, on a aussi $m \leqslant p$. Ainsi, par antisymétrie[8], on a $m = p$. □

PROPooUJJEooPBUenw

Proposition 1.35 ([1])**.**
Si $(E, \leqslant)$ est totalement ordonné, et si $A \subset E$, un élément est un minimum de A si et seulement si il est minimal dans A.

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que p est un minimum de A. Soit $x \in A$ avec $x \leqslant p$. Vu que p est est minimum, il est un minorant et donc $p \leqslant x$. Nous avons donc $p \geqslant x$ et $p \leqslant x$. Donc $p = x$.

[8] Point (2) de la définition 1.23.

(2) $\Leftarrow$ Nous supposons que p est un élément minimal dans A. Soit $a \in A$. Il y a deux possibilités : soit $a \leqslant m$ soit $a > m$. Dans le premier cas $a = m$, et dans le second $m \leqslant a$.

□

NORMooPlusPetitElement

1.36.
On peut ainsi parler, lorsqu'une partie possède un minimum, de « plus petit élément » de la partie. Attention : il n'en existe pas toujours. D'innombrables exemples pourront être vus lorsque nous aurons construit $\mathbb{Q}$ et $\mathbb{R}$. Typiquement les intervalles du type $]a, b[$.

NORMooVHIBooJAOsou

1.37.
Notons qu'il n'est pas demandé à un élément maximal[9] d'être comparable à tous les autres éléments. Si $(E, \leqslant)$ n'est pas totalement ordonné, un élément maximal peut ne majorer qu'une partie de E.

Un élément maximal est plus grand que tous les éléments avec lesquels il est comparable.

Dans un ensemble totalement ordonné, les notions d'élément maximal de E et de maximum[10] de E coïncident ; dans le cas d'un ordre partiel, ces notions sont distinctes.

Il se peut que nous parlions d'un « maximum » ou « élément maximum » au lieu d'un « élément maximal », en particulier en utilisant le lemme de Zorn. Si vous voyez de telles choses, n'hésitez pas à me le dire.

Par exemple, quand on applique le lemme de Zorn pour démontrer l'existence d'une base dans un espace vectoriel de dimension infinie, on obtient une famille libre qui est maximale, c'est-à-dire qui est un élément maximal dans l'ensemble, ordonné par inclusion, des familles libres de l'espace vectoriel. C'est un élément maximal, et non un maximum, car l'ensemble des familles libres d'un espace vectoriel non réduit à $\{0\}$ n'admet pas de maximum (pour l'inclusion).

Voir 6.28 et 6.30.

ExeooMaximalPasMajorant

Exemple 1.38 ([1]).
Soit un ensemble E ainsi que $a \neq b$ dans E. Nous considérons les parties

$$A = \{P \subset E \text{ tel que } a \in P, b \notin P\} \tag{1.9a}$$
$$B = \{P \subset E \text{ tel que } b \in P, a \notin P\}. \tag{1.9b}$$

Et enfin nous considérons l'ensemble $F = A \cup B$, c'est-à-dire l'ensemble des parties de E qui contiennent soit a soit b mais pas les deux. Nous ordonnons partiellement F par l'inclusion.

Dans $(F, \subset)$, l'élément $E \setminus \{b\}$ est un élément maximal, mais pas un majorant. △

DEFooLJEAooBLGsiS

Définition 1.39.
Un ensemble ordonné est ***bien ordonné*** *si toute partie non vide possède un plus petit élément.*

Autrement dit, l'ensemble ordonné E est bien ordonné si pour toute partie non vide A, il existe $x \in A$ tel que $x \leqslant y$ pour tout $y \in A$.

NorooOrdreBienOrdonne

1.40.
Quelques remarques.

(1) L'inégalité stricte (définie par : $x < y$ si et seulement si $x \leqslant y$ et $x \neq y$) n'est pas une relation d'ordre parce qu'elle n'est pas réflexive.

(2) Nous verrons dans la remarque 4.61 que l'intervalle $[-1, 1]$ dans $\mathbb{R}$ n'est pas bien ordonné.

(3) Un ensemble bien ordonné est forcément totalement ordonné parce que toutes les parties de la forme $\{x, y\}$ possèdent un minimum. Par conséquent x et y doivent être comparables : $x \leqslant y$ ou $y \leqslant x$.

1.2.6 Lemme de Zorn

SUBooDefGHEZyu

Définition 1.41 (Ensemble inductif[16]).
Un ensemble est ***inductif*** *si toute partie totalement ordonnée admet un majorant.*

LemUEGjJBc

Lemme 1.42 (Lemme de Zorn[17]).
Tout ensemble ordonné inductif non vide admet au moins un élément maximal.

PROPooFOETooWYLOeq

Proposition 1.43 ([18]).
Soient un ensemble inductif $(E, \leqslant)$ et $b \in E$. Il existe un élément maximal[11] $m \in E$ tel que $b \leqslant m$.

[9] Définition 1.33
[10] Définition 1.32.
[11] Définition 1.33.

Démonstration. En plusieurs parties.

(1) **Un ensemble** Nous considérons

$$E_b = \{x \in E \text{ tel que } b \leqslant x\}. \tag{1.10}$$

(2) **E_b est inductif** Soit une partie non vide totalement ordonnée $A \subset E_b$; démontrons que A admet un majorant dans E_b. Puisque $E_b \subset E$, par transitivité de l'inclusion, $A \subset E$ et puisque E est inductif, la partie A admet un majorant $m' \in E$: justifions maintenant que $m' \in E_b$.

Comme A est non vide, nous pouvons considérer $x \in A$. Nous avons $b \leqslant x$ parce que $x \in A \subset E_b$. Mais comme m' est un majorant de A, $x \leqslant m'$. Bref, nous avons les inégalités

$$b \leqslant x \leqslant m'. \tag{1.11}$$

Par transitivité de l'ordre, $b \leqslant m'$ et donc $m' \in E_b$.

Nous avons ainsi prouvé que m' est un majorant de A contenu dans E_b. Donc E_b est inductif.

(3) **Zorn** Puisque $(E_b, \leqslant)$ est inductif, le lemme de Zorn 1.42 nous indique que E_b a un élément maximal. Nous le notons m.

(4) **m est maximal dans E** Supposons avoir un élément $a \in E$ tel que $m \leqslant a$. Comme $m \in E_b$, nous avons les inégalités

$$b \leqslant m \leqslant a, \tag{1.12}$$

et donc $a \in E_b$ par transitivité. Mais m est maximal dans E_b, donc $a \leqslant m$, d'où $a = m$ par antisymétrie.

□

PROPooRHNFooHFUOEx

Proposition 1.44 ([1]).
Soit A et Bă deux ensembles non vides, et une application surjective $f\colon A \to B$. Il existe une application $\alpha\colon B \to A$ telle que

$$\alpha(b) \in f^{-1}(b) \tag{1.13}$$

pour tout $b \in B$.

Démonstration. Nous considérons l'ensemble

$$\mathcal{A} = \{(X, \alpha) \text{ tel que } X \subset B, \alpha\colon X \to A \text{ tel que } \alpha(x) \in f^{-1}(x) \forall x \in X\} \tag{1.14}$$

que nous ordonnons par inclusion pour X et par extension pour α.

D'abord, $\mathcal{A}$ est non vide : considérons un élément $a \in A$ et posons $b = f(a)$; en posant $X = \{b\}$ et $\alpha\colon \{b\} \to A$ donné par $\alpha(b) = a$, le couple (X, α) est bien un élément de $\mathcal{A}$.

Ensuite, $\mathcal{A}$ est inductif. En effet, soit une partie $\mathcal{F} = \{(X_i, \alpha_i)\}_{i \in I}$ totalement ordonnée de $\mathcal{A}$. Nous posons $X = \bigcup_i X_i$ et $\alpha\colon X \to A$ par $\alpha(b) = \alpha_i(b)$ dès que $b \in X_i$. L'élément (X, α) est dans $\mathcal{A}$ et majore $\mathcal{F}$.

Nous pouvons donc utiliser le lemme de Zorn[12], et affirmer que l'ensemble $\mathcal{A}$ contient un maximum (Y, β). Montrons alors par l'absurde que $Y = B$.

Supposons que $Y \neq B$. Alors il existe $b \in B \setminus Y$. Comme $f\colon A \to B$ est surjective, il existe $a \in A$ tel que $f(a) = b$[13]. Nous posons alors $Y' = Y \cup \{b\}$ et

$$\beta'(x) = \begin{cases} \beta(x) & \text{si } x \in B \\ a & \text{si } x = b. \end{cases} \tag{1.15}$$

Le couple (Y', β') majore (Y, β) et nous avons une contradiction avec la maximalité de Y. □

1.2.7 Quelques relations ensemblistes

LEMmRAEnsDQfGtM

Lemme 1.45 ([1]).
Si $B \subset A$, alors $X \setminus A \subset X \setminus B$.

Démonstration. Si $x \in X \setminus A$, alors x n'est pas dans A. Si x était dans B, nous aurions $x \in B \subset A$. Donc x n'est pas dans B et donc $x \in X \setminus B$. □

[12] Lemme 1.42.

[13] Toute la subtilité de l'axiome du choix. Si on a un élément b, on a le droit de considérer un élément $a \in f^{-1}(b)$, mais on n'a pas le droit de considérer un tel élément de A pour tout élément de B.

LEMooHRKAooRskzQL

Lemme 1.46 (Quelques relations ensemblistes)**.**
Soient $A, B, C \subset X$. Nous avons

ITEMooIXUAooXDPtWj

(1) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$.

ITEMooQCGUooKnWfBo

(2) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$.

ITEMooXWKCooUASxlh

(3) $A \cap (B \setminus C) = (A \cap B) \setminus C$.

ITEMooRXJOooUYPaCp

(4) $A \cap (X \setminus B) = A \setminus B$.

ITEMooYYWAooLnADjR

(5) Si I est un ensemble et que $A_i \subset X$ pour tout $i \in I$ alors

$$X \setminus \left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I}(X \setminus A_i). \tag{1.16}$$

Démonstration. En plusieurs parties.

(1) **Pour (1)** Deux inclusions.

(1a) **Dans un sens** Si $x \in X \setminus (A \cap B)$. Il y a deux possibilités : soit $x \in A$, soit $x \notin A$. Si $x \in A$, alors $x \notin B$, sinon nous aurions $x \in A \cap B$. Donc $x \in X \setminus B$. Le cas $x \notin A$ est similaire.

(1b) **Dans l'autre sens** Soit $x \in X \setminus A$. Vu que $A \cap B \subset A$, le lemme 1.45 dit que $x \in X \setminus (A \cap B)$.

(2) **Pour (2)** Deux inclusions.

(2a) **Premier sens** Soit $x \in X \setminus (A \cup B)$. Si x était dans A, il serait dans $A \cup B$. Or il n'est pas dans $A \cup B$ donc x n'est pas dans A. On montre de même que $x \in X \setminus B$.

(2b) **Dans l'autre sens** Soit $x \in (X \setminus A) \cap (X \setminus B)$. Supposons que $x \in A \cup B$, et disons $x \in A$ pour fixer les idées. Nous savons que $x \in X \setminus A$; contradiction. Donc $x \notin A$. Nous obtenons la même contradiction si $x \in B$.

(3) **Pour (3)** Deux inclusions.

(3a) **Premier sens** Supposons que $x \in A \cap (B \setminus C)$. D'une part $x \in A$. Or $x \in B \setminus C$, donc $x \in B$. Nous avons déjà $x \in A \cap B$. Mais $x \in B \setminus C$ implique $x \notin C$. Donc $x \in (A \cap B) \setminus C$.

(3b) **Deuxième sens** Nous avons :

ITEMooMGGEooVRxrB

(3b.i) $x \in A \cap B$ donc $x \in A$.

ITEMooOIQCooUAwng

(3b.ii) $x \in A \cap B$ donc $x \in B$.

ITEMooCTHOooBLcsZv

(3b.iii) $x \in (A \cap B) \setminus C$ donc $x \notin C$.

Les points (3b.ii) et (3b.iii) font $x \in B \setminus C$. En ajoutant (3b.i) nous avons $x \in A \cap (B \setminus C)$.

(4) **Pour (4)** C'est un cas particulier de (3) avec $B = X$.

(5) **Pour (5)** En deux inclusions.

(5a) **Dans un sens** Soit $x \in X \setminus (\bigcap_{i\in I} A_i$. Vu que x n'est pas dans $\bigcap_{i\in I} A_i$, il existe $j \in I$ tel que $x \notin A_j$, et donc tel que $x \in X \setminus A_j$.

(5b) **Dans l'autre sens** Si $x \in \bigcup_{i\in I}(X \setminus A_i)$, alors il existe $j \in I$ tel que $x \in X \setminus A_j$. Donc x n'est pas dans A_j et à fortiori pas dans $\bigcap_{i\in I} A_i$.

□

LEMooBGQRooCVLGsh

Lemme 1.47 ([1])**.**
Si $A \subset B$ et si $f : B \to B$ est injective, alors

$$f(A) = f(B) \setminus f(B \setminus A). \tag{1.17}$$

EQooHLEHooADUbIO

Démonstration. Les deux inclusions.

(1) $\subseteq$ Soit $a \in A$. Alors $a \in A \subset B$, de telle sorte que $f(a) \in f(B)$. Mais a n'est pas dans $B \setminus A$, disjoint de A, et comme f est injective, grâce à la propriété 1.21(3), $f(A) \cap f(B \setminus A) = \varnothing$. Comme $f(a) \in f(A)$, nous avons $f(a) \notin f(B \setminus A)$.

(2) **Dans l'autre sens** Suppose $y \in f(B) \setminus f(B \setminus A)$. Vu que $y \in f(B)$, il existe $b \in B$ tel que $y = f(b)$. Mais comme $y \notin f(B \setminus A)$, nous avons $b \notin B \setminus A$. Donc, $b \in B \cap A$, d'où $b \in A$ et par suite $f(b) \in f(A)$.

□

LEMooHPUNooPmViwi

Lemme 1.48 ([19]).
Pour tous ensembles A, B, C nous avons

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C); \tag{1.18}$$
$$\text{et } A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{1.19}$$

Démonstration. Nous démontrons la première égalité d'ensembles par double inclusion.

(1) **Inclusion dans un sens** Nous supposons que $x \in A \cap (B \cup C)$. Il y a deux possibilités : soit x est dans $A \cap B$ soit non. Si $x \in A \cap B$ c'est bon. Sinon, nous allons prouver que $x \in A \cap C$.

Vu que $x \in A$ et $x \notin A \cap B$, nous avons $x \notin B$. Mais $x \in B \cup C$. Donc $x \in C$. Nous avons prouvé que $x \in A \cap C$.

(2) **Inclusion inverse** Soit $x \in (A \cap B) \cup (A \cap C)$. Nous allons prouver que $x \in A \cap (B \cup C)$.

(2a) **Si $x \in A \cap B$** Nous supposons que $x \in A \cap B$. Directement $x \in A$. Et comme $x \in B$, nous avons aussi $x \in B \cup C$. Donc $x \in A \cap (B \cup C)$.

(2b) **Si $x \in A \cap C$** Même raisonnement.

L'autre égalité d'ensembles se démontre de manière similaire (quoique plus simple).

(1) **Inclusion dans un sens** Si $x \in A \cup (B \cap C)$, alors, il est dans A, ou bien il est à la fois dans B et dans C.

- Si $x \in A$, alors il est aussi dans $A \cup B$, et dans $A \cup C$; donc il se trouve dans $(A \cup B) \cap (A \cup C)$.
- Si $x \in B$, alors il est dans $A \cup B$. Si, en même temps, $x \in C$, alors il est dans $A \cup C$. Donc il se trouve dans l'intersection $(A \cup B) \cap (A \cup C)$.

(2) **Inclusion inverse** Soit $x \in (A \cup B) \cap (A \cup C)$. Il est donc à la fois dans $A \cup B$ et dans $A \cup C$.

- Si $x \in A$, alors il est bien dans $A \cup (B \cap C)$.
- Sinon, il doit se trouver à la fois dans B et dans C, car dans le cas contraire il ne pourrait pas se trouver dans les unions ci-dessus. Ainsi $x \in B \cap C$, et donc $x \in A \cup (B \cap C)$.

□

LemPropsComplement

Lemme 1.49.
Quelques propriétés à propos des complémentaires[14]*. Si E est un ensemble et si A et B sont des sous-ensembles de E, nous avons*

ITEMooComplementDisjoint
(1) $A \cap (E \setminus A) = \varnothing$.

ITEMooComplementPartition
(2) *A et $E \setminus A$ forment une partition*[15] *de E.*

ITEMooWIYBooKMLVnZ
(3) $\complement\complement A = A$, *en d'autres termes,* $E \setminus (E \setminus A) = A$.

ItemLemPropComplementiii
(4) $A \setminus B = A \cap \complement B$.

ITEMooNHDUooWtURqQ
(5) $(A \setminus B)^c = A^c \cup B$.

ITEMooTBWKooTChOmC
(6) $A^c \setminus B^c = B \setminus A$.

Démonstration. Point par point.

(1) **Pour (1)** Par définition même du complémentaire, on ne peut avoir en même temps $x \in A$ et $x \notin A$.

(2) **Pour (2)** On a clairement $A \subset E$ et $E \setminus A \subset E$. Le point précédent nous justifie que l'intersection est vide. On a aussi $A \cup (E \setminus A) \subset E$: prouvons l'inclusion inverse.

Si $x \in E$, alors ou bien $x \in A$, ou bien $x \notin A$, et donc par définition du complémentaire, $x \in E \setminus A$.

[14] Définition 1.6.
[15] Définition 1.8.

(3) **Pour (3)** On peut faire une preuve avec une double inclusion.

(3a) **Si $x \in E \setminus (E \setminus A)$** Alors $x \notin E \setminus A$. Par l'absurde, si $x \notin A$, alors $x \in E \setminus A$, ce qui est contradictoire. Ainsi, la possibilité $x \notin A$ est exclue et donc $x \in A$.

(3b) **Si $x \in A$** Alors $x \notin (E \setminus A)$. c'est-à-dire $x \in E \setminus B = E \setminus (E \setminus A)$.

Une autre preuve consiste à utiliser le point (2) d'abord avec A, ensuite avec $E \setminus A$. Dans les deux cas, on partitionne E en deux ; l'un des ensembles est $E \setminus A$, l'autre est respectivement A et $E \setminus (E$ă $\setminus A)$, qui sont dès lors nécessairement égaux.

(4) **Pour (4)** En deux parties.

(4a) **Si $x \in A \setminus B$** Alors deux choses :

(4a.i) $x \in A$.

(4a.ii) $x \notin B$, c'est-à-dire $x \in E \setminus B$.

Donc $x \in A \cap (E \setminus B)$.

(4b) **Si $x \in A \cap (E \setminus B)$** Alors deux choses :

(4b.i) $x \in A$.

(4b.ii) $x \in E \setminus B$, ce qui implique[16] que $x \notin B$.

Donc $x \in A \cap (E \setminus B)$.

(5) **Pour (5)** Il faut le faire en deux inclusions.

(5a) **$(A \setminus B)^c \subset A^c \cup B$** Supposons que $x \in (A \setminus B)^c$. Si $x \in A^c$, c'est bon. Supposons que x n'est pas dans A^c, et montrons que $x \in B$. Le fait que x ne soit pas dans A^c signifie que $x \in A$. Si x n'était pas dans B, alors x serait dans $A \setminus B$, ce qui est contraire à l'hypothèse. Donc $x \in B$.

(5b) **$A^c \cup B \subset (A \setminus B)^c$** Supposons d'abord que $x \in A^c$. Comme $A \setminus B \subset A$, si $x \in A^c$, alors $x \in (A \setminus B)^c$.

Si $x \in B$, alors x n'est pas dans $A \setminus B$ et donc x est dans $(A \setminus B)^c$.

(6) **Pour (6)** Pour cette égalité, nous séparons 4 cas suivant que x est dans A ou B ou non. Bref, nous écrivons la table de vérité :

A	1	1	0	0
B	1	0	1	0
$A^c \setminus B^c$	0	0	1	0
$B \setminus A$	0	0	1	0

(1.20)

Les deux dernières lignes étant égales, nous avons l'égalité d'ensembles annoncée.

□

LEMooMDTPooAhmYqv

Lemme 1.50 ([1]).
Soient des parties $(A_j)_{j\in I}$ de X. Nous avons

$$\bigcup_{j\in I} A_j = X \setminus \Big(\bigcap_{j\in I} (X \setminus A_j) \Big). \tag{1.21}$$

Démonstration. En deux inclusions.

(1) **Sens direct** Si $x \in A_i$, alors $x \notin (X \setminus A_i)$. Or $\bigcap_{j\in I}(X \setminus A_j) \subset (X \setminus A_i)$, donc

$$x \in X \setminus \Big(\bigcap_{j\in I} (X \setminus A_j) \Big). \tag{1.22}$$

(2) **Dans l'autre sens** Dire que $x \in X \setminus \Big(\bigcap_{j\in I}(X \setminus A_j) \Big)$, c'est dire que x n'est pas dans l'intersection des $X \setminus A_i$. Il existe donc un $i \in I$ tel que $x \notin (X \setminus A_i)$, c'est-à-dire tel que $x \in A_i$. Donc $x \in \bigcup_{i\in I} A_i$.

□

[16] Je vous laisse disserter sur le fait que ce soit une implication ou juste une reformulation, vu que sous-entendu $x \in E$.

LEMooPWUHooMBKquL

Lemme 1.51 ([1]).
Soient des ensembles $\{A_i\}_{i\in I}$ et $\{B_j\}_{j\in J}$. Alors

$$\Big(\bigcup_{i\in I} A_i\Big)\cap\Big(\bigcup_{k\in J} B_j\Big) = \bigcup_{(i,j)\in I\times J}(A_i\cap B_j). \tag{1.23}$$

Démonstration. L'inclusion dans un sens. Si $x\in(\bigcup_i A_i)\cap(\bigcup_j B_j)$, alors il existe $i\in I$ et $j\in J$ tels que $x\in A_i$ et $x\in B_j$, c'est-à-dire $x\in A_i\cap B_j$.

Pour l'autre sens, si $x\in A_{i_0}\cap B_{j_0}$, alors $x\in\bigcup_{i\in I}A_i$ et $x\in\bigcup_{j\in J}B_j$. □

DefBMLooVjlSG

Définition 1.52 (différence symétrique).
*Si A et B sont des ensembles, l'ensemble $A\Delta B$ est la **différence symétrique** d'ensembles :*

$$A\Delta B = (A\cup B)\setminus(A\cap B). \tag{1.24}$$

C'est l'ensemble des éléments étant soit dans A soit dans B mais pas dans les deux, ni dans aucun des deux.

REMooTableVeriteDiffSym

Remarque 1.53.
La table de vérité de $A\Delta B$ est intéressante :

A	1	1	0	0
B	1	0	1	0
$A\Delta B$	0	1	1	0

EQooOJBOooKkKbYp (1.25)

La deuxième colonne signifie que si $x\in A$ et $x\in B^c$, alors $x\in A\Delta B$.

LemCUVoohKpWB

Lemme 1.54 ([20]).
Si A et B sont des parties d'un ensemble, nous avons

$$A\Delta B = (A\setminus B)\cup(B\setminus A), \tag{1.26}$$

EQooMWTNooKXfFvU

et aussi

ItemVUCooHAztC

(1) $A^c\Delta B^c = A\Delta B$.

ItemVUCooHAztCii

(2) $(A\Delta B)\Delta B = A$.

ITEMooSPZXooPTgisP

(3) $(A\Delta B)^c = (A^c\cap B^c)\cup(A\cap B)$.

ITEMooSMXWooYcWsRC

(4) Associativité : $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.

Démonstration. Pour (1.26), il suffit de réfléchir un peu : $A\Delta B$ contient précisément les éléments de A qui ne sont pas dans B, ainsi que les éléments de B qui ne sont pas dans A. On peut d'ailleurs voir que la table de vérité de $(A\setminus B)\cup(B\setminus A)$ est la même que (1.25).

Et pour le reste, c'est parti.

(1) **Pour (1)** Nous rappelons l'égalité $X^c\setminus Y^c = Y\setminus X$ du lemme 1.49(6). De là nous écrivons

$$A^c\Delta B^c = (A^c\cup B^c)\setminus(A^c\cap B^c) = (A^c\cap B^c)^c\setminus(A^c\cup B^c)^c = (A\cup B)\setminus(A\cap B) = A\Delta B. \tag{1.27}$$

(2) **Pour (2)** Ici, il faut remarquer que $(A\Delta B)\cup B = A\cup B$ et que $(A\Delta B)\cap B = B\setminus A$, donc

$$(A\Delta B)\Delta B = ((A\Delta B)\cup B)\setminus((A\Delta B)\cap B) \tag{1.28}$$
$$= (A\cup B)\setminus(B\setminus A). \tag{1.29}$$

Donc tous les éléments de $(A\Delta B)\Delta B$ sont dans $A\cup B$ mais pas dans $B\setminus A$.

- Un élément de $A\cup B$ est dans A ou bien dans B ; s'il n'est pas dans $B\setminus A$, il se trouve nécessairement dans A.
- Réciproquement, tous les éléments de A sont dans $A\cup B$ et ne sont pas dans $B\setminus A$.

Ainsi, on a bien $(A\Delta B)\Delta B = A$.

(3) **Pour (3)** Il s'agit d'utiliser le lemme 1.49(5) :

$$(A\Delta B)^c = \Big((A\cup B)\setminus(A\cap B)\Big)^c \tag{1.30a}$$
$$= (A\cup B)^c \cup (A\cap B) \tag{1.30b}$$
$$= (A^c\cap B^c)\cup(A\cap B). \tag{1.30c}$$

(4) **Pour l'associativité (4)** Nous écrivons les tables de vérités selon que x est dans A, B, C ou non. D'abord

A	1	1	1	1	0	0	0	0
B	1	1	0	0	1	1	0	0
C	1	0	1	0	1	0	1	0
$B\Delta C$	0	1	1	0	0	1	1	0
$A\Delta(B\Delta C)$	1	0	0	1	0	1	1	0

(1.31)

La quatrième ligne s'écrit sur le modèle de (1.25) en regardant les deuxièmes et troisièmes lignes. La dernière ligne se fait avec la première et la quatrième.

L'autre table de vérité se fait de la même manière :

A	1	1	1	1	0	0	0	0
B	1	1	0	0	1	1	0	0
C	1	0	1	0	1	0	1	0
$A\Delta B$	0	0	1	1	1	1	0	0
$(A\Delta B)\Delta C$	1	0	0	1	0	1	1	0

EQooMHPCooHpzBcY (1.32)

Puisque les lignes pour $A\Delta(B\Delta C)$ et pour $(A\Delta B)\Delta C$ sont identiques, nous avons égalité.

□

1.2.8 Relations d'équivalence

appDefRelEquiv

Définition 1.55.
*Si E est un ensemble, une **relation d'équivalence** sur E est une relation binaire*[17] *$\sim$ qui est à la fois*

réflexive *$x\sim x$ pour tout $x\in E$,*

symétrique *$x\sim y$ si et seulement si $y\sim x$;*

transitive *si $x\sim y$ et $y\sim z$, alors $x\sim z$.*

DEFooRHPSooHKBZXl

Définition 1.56.
*Si E est un ensemble et si $\sim$ est une relation d'équivalence sur E, alors nous notons $E/\sim$ l'**ensemble quotient**, c'est-à-dire l'ensemble des classes d'équivalence dans E. Un élément de $E/\sim$ est de la forme*

$$[a] = \{x\in E \text{ tel que } x\sim a\}. \tag{1.33}$$

Les éléments de $E/\sim$ sont donc des sous-ensembles de E.

LEMooEgaliteClassesGen

Lemme 1.57.
Soit un ensemble E et une relation d'équivalence $\sim$. Pour $a,b\in E$, nous avons $[a]=[b]$ si et seulement si $a\sim b$.

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que $[a]=[b]$. Par réflexivité, $a\sim a$ et nous avons $a\in[a]=[b]$. Mais $a\in[b]$ signifie $a\sim b$, ce qu'il fallait.

(2) $\Leftarrow$ Nous supposons que $a\sim b$, et nous démontrons que $[a]\subset[b]$. Si $x\in[a]$, alors $x\sim a$. Mais $a\sim b$. Donc $x\sim a\sim b$, ce qui implique $x\sim b$ par transitivité. Or dire $x\sim b$ implique $x\in[b]$. Pour l'inclusion $[b]\subset[a]$, il suffit de réécrire : on vous laisse faire.

□

[17] Définition 1.10.

1.2.9 Applications bien définies

La proposition suivante est ce qui est utilisé à chaque fois qu'on dit « telle formule définit bien une fonction » ou « cette fonction est bien définie parce que … »

PROPooCONJooTpJwBe

Proposition 1.58 ([1])**.**
Soient deux ensembles E et A. Nous considérons une relation d'équivalence $\sim$ sur E et une application $g\colon E\to A$ telle que si $a\sim b$ alors $g(a)=g(b)$.

Alors il existe une unique application $\tilde{g}\colon E/\sim\to A$ vérifiant

$$\tilde{g}([x])=g(x) \tag{1.34}$$

EQooCTHKooTXBfvh

pour tout $x\in E$.

Démonstration. En deux parties.

(1) **Existence**

Nous considérons $\mathcal{P}(A)$ l'ensemble des parties de A ainsi que S l'ensemble des singletons de A. Nous définissons l'application

$$\begin{aligned} g_P\colon E/\sim &\to \mathcal{P}(A)\\ \alpha &\mapsto \{g(x) \text{ tel que } x\in\alpha\}. \end{aligned} \tag{1.35}$$

Soit $\alpha\in E/\sim$. Prouvons que si $a\in\alpha$, alors $g_P(\alpha)=\{g(a)\}$. Par construction nous avons $g(a)\in\{g(x) \text{ tel que } x\in\alpha\}$ et donc l'inclusion $\{g(a)\}\subset g_P(\alpha)$. Pour l'inclusion dans l'autre sens, nous considérons $x\in\alpha$ et nous montrons que $g(x)\in\{g(a)\}$. En effet $x,a\in\alpha$, donc $g(x)=g(a)$.

Tout cela pour dire que g_P prend ses valeurs dans S et que $g_P([a])=\{a\}$ pour tout $a\in E$.

Nous introduisons maintenant l'opération d'extraction

$$\begin{aligned} e\colon S &\to A\\ \{x\} &\mapsto x, \end{aligned} \tag{1.36}$$

et nous considérons $\tilde{g}=e\circ g_P$. Vérifions que c'est bon.

Soit $x\in E$. Nous avons $x\in[x]$ et donc $g_P([x])=\{x\}$. Donc

$$\tilde{g}\big([x]\big)=(e\circ g_P)([x])=e\big(\{x\}\big)=x. \tag{1.37}$$

(2) **Unicité** Soit une autre application $\tilde{g}_2\colon E/\sim\to A$ vérifiant la condition (1.34). Soit $\alpha\in E/\sim$. Soit $a\in\alpha$. Nous avons $\tilde{g}(\alpha)=\tilde{g}([a])=a$. Et aussi $\tilde{g}_2(\alpha)=\tilde{g}_2([a])=a$. Donc $\tilde{g}(\alpha)=\tilde{g}_2(\alpha)$.

□

EXooYDRVooHsANlC

Exemple 1.59.
Sur l'ensemble de tous les polygones du plan, la relation « a le même nombre de côtés » est une relation d'équivalence. Plus précisément, si P et Q sont deux polygones, nous disons que $P\sim Q$ si et seulement si P et Q ont le même nombre de côtés. C'est une relation d'équivalence :

- un polygone P a toujours le même nombre de côtés que lui-même : $P\sim P$;
- si P a le même nombre de côtés que Q ($P\sim Q$), alors Q a le même nombre de côtés que P ($Q\sim P$) ;
- si P a le même nombre de côtés que Q ($P\sim Q$) et que Q a le même nombre de côtés que R ($Q\sim R$), alors P a le même nombre de côtés que R ($P\sim R$).

△

EXooProjCanoniqueEquivAppl

Exemple 1.60.
Soit f une application entre deux ensembles E et F. Nous définissons une relation d'équivalence sur E par

$$x\sim y\Leftrightarrow f(x)=f(y). \tag{1.38}$$

Nous notons par $\pi\colon E\to E/\sim$ la projection canonique. L'application

$$\begin{aligned} g\colon E/\sim &\to F\\ [x] &\mapsto f(x) \end{aligned} \tag{1.39}$$

est bien définie et injective[18]. Elle n'est pas surjective tant que f ne l'est pas. La **décomposition canonique** de f est

$$f = g \circ \pi. \tag{1.40}$$

△

La proposition suivante est souvent utilisée pour créer un majorant quand on veut vérifier les hypothèses du lemme de Zorn.

PROPooKXBGooJYUbtF

Proposition 1.61 ([1])**.**
Soit un ensemble d'ensembles $\{X_i\}_{i\in I}$ et des applications $f_i\colon X_i \to A$ telles que

$$f_i(x) = f_j(x) \tag{1.41}$$

pour tout $i, j \in I$ et $x \in X_i \cap X_j$. Nous posons $X = \bigcup_{i\in I} X_i$.

Alors il existe une unique application $f\colon X \to A$ telle que $f(x) = f_i(x)$ pour tout $i \in I$ et $x \in X$ tels que $x \in X_i$.

Démonstration. Nous commençons par prouver l'existence. Pour chaque $x \in X$ nous posons $I_x = \{i \in I \text{ tel que } x \in X_i\}$, et nous posons

$$\begin{aligned} \varphi_x\colon I_x &\to A \\ i &\mapsto f_i(x). \end{aligned} \tag{1.42}$$

Prouvons que $\varphi_x\colon I_x \to A$ est constante. Soient $i, j \in I_x$. Alors $\varphi_x(i) = f_i(x)$ et $\varphi_x(j) = f_j(x)$. Vu que $i \in I_x$, nous avons $x \in X_i$ et vu que $j \in I_x$, nous avons $x \in X_j$. Donc $x \in X_i \cap X_j$, et par hypothèse, $f_i(x) = f_j(x)$. Cela montre que $\varphi_x(i) = \varphi_x(j)$.

Et nous posons

$$f(x) = e\big(\varphi_x(I_x)\big) \tag{1.43}$$

où e est l'application qui à un singleton fait correspondre l'élément qui est dedans.

Soient $i \in I$ et $x \in X$ tels que $x \in X_i$. Alors $f_i(x) \in \varphi_x(I_x)$ et donc $\varphi_x\big(I_x\big) = \{f_i(x)\}$ et finalement $f(x) = f_i(x)$.

En ce qui concerne l'unicité, nous supposons que $f\colon X \to A$ et $g\colon X \to A$ aient les propriétés requises. Soit $x \in X$; il existe $i \in I$ tel que $x \in X_i$. Pour un tel i, nous avons $f(x) = f_i(x)$ et $g(x) = f_i(x)$ et donc $f(x) = g(x)$. □

1.2.10 Relations ternaires, opérations

NORMooRelationsTernaires

1.62.
Comme pour les fonctions construites sur base des relations binaires, on peut en construire pour les relations ternaires[19].

NORMooFonctionDeuxVariables

1.63.
Soit G une relation ternaire sur les ensembles $E_1,\ E_2,\ E_3$. Supposons que, étant donnés $x_1 \in E_1$ et $x_2 \in E_2$, il existe un unique $x_3 \in E_3$ tel que $(x_1, x_2, x_3) \in G$. On définit alors la fonction

$$\begin{aligned} f\colon E_1 \times E_2 &\to E_3 \\ (x_1, x_2) &\mapsto \text{le } x_3 \text{ dans la relation } G. \end{aligned} \tag{1.44}$$

DEFooOperation

Définition 1.64.
*On appelle **opération** sur l'ensemble E une fonction définie sur $E \times E$ et à valeurs dans E. Cette opération peut être notée sous forme préfixe ($f(x, y)$) ou sous forme infixe, c'est-à-dire entre les deux éléments que l'on opère ($x * y$).*

*Parfois, on dit aussi que $*$ est une **loi de composition interne** sur E, ou encore que E, muni de l'opération $*$, est un **magma**.*

DEFooMagmaNeutre

Définition 1.65 (neutres dans un magma)**.**
Soit E un ensemble muni d'une opération $*\colon E \times E \to E$. On dit d'un élément $e \in E$ qu'il est :

*(1) **neutre à gauche** si, pour tout $x \in E$, on ait $e * x = x$;*

*(2) **neutre à droite** si, pour tout $x \in E$, on ait $x * e = x$;*

[18] Proposition 1.58.
[19] Voire des relations avec plus d'ensembles, mais nous n'en avons pas (encore) besoin.

(3) ***neutre*** *s'il est neutre à gauche et à droite.*

PROPooDEFMagmaUnifere

Proposition-Définition 1.66.
Soit $(E,*)$ un magma admettant un neutre à gauche $e\in E$ et un neutre à droite $n\in E$. Alors :

(1) on a $e=n$;

*(2) il n'y a pas d'autre neutre (à gauche ou à droite) que e*ă*.*

Ainsi, l'élément e est appelé ***neutre*** *du magma $(E,*)$ et on dit que E est un* ***magma unifère****.*

Démonstration. On sait que $e*n$ vaut n, car e est neutre à gauche, mais vaut aussi e car n est neutre à droite. Bref, on a

$$n=e*n=e.$$

Si e' était un autre neutre à gauche, alors $e'=e'*n=n=e$: la première égalité venant du fait que n est neutre à droite, la deuxième que e' est neutre à gauche, la troisième de l'égalité ci-dessus. De la même façon, si n' était un autre neutre à droite, alors $n'=e*n'=e=n$. □

DEFooMagmaCommutatif

Définition 1.67 (magma commutatif)**.**
Soit E un ensemble muni d'une opération $*\colon E\times E\to E$. On dit que E est un ***magma commutatif*** *si pour tout $x,y\in E$, on a $x*y=y*x$.*

DEFooIJIEooZaAdSs

Définition 1.68 (élément régulier[21])**.**
Soit un ensemble E muni d'une opération $*\colon E\times E\to E$. Un élément $s\in E$ est ***régulier à gauche*** *si pour tout $x,y\in E$ nous avons*

$$s*x=s*y\Rightarrow x=y. \tag{1.45}$$

L'élément s est ***régulier à droite*** *si pour tout $x,y\in E$ nous avons*

$$x*s=y*s\Rightarrow x=y. \tag{1.46}$$

Il est ***régulier*** *si il est régulier à gauche et à droite.*

REMooMagmasEltsReguliers

Remarque 1.69.
Dans un magma E, si e est un neutre à gauche (respectivement à droite), alors il est forcément régulier à gauche (resp. à droite).

On verra plus tard la notion de groupe[20], qui étend celle de magma : nous verrons que tous les éléments d'un groupe sont réguliers, et pour cause : ils admettent tous un inverse qui permet de simplifier.

On aura plus tard la notion d'anneau[21]. Dans ce cadre, la régularité des éléments vis-à-vis de l'opération de multiplication sera moins évidente ; en particulier, elle sera loin d'être automatique.

1.3 Cardinalité

SECooCardinalite

1.3.1 Équipotence, surpotence, subpotence

NOTAooEquiSurSubpotence

1.70.
Les notions d'équipotence, surpotence et de subpotence permettent de comparer les « tailles » des ensembles sans avoir besoin de la théorie des ordinaux. Tout ceci ne sera pas très souvent utile par la suite. Un exemple d'utilisation de ces notions est le théorème de Steinitz 8.134 qui démontre l'existence de clôture algébrique pour tout corps.

DEFooXGXZooIgcBCg

Définition 1.71 ([22, 23])**.**
Soient deux ensembles A et B.

(1) Les ensembles A et B sont ***équipotents*** *si il existe une bijection entre A et B. Nous notons $A\approx B$.*

(2) L'ensemble A est ***surpotent*** *à B si il existe une surjection de A vers B. Nous notons $A\succeq B$.*

(3) L'ensemble A est ***subpotent*** *à B si il existe une injection de A vers B. Nous notons $A\preceq B$.*

Nous disons également « strictement » surpotent quand il y a surpotence mais pas équipotence, et de même pour la subpotence. Les symboles $\succ$ et $\prec$ sont alors utilisés.

[20] Définition 1.92.
[21] Définition 1.100.

PROPooWSXTooMQPcNG

Proposition 1.72 ([1, 18]).
L'ensemble A est subpotent à B si et seulement si B est surpotent à A.

Démonstration. En deux parties.

(1) $\underline{\Rightarrow}$ Nous supposons que A est subpotent à B. Il existe une injection $\varphi\colon A \to B$. Nous définissons $f\colon B \to A$ par

$$f(x) = \begin{cases} \varphi^{-1}(x) & \text{si } x \in \varphi(A) \\ a & \text{sinon} \end{cases} \tag{1.47}$$

où a est un élément quelconque de A. Cette application est bien définie parce que φ est injective, de telle sorte que φ^{-1} est bien définie. Puisque φ est définie sur tout A, l'application f est une surjection.

(2) $\underline{\Leftarrow}$ Nous supposons que B est surpotent à A. Il existe donc une surjection $\varphi\colon B \to A$. Pour chaque $x \in A$ nous considérons un élément $b_x \in \varphi^{-1}(x)$, qui existe parce que φ est surjective. Nous considérons ensuite l'application

$$\begin{aligned} f\colon A &\to B \\ x &\mapsto b_x. \end{aligned} \tag{1.48}$$

Nous prouvons que f est une injection. Supposons que $x, y \in A$ soient tels que $f(x) = f(y)$. Nous avons $b_x = b_y$. Donc

$$x = \varphi(b_x) = \varphi(b_y) = y. \tag{1.49}$$

Nous avons prouvé que $x = y$, et donc que f est injective.

□

1.3.2 Un peu d'infinité

NORooPasDeClassesi

1.73.
Vu que l'ensemble des ensembles n'existe pas[22], nous n'allons pas énoncer le fait que ces notions donnent une relation d'ordre sur les ensembles ; il faudrait parler de classes et nous ne nous en sortirions pas. Nous allons toutefois énoncer quelques résultats qui vont dans ce sens. Pour en savoir plus, vous pouvez lire les différentes pages de Wikipédia sur les nombres cardinaux.

DefEOZLooUMCzZR

Définition 1.74 (ensemble Dedekind infini).
*Un ensemble est **infini** si il peut être mis en bijection avec un de ses sous-ensembles propres (c'est-à-dire différent de lui-même).*

*Un ensemble est **fini** si il n'est pas infini.*

NORooQuelleDefEnsInfini

1.75.
Nous adoptons les notions d'ensembles finis et infinis au sens de Dedekind. De nombreuses sources (dont Wikipédia [24, 25]) définissent un ensemble fini comme étant un ensemble en bijection avec une partie de $\mathbb{N}$ de la forme $\{0, \dots, N\}$. Alors un ensemble est infini si il n'est pas fini.

Cependant, d'une part *les deux définitions d'ensembles infinis ne sont pas équivalentes*, mais d'autre part, elles sont équivalentes si on accepte l'axiome du choix[23]. Or le Frido accepte l'axiome du choix sans vergogne et sous toutes ses formes. Nous démontrerons donc, en utilisant le lemme de Zorn, qu'un ensemble A est fini (définition 1.74) si et seulement si il existe une bijection $\{0, \dots, N\} \to A$ pour un certain $N \in \mathbb{N}$. Ce sera le théorème 2.24.

LEMooTUIRooEXjfDY

Lemme 1.76.
Toute partie d'un ensemble fini est finie.

Démonstration. Nous allons prouver la contraposée : si un ensemble contient une partie infinie, alors il est infini. Soit $A \subset B$ où A est infini. Nous allons prouver que B est infini. En vertu de la définition 1.74, il existe une partie $A' \subsetneq A$ et une bijection $\sigma\colon A' \to A$.

Nous considérons la partie $B' = A' \cup (B \setminus A)$, qui est une partie stricte de B. Puisque $A' \cap (B \setminus A) = \varnothing$, nous pouvons définir

$$\begin{aligned} \varphi\colon B' &\to B \\ x &\mapsto \begin{cases} \sigma(x) & \text{si } x \in A' \\ x & \text{si } x \in B \setminus A. \end{cases} \end{aligned} \tag{1.50}$$

[22] Voir le corolaire 1.90.
[23] Et même seulement l'axiome du choix dénombrable ; si vous voulez en savoir plus, lisez la page Wikipédia [26].

Montrons que φ est une bijection.

(1) **Surjectif** Nous avons $\varphi(A') = A$ et $\varphi(B \setminus A) = B \setminus A$. Donc

$$\varphi(B') = \varphi(A') \cup \varphi(B \setminus A) = A \cup (B \setminus A) = B. \tag{1.51}$$

(2) **Injectif** Si $\varphi(x) = \varphi(y)$, nous avons 4 possibilités suivant que x et y sont dans A' ou $B \setminus A$.

Si $x, y \in A'$, alors $\varphi(x) = \varphi(y)$ implique $\sigma(x) = \sigma(y)$ et donc $x = y$ parce que σ est injective.

Si $x \in A'$ et $y \in B \setminus A$ alors $\varphi(x) = \sigma(x) \in A$ et $\varphi(y) = y \in B \setminus A$. Ce cas n'est pas possible. Le cas $x \in B \setminus A$ et $y \in A'$ n'est pas possible non plus.

Si $x, y \in B \setminus A$, alors $\varphi(x) = \varphi(y)$ implique immédiatement $x = y$.

Nous avons une bijection entre B' et B alors que B' est un sous-ensemble strict de B. Donc B est infini. □

Voici une proposition qui dit que si on n'a pas de maximum, on est infini. Une preuve alternative beaucoup plus simple[24] sera donnée dans le lemme 2.31. Ici, nous démontrons sans utiliser la construction des naturels.

PROPooVZRVooAncMjb

Proposition 1.77 ([27])**.**
Si $(A, \leqslant)$ est un ensemble totalement ordonné[25] fini, alors il a un maximum[26].

Démonstration. Nous considérons un ensemble totalement ordonné A (que nous supposons non vide). Nous supposons que A n'a pas de maximum et nous démontrons que A est infini. Nous fixons un élément $a \in A$ et nous considérons l'ensemble suivant :

$$\mathcal{A} = \Big\{ (X, f) \text{ tel que } \begin{cases} X \subset A \\ f : X \to A \text{ est injective} \\ X \setminus f(X) = \{a\} \\ f(X) \setminus X = \varnothing \text{ ou } f(X) \setminus X = \max\big(f(X)\big) \end{cases} \Big\}. \tag{1.52}$$

Nous ordonnons les couples (X, f) en disant que $(X_1, f_1) \leqslant (X_2, f_2)$ lorsque $X_1 \subset X_2$ et $f_1(x) = f_2(x)$ pour tout $x \in X_1$, c'est-à-dire lorsque f_2 étend f_1.

Nous rappelons que si une partie a un maximum, alors le maximum est unique par 1.34. Nous ne le répéterons pas à chaque fois.

(1) **$\mathcal{A}$ est non vide** Vu que A n'a pas de maximum, il existe $b \in A$ avec $b > a$. Alors l'application $f : \{a\} \to \{b\}$ est une bijection et $\big(\{a\}, f\big) \in \mathcal{A}$ parce que $\{a\} \setminus \{b\} = \{a\}$ et $\{b\} \setminus \{a\} = \{b\} = \max(\{b\})$.

(2) **$\mathcal{A}$ est inductif** Nous considérons une partie totalement ordonnée $\mathcal{F} = \{(X_i, f_i)\}_{i \in I}$ et nous montrons qu'elle admet un majorant dans $\mathcal{A}$. Nous posons $X_u = \bigcup_{i \in I} X_i$, et nous considérons l'unique application $f_u : X \to A$ vérifiant[27] $f_u(x) = f_i(x)$ dès que $x \in X_i$.

Le fait que (X_u, f_u) soit un majorant de $\mathcal{F}$ est immédiat. Ce qui est moins immédiat est que $(X_u, f_u) \in \mathcal{A}$. C'est ce que nous prouvons à présent.

(2a) $X_u \subset A$ Parce que X_u est une réunion de parties de A. Ok. Ça commence facile.

(2b) **f_u est injective** Soient $x, y \in X_u$ tels que $f_u(x) = f_u(y)$. Il existe $i, j \in I$ tels que $x \in X_i$ et $y \in X_j$. Supposons que $X_i \subset X_j$ (si c'est pas le cas, il faut juste inverser i et j dans ce que qui suit). Alors $f_u(x) = f_j(x)$ et $f_u(y) = f_j(y)$. Mais comme f_j est injective, nous en déduisons que $x = y$.

(2c) $X_u \setminus f_u(X_u) = \{a\}$ Vu que $\mathcal{F}$ est non vide, il contient un (X_i, f_i) où X_i vérifie $X_i \setminus f(X_i) = \{a\}$. Nous avons alors $a \in X_i \subset X_u$. Mais $f(X_u) = \bigcup_{i \in I} f(X_i)$ alors que a n'est dans aucun des $f(X_i)$. Donc a n'est pas dans $f(X_u)$. Bref $a \in X_u \setminus f(X_u)$. Il nous reste à prouver que a est le seule élément de $X_u \setminus f(X_u)$.

Soit $b \in X_u \setminus f(X_u)$. Vu que $b \in X_u$, il existe $i \in I$ tel que $b \in X_i$. Il y a deux possibilités : soit $b \in f(X_i)$ soit non. Si oui, alors $b \in f(X_i) \subset f(X_u)$ alors que nous venions de dire que $b \notin f(X_u)$. Pas possible. Donc $b \notin f(X_i)$. Dans ce cas, $b \in X_i \setminus f(X_i) = \{a\}$ et donc $b = a$.

[24] Plus simple ? À nuancer parce que celle que nous donnons ici ne demande pas la construction de $\mathbb{N}$ – qui est un gros morceau.
[25] Définition 1.26.
[26] Définition 1.32.
[27] Penser à utiliser la proposition 1.58 pour vérifier que ça existe et que c'est unique.

(2d) $f(X_u) \setminus X_u = \varnothing$ **ou** $f(X_u) \setminus X_u = \max\big(f(X_u)\big)$ Si $f(X_u)\setminus X_u = \varnothing$ on est bon. Nous supposons que ce n'est pas le cas et nous prouvons que si $y \in f(X_u) \setminus X_u$, alors $y = \max\big(f(X_u)\big)$.

Soit $z \in f(X_u)$. Vu que $y, z \in f(X_u)$ il existe des $i, j \in I$ tels que $y \in f_i(X_i)$ et $z \in f_j(X_j)$. Étant donné que $\mathcal{F}$ est totalement ordonné, nous avons $(X_i, f_i) \leqslant (X_j, f_j)$ ou le contraire. Nous posons

$$(X_0, f_0) = \max\big\{(X_i, f_i), (X_j, f_j)\big\}. \tag{1.53}$$

Nous avons $X_i \subset X_0$ et $X_j \subset X_0$ et donc $f_i = f_j$ sur X_0 et donc $x, y \in f_0(x_0)$. Rappel que nous avions pris $y \in f(X_u) \setminus X_u$. Et particulier $y \notin X_0$ parce que $X_0 \subset X_u$. Donc $y \in f_0(X_0) \setminus X_0$.
Vu que $(X_0, f_0) \in \mathcal{F}$, nous avons $y = \max\big(f(X_0)\big)$. Et comme $z \in f(X_0)$ nous avons $y \geqslant z$. Nous avons prouvé que y est un majorant de $f(X_u)$. Vu que $y \in f(X_u)$, il est bien le maximum.
Nous avons montré que si $y \in f(X_u) \setminus X_u$, alors $y = \max\big(f(X_u)\big)$. Nous en déduisons que $f(X_u) \setminus X_u = \max\big(X_u\big)$.

Et voilà. Le lemme de Zorn 1.42 s'applique : $\mathcal{A}$ a un élément maximal que nous allons nommer (X_m, f_m). Nous pouvons passer à la suite.

(1) $f(X_m) \setminus X_m = \varnothing$

Supposons que ce ne soit pas le cas. Alors $f(X_m)\setminus X_m = \{y\}$ où $y = \max\big(f_m(X_m)\big)$. Mais nous avons dit par hypothèse que A n'avait pas de maximum. Donc ni y ni a n'en sont et il existe $z \in A$ tel que $z > \max(a, y)$. Nous posons

$$X_M = X_m \cup \{y\}. \tag{1.54}$$

Vu que y n'est pas dans X_m, la partie X_M est strictement plus grande que X_m. Nous prenons ensuite $f_M\colon X_M \to f(X_m) \cup \{z\}$ qui étend f_m en posant $f_M(y) = z$.

Nous prouvons que $(X_M, f_M) \in \mathcal{A}$.

(1a) f_M **est injective** C'est parce que f_m est injective et que $f_M(y) = z$ alors que z n'est pas dans $f_M(X_m)$ parce que

$$z > \max(a, y) \geqslant y = \max\big(f_m(X_m)\big). \tag{1.55}$$

(1b) $X_M \setminus f_M(X_M) = \{a\}$ Nous avons $a \in X_m \setminus f_m(X_m)$. Donc $a \in X_m \subset X_M$ et a est hors de $f_m(X_m)$. Mais $f_M(X_M) = f_m(X_m) \cup \{z\}$. Vu que $a \neq z$ nous avons bien $a \neq f_M(X_M)$ et donc $a \in X_M \setminus f_M(X_M)$. Reste à prouver que a est tout seul dans $X_M \setminus f_M(X_M)$.
Soit $b \in X_M \setminus f_M(X_M)$. Notre objectif est de prouver soit que $b = a$ soit de trouver une absurdité. Il y a deux possibilités : soit $b \in X_m$ soit $b = y$.

(1b.i) **Si** $b \in X_m$ Dans ce cas, $b \in X_M \setminus f_M(X_M)$ et $b \in X_m$. Donc

$$b \in X_m \setminus f_M(X_M) = X_m \setminus \big(f_m(X_m) \cup \{z\}\big) \subset X_m \setminus f_m(X_m) = \{a\} \tag{1.56}$$

parce que $(X_m, f_m) \in \mathcal{A}$. Donc $b = a$.

(1b.ii) **Si** $b = y$ Ici il y a une impossibilité parce que d'une part $y = \max\big(f_m(X_m)\big)$, mais d'autre part $y = b \in X_M \setminus f_M(X_M)$. Donc b n'est pas dans $f_M(X_M)$, qui contient $f_m(X_m)$.

Nous avons montré que $b = a$ et donc que $X_M \setminus f_M(X_M) = \{a\}$.

(1c) $z = \max\big(f_M(X_M)\big)$ Nous avons choisi $z > \max(a, y)$ et $X_M = X_m \cup \{y\}$. Donc $z > y = \max\big(f_m(X_m)\big)$ et $z \geqslant z$, donc

$$z \geqslant \max\big(f_m(X_m) \cup \{z\}\big) = \max\big(f_M(X_M)\big). \tag{1.57}$$

Mais comme en même temps $z = f_M(y) \in f_M(X_M)$, nous avons $z = \max\big(f_M(X_M)\big)$.

(1d) $f_M(X_M) \setminus X_M = \{z\}$ En plusieurs points.

(1d.i) $z \in f_M(X_M)$ Parce que $z = f_M(y)$.

(1d.ii) $z \notin X_M$ Supposons que $z \in X_M$ et déduisons une absurdité. Il y a deux possibilités : soit $z \in X_m$ soit $z = y$. Vu que $z > \max(a, y)$ la seconde possibilité est exclue. Reste $z \in X_m$. Vu que

$$z > \max(a, y) \geqslant y = \max\big(f_m(X_m)\big)), \tag{1.58}$$

nous avons $z \notin f_m(X_m)$. Donc $z \in X_m \setminus f_m(X_m) = \{a\}$. Donc $z = a$, qui n'est pas possible parce que $y > \max(a, y) \geqslant a$.
Nous avons donc bien démontré que $z \notin X_M$.

(1d.iii) z **est seul dans** $f_M(X_M) \setminus X_M$ Soit $z' \in f_M(X_M) \setminus X_M$. Vu que $f_M(X_M) = f_m(X_m) \cup \{z\}$, nous avons deux possibilités : soit $z' \in f_m(X_m)$ soit $z' = z$. Le seconde possibilité nous va parfaitement.
Voyons ce qu'il se passe si $z' \in f_m(X_m)$. Nous avons

$$z' \in f_m(X_m) \setminus X_M \subset f_m(X_m) \setminus X_m = \{y\}. \tag{1.59}$$

Mais il n'est pas possible d'avoir $z' = y$ parce que $y \in X_M$ alors que $z' \notin X_M$.

Nous avons fini de prouver que $(X_M, f_M) \in \mathcal{A}$. Par construction nous avons cependant que $(X_M, f_M) \geqslant (X_m, f_m)$, qui contredit la maximalité de (X_m, f_m). Nous en déduisons que le y n'existe pas et donc que $f_m(X_m) \setminus X_m = \varnothing$.

(2) **La suite** Ici nous savons que $f_m(X_m) \setminus X_m = \varnothing$. L'application $f_m \colon X_m \to f_m(X_m)$ est une bijection vérifiant

(2a) $X_m \setminus f_m(X_m) = \{a\}$
(2b) $f_m(X_m) \setminus X_m = \varnothing$.

Notez que le deuxième point implique que $f_m(X_m) \subset X_m$.

(3) **L'application** g Nous considérons l'application

$$\begin{aligned} g \colon A &\to A \\ x &\mapsto \begin{cases} f_m(x) & \text{si } x \in X_m \\ x & \text{sinon.} \end{cases} \end{aligned} \tag{1.60}$$

(4) g **est injective** Il y a 4 possibilités suivant que x et y sont dans X_m ou non.

(4a) **Si** $x, y \in X_m$ Alors $g(x) = f_m(x)$ et $g(y) = f_m(y)$. Donc $f_m(x) = f_m(y)$ et donc $x = y$ parce que f_m est injective.

(4b) **Si** $x \in X_m$ **et** $y \notin X_m$ Alors

$$g(x) = f_m(x) \in f_m(X_m) \subset X_m, \tag{1.61}$$

alors que $g(y) \notin X_m$. Il n'est donc pas possible que $g(x) = g(y)$ dans ce cas.

(4c) **Si** $x, y \notin X_m$ Alors $g(x) = x$ et $g(y) = y$. Et donc $x = y$.

Cela prouve que g est injective.

(5) $a \notin g(A)$ Supposons que $a = g(x)$ pour un certain $x \in A$. Il y a deux possibilités : $x \in X_m$ ou $x \notin X_m$.
Dans le premier cas, nous avons $a = g(x) = f_m(x) \in f_m(X_m)$ qui n'est pas possible parce que $a \notin f_m(X_m)$ du fait que $X_m \setminus f_m(X_m) = \{a\}$.

Dans le second cas, nous avons $a = g(x) = x \notin X_m$, qui n'est pas possible parce que nous savons que $x \in X_m$.

(6) **Conclusion** Nous avons construit une injection $g \colon A \to A \setminus \{a\}$. Cela prouve que A est infini.

□

PROPooVOKDooOStPzU

Proposition 1.78 ([1, 18])**.**
Si A est fini et si $\omega \notin A$, alors $A \cup \{\omega\}$ est fini.

Démonstration. Supposons que $A \cup \{\omega\}$ est infini. Il existe un sous-ensemble strict de $A \cup \{\omega\}$ en bijection avec $A \cup \{\omega\}$. Soient donc $B \subsetneq A \cup \{\omega\}$ et $\sigma \colon B \to A \cup \{\omega\}$ une bijection.
Il y a deux possibilités : soit ω est dans B, soit non.

(1) $\omega \notin B$ Alors $B \subset A$, et il existe $x \in B$ tel que $\sigma(x) = \omega$. Considérons $B' = B \setminus \{x\}$; cela est une partie propre de A. Ensuite nous définissons

$$\begin{aligned} \varphi \colon B \setminus \{x\} &\to A \\ a &\mapsto \sigma(a). \end{aligned} \tag{1.62}$$

C'est injectif parce que σ est injective, et c'est surjectif parce que

$$\varphi\big(B \setminus \{x\}\big) = \sigma(B) \setminus \sigma(\{\omega\}) = \sigma(B) \setminus \{\omega\} = (A \cup \{\omega\}) \setminus \{\omega\} = A. \tag{1.63}$$

Pour la dernière égalité nous avons utilisé le fait que ω n'est pas dans A.

(2) **Si $\omega \in B$** Plusieurs choses à dire.

(2a) $\sigma(\omega) \neq \omega$
Si $\omega \in B$, nous commençons par prouver que $\sigma(\omega) \neq \omega$. En effet si $\sigma(\omega) = \omega$, alors nous pouvons poser

$$\begin{aligned} \sigma' \colon B \setminus \{\omega\} &\to A \\ x &\mapsto \sigma(x). \end{aligned} \tag{1.64}$$

Ce σ' est une bijection entre A et la partie propre $B \setminus \{A\}$. Cela est impossible parce que nous avons supposé que A est fini.

(2b) **Definition de φ** Puisque B est une partie propre de $A \cup \{\omega\}$, il existe $x \in A \setminus B$. Nous considérons $B' = \big(B \setminus \{\omega\}\big) \cup \{x\}$ et nous définissons

$$\begin{aligned} \varphi \colon B' &\to A \\ b &\mapsto \begin{cases} \sigma(b) & \text{si } b \neq x \\ \sigma(\omega) & \text{si } b = x. \end{cases} \end{aligned} \tag{1.65}$$

Nous montrons à présent que φ est une bijection.

(2c) **Injectif** Soient $u, v \in B'$ tels que $\varphi(u) = \varphi(v)$. Il y a 4 possibilités suivant que u ou v est égal à x.

- Si $u = v = x$ on est bon.
- Si $u = x$ et $v \neq x$. D'une part $\varphi(u) = \varphi(v) = \sigma(v)$ parce que $v \neq x$. Mais d'autre part $\varphi(u) = \varphi(x) = \sigma(\omega)$. Donc $\sigma(v) = \sigma(\omega)$ et $v = \omega$ par injectivité de σ. Or cela est impossible parce que $v \in B'$ alors que $\omega \notin B'$. Ici nous utilisons le fait que ω ne peut pas être égal à x parce que $x \in A$ alors que ω est hors de A.
  Bref, ce cas est impossible.
- Si $u \neq x$ et $v = x$, alors c'est le même cas que le précédent avec quelques adaptations.
- Si $u \neq x$ et $v \neq x$, alors $\varphi(u) = \sigma(u)$ et $\varphi(v) = \sigma(v)$, de telle sorte que $\sigma(u) = \sigma(v)$ et donc $u = v$ par injectivité de σ.

(2d) **Surjective** Soit $y \in A$. Vu que $\sigma \colon B \to A \cup \{\omega\}$ est surjective, il existe $b \in B$ tel que $\sigma(b) = y$. Notez que $b \neq x$ parce que $x \in A \setminus B$.
Si $b \neq \omega$ alors $b \in B \setminus \{\omega\} \subset B'$. Nous pouvons calculer $\varphi(b)$. Étant donné que $b \neq x$, nous avons $\varphi(b) = \sigma(b) = y$.
Si au contraire $b = \omega$, alors $\varphi(x) = \sigma(\omega) = y$. Dans les deux cas, y est dans l'image de φ.

Dans tous les cas nous avons construit une bijection entre une partie propre $B' \subsetneq A$ et A, ce qui est absurde parce que A est un ensemble fini. □

PROPooWKSIooHcfYPN

Proposition 1.79 ([1]).
Si A est infini et si $\sigma \colon A \to B$ est injective, alors B est infini.

Démonstration. Nous allons prouver que $\sigma(A)$ est une partie infinie de B. Puisque A est infini, nous pouvons considérer une partie $A' \subsetneq A$ et une bijection $\varphi_A \colon A' \to A$. Nous définissons

$$\begin{aligned} \varphi_B \colon \sigma(A') &\to \sigma(A) \\ y &\mapsto \sigma\Big(\varphi_A\big(\sigma^{-1}(y)\big)\Big). \end{aligned} \tag{1.66}$$

Cette définition a un sens parce que si $y \in \sigma(A')$, alors il existe un unique $x \in A'$ tel que $\sigma(x) = y$ parce que σ est injective. De là, $\varphi_A(x) \in A$ et nous pouvons lui appliquer σ.

Nous montrons que φ_B est une bijection.

(1) **Injective** Supposons que $\varphi_B(a) = \varphi_B(b)$, c'est-à-dire que

$$(\sigma \circ \varphi_A \circ \sigma^{-1})(a) = (\sigma \circ \varphi_A \circ \sigma^{-1})(b). \tag{1.67}$$

Étant donné que σ et φ_A sont injectives, nous avons $\sigma^{-1}(a) = \sigma^{-1}(b)$. En appliquant σ des deux côtés, nous trouvons $a = b$.

(2) **surjective** Soit $y \in \sigma(A)$. En prenant $x \in (\sigma \circ \varphi_A^{-1} \circ \sigma^{-1})(y)$ nous avons $\varphi_B(x) = y$.

Donc B contient une partie infinie ($\sigma(A)$). Le lemme 1.76 conclut que B est infini. □

LEMooPGPVooZzlFvf

Lemme 1.80.
À propos d'applications entre ensembles finis.

ITEMooNCCUooBGrtdn

(1) Si $\sigma\colon A \to B$ est une application quelconque et si A est fini, alors $\sigma(A)$ est une partie finie de B.

ITEMooKQMFooSzmXrd

(2) Si $\sigma\colon A \to B$ est surjective et si A est fini, alors B est fini.

Démonstration. Nous allons utiliser le lemme de Zorn. Nous considérons l'ensemble

$$\mathcal{A} = \{X \subset A \text{ tel que } \sigma\colon X \to \sigma(A) \text{ est injective}\} \tag{1.68}$$

que nous ordonnons (partiellement) par l'inclusion.

(1) **$\mathcal{A}$ est inductif** Soit une partie totalement ordonnée $\mathcal{F}$ de $\mathcal{A}$. Nous considérons $Y = \bigcup_{X\in\mathcal{F}} X$, et nous prouvons que Y est un majorant de $\mathcal{F}$.

Pour cela nous commençons par prouver que $Y \in \mathcal{A}$. Soient $a, b \in Y$ tels que $\sigma(a) = \sigma(b)$. Il existe $X_1, X_2 \in \mathcal{F}$ tels que $a \in X_1$ et $b \in X_2$. Supposons pour fixer les idées que $X_1 \leqslant X_2$ ($\mathcal{F}$ étant totalement ordonné nous avons toujours $X_1 \leqslant X_2$ ou $X_2 \leqslant X_1$). Puisque l'ordre est l'inclusion, cela signifie que $X_1 \subset X_2$. Nous avons donc $a, b \in X_2$, alors que σ est injective sur X_2. Donc $\sigma(a) = \sigma(b)$ implique $a = b$, et σ est injective sur Y. Nous avons donc prouvé que $Y \in \mathcal{A}$.

Puisque pour tout $X \in \mathcal{F}$ nous avons $X \subset Y$, nous avons $X \leqslant Y$ (dans $\mathcal{A}$) pour tout $X \in \mathcal{F}$. Bref, Y est un majorant de $\mathcal{F}$ dans $\mathcal{A}$.

Toute partie totalement ordonnée de $\mathcal{A}$ est majorée. Cela signifie que $\mathcal{A}$ est inductif[28].

(2) **Zorn** L'ensemble $\mathcal{A}$ étant inductif et non vide (les singletons dans A sont dans $\mathcal{A}$), il possède un élément maximal[29] par le lemme de Zorn 1.42. Nous nommons A' un élément maximal dans $\mathcal{A}$.

(3) **Bijective** L'application $\sigma\colon A' \to \sigma(A)$ est injective parce que $A' \in \mathcal{A}$. Nous devons prouver qu'elle est surjective.

Supposons que $y \in \sigma(A) \setminus \sigma(A')$. Alors il existe $a \in A \setminus A'$ tel que $\sigma(a) = y$. Dans ce cas, la partie $A' \cup \{a\}$ est un majorant de A' dans $\mathcal{A}$, ce qui est impossible.

Donc $\sigma\colon A' \to \sigma(A)$ est bijective.

(4) **Conclusion** L'ensemble A' est fini en tant que partie de l'ensemble fini A (lemme 1.76). L'application σ étant injective, la proposition 1.79 conclut que $\sigma(A')$ est fini. Et comme $\sigma(A')$ n'est autre que $\sigma(A)$ nous avons fini.

La partie (1) est prouvée. La partie (2) est maintenant facile. La partie (1) dit que $\sigma(A)$ est une partie finie de B, mais si σ est surjective, alors $\sigma(A) = B$. □

PROPooGJLEooCQdegS

Proposition 1.81 ([1]).
Toute union finie d'ensembles finis et finie.

PROPooYCDWooXBWVrW

Proposition 1.82 ([1]).
Soient un ensemble infini A, un ensemble fini B et une application $\phi\colon A \to B$. Alors il existe un $s \in B$ tel que $\phi^{-1}(s)$ est infini.

Démonstration. Nous avons $A = \bigcup_{b\in B} \phi^{-1}(b)$. Donc si $\phi^{-1}(b)$ était fini pour tout $b \in B$, l'ensemble A serait une union finie d'ensembles finis et donc fini par la proposition 1.81. □

1.3.3 Théorème de Cantor-Schröder-Bernstein

SUBooCaEMrSCTNoMHoBeBpstein

Lemme 1.83 ([28]).
Soient un ensemble A et une partie B de A. Si il existe une injection $f\colon A \to B$ alors il existe une bijection $\alpha\colon A \to B$.

Nous donnons deux preuves de ce lemme.

Première preuve de 1.83. Nous posons $Y = A \setminus B$ et nous décomposons la preuve en étapes.

[28] Plus précisément c'est l'ensemble ordonné $(\mathcal{A}, \subset)$ qui est inductif.
[29] Définition 1.33 ; voir aussi 1.37.

(1) **Les $f^k(Y)$ sont disjoints** Vu que f prend ses valeurs dans B, nous avons $f^k(Y) \subset B$ pour tout k. Et vu que $Y = A \setminus B$, nous avons

$$f^k(Y) \cap Y = \varnothing \tag{1.69}$$

EQooDNHJooFJBrDq

pour tout k. L'application f étant injective, elle vérifie $f(C \cap D) = f(C) \cap f(D)$. Nous appliquons f^m des deux côtés de (1.69) :

$$f^{k+m}(Y) \cap f^m(Y) = \varnothing \tag{1.70}$$

pour tout $k, m \in \mathbb{N}$.

(2) **Une décomposition** Nous posons

$$X = \bigcup_{k\in\mathbb{N}} f^k(Y) = Y \cup \bigcup_{k=1}^{\infty} f^k(Y). \tag{1.71}$$

Vu que $f(X) \subset B$ nous avons l'égalité

$$B = f(X) \cup \big(B \setminus f(X)\big). \tag{1.72}$$

(3) **$A \setminus X = B \setminus f(X)$** Supposons $x \in A \setminus X$. Vu que $Y = A \setminus B$ est dans X, l'élément x n'est pas dans $A \setminus B$ et donc est dans B parce qu'il est dans A. Mais x n'est pas dans X et en particulier pas dans $f(X)$ parce que $f(X) \subset X$. Donc x est dans $B \setminus f(X)$.

Dans l'autre sens, nous supposons que $x \in B \setminus f(X)$. Vu que $B \subset A$ nous avons $x \in A$. Comme x est hors de $f(X)$, il est hors des $f^k(Y)$ pour $k \geqslant 1$. Mais $x \in B$, donc x est hors de $A \setminus B = f^0(Y)$. Donc x est hors de $f^k(Y)$ pour tout $k \geqslant 0$. Donc x est hors de X.

(4) **La bijection** Nous considérons l'application

$$\begin{aligned} \alpha\colon A &\to B \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in X \\ x & \text{si } x \in A \setminus X. \end{cases} \end{aligned} \tag{1.73}$$

Nous démontrons dans les points suivants que α est bijective.

(5) **Injective** Nous supposons $\alpha(x) = \alpha(y)$. Il y a 4 possibilités suivant que x et y soient dans X ou $A \setminus X$.

Si $x, y \in X$ alors $f(x) = f(y)$ et donc $x = y$ parce que f est injective.

Si $x \in X$ et $y \in A \setminus X$, alors $f(x) = y$. Mais $f(x) \in f(X)$ et $y \in A \setminus X = B \setminus f(X)$. Donc l'élément $f(x) = y$ est dans $f(X) \cap \big(B \setminus f(X)\big) = \varnothing$. Il n'est donc pas possible d'avoir $\alpha(x) = \alpha(y)$ avec $x \in X$ et $y \in A \setminus X$.

Si $x \in A \setminus X$ et $y \in X$, c'est la même chose.

Si $x, y \in A \setminus X$, alors $x = \alpha(x) = \alpha(y) = y$.

(6) **Surjective** Soit $y \in B$. Il y a deux possibilités : $y \in X$ et $y \in A \setminus X$. La première se divise en deux : $y \in Y$ et $y \in \bigcup_{k=1}^{\infty} f^k(Y)$. On y va.

(6a) $y \in Y$ Ce cas n'est pas possible parce que $y \in B$ alors que $Y = A \setminus B$.

(6b) $y \in f^k(Y)$ **avec** $k \geqslant 1$ Nous avons

$$y \in f\big(f^{k-1}(Y)\big) \subset f(X) \subset \alpha(A). \tag{1.74}$$

(6c) $y \in A \setminus X$ Alors $y = \alpha(y)$.

□

Deuxième preuve de 1.83[18]. Nous posons $Y = A \setminus B$ et

$$\mathcal{M} = \{M \subset A \text{ tel que } Y \cup f(M) \subset M\}. \tag{1.75}$$

Nous allons dire de nombreuses choses à propos de ce $\mathcal{M}$.

(1) **$\mathcal{M}$ est non vide** Nous avons $A \in \mathcal{M}$ parce que Y et $f(A)$ sont dans A.

(2) **Si $M \in \mathcal{M}$ alors $Y \subset M$** C'est dans la définition de $\mathcal{M}$.

(3) **Encore un ensemble** Vu que $\mathcal{M}$ est non vide, nous pouvons poser

$$X = \bigcap_{M \in \mathcal{M}} M \tag{1.76}$$

sans nous poser trop de questions. Cela étant fait, nous pouvons passer aux choses sérieuses.

(4) **$f(X) \subset M$ pour tout $M \in \mathcal{M}$** Soit $M \in \mathcal{M}$. Nous avons

$$\begin{aligned} f(X) &\subset f(M) && \text{SUBEQooRJKWooQRoLZR (1.77a)}\\ &\subset Y \cup f(M) && (1.77b)\\ &\subset M && \text{SUBEQooSAVZooPXYXqC (1.77c)} \end{aligned}$$

Justifications.

- Pour (1.77a). Parce que $X \subset \mathcal{M}$.
- Pour (1.77c). Parce que $M \in \mathcal{M}$.

(5) **$X \in \mathcal{M}$** Vu que $Y \subset M$ pour tout M dans $\mathcal{M}$, nous avons $Y \subset \bigcap_{M \in \mathcal{M}} M = X$. Nous devons prouver $f(X) \subset X$. Nous venons de prouver que $f(X) \subset M$ pour tout $M \in \mathcal{M}$, donc

$$f(X) \subset \bigcap_{M \in \mathcal{M}} M = X. \tag{1.78}$$

L'ensemble X est le plus petit élément de $\mathcal{M}$ pour l'inclusion.

(6) **$Y \cup f(X) \subset X$** Ça fait partie de $X \in \mathcal{M}$. Mais c'est bien de le dire explicitement parce que nous allons l'utiliser quelques fois dans la suite.

(7) **$Y \cup f(X) \in \mathcal{M}$** Vu que $X \in \mathcal{M}$, nous savons déjà que $Y \cup f(X) \subset X$. En appliquant f des deux côtés,

$$f\big(Y \cup f(X)\big) \subset f(X). \tag{1.79}$$

En ajoutant Y des deux côtés,

$$Y \cup f\big(Y \cup f(X)\big) \subset Y \cup f(X), \tag{1.80}$$

et donc $Y \cup f(X) \in \mathcal{M}$.

(8) **$Y \cup f(X) = X$** Nous savons déjà que $Y \cup f(X) \in \mathcal{M}$. Vu que X est le plus petit élément de $\mathcal{M}$, nous avons

$$X \subset Y \cup f(X). \tag{1.81}$$

L'inclusion inverse étant déjà faite, nous avons l'égalité.

(9) **$B \setminus f(X) = A \setminus X$** Nous avons :

$$\begin{aligned} A \setminus X &= A \setminus \big(Y \cup f(X)\big) && (1.82a)\\ &= (A \setminus Y) \cap \big(A \setminus f(X)\big) && \text{SUBEQooBVZCooAEUHtT (1.82b)}\\ &= B \cap \big(A \setminus f(X)\big) && \text{SUBEQooUATVooPEqpHT (1.82c)}\\ &= (B \cap A) \setminus f(X) && \text{SUBEQooKWVWooQMLzrv (1.82d)}\\ &= B \setminus f(X). && \text{SUBEQooQTTSooIFSFKo (1.82e)} \end{aligned}$$

Justifications :

- Pour (1.82b). Complémentaire de réunion, lemme 1.46(2).
- Pour (1.82c). Parce que $A \setminus Y = B$ du fait que $Y = A \setminus B$.
- Pour (1.82d). Lemme 1.46(3).
- Pour (1.82e). Parce que $B \subset A$.

(10) **Notre bijection** Nous voulons définir

$$\begin{aligned} \alpha\colon A &\to B \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in X \\ x & \text{si } x \in A \setminus X. \end{cases} \end{aligned} \tag{1.83}$$

Pour y parvenir, nous devons prouver que α prend effectivement ses valeurs dans B. Ensuite nous prouverons que α est une bijection.

(11) **α prend ses valeurs dans B** Si $x \in X$ nous avons $\alpha(x) = f(x) \in B$. Si au contraire $x \in A \setminus X$ nous avons

$$\alpha(x) = x \in A \setminus X = B \setminus f(X) \subset B. \tag{1.84}$$

(12) **α est injective** Soient $x, y \in A$ tels que $\alpha(x) = \alpha(y)$. Il y a quatre possibilités suivant que x et y sont dans X ou dans $A \setminus X$.

(12a) **$x \in X$, $y \in X$** Alors $f(x) = \alpha(x) = \alpha(y) = f(y)$. Vu que f est injective, nous trouvons que $x = y$.

(12b) **$x \in X$, $y \in A \setminus X$** Nous avons $\alpha(x) = f(x) \in f(X)$ et $\alpha(y) = y \in A \setminus X = B \setminus f(X)$. Il n'est donc pas possible d'avoir $\alpha(x) = \alpha(y)$ dans ce cas.

(12c) **$x \in A \setminus X$, $y \in X$** Idem.

(12d) **$x \in A \setminus X$, $y \in A \setminus X$** Dans ce cas nous avons $\alpha(x) = x$ et $\alpha(y) = y$. Donc $x = y$.

(13) **α est surjective** Soit $b \in B$. Il y a deux possibilités : $b \in f(X)$ ou $b \notin f(X)$.

(13a) **Si $b \in f(X)$** Soit $x \in X$ tel que $f(x) = b$. Alors $\alpha(x) = f(x) = b$.

(13b) **Si $b \notin f(X)$** Alors $b \in B \setminus f(X) = A \setminus X$, et donc $\alpha(b) = b$.

□

THOooRYZJooQcjlcl

Théorème 1.84 (Cantor-Schröder-Bernstein)**.**
Soient deux ensembles A et B pour lesquels il existe des injections $f\colon A \to B$ et $g\colon B \to A$. Alors il existe une bijection entre A et B.

Démonstration. La composée $g \circ f\colon A \to A$ est injective et prend ses valeurs dans $g\big(f(A)\big) \subset g(B) \subset A$. Bref, l'application $g \circ f\colon A \to g(B)$ est injective. Le lemme 1.83 donne alors une bijection $\varphi\colon A \to g(B)$.

Nous montrons que $g^{-1} \circ \varphi\colon A \to B$ est une bijection.

(1) **Injective** Nous supposons $x, y \in A$ tels que

$$g^{-1}\big(\varphi(x)\big) = g^{-1}\big(\varphi(y)\big). \tag{1.85}$$

Nous appliquons g des deux côtés : $\varphi(x) = \varphi(y)$. Puisque φ est une bijection, cela entraîne $x = y$.

(2) **Surjective** Soit $b \in B$. En posant $a = \varphi^{-1}\big(g(b)\big)$ nous avons bien $(g^{-1} \circ \varphi)(a) = b$.

□

1.3.4 Comparabilité cardinale

SNBRoCTmpCabiliteCardInule

1.85.
Le théorème de comparabilité cardinale énonce que si A et B sont des ensembles, alors nous avons toujours $A \succeq B$ ou $A \preceq B$ (ou les deux ; dans ce cas $A \approx B$ par Cantor-Schröder-Bernstein).

THOooCBSKooCmzfUf

Théorème 1.86 (Théorème de comparabilité cardinale[1, 29, 30])**.**
Entre deux ensembles, il existe forcément une injection de l'un dans l'autre.

Démonstration. Nous allons montrer que le graphe d'une injection de A dans B ou de B dans A est donné par un élément maximal (au sens de l'inclusion) de l'ensemble (inductif) des graphes d'injections d'une partie de A dans une partie de B.

Nous allons utiliser le lemme de Zorn 1.42 à l'ensemble[30]

$$\mathcal{A} = \left\{ (X, Y, \varphi) \text{ tel que } \begin{cases} X \subset A \\ Y \subset B \\ \varphi\colon X \to Y \text{ est injective.} \end{cases} \right\} \tag{1.86}$$

que nous ordonnons par l'inclusion, c'est-à-dire par $(X_1, Y_1, \varphi_1) < (X_2, Y_2, \varphi_2)$ lorsque $X_1 \subset X_2$, $Y_1 \subset Y_2$ et $\varphi_2|_{X_1} = \varphi_1$.

Nous passons rapidement sur le fait que cet ensemble est inductif, et nous considérons tout de suite un élément maximal (X, Y, φ). Il y a deux possibilités : soit $\varphi(X) = B$, soit $\varphi(X) \neq B$.

(1) **Si $\varphi(X) = B$** Dans ce cas, $\varphi\colon X \to B$ est une surjection. L'ensemble A est donc surpotent à B. La proposition 1.72 conclut que B est subpotent à A.

(2) **Si $\varphi(X) \neq B$** Nous subdivisons en deux nouveaux cas : soit $X = A$, soit $X \neq A$.

(2a) **Si $X = A$** Alors nous avons une injection $\varphi\colon A \to B$, et c'est bon.

(2b) **Si $X \neq A$** Nous sommes dans le cas $X \neq A$ et $\varphi(X) \neq B$. Soient $a \in A \setminus X$ et $b \in B \setminus \varphi(X)$. Nous considérons l'application

$$\begin{aligned} \psi\colon X \cup \{a\} &\to Y \cup \{b\} \\ x &\mapsto \begin{cases} \varphi(x) & \text{si } x \in X \\ b & \text{si } x = a. \end{cases} \end{aligned} \tag{1.87}$$

C'est une application injective. Donc le triplet $(X \cup \{a\}, Y \cup \{b\}, \psi)$ majore (X, Y, φ). Nous avons une contradiction et ce cas n'est pas possible.

□

NORMooOrdreSurEnsembles

1.87.
Le théorème de comparabilité cardinale couplé au théorème de Cantor-Schröder-Bernstein nous indique que pour tout ensembles A et B, nous avons soit $A \preceq B$, soit $B \preceq A$. Et si $A \preceq B \preceq A$, alors $A \approx B$.

Nous ne sommes pas loin de dire que la relation $\preceq$ donne un ordre total sur l'ensemble des ensembles. C'est très beau sauf que l'ensemble des ensembles n'existe pas[31]. Il faudrait parler de *classe* des ensembles, mais ça nous mènerait trop loin. Toujours est-il que ces deux théorèmes montrent qu'on n'est pas loin d'avoir un ordre sur les ensembles, et que cela est une des bases possibles pour développer les nombres cardinaux.

1.3.5 Théorème de Cantor, ensemble des ensembles

THOcSUBNFThWCxLtd

Théorème 1.88 (Cantor[31])**.**
Un ensemble est toujours strictement subpotent à son ensemble des parties.

Démonstration. Soit un ensemble E et son ensemble des parties $\mathcal{P}(E)$. Nous commençons par prouver qu'il n'existe pas de surjection $E \to \mathcal{P}(E)$. Soit en effet une application $f\colon E \to \mathcal{P}(E)$. Nous posons

$$D = \{x \in E \text{ tel que } x \notin f(x)\}. \tag{1.88}$$

Nous prouvons que D ne peut pas être dans l'image de f. Supposons que $y \in E$ soit tel que $f(y) = D$.

(1) **Si $y \in D$** Alors par définition de D, nous avons $y \notin f(y) = D$. Contradiction.

(2) **Si $y \notin D$** Alors $y \in f(y) = D$, contradiction.

Donc aucune surjection $f\colon E \to \mathcal{P}(E)$ n'existe. En particulier pas de bijections.

Par ailleurs, l'application $g\colon \mathcal{P}(E) \to E$ qui fait $g(\{a\}) = a$ (et n'importe quoi d'autre sur les autres éléments de $\mathcal{P}(E)$) est une surjection $\mathcal{P}(E) \to E$.

Donc $\mathcal{P}(E)$ est toujours strictement surpotent à E. □

NORooSensEnsSurpotent

1.89.
Le théorème de Cantor implique en particulier qu'il existe (au moins) une infinité dénombrable d'ensembles infinis de cardinalité différentes (plus évidemment une infinité dénombrable d'ensembles finis de cardinalité différentes).

Pour tout ensemble A, il est donc possible de dire « soit E, un ensemble strictement surpotent à A ».

[30] Attention : dans le Frido, la notation $f\colon A \to B$, signifie que f est définie sur tout l'ensemble A, mais pas qu'elle est surjective sur B.

[31] Corolaire 1.90.

CORooZMAOooPfJosM

Corolaire 1.90.
Il n'existe pas d'ensemble contenant tous les ensembles.

Démonstration. Si E était un tel ensemble, nous aurions $\mathcal{P}(E) \subset E$ parce que les éléments de $\mathcal{P}(E)$ sont des ensembles. Or cela donnerait une surjection $E \to \mathcal{P}(E)$ alors que cela est impossible par le théorème de Cantor 1.88. □

1.4 Quelques structures algébriques

NORMooEGooStructuresAlgebriques

1.91.
Nous collectons ici les définitions des principales structures algébriques.

DEFooBMUZooLAfbeM

Définition 1.92 (Groupe)**.**
Un ***groupe*** *est un ensemble G muni d'une opération interne $\cdot : G \times G \to G$ telle que*

(1) pour tous g, h, $k \in G$, $g \cdot (h \cdot k) = (g \cdot h) \cdot k$,

(2) il existe un élément $e \in G$ tel que $e \cdot g = g \cdot e = g$ pour tout $g \in G$,

(3) pour tout $g \in G$, il existe un élément $h \in G$ tel que $g \cdot h = h \cdot g = e$.

Un groupe est ***commutatif*** *ou* ***abélien*** *si $g \cdot h = h \cdot g$ pour tout $g, h \in G$.*

REMooNotationOperationGroupe

Remarque 1.93.
Remarquez que nous avons écrit $g \cdot h$ et non $\cdot(g, h)$ comme une notation purement fonctionnelle nous l'aurait suggéré. Dans les exemples concrets, selon les cas, la loi de groupe appliquée à g et h sera notée tantôt $g + h$, tantôt $g \cdot h$ ou, le plus souvent pour un groupe générique, simplement gh.

DEFooSousGroupe

Définition 1.94 (Sous-groupe)**.**
Soit G un groupe et H un sous-ensemble de G. On dit que H est un ***sous-groupe*** *de G si H, muni de l'opération héritée de G, est un groupe. Plus précisément, H est un sous-groupe de G si :*

(1) l'opération interne $\cdot : G \times G \to G$ restreinte à $H \times H$ a ses images dans H ;

(2) l'élément e est un élément de H ;

(3) lorsque $g \in H$, l'élément h tel que $g \cdot h = h \cdot g = e$ est en réalité dans H.

DEFooBEHTooMeCOTX

Définition 1.95 (morphisme, automorphisme)**.**
Soient deux groupes G et H. Un ***morphisme*** *entre G et H est une application $\alpha : G \to H$ telle que pour tous $g, h \in G$ nous ayons $\alpha(g \cdot_G h) = \alpha(g) \cdot_H \alpha(h)$.*

Comme d'habitude, un isomorphisme est un morphisme bijectif.

Un ***automorphisme*** *de G est un isomorphisme de G vers G lui-même. L'ensemble des automorphismes de G est noté* $\mathrm{Aut}(G)$.

PROPooJHHPooIpciPA

Proposition 1.96.
Si $\alpha : G \to H$ est un morphisme de groupes, alors $\alpha(G)$ est un sous-groupe de H.

Démonstration. Point par point vis-à-vis de la définition 1.94. On notera $\cdot$ l'opération de H et $\cdot_G$ celle de G.

(1) **Opération interne** Si h et h' sont deux éléments de $\alpha(G)$, il existe deux éléments g et g' de G tels que $h = \alpha(g)$ et $h' = \alpha(g')$. Alors

$$h \cdot h' = \alpha(g) \cdot \alpha(g') = \alpha(g \cdot_G g'),$$

puisque α est un morphisme de groupes. Ainsi $h \cdot h' \in \alpha(G)$ car il est l'image de $g \cdot_G g'$.

(2) **Neutre** On a $e_H = \alpha(e_G)$ quel que soit le morphisme α.

(3) **Inverse** L'inverse d'un élément $h = \alpha(g)$ est l'élément $\alpha(g^{-1})$.

□

LEMooKJMWooQeIwgF

Lemme 1.97.
Si G est un groupe, alors $\mathrm{Aut}(G)$ *est un groupe pour la composition.*

Démonstration. Soient α et β des automorphismes de G. Alors nous prouvons que $\alpha\circ\beta$ est un automorphisme de G :

$$(\alpha\circ\beta)(gh)=\alpha\big(\beta(g)\beta(h)\big)=\alpha\big(\beta(g)\big)\alpha\big(\beta(h)\big)=(\alpha\circ\beta)(g)(\alpha\circ\beta)(h). \tag{1.89}$$

□

PROPooWTLOooQmomoU

Proposition 1.98 ([1]).
Si $f\colon G\to H$ est un morphisme de groupes, et si A est un sous-groupe de H, alors $f^{-1}(A)$ est un sous-groupe de G.

Démonstration. Soient $x,y\in f^{-1}(A)$. Nous posons $a=f(x)$ et $b=f(y)$. Vu que f est un morphisme, $ab=f(xy)$, de telle sorte que $xy\in f^{-1}(ab)\subset f^{-1}(A)$. □

LEMooDPISooRoAFmt

Lemme 1.99.
Si G et H sont des groupes isomorphes, alors les groupes $\mathrm{Aut}(G)$ et $\mathrm{Aut}(H)$ sont isomorphes.

Démonstration. Soit un isomorphisme $f\colon G\to H$. D'abord pour tout $\alpha\in\mathrm{Aut}(G)$, l'application $f\circ\alpha\circ f^{-1}$ est un automorphisme de H. Cela est rapidement vérifié parce que f, α et f^{-1} sont des bijections et des morphismes.

Nous pouvons donc considérer l'application

$$\begin{aligned}\psi\colon\ \mathrm{Aut}(G)&\to\mathrm{Aut}(H)\\ \alpha&\mapsto f\circ\alpha\circ f^{-1}.\end{aligned} \tag{1.90}$$

(1) ψ **est un morphisme** Soient $\alpha,\beta\in\mathrm{Aut}(G)$. Vu que f est une bijection, nous pouvons introduire $f^{-1}\circ f$ partout où ça nous plaît :

$$\psi(\alpha\beta)=f\circ\alpha\circ\beta\circ f^{-1}=f\circ\alpha\circ f^{-1}\circ f\circ\beta\circ f^{-1}=\psi(\alpha)\circ\psi(\beta). \tag{1.91}$$

(2) ψ **est injective** Si $\alpha\beta\in\mathrm{Aut}(G)$ sont tels que $\psi(\alpha)=\psi(\beta)$, alors

$$f\circ\alpha\circ f^{-1}=f\circ\beta\circ f^{-1}. \tag{1.92}$$

Comme f est une bijection, cela implique que $\alpha=\beta$.

(3) ψ **est surjective** Si $\alpha\colon H\to H$ est un automorphisme, alors $\sigma=\psi(f^{-1}\circ\sigma\circ f)$ où il est facile de vérifier que $f^{-1}\circ\sigma\circ f\in\mathrm{Aut}(G)$.

□

DefHXJUooKoovob

Définition 1.100 (Anneau[32]).
*Un **anneau**[32] est un triplet $(A,+,\ \cdot\ )$ avec les conditions*

(1) $(A,+)$ est un groupe[33] commutatif. Nous notons 0 le neutre.

(2) La multiplication est associative et admet un neutre, que nous notons 1.

ITEMooGMNOooSTGiXw

(3) La multiplication est distributive (à gauche et à droite) par rapport à l'addition. Cela signifie que, pour tous a, b et c de A, nous avons les deux égalités

$$a(b+c)=ab+ac\qquad\text{et}\qquad(a+b)c=ac+bc. \tag{1.93}$$

*L'anneau $(A,+,\ \cdot\ )$ est **commutatif** si pour tout $a,b\in A$ nous avons $a\cdot b=b\cdot a$.*

LEMooVUSMooWisQpD

Lemme 1.101.
Pour tout élément a d'un anneau nous avons $a\cdot 0=0$ et $0\cdot a=0$

Démonstration. L'élément 0 est le neutre de l'addition. Il peut être écrit $1+(-1)$, et en utilisant la distributivité (à gauche),

$$a\cdot 0=a\cdot(1+(-1))=a+(-a)=0. \tag{1.94}$$

L'autre égalité se prouve de même avec la distributivité à droite. □

[32] Nous faisons le choix qu'un anneau admet toujours un neutre pour la multiplication. Certains ouvrages parlent dans ce cas d'anneau unitaire.

[33] Groupe, définition 1.92.

PROPooNCCGooXjVyVt

Proposition 1.102.
Dans un anneau[34] *non nul, le neutre pour l'addition est distinct du neutre pour la multiplication.*

Démonstration. Supposons par contraposée que dans un anneau A, nous ayons $1 = 0$. Alors, pour tout $a \in A$, on a $a = 1a = 0a = 0$: les égalités étant justifées respectivement par la définition de 1, l'hypothèse $1 = 0$, et le lemme 1.101. Ainsi, $a = 0$ pour tout $a \in A$ et l'anneau est nul. □

LEMooLTERooVKgqjn

Lemme 1.103 ([1])**.**
Un peu d'arithmétique. Soit un anneau A et deux éléments $a, b \in A$. Nous avons les égalités suivantes :

ITEMooWNPVooFeMQAp

(1) *Si $a \neq 0$ alors $-a \neq 0$.*

ITEMooUGHCooOPgoeR

(2) $1 \times 1 = 1$.

ITEMooJMBSooVgvVwg

(3) $(-1) \times a = -a$.

ITEMooXJGMooKNLlHU

(4) $-(-a) = a$.

ITEMooYMRKooHVYYKU

(5) $(-1) \times (-1) = 1$.

ITEMooAnneauArith5

(6) $(-a)b = -ab$

ITEMooHUJFooKkylVt

(7) $(-a)(-b) = ab$

Démonstration. En plusieurs parties.

(1) **Pour (1)** Si $-a = 0$ alors en ajoutant a deux côtés, nous avons $0 = a$ qui est contraire à l'hypothèse.

(2) **Pour (2)** La définition de 1 est que $1 \times a = a$ pour tout a. En particulier pour $a = 1$ nous avons le résultat.

(3) **Pour (3)** Nous avons

$$(-1) \times a + a = a \times \big((-1) + 1\big) = a \times 0 = 0. \tag{1.95}$$

Nous avons utilisé le fait que la multiplication était distributive et que le zéro était absorbant (lemme 1.101).

(4) **Pour (4)** Nous avons $-a + a = 0$ par définition de la notation $-a$. Donc a est bien l'inverse de $-a$ pour l'addition.

(5) **Pour (5)** En utilisant les points (3) et (4) nous avons

$$(-1) \times (-1) = -(-1) = 1. \tag{1.96}$$

(6) **Pour (6) et (7)** Par propriété de distributivité[35], on a $ab + (-a)b = (a + (-a))b = 0b = 0$; donc l'opposé de ab s'écrit $-ab$ ou bien $(-a)b$.

Par la même propriété (avec l'autre égalité), on a $(-a)b + (-a)(-b) = (-a)(b + (-b)) = (-a)0 = 0$, donc $(-a)b$ a pour opposé $(-a)(-b) = ab$.

□

NORooDistributiviteSoustraction

1.104.
La distributivité de la partie (3) de la définition 1.100 ne traite que de l'addition ; pas de la soustraction. Voici un lemme qui dit que la distriutivité fonctionne aussi avec les soustractions.

LEMooVPYUooRzexke

Lemme 1.105 ([18])**.**
Soient un anneau A ainsi que $a, b, c \in A$. Alors

$$a(b - c) = ab - ac. \tag{1.97}$$

Démonstration. Nous avons le calcul suivant :

SUBEQooKCOWooFeQHUM

$$a(b - c) + ac = a\big((b - c) + c\big) \tag{1.98a}$$

SUBEQooMLLOooNRmIYM

$$= ab. \tag{1.98b}$$

Justifications :

[34] Définition 1.100.
[35] Définition 1.100, point (3).

- Pour 1.98a. Distributivité.
- Pour 1.98b. Parce que $(b-c)+c=b$.

Nous avons donc $a(b-c)+ac=ab$ et donc l'égalité demandée en ajoutant $-ac$ des deux côtés. □

DEFooSPHPooCwjzuz

Définition 1.106 (Morphisme d'anneaux[33]).
Si $(A,+,\cdot)$ et $(B,+,\cdot)$ sont des anneaux[36]*, un **morphisme d'anneaux** est une application $f\colon A\to B$ telle que*

(1) $f(a+b)=f(a)+f(b)$

(2) $f(a\cdot b)=f(a)\cdot f(b)$

(3) $f(1)=1$.

Étant bien entendu que les significations de 1, $+$ et $\cdot$ sont différentes à gauche et à droite.

1.4.1 Positivité

SUREFooZRMPooGtmMox

Définition 1.107 ([1]).
Soit un anneau[37] *A. Une **positivité** sur A est une partie $A^+\subset A$ telle que*

(1) Pour tout $a\neq 0$ dans A, nous avons[38] *$a\in A^+$ xor $-a\in A^+$.*

(2) Pour tout $a,b\in A^+$, nous avons $a+b\in A^+$.

Oui, il faudrait dire une stricte *positivité.*

PROPooKLOPooBgQqhM

Proposition 1.108 ([1]).
Soit A^+ une positivité[39] *sur A. Pour $a,b\in A$, on définit la relation $a\leqslant b$ si et seulement si $b-a\in A^+\cup\{0\}$. Cette relation est une relation d'ordre*[40] *sur A.*

Démonstration. Nous vérifions les conditions de la définition 1.23.

(1) **Réflexivité** Vu que $a-a=0$ et que $0\in A^{\cup}\{0\}$, nous avons $a\leqslant a$.

(2) **Antisymétrie** Si $a\leqslant b$ et $b\leqslant a$, nous avons

$$\begin{cases} b-a\in A^+\cup\{0\} & (1.99a)\\ a-b\in A^+\cup\{0\}. & (1.99b)\end{cases}$$

Par définition de la positivité, on ne peut avoir $a-b$ et $b-a$ tous les deux dans A^+. Donc soit $a-b=0$, soit $b-a=0$ (ou les deux en même temps, ce qui est le cas). Quoi qu'il en soit, on en déduit $a=b$.

(3) **Transitivité** Supposons que $a\leqslant b$ et $b\leqslant c$. Nous avons alors

$$\begin{cases} b-a\in A^+\cup\{0\} & (1.100a)\\ c-b\in A^+\cup\{0\}. & (1.100b)\end{cases}$$

Si l'un des deux est nul, c'est facile. Nous supposons qu'ils sont tous les deux dans A^+. Alors leur somme est dans A^+ : $(b-a)+(c-b)\in A^+$. Cela donne tout de suite $c-a\in A^+$ et donc $a\leqslant c$ comme demandé.

□

[36] Définition 1.100.
[37] Définition 1.100.
[38] *xor* est le ou exclusif. L'un ou bien l'autre est vrai, mais on ne peut avoir les deux en même temps.
[39] Définition 1.107.
[40] Définition 1.23.

1.4.2 Diviseurs, pgcd et ppcm

SUBooDiviseursPGCDPPCM

Définition 1.109 (Diviseurs dans un anneau)**.**
Soit un anneau[41] *A. Soient $a, b \in A$. On dit que a divise b, ou que a est un **diviseur (à gauche)** de b si il existe $c \in A$ tel que $ac = b$. On dit que c'est un diviseur de b à droite si $ca = b$ pour un certain $c \in A$.*

*Dans un anneau commutatif, nous disons que a **divise** b si il existe $x \in A$ tel que $ax = b$. Dans ce cas nous écrivons $a \mid b$.*

NORMooAnneauIntegreIntro

1.110.
Un cas particulier est le cas des diviseurs de zéro. L'absence de tels diviseurs dans un anneau est une propriété intéressante : on dit dans ce cas que l'anneau est *intègre*. Nous définirons cela proprement en la définition 3.22, grâce à des propriétés équivalentes.

DEFooAnneauEltRegulier

Définition 1.111.
*Un élément $a \in A$ est **régulier à droite** si, dès lors qu'un élément $b \in a$ est tel que $ba = 0$, alors $b = 0$. Il est régulier à gauche si $ab = 0$ implique $b = 0$.*

PROPooRegulierMagmaAnneau

Proposition 1.112.
Soit A un anneau. La notion de régularité dans un anneau est équivalente à la notion de régularité[42] *dans le magma A muni de l'opération de multiplication.*

Démonstration. En deux étapes. On ne va faire que la régularité à gauche, il suffit d'adapter pour la régularité à droite.

(1) **Régulier dans le magma implique régulier dans l'anneau** Soit $a \in A$. On sait, par régularité de A dans le magma, que pour tous x et y de A, dès lors que $ax = ay$, alors $x = y$.

Soit $b \in A$. Supposons que $ab = 0$. Le lemme 1.101 permet d'écrire $ab = a0$. En prenant $x = b$ et $y = 0$, on en déduit $b = 0$, soit la régularité de a dans l'anneau.

(2) **Régulier dans l'anneau implique régulier dans le magma** Soit $a \in A$. On sait que l'égalité $ab = 0$ implique $b = 0$.

Soit $x, y \in A$. Supposons que $ax = ay$; alors $ax - ay = 0$ et par distributivité soustractive[43], $a(x-y) = 0$. Mais la régularité d'anneau dit alors que $x - y = 0$, et donc que $x = y$. Donc a est régulier dans le magma A.

□

DefrYwbct

Définition 1.113.
*Soient A un anneau commutatif et $S \subset A$. Nous disons que $\delta \in A$ est un **PGCD** de S si*

(1) δ divise[44] *tous les éléments de S.*

ITEMooVCKGooWDXZOj

(2) si d divise également tous les éléments de S, alors d divise δ.

*Nous disons que $\mu \in A$ est un **PPCM** de S si*

(1) $S \mid \mu$,

(2) si $S \mid m$, alors $\mu \mid m$.

Si P et Q sont des polynômes, ce que nous notons $\gcd(P, Q)$ *est l'unique polynôme unitaire dans* $\gcd\big(\{P, Q\}\big)$. *Voir 8.53.*

REMooExistenceUnicitePGCD

Remarque 1.114.
On parle d'existence de pgcd dans 3.191.

Au sens de la définition 1.113, le pgcd n'est pas unique. Dans $\mathbb{Z}$ par exemple les nombres 4 et -4 sont tous deux pgcd de $\{4, 16\}$.

Dans $\mathbb{Z}$ cependant, nous modifions implicitement la définition et nous n'acceptons que les positifs, de telle sorte que l'unique pgcd soit effectivement le plus grand pour l'ordre usuel sur $\mathbb{Z}$.

Pour l'unicité dans $\mathbb{Z}$, voir 3.155.

[41] Anneau,définition 1.106.
[42] Définition 1.68
[43] Lemme 1.105.
[44] Définition 1.109.

1.4.3 Règle des signes dans un anneau totalement ordonné

SUBDefiqwAGWTooIQwdXkd

Définition 1.115 (Anneau totalement ordonné[1])**.**
*Un anneau A est **totalement ordonné** si, sur A, il existe une relation d'ordre total*[45] *compatible avec la structure d'anneau, c'est-à-dire tel que*

ITEMooZISJooWNxnBj

(1) $x \leqslant y$ implique $x+z \leqslant y+z$ pour tout $x,y,z \in A$

CONDooBYYDooElXgPO

(2) $x \geqslant 0$ et $y \geqslant 0$ implique $xy \geqslant 0$.

PROPooELXCooCYzEVD

Proposition 1.116 ([1])**.**
Soit un anneau totalement ordonné A.

ITEMooRRUGooRUpYwt

(1) Si $a \leqslant 0$ alors $-a \geqslant 0$.

ITEMooNKYCooCmqHsO

(2) Si $a \geqslant 0$ alors $-a \leqslant 0$

ITEMooXOTGooYxKubR

(3) Si $a,b \geqslant 0$ alors $a+b \geqslant 0$

Démonstration. Point par point.

(1) **Pour (1)** En vertu de 1.115(1) nous pouvons ajouter $-a$ est deux côtés de $a \leqslant 0$: $a-a \leqslant 0-a$ et donc $0 \leqslant -a$.

(2) **Pour (2)** On écrit $a \geqslant 0$ et nous faisons $-a$ des deux côtés pour obtenir $a-a \geqslant 0-a$, c'est-à-dire $0 \geqslant -a$.

(3) **Pour (3)** Nous avons $a \geqslant 0$. Nous ajoutons b des deux côtés pour avoir $a+b \geqslant b \geqslant 0$.

□

LEMooXJTAooZauchx

Lemme 1.117 (Règle des signes[34])**.**
Soit un anneau totalement ordonné A ainsi que $x,y \in A$. Nous avons :

ITEMooHESRooKrDult

(1) Si $x,y \geqslant 0$ alors $xy \geqslant 0$.

ITEMooNLAQooHtERZJ

(2) Si $a \geqslant 0$ et $b \leqslant 0$ alors $ab \leqslant 0$.

ITEMooDZUJooVWuLbD

(3) Si $a,b \leqslant 0$ alors $ab \geqslant 0$

ITEMooRGYAooCUIfss

(4) $0 < 1$.

ITEMooMRNHooLglPKn

(5) Si $x \geqslant 0$ et x est inversible dans A, alors $x^{-1} \geqslant 0$.

Démonstration. Plusieurs points.

(1) **Pour (1)** C'est directement la définition 1.115(2).

(2) **Pour (2)** En posant $x=a$ et $y=-b \geqslant 0$ (par la proposition 1.116(1)), nous avons $xy \geqslant 0$ par la définition 1.115(2). Nous avons alors $a(-b) = -ab \geqslant 0$ par (1), et donc $ab \leqslant 0$.

(3) **Pour (3)** Nous posons $a' = -a$ et $b' = -b$. Par 1.116(1) nous avons $a', b' \geqslant 0$. Donc $a'b' \geqslant 0$ par le point (2). Mais $a'b' = (-a)(-b) = ab$ par le lemme 1.103(7).

(4) **Pour (4)** Supposons par l'absurde que $1 \leqslant 0$. L'utilisation de (3) avec $a = b = 1$ donne $ab = 1 \cdot 1 = 1 \geqslant 0$, ce qui nous contredit. Ainsi, $1 > 0$.

(5) **Pour (5)** Si $x^{-1} < 0$, alors $1 = xx^{-1} < 0$. Mais comme nous venons de voir que $1 \geqslant 0$ nous déduisons que $x^{-1} \geqslant 0$.

□

[45] Définition 1.26.

1.4.4 Valeur absolue, corps valué

SUFooVaVAXCoAjsVBRoS

Définition 1.118 (Valeur absolue, corps valué[35, 36]).
*Un **anneau valué** A est un annau totalement ordonné muni d'une application $|.|\colon A \to \mathbb{K}$ telle que*

(1) $|x| \geqslant 0$ *pour tout* $x \in \mathbb{K}$,

(2) $|x| = 0$ *si et seulement si* $x = 0$,

(3) $|x + y| \leqslant |x| + |y|$

(4) $|xy| \leqslant |x||y|$.

*Une telle application est une **valeur absolue**.*

NORooLienCorpsValueEspaceMetrique

1.119.
Un corps valué sera un espace topologique métrique dans la définition 9.255. Dans le cas d'un corps totalement ordonné, nous avons une valeur absolue donnée par 1.121 et les principales propriétés dans le lemme 1.122.

NORooValAbsGenerale

1.120.
La plupart du temps, la valeur absolue $|.|$ sera à valeurs dans $\mathbb{R}^+$. Cependant nous avons besoin d'une définition générale parce que nous allons devoir définir ce qu'est une suite de Cauchy (définition 3.249(1)) dans un corps avant la définition des réels ; les réels étant définis comme étant des suites de Cauchy dans $\mathbb{Q}$.

DEFooJXKVooErANPh

Proposition-Définition 1.121 (Valeur absolue[1]).
Si A est un anneau totalement ordonné[46]*, alors l'application*

$$|x| = \begin{cases} -x & si\ x < 0 \\ 0 & si\ x = 0 \\ x & si\ x > 0. \end{cases} \tag{1.101}$$

EQooNONAooHLSERQ

est une valeur absolue[47]*. Elle vérifie de plus*

$$|xy| = |x||y|. \tag{1.102}$$

EQooORNAooBYFeFk

Par défaut, lorsque nous parlons de la valeur absolue sur A, c'est celle-ci.

Démonstration. Il faut vérifier les conditions de la définition 1.118.

(1) $|x| = 0$ **si et seulement si** $x = 0$ C'est la définition et le fait que $-x \neq 0$ lorsque $x \neq 0$ par le lemme 1.103(1).

(2) $|x + y| \leqslant |x| + |y|$ Il y a 4 possibilités suivant la positivité de x et y.

(2a) **Si** $x, y \geqslant 0$ Alors $x + y \geqslant 0$ par la proposition 1.116(3). Donc $|x| = x$, $|y| = y$ et $|x + y| = x + y$.

(2b) **Si** $x \geqslant 0$ **et** $y < 0$ Nous posons $y' = -y$, et nous avons deux possibilités : $y' \geqslant x$ et $y' < x$.

(2b.i) **Si** $y' < x$ Alors en posant $a = x - y'$ nous avons $a > 0$. Nous avons ensuite :

$$|x + y| = |y' + a + y| = |y' + a - y'| = |a| = a. \tag{1.103}$$

Mais

$$|x| + |y| = x + y' = y' + a + y' = a + 2y' \geqslant a = |x + y|. \tag{1.104}$$

(2b.ii) **Si** $y' \geqslant x$ Alors en posant $a = y' - x$ nous avons $a \geqslant 0$ et

$$|x + y| = |x - y'| = |x - (x + a)| = |-a| = a. \tag{1.105}$$

Mais aussi

$$|x| + |y| = x + y' = x + x + y = 2x + a \geqslant a. \tag{1.106}$$

Les autres cas sont du même style.

[46] Définition 1.115.
[47] Définition 1.118.

(3) $|xy| = |x||y|$

Il y a 4 possibilités.

(3a) **Si $x, y \geqslant 0$** Nous avons directement $|x| = x$, $|y| = y$. Par ailleurs A est un anneau totalement ordonné ; la définition 1.115(2) donne $xy \geqslant 0$ et donc $|xy| = xy$.

(3b) **Si $x \geqslant 0$ et $y \leqslant 0$** La définition de la valeur absolue donne $|x| = x$ et $|y| = -y$. Par ailleurs la proposition 1.117(2) dit que $xy \leqslant 0$ de telle sorte que $|xy| = -xy$.

(3c) **Si $x \leqslant 0$ et $y \geqslant 0$** Même chose.

(3d) **Si $x, y \leqslant 0$** Même chose, en utilisant 1.117(3).

□

LemooANTJooYxQZDw

Lemme 1.122 (Propriétés de la valeur absolue)**.**
Soit A un anneau totalement ordonné muni de la valeur absolue usuelle (définition 1.121). Si $x, y \in A$, alors :

ITEMooSDNHooDnjScE

(1) $|x| \geqslant 0$

ITEMooLQLTooTJTPVM

(2) $|x| = 0$ *si et seulement si* $x = 0$

ITEMooVJAEooOEatzY

(3) $|-x| = |x|$.

ItemooOMKNooRlanvk

(4) $|x + y| \leqslant |x| + |y|$.

ITEMooISWFooMeOtjZ

(5) $|x - y| \leqslant |x - z| + |z - y|$.

ITEMooEFMLooYVCuHD

(6) $|xy| = |x||y|$

ITEMooLWPTooEvHzvO

(7) Si $x \geqslant a$ et $x \geqslant -a$ alors $x \geqslant |a|$.

Démonstration. Point par point

(1) **Pour (1)** Si $x \geqslant 0$ alors c'est vrai. Sinon, $x \leqslant 0$ et $|x| = -x \geqslant 0$ par le point (1) de la proposition 1.116.

(2) **(2)** Si $x = 0$ alors $x = -x$ et $|x| = 0$. Si $x \neq 0$ alors $-x \neq 0$ (par le lemme 1.103 point (1)). Que l'on ait x positif ou x négatif, nous aurons toujours $|x| \pm x \neq 0$.

(3) **Pour (3)** Il faut décomposer en deux cas selon que $x \geqslant 0$ ou $x \leqslant 0$.

Lorsque $x \leqslant 0$, on a $|x| = -x$ par définition, et par ailleurs, $-x \geqslant 0$ grâce au point (2) du lemme 1.103, donc $|-x| = -x = |x|$.

Supposons $x \geqslant 0$. Alors d'une part $|x| = x$. D'autre part $-x \leqslant 0$ par le point (1) de la proposition 1.116, de telle sorte que

$$|-x| = -(-x) = x, \tag{1.107}$$

cette dernière égalité étant justifiée par le point (4) du lemme 1.103.

Nous avons donc bien $|x| = |-x|$ quel que soit le cas considéré.

(4) **Pour (4)** Nous supposons que $x \leqslant y$ et nous distinguons divers cas suivant la positivité de x et y.

(4a) Si $x, y \geqslant 0$. Dans ce cas, $x + y \geqslant y \geqslant 0$, donc $|x + y| = x + y = |x| + |y|$.

(4b) Si $x, y \leqslant 0$. Dans ce cas, $x + y \leqslant 0$ et nous avons $|x + y| = -x - y = |x| + |y|$.

(4c) Si $x \leqslant 0$ et $y \geqslant 0$. Nous subdivisons encore en deux cas suivant que $x + y$ est positif ou négatif. Si $x + y \geqslant 0$, alors nous écrivons successivement

$$x \leqslant 0 \tag{1.108a}$$
$$x + y \leqslant y \leqslant y + |x| = |x| + |y| \tag{1.108b}$$

et donc $|x + y| = x + y \leqslant |x| + |y|$.

Nous supposons à présent que $x \leqslant 0$, $y \geqslant 0$ et $x + y \leqslant 0$. Dans ce cas il suffit d'écrire $|x + y| = |(-x) + (-y)|$ pour retomber dans le cas précédent à inversion près de x et y.

(5) **Pour (5)** Soient $x, y, z \in \mathbb{K}$. En utilisant (4) nous avons

$$|x - y| = |(x - z) + (z - y)| \leqslant |x - z| + |z - y|. \tag{1.109}$$

(6) **Pour (6)** Il suffit de prendre les 4 cas suivant les signes de x et y, et d'utiliser les règles de signes du lemme 1.117 dans la définition (1.101).

(7) **Pour (7)** Il y a 2 possibilités : $a \geqslant 0$ et $a < 0$. Si $a \geqslant 0$ alors $|a| = a$. Donc $x \geqslant a = |a|$. Si $a < 0$ alors $|a| = -a$ et donc $x \geqslant -a = |a|$.

□

1.5 Les entiers naturels

NORMooFESMooNaturel

1.123 ([37]).
Comme le dit la page de Wikipédia consacrée aux nombres entiers, il faut savoir ce dont on parle. Les collégiens français apprennent que les entiers sont les nombres positifs ; les Québécois et les Belges y ajoutent les négatifs…

Dans le Frido, on dira « entier naturel » voire « naturel » pour les positifs, et « entier relatif » voire « entier » quand on accepte les négatifs. C'est un choix pas standard dont il faut avoir conscience.

1.5.1 Importance des naturels dans les ensemble

NORMooLNLHooLYKwDu

1.124.
Je suis certain qu'on peut définir les naturels comme étant un objet avec une propriété universelle bien particulière dans la catégorie des ensembles[48].

En tout cas j'ai l'impression qu'on ne peut rien prouver à propos des ensembles Dedekind-finis[49] sans passer par une bijection avec une partie des naturels.

Voici quelques résultats que je doute être possible de démontrer sans passer par les naturels.

(1) La proposition 1.185 dit que tout ensemble fini partiellement ordonné possède un élément maximal. Voir aussi [38].

(2) Si E est fini, alors son ensemble des parties $\mathcal{P}(E)$ est fini.

1.5.2 Triplet naturel

DEFooBTBQmWaluAx

Définition 1.125 ([39]).
*Un **triplet naturel** est un triplet $(\mathcal{N}, o, s)$ où $\mathcal{N}$ est un ensemble, o est un élément de $\mathcal{N}$ et s est une application $s\colon \mathcal{N} \to \mathcal{N}$ satisfaisant les propriétés suivantes :*

(1) s est injective,

ITEMooQAKJooGKdJsM

(2) $s(\mathcal{N}) = \mathcal{N} \setminus \{o\}$

ITEMooXPYEooFajywh

(3) Si $\mathcal{A} \subset \mathcal{N}$ est tel que $o \in \mathcal{A}$ et $s(\mathcal{A}) \subset \mathcal{A}$, alors $\mathcal{A} = \mathcal{N}$.

NORMooTripletNaturelGratterTheoEns

1.126.
Le théorème suivant est typiquement de ceux qui vont demander de gratter la théorie axiomatique des ensembles avec une certaine précision. Comme nous l'avons dit en introduction 1.1, nous n'avons pas l'intention de préciser nos axiomes, mais notre principe de construction est connu et dû à John Von Neumann.

Nous verrons plus tard, en 1.159, que toute partie infinie d'un triplet naturel fournit un nouveau triplet naturel ; il en existe donc plusieurs.

THOooOXMHooXYgMqb

Théorème 1.127.
Il existe un triplet naturel.

NORMooConstructionTripletNaturel

1.128 (Idée de la construction[40, 41]).
Nous effectuons une construction de plusieurs ensembles, puis vérifier que l'ensemble final, muni du nécessaire, forme un triplet naturel.

(1) **Le premier élément** On pose $o = \varnothing$. Dans une axiomatisation raisonnable, l'ensemble vide existe toujours.

[48] Évidemment : https://en.wikipedia.org/wiki/Natural_numbers_object.

[49] Un ensemble des Dedekind-infini si il est en bijection avec une partie propre ; c'est la définition du Frido de « infini » tout court.

(2) **Le principe de construction** On construit $A_1 = o \cup \{o\}$ et on pose $s(o) = A_1$. Puis on définit $A_2 = A_1 \cup \{A_1\}$, et on pose $s(A_1) = A_2$.

De manière générale[50], une fois un ensemble A_i construit sur ce principe, on ajoute l'ensemble $A_i \cup \{A_i\}$ à notre construction, et on pose $s(A_i) = A_i \cup \{A_i\}$.

Finalement, l'ensemble $\mathcal{N}$ est la réunion[51] de tous les ensembles A_i ainsi construits, et l'application să est définie par $s(A) = A \cup \{A\}$.

(3) **Une remarque intéressante** En observant bien, on remarque que $o \in A_1$ mais aussi $o \subset A_1$. De même, $A_1 \subset A_2$ et donc $o \in A_2$ tout comme $A_1 \in A_2$. On a aussi $o \subset A_2$

En fait, dans tous les ensembles que l'on construit, on aura toujours un principe d'inclusion, et aussi d'appartenance. Bien que l'intuition nous fait penser que ça fonctionne, la preuve n'est pas évidente.

(4) **On a un triplet naturel** Montrons que $(\mathcal{N}, o, s)$ est bien un triplet naturel.

(4a) s est-elle injective ? Si A et B sont deux éléments de $\mathcal{N}$ avec $A \neq B$, alors par la remarque ci-dessus, et quitte à inverser A et B, on a $A \subset B$. On en déduit que B est construit après A, et donc $A \cup \{A\} \subset B$. Mais, toujours par construction, $\{B\}$ ne peut être dans A, ni être égal au singleton $\{A\}$: ainsi $A \cup \{A\} \subset B \cup \{B\}$ mais $A \cup \{A\} \neq B \cup \{B\}$, soit $s(A) \neq s(B)$.

(4b) A-t-on $s(\mathcal{N}) = \mathcal{N} \setminus \{o\}$? Par construction, un élément $B \in \mathcal{N} \setminus \{o\}$ est de la forme $A \cup \{ăA\}$ pour un certain ensemble A, lui-même dans $\mathcal{N}$.

(4c) Soit $\mathcal{A}$ une partie de $\mathcal{N}$ tel que $o \in \mathcal{A}$ et $s(\mathcal{A}) \subset \mathcal{A}$. Cette dernière hypothèse nous dit que, dès que $A \in \mathcal{A}$, alors $A \cup \{A\} \in \mathcal{A}$. Comme $\mathcal{A}$ contient $o = \varnothing$, il contient aussi A_1, donc aussi A_2, et par suite $\mathcal{N}$ tout entier. Finalement, $\mathcal{A} \subset \mathcal{N}$ et $\mathcal{N} \subset \mathcal{A}$, donc l'égalité.

NORooDefinitionNChoixTriplet

1.129 (Définition de $\mathbb{N}$)**.**
Pour la suite, nous considérons un triplet naturel $(\mathcal{N}, o, s)$ et nous notons $\mathbb{N} = \mathcal{N}$. Donc la nature de tous les objets que nous allons considérer à partir de maintenant dépend du choix de triplet naturel que nous faisons à présent. Le théorème 1.173 nous assurera que peu de choses devraient réellement dépendre de ce choix.

Nous notons 0 l'élément o et 1 l'élément $s(0)$. C'est tout ce dont nous avons besoin dans l'immédiat.

1.5.3 Applications définies par récurrence

SUBPROPooXATRGRekwrWkq

Proposition 1.130 (Récurrence[39])**.**
Soit un triplet naturel $(\mathcal{N}, o, s)$ et une application $P\colon \mathcal{N} \to \{0, 1\}$ vérifiant[52]

(1) $P(o) = 1$,

(2) pour tout $a \in \mathcal{N}$, si $P(a) = 1$, alors $P\big(s(a)\big) = 1$.

Alors $P(x) = 1$ pour tout $x \in \mathcal{N}$.

Démonstration. Nous posons

$$A = \{x \in \mathcal{N} \text{ tel que } P(x) = 1\}. \tag{1.110}$$

Cet ensemble vérifie la propriété 1.125(3). Donc $A = \mathcal{N}$. □

THOooEJPYooZFVnez

Théorème 1.131 ([18, 42])**.**
Soient E un ensemble, une application $g\colon E \to E$, et b un élément de E. Alors il existe une unique application $f\colon \mathbb{N} \to E$ telle que :

(1) $f(0) = b$

(2) $f\big(s(n)\big) = g\big(f(n)\big)$ *pour tout* $n \in \mathbb{N} \setminus \{0\}$.

[50] Ici on voit que nous ne sommes pas en train d'écrire une vraie démonstration parce que « de manière générale » n'est pas quelque chose de précisément défini. En particulier nous ne disposons pas encore de théorèmes formalisant les constructions par récurrence ;on serait tenté d'utiliser le théorème 1.131.

[51] Ici aussi c'est compliqué parce que rien ne garantit qu'il existe un ensemble contenant tous les A_i. Une construction un peu similaire construit les ordinaux, et dans ce cas, il n'existe pas d'ensembles contenant tous les ordinaux.

[52] Les plus pointilleux diront que 1 n'est pas encore défini. Bon j'avoue. Ce qui est important est que P prenne ses valeurs dans un ensemble contenant deux éléments distincts. Si maintenant vous râlez parce que « deux » est encore moins défini, prenez un ensemble quelconque A et dites que P prend ses valeurs dans $\{A, \mathcal{P}(A)\}$. Mais êtes-vous bien certain que $\mathcal{P}(A) \neq A$?

Démonstration. Nous commençons par l'unicité. Soient f_1 et f_2 deux telles applications. Nous posons

$$A = \{n \in \mathbb{N} \text{ tel que } f_1(n) = f_2(n)\}. \tag{1.111}$$

Nous avons $0 \in A$ parce que $f_1(0) = f_2(0) = b$.

Supposons que $f_1(k) = f_2(k)$. Alors nous avons

$$f_1\big(s(k)\big) = g\big(f_1(k)\big) = g\big(f_2(k)\big) = f_2\big(s(k)\big). \tag{1.112}$$

Nous en déduisons que $s(k) \in A$. Autrement dit $s(A) \subset A$. La définition 1.125(3) nous indique alors que $A = \mathbb{N}$, c'est-à-dire que $f_1 = f_2$.

Nous montrons à présent l'existence en plusieurs étapes.

(1) **L'ensemble est assez grand** Nous considérons l'ensemble $\mathcal{A}$ des parties $A \subset \mathbb{N} \times E$ telles que

(1a) $(0, b) \in A$

(1b) $(n, x) \in A \Rightarrow \big(s(n), g(x)\big) \in A$.

L'ensemble $\mathcal{A}$ est non vide parce que $\mathbb{N} \times E \in \mathcal{A}$.

(2) **Le plus petit** Nous posons

$$G = \bigcap_{A \in \mathcal{A}} A, \tag{1.113}$$

et nous prouvons que $G \in \mathcal{A}$. D'abord $(0, b) \in G$ parce que cet élément est dans chacun des $A \in G$. Ensuite si $(n, x) \in G$, alors pour tout $A \in \mathcal{A}$ nous avons $(n, x) \in A$ et donc $\big(s(n), g(x)\big) \in A$. Par conséquent $\big(s(n), g(x)\big) \in \bigcup_{A \in \mathcal{A}} A = G$.

Pour $n \in \mathbb{N}$ nous posons

$$G_n = \{x \in E \text{ tel que } (n, x) \in G\}. \tag{1.114}$$

Nous avons en particulier que $b \in G_0$ parce que $(0, b) \in G$.

(3) G **contient un** (n, x) **pour tout** n Nous prouvons que pour tout $n \in \mathbb{N}$, il existe $x \in E$ tel que $(n, x) \in G$. Nous faisons ça avec la proposition 1.130 en posant

$$\begin{aligned} P\colon \mathbb{N} &\to \{0, 1\} \\ n &\mapsto \begin{cases} 1 & \text{si } G_n \neq \varnothing \\ 0 & \text{sinon.} \end{cases} \end{aligned} \tag{1.115}$$

Puisque $(0, b) \in G$ nous avons $P(0) = 1$. Supposons que $P(k) = 1$ et montrons que $P\big(s(k)\big) = 1$. Comme $P(k) = 1$, il existe $x \in E$ tel que $(k, x) \in G$. De ce fait, $\big(s(k), g(x)\big) \in G$, ce qui donne $G_{s(k)} \neq \varnothing$ et $P\big(s(k)\big) = 1$.

(4) G_n **est un singleton** Nous avons vu que G_n n'est jamais vide. Nous allons montrer que G_n est un singleton pour tout n. Pour cela nous posons

$$\begin{aligned} P\colon \mathbb{N} &\to \{0, 1\} \\ n &\mapsto \begin{cases} 1 & \text{si } G_n \text{ est un singleton} \\ 0 & \text{sinon.} \end{cases} \end{aligned} \tag{1.116}$$

Nous prouvons par récurrence que $P(n) = 1$ pour tout n.

(4a) $P(0) = 1$ Nous commençons par prouver que $P(0) = 1$. Nous savons que $(0, b) \in G_0$. Supposons $a \neq b$ tel que $(0, a) \in G_0$. Alors en posant $G' = G \setminus \{(0, a)\}$ nous avons $G' \in \mathcal{A}$.

En effet $(0, b) \in G'$ parce que $(0, b) \in G$ et $(0, b) \neq (0, a)$. De plus si $(n, x) \in G'$, alors $\big(s(n), g(x)\big) \in G$. Mais comme $s(n) \neq 0$ nous avons $\big(s(n), g(x)\big) \neq (0, a)$ et donc $\big(s(n), g(x)\big) \in G'$. L'ensemble G' serait un élément de $\mathcal{A}$ strictement inclus dans G. Impossible. Donc G_0 est un singleton.

(4b) **Récurrence** Supposons que $P(k) = 1$, c'est-à-dire que G_k est un singleton. Soit e l'unique élément de G_k : $(k, e) \in G$. Nous avons alors aussi que $\big(s(k), g(e)\big) \in G$. Nous devons prouver que si $y \in G_{s(k)}$, alors $y = g(e)$.

Supposons donc $y \neq g(e)$ soit dans $G_{s(k)}$. Nous posons

$$G' = G \setminus \{\big(s(k), y\big)\}. \tag{1.117}$$

Nous prouvons que $G' \in \mathcal{A}$. D'abord $(0, b) \in G'$ parce que $s(k) \neq 0$. Soit ensuite $(m, z) \in G'$. Si $m = k$, alors $z = e$ (parce que par hypothèse G_k est un singleton) et nous savons que $\big(s(m), g(e)\big) \in G'$. Si par contre $m \neq k$, comme s est injective, nous avons aussi $s(m) \neq s(k)$. Donc $\big(s(m), g(z)\big) \neq \big(s(k), y\big)$ et $\big(s(m), g(z)\big) \in G'$. Donc $G' \in \mathcal{A}$ et est strictement plus petit que G. Contradiction.

Nous concluons que $G_{s(k)}$ est un singleton, c'est-à-dire que $P\big(s(k)\big) = 1$.

(4c) **Conclusion** Nous avons prouvé que G_n est un singleton pour tout n.

(5) **Et enfin**

Nous définissons $f(n)$ comme étant l'unique élément de G_n. Puisque $(0, b) \in G$ nous avons $G_0 = \{b\}$ et donc $g(0) = b$.

Par définition de f, nous avons $\big(n, f(n)\big) \in G$. Parce que $G \in \mathcal{A}$ nous avons alors

$$\big(s(n), g\big(f(n)\big)\big) \in G. \tag{1.118}$$

Autrement dit, $G_{s(n)} = \{g\big(f(n)\big)\}$. Cela montre que

$$f\big(s(n)\big) = g\big(f(n)\big), \tag{1.119}$$

et donc que f vérifie les propriétés demandées.

□

1.132.
Le théorème 1.131 permet de faire des démonstration par récurrence en posant $P\colon \mathbb{N} \to \{0, 1\}$ où $P(n) = 0$ si la proposition à prouver est fausse pour n et $P(n) = 1$ si elle est vraie. Et on démontre que $P(n) = 1$ pour tout n.

Parfois, implicitement, nous dirons que $P(n) = 1$ si la propriété est vraie pour tous les ensembles de cardinal plus petit ou égal à n.

NORMooPUOAooGnFjaX

1.133.
Lorsque nous disons faire une récurrence sur le cardinal d'un ensemble, nous posons la fonction $P\colon \mathbb{N} \to \{0, 1\}$ définie par $P(n) = 1$ si la propriété est vraie pour tout ensemble de cardinal n et $P(n) = 0$ si il existe un ensemble de cardinal n ne vérifiant pas la propriété.

NORMooLNXMooWIblPf

1.134 ([1])**.**
Le théorème 1.131 nous permet de définir une suite $(x_n)_{n\in\mathbb{N}}$ par récurrence en posant par exemple

$$\begin{cases} x_1 = b & \text{(1.120a)} \\ x_{n+1} = f(x_n). & \text{(1.120b)} \end{cases}$$

Parfois nous pouvons avoir envie de définir une suite par récurrence de telle sorte que chaque nouveau terme dépende de tous les précédents :

$$\begin{cases} x_1 = b & \text{(1.121a)} \\ x_{n+1} = g(x_1, \dots, x_{n-1}). & \text{(1.121b)} \end{cases}$$

Pour ce faire, il faut un peu adapter.

Posons $E' = E \cup (E \times E) \cup (E \times E \times E) \cup \dots$. Nous supposons avoir une application $g\colon E' \to E'$ qui ne prend ses valeurs que dans E : $g(E') \subset E$. De plus nous considérons l'application

$$\begin{aligned} a\colon \mathbb{N} &\to E' \\ n &\mapsto \big(f(0), \dots, f(n)\big). \end{aligned} \tag{1.122}$$

Le théorème 1.131 appliqué à $g \circ a$ nous donne l'existence et l'unicité d'une application $f\colon \mathbb{N} \to E'$ telle que

$$\begin{cases} f(0) = b & \text{(1.123a)} \\ f(n+1) = g\big(f(0), \dots, f(n)\big). & \text{(1.123b)} \end{cases}$$

COROooVNHKooRkKtXf

Corolaire 1.135 ([18]).
Soient deux ensembles X, Y, une application $\alpha\colon X \to Y$ et une application $\beta\colon Y \to Y$. Alors il existe une unique application $H\colon X \times \mathbb{N} \to Y$ telle que

(1) $H(x,0) = \alpha(x)$ pour tout élément $x \in X$;

(2) $H(x,n+1) = \beta(H(x,n))$ pour tout élément $x \in X$ et pour tout $n \in \mathbb{N}$.

Démonstration. Pour faire le lien avec les notations du théorème 1.131, nous notons $E = \mathrm{Fun}(X,Y)$, $b = \alpha \in E$ et

$$\begin{aligned} g\colon E &\to E \\ s &\mapsto \beta \circ s. \end{aligned} \tag{1.124}$$

Le théorème 1.131 donne alors l'existence d'une application $f\colon \mathbb{N} \to E$ telle que

(1) $f(0) = b$

(2) $f(n+1) = g\big(f(n)\big)$.

Nous définissons alors

$$\begin{aligned} H\colon X \times \mathbb{N} &\to Y \\ (x,n) &\mapsto f(n)x, \end{aligned} \tag{1.125}$$

et nous vérifions qu'elle satisfait aux exigences.

(1) D'abord nous avons

$$H(x,0) = f(0)x = b(x) = \alpha(x). \tag{1.126}$$

(2) Ensuite, pour $x \in X$ et $n \in \mathbb{N}$ nous avons :

$$\begin{aligned} H(x,n+1) &= f(x+1)x && \text{(1.127a)} \\ &= g\big(f(n)\big)x && \text{(1.127b)} \\ &= g\big(f(n)\big)x && \text{(1.127c)} \\ &= \big(\beta \circ f(n)\big)x && \text{(1.127d)} \\ &= \beta\big(f(n)x\big) && \text{(1.127e)} \\ &= \beta\big(H(x,n)\big). && \text{(1.127f)} \end{aligned}$$

Et voilà. □

1.5.4 Addition sur les naturels

PROPooVFOXooXmwpFh

Proposition-Définition 1.136 ([39, 1]).
Il existe une unique fonction $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ vérifiant

ITEMooILZSooNYIkYR

(1) $f(a,0) = a$ pour tout $a \in \mathbb{N}$

ITEMooZWHQooBAjZyE

(2) $f\big(a,s(b)\big) = s\big(f(a,b)\big)$ pour tout $a,b \in \mathbb{N}$.

Pour $a,b \in \mathbb{N}$ nous notons $f(a,b) = a+b$.

Démonstration. Soit $a \in \mathbb{N}$. Le théorème 1.131 dit qu'il existe une unique application $f_a\colon \mathbb{N} \to \mathbb{N}$ telle que pour tout $x \in \mathbb{N}$, SUBEQSooWUGPooSxezFi

$$\begin{cases} f_a(0) = a & \text{EQooVOCZooOCHZLn} \quad \text{(1.128a)} \\ f_a\big(s(x)\big) = s\big(f_a(x)\big). & \text{EQooMEYWooEsWofl} \quad \text{(1.128b)} \end{cases}$$

Montrons qu'une telle application vérifie $f_0(a) = a$ pour tout $a \in \mathbb{N}$. Pour cela nous utilisons la récurrence de la proposition 1.130 en posant

$$\begin{aligned} P\colon \mathbb{N} &\to \{0,1\} \\ n &\mapsto \begin{cases} 1 & \text{si } f_0(n) = n \\ 0 & \text{sinon.} \end{cases} \end{aligned} \tag{1.129}$$

Nous avons $f_0(0)=0$ en posant $a=0$ dans (1.128a). Supposons ensuite que $P(a)=1$. Nous avons

$$f_0\big(s(a)\big)=s\big(f_0(a)\big) \tag{1.130a}$$
$$=s(a) \qquad \text{pcq } P(a)=1. \tag{1.130b}$$

Donc $P\big(s(a)\big)=s(a)$. Nous en déduisons que $P(x)=1$ pour tout $x\in\mathbb{N}$ et donc que

$$f_0(x)=x \tag{1.131}$$

EQooIKGVooHQMQqX

pour tout x.

Avec ça, nous prouvons ce qu'il faut.

(1) **Existence** Nous posons $f(a,b)=f_a(b)$, et nous prouvons les deux conditions.

(1a) **Condition (1)** Nous avons $f(a,0)=f_a(0)=a$ par (1.131).

(1b) **Condition (2)** Nous avons :

$$f\big(a,s(b)\big)=f_a\big(s(b)\big)=s\big(f_a(b)\big)=s\big(f(a,b)\big). \tag{1.132}$$

(2) **Unicité** Soient f et g deux applications vérifiant les conditions. Nous posons

$$\begin{aligned} f_a\colon\mathbb{N}&\to\mathbb{N}\\ x&\mapsto f(a,x) \end{aligned} \tag{1.133}$$

et $g_a\colon\mathbb{N}\to\mathbb{N}$ de la même manière. Nous prouvons que f_a et g_a vérifient tous deux les conditions (1.128). Cela donnera $f_a=g_a$ et donc $f=g$.

D'abord

$$f_a\big(s(b)\big)=f\big(a,s(b)\big)=s\big(f(a,b)\big)=s\big(f_a(b)\big). \tag{1.134}$$

Ensuite nous prouvons par récurrence que $f_a(0)=a$ pour tout $a\in\mathbb{N}$. D'abord $f(0,0)=0$, ensuite

$$f\big(0,s(a)\big)=s\big(f(0,a)\big)=s(a). \tag{1.135}$$

De même g_a vérifie les conditions.

□

LEMooMJMTooOtUuJT

Lemme 1.137 ([39]).
Pour tout $a\in\mathbb{N}$ nous avons $s(a)=a+1$.

Démonstration. Nous avons :

$$s(a)=s(a+0) \tag{1.136a}$$
$$=a+s(0) \tag{1.136b}$$
$$=a+1. \tag{1.136c}$$

SUBEQooMNBLooTQruhE
SUBEQooAGUSooGiIYGi
SUBEQooUZQDooWtNBHQ

Justifications.

(1) Pour (1.136a) c'est dans la définition 1.136(1) de la somme.

(2) Pour (1.136b), c'est dans la définition 1.136(2) de la somme.

(3) Pour (1.136c). Le symbole « 1 » désigne l'élément $s(0)$ dans $\mathbb{N}$.

□

PROPooTLTSooGNMTmV

Proposition 1.138 ([39]).
En ce qui concerne la somme dans $\mathbb{N}$.

ITEMooIFFPooXfftfG

(1) La somme est associative et commutative.

ITEMooSGRVooPAVFYK

(2) L'élément 0 est neutre.

ITEMooNUTHooJWWzGv

(3) Tous les éléments de $\mathbb{N}$ sont réguliers[53] par rapport à l'addition, c'est-à-dire que si $a+x=a+y$ alors $x=y$.

[53] Élément régulier pour une opération, définition 1.68.

Démonstration. En plusieurs parties.

(1) **Associative** Nous devons prouver que $(a+b)+c=a+(b+c)$ pour tout $a,b,c\in\mathbb{N}$. Pour ce faire, nous fixons $a,b\in\mathbb{N}$ et nous prouvons l'égalité demandée par récurrence sur c.

Pour $c=0$, nous avons $(a+b)+c=a+b$ et $a+(b+c)=a+b$. Donc nous sommes d'accord[54].

Nous vérifions avec $s(c)$:

$$\begin{aligned}(a+b)+s(c)&=s\big((a+b)+c\big) && (1.137a)\\ &=s\big(a+(b+c)\big) && (1.137b)\\ &=a+s(b+c) && (1.137c)\\ &=a+\big(b+s(c)\big). && (1.137d)\end{aligned}$$

SUBEQooDDUBooAjuuZq

Justifications.

- Pour (1.137b). C'est l'hypothèse de récurrence. À ce stade, je vous conseille d'être capable de rédiger complètement la récurrence et l'appel au théorème 1.131.

(2) **Neutre** La définition de l'addition contient déjà $a+0=a$. Nous prouvons par récurrence que $0+a=a$ pour tout $a\in\mathbb{N}$.

Pour $a=0$, l'égalité demandé est correcte : $0+0=0$ parce que pour tout x dans $\mathbb{N}$, $0+x=x$. Pour $s(a)$ nous avons

$$0+s(a)=s(0+a)=s(a). \tag{1.138}$$

La dernière égalité est l'hypothèse de récurrence.

Nous posons

$$A=\{a\in\mathbb{N}\text{ tel que }0+a=a\}. \tag{1.139}$$

Nous avons prouvé que $0\in A$ et que $s(A)\subset A$. Le théorème 1.131 nous assure alors que $A=\mathbb{N}$.

(3) **Commutativité** Nous fixons $a\in\mathbb{N}$ et nous prouvons par récurrence sur b que $a+b=b+a$ pour tout $b\in\mathbb{N}$. Cela va être décomposé en plusieurs étapes.

(4) $a+0=0+a$ Pour $b=0$ c'est correct, car $b+0=0+b=b$ parce que 0 est neutre.

(5) $a+1=1+a$ Nous démontrons par récurrence sur a que $a+1=1+a$. Avec $a=0$ c'est déjà fait. Pour les autres,

$$\begin{aligned}s(a)+1&=(a+1)+1 && \text{lemme 1.137} && (1.140a)\\ &=(1+a)+1 && \text{hypothèse récurrence} && (1.140b)\\ &=1+(a+1) && \text{associativité} && (1.140c)\\ &=1+s(a). && && (1.140d)\end{aligned}$$

(6) $a+b=b+a$ Nous y voici. Nous fixons a et nous prouvons par récurrence que $a+b=b+a$. Pour $b=0$ c'est déjà fait. Pour les autres,

$$\begin{aligned}a+s(b)&=a+(b+1) && && (1.141a)\\ &=(a+b)+1 && && (1.141b)\\ &=(b+a)+1 && \text{hypothèse récurrence} && (1.141c)\\ &=b+(a+1) && && (1.141d)\\ &=b+(1+a) && \text{commutativité avec 1} && (1.141e)\\ &=(b+1)+a && \text{associativité} && (1.141f)\\ &=s(b)+a. && && (1.141g)\end{aligned}$$

Récurrence terminée.

[54] Notez que nous n'avons pas utilisé le fait que 0 était neutre des deux côtés – chose que nous n'avons pas encore démontré. Nous avons seulement utilisé $a+0=a$, qui est dans la définition de la somme.

(7) **Régularité** Nous devons prouver que, pour tout $a,x,y\in\mathbb{N}$, si $a+x=a+y$ alors $x=y$. Nous allons procéder par récurrence en posant

$$A=\{a\in\mathbb{N}\text{ tel que }\forall x,y\in\mathbb{N},a+x=a+y\Rightarrow x=y\}. \tag{1.142}$$

Puisque $0+x=x$ et $0+y=y$, nous avons $0\in A$. Supposons à présent que $a\in A$ et montrons que $s(a)\in A$. Soient $x,y\in\mathbb{N}$ tels que $a+x=a+y$. Nous avons :

$$\begin{aligned}
& s(a)+x=s(a)+y && \text{(1.143a)}\\
\Rightarrow\quad & s(a+x)=s(a+y) && \text{(1.143b)}\\
\Rightarrow\quad & a+x=a+y && \text{(1.143c)}\\
\Rightarrow\quad & x=y && \text{(1.143d)}
\end{aligned}$$

SUBEQooNJHZooSIKPxN
SUBEQooWDJLooJhzIFe
SUBEQooTLYZooFsMaJD

Justifications.

- Pour (1.143b). En utilisant la définition de l'addition et la commutativité, nous avons $s(a)+x=s(a+x)$.
- Pour (1.143c). Parce que s est injective ; c'est dans la définition 1.125 d'un triplet naturel.
- Pour (1.143d). Parce que $a\in A$.

Nous avons prouvé que $s(A)\subset A$, et donc que $A=\mathbb{N}$.

□

LEMooCOMSooEWrumL

Lemme 1.139.
Nous avons $0\neq 1$.

Démonstration. Par définition $1=s(0)$. Comme s est à valeurs dans $\mathbb{N}\setminus\{0\}$, nous ne pouvons pas avoir $s(0)=0$. □

LEMooQBHFooCuCusQ

Lemme 1.140 ([1])**.**
Si $a+b=0$*, alors* $a=b=0$.

Démonstration. Soient $a,b\in\mathbb{N}$ tels que $a+b=0$, et supposons que $b\neq 0$. Par la définition 1.125(2), nous avons $b=s(c)$ pour un certain $c\in\mathbb{N}$.

Dans ce cas nous avons $a+b=a+s(c)=s(a+c)\neq 0$ parce que l'image de s ne contient pas 0. Hélas, par hypothèse nous avons $a+b=0$. Nous avons obtenu une contradiction, et nous déduisons que $b=0$.

Maintenant que nous savons que $b=0$, il reste $0=a+b=a+0=a$. □

1.5.5 Ordre sur les naturels

DEFooXZZooNEHMjM

Définition 1.141 (Relation d'ordre[39])**.**
Pour $a,b\in\mathbb{N}$*, nous notons* $a\leqslant b$ *si il existe* $x\in\mathbb{N}$ *tel que* $a+x=b$.

Nous notons également $a<b$ *si* $a\leqslant b$ *et* $a\neq b$.

LEMooVOTAooALatDu

Proposition-Définition 1.142 ([1])**.**
Si $a\leqslant b$*, il existe un unique* $x\in\mathbb{N}$ *tel que* $a+x=b$.

Nous notons $b-a$ *l'unique élément de* $\mathbb{N}$ *tel que*

$$a+(b-a)=b. \tag{1.144}$$

Démonstration. L'existence est juste la définition 1.141. En ce qui concerne l'unicité, si $a+x=b=a+y$, alors la proposition 1.138(3) donne $x=y$. □

LEMooWMYPooLTMyWb

Lemme 1.143.
Nous avons $a\leqslant s(a)$ *pour tout* $a\in\mathbb{N}$.

Démonstration. Cela est une conséquence du lemme 1.137 : $s(a)=a+1$. □

PROPooVXBBooZcghrA

Proposition 1.144.
La relation $\leqslant$ *est une relation d'ordre compatible avec l'addition.*

Démonstration. Plusieurs choses à vérifier.

(1) **Réflexive** Nous avons $a\leqslant a$ parce que $a+0=a$.

(2) **Antisymétrique** Soient $a, b \in \mathbb{N}$ tels que $a \leqslant b$ et $b \leqslant a$. Il existe $x, y \in \mathbb{N}$ tels que

$$b = a + x \tag{1.145a}$$
$$a = b + y. \tag{1.145b}$$

En substituant la seconde équation dans la première, $b = (b + y) + x$ que nous récrivons, en utilisant l'associativité[55],

$$0 + b = b + (x + y). \tag{1.146}$$

En utilisant la régularité, $0 = x + y$ et donc $x = y = 0$ par le lemme 1.140. Cela donne alors $a = b$.

(3) **Transitive** Si $a \leqslant b$ et $b \leqslant c$, nous avons $n, p \in \mathbb{N}$ tels que $b = a + n$ et $c = b + p$. Donc

$$c = (a + n) + p = a + (n + p), \tag{1.147}$$

ce qui signifie que $a \leqslant c$. Notez l'utilisation de l'associativité de la somme, démontrée en la proposition 1.138(1).

(4) **Compatibilité** Soient $a, b, n \in \mathbb{N}$ tels que $a \leqslant b$. Nous devons montrer que $a + n \leqslant b + n$. Puisque $a \leqslant b$, il existe $x \in \mathbb{N}$ tel que $b = a + x$. Par conséquent,

$$b + n = a + x + n = (a + n) + x, \tag{1.148}$$

qui signifie bien que $a + n \leqslant b + n$.

□

LEMooPVRQooXPMKTt

Lemme 1.145.
À propos d'ordre et de stricte inégalité.

ITEMooGWWFooYGPCZw

(1) *Si $x \leqslant a$ et $b \neq 0$, alors $x < a + b$.*

ITEMooRWGWooAfkrri

(2) *Si $x \leqslant a$, alors $x < s(a)$.*

ITEMooWCOIooMWrCag

(3) *Si $x < a$, alors $s(x) \leqslant a$.*

Démonstration. En plusieurs parties.

(1) **Pour (1)** Si $x \leqslant a$, il existe $d \in \mathbb{N}$ tel que $x + d = a$. Nous avons alors aussi

$$x + d + b = a + b, \tag{1.149}$$

ce qui signifie que $x \leqslant a + b$. Mais si x était égal à $a + b$, nous aurions $d + b = 0$, ce qui impliquerait[56] $d = b = 0$, alors que l'hypothèse stipule que $b \neq 0$. Donc $x \neq a + b$.

(2) **Pour (2)** Il s'agit seulement d'utiliser le point (1) avec $b = 1$ et le fait que $s(a) = a + 1$ par le lemme 1.137.

(3) **Pour (3)** Par hypothèse, il existe $b \neq 0$ tel que $x + b = a$. Puisque $b \neq 0$, il existe $c \in \mathbb{N}$ tel que $b = s(c)$ et donc, tel que

$$x + s(c) = a. \tag{1.150}$$

En utilisant le fait que $s(c) = c + 1$ ainsi que l'associativité et la commutativité de l'addition (proposition 1.138(1)) nous avons

$$a = x + s(c) = s(x) + c, \tag{1.151}$$

ce qui prouve que $s(x) \leqslant a$.

□

PROPooAKLVooBkRIAT

Proposition 1.146 ([1]).
Soient $a, b, k \in \mathbb{N}$. Nous avons

ITEMooFMQCooSjuCDV

(1)

$$(a - k) + b = (a + b) - k. \tag{1.152}$$

[55] Proposition 1.138(1).
[56] Par le lemme 1.140.

ITEMooKHLDooEEXjmF

(2)

$$(a-k)+k=(a+k)-k=a. \tag{1.153}$$

Démonstration. En plusieurs parties.

(1) **Pour (1)**
Nous posons $A=(a-k)+b$ et $B=(a+b)-k$. En utilisant l'associativité et la symétrie de l'addition,

$$\begin{aligned} A+k&=(a-k)+b+k & \text{(1.154a)}\\ &=\big((a-k)+k\big)+n & \text{(1.154b)}\\ &=a+b & \text{(1.154c)}\end{aligned}$$

parce que par définition $(a-k)+k=a$. Nous avons aussi

$$\big((a+b)-k\big)+k=a+b. \tag{1.155}$$

Donc $A+k=B+k$ et donc $A=B$ par 1.138(3), nous avons $A=B$.

(2) **Pour (2)** En utilisant le point (1) avec $b=k$ nous avons déjà $(a-k)+k=(a+k)-k$. Or par définition l'élément $(a+k)-k$ est le x tel que $x+k=a+k$. Cela est forcément $x=a$ par la proposition 1.138(3).

□

PROPooJSZHooVDzBDE

Proposition 1.147 ([1]).
Plusieurs choses.

ITEMooVSLRooGhGFgX

(1) Soit $a\leqslant b$ dans $\mathbb{N}$. Si $k\leqslant a$ et $k\leqslant b$ alors

$$a-k\leqslant b-k. \tag{1.156}$$

ITEMooYGOAooWRbKdj

(2) Nous avons

$$a-k<a \tag{1.157}$$

pour tout $k\neq 0$ dans $\mathbb{N}$.

Démonstration. Nous commençons par prouver (1). Vu que $a\leqslant b$, il existe un $y\in\mathbb{N}$ tel que $a+y=b$, et ce y est nommé $b-a$ (par définition 1.142 de la soustraction). Voyons maintenant

$$\begin{aligned} (a-k)+y&=(a+y)-k & \text{prop. 1.146} & \text{(1.158a)}\\ &=b-k & \text{pcq. } a+y=b. & \text{(1.158b)}\end{aligned}$$

Cela signifie que $a-k\leqslant b-k$.

Pour (2). D'abord nous avons $(a-k)+k=a$ par la proposition 1.146(2). Cela prouve que $a-1\leqslant a$. Ensuite nous supposons que $a-k=a$ et nous prouvons que $k=0$. Pour cela nous ajourons a des deux côtés :

$$(a-k)+k=a+k. \tag{1.159}$$

En utilisant à nouveau le fait que $(a-k)+k=a$ nous avons $a=a+k$. Et nous en déduisons $k=0$ avec la proposition 1.138(3). □

PROPooHRCOooBkEvud

Proposition 1.148 ([1]).
Soient $a,x\in\mathbb{N}$. Nous avons $x\leqslant a-1$ si et seulement si $x<a$.

Démonstration. En deux sens.

(1) $\Rightarrow$ Nous supposons que $x\leqslant a-1$. Grâce à la proposition 1.147(2) nous avons $x\leqslant a-1<a$.

(2) $\Leftarrow$ Nous supposons que $x<a$. Par le lemme 1.145(3), nous avons $x+a\leqslant a$. La proposition 1.147 donne alors

$$(x+1)-1\leqslant a-1. \tag{1.160}$$

Et maintenant la proposition 1.146(2) donne $x\leqslant a-1$.

□

LEMooCSIXooHeuWEd

Lemme 1.149.
L'élément 0 *est l'unique plus petit élément de* $\mathbb{N}$.

Démonstration. Puisque 0 est neutre pour l'addition[57], nous avons $a+0=a$ pour tout $a\in\mathbb{N}$ et donc $0\leqslant a$ pour tout a. Cela veut dire que 0 est plus petit que tout élément de $\mathbb{N}$.

En ce qui concerne l'unicité, soit $z\in\mathbb{N}$ tel que $z\leqslant a$ pour tout $a\in\mathbb{N}$. Si $z\neq 0$, il existe $x\in\mathbb{N}$ tel que $z=s(x)$. Nous avons donc $z\geqslant x$ en même temps que $x\leqslant z$. Cela implique $z=x$ (parce qu'une relation d'ordre est symétrique) et donc $z=z+1$. En utilisant la régularité de z pour l'addition nous en déduisons que $0=1$, ce qui est impossible par le lemme 1.139. □

LEMooJRZKooOMhOkH

Lemme 1.150.
Si $a\leqslant b$ *et* $b\leqslant a$, *alors* $a=b$.

Démonstration. L'inégalité $a\leqslant b$ dit qu'il existe $x\in\mathbb{N}$ tel que $a+x=b$. En mettant cela dans l'inégalité $b\leqslant a$ nous trouvons $a+x\leqslant a$ qui donne, via la proposition 1.144 : $x\leqslant 0$. Nous en déduisons que $x=0$ parce que zéro est l'unique minimum de $\mathbb{N}$ par le lemme 1.149. □

PROPooGCCRooFBYrlo

Proposition 1.151.
Le couple $(\mathbb{N},\leqslant)$ *est totalement ordonné*[58].

Démonstration. Soit $a\in\mathbb{N}$. Nous devons prouver que pour tout $x\in\mathbb{N}$ nous avons $x\leqslant a$ ou $a\leqslant x$ (non exclusifs). Nous posons

$$A=\{x\in\mathbb{N}\text{ tel que }x\leqslant a\}\tag{1.161a}$$
$$B=\{x\in\mathbb{N}\text{ tel que }a\leqslant x\},\tag{1.161b}$$

et nous prouvons que $A\cup B=\mathbb{N}$ en montrant que $0\in A\cup B$ et que $s(A\cup B)\subset A\cup B$.

Nous avons $0\in A\subset A\cup B$ par le lemme 1.149.

Pour étudier $s(A\cup B)$, nous considérons $x\in A\cup B$ et nous subdivisons en deux cas selon que $x\in A$ ou $x\in B$.

(1) **Si $x\in B$** Si $x\in B$, alors $a\leqslant x\leqslant s(x)$ parce que $x\leqslant s(x)$ par le lemme 1.143. Donc $s(x)\in B\subset A\cup B$.

(2) **Si $x\in A$** Si $x\in A$, il y a deux possibilités : $x=a$ et $x\neq a$. Si $x=a$, alors $a\leqslant s(x)$ et donc $s(x)\in A\subset A\cup B$.

Si $x\neq a$, alors le lemme 1.145(3) nous indique que $s(x)\leqslant a$ et donc $s(x)\in A\subset A\cup B$.

Nous avons donc prouvé que $s(A\cup B)\subset A\cup B$, et donc que $A\cup B=\mathbb{N}$. □

PROPooMZOWooHmsXzI

Proposition 1.152 ([39, 1])**.**
L'ensemble ordonné $(\mathbb{N},\leqslant)$ *vérifie les propriétés suivantes.*

ITEMooJLAHooDKukfH

(1) L'élément 0 *est l'unique minimum de* $\mathbb{N}$.

ITEMooYAJIooEFmOpB

(2) Toute partie non vide a un unique plus petit élément.

ITEMooSRGOooNYJJHY

(3) L'ensemble $\mathbb{N}$ *n'a pas de plus grand élément.*

ITEMooKIHZooDRTCdx

(4) Toute partie non vide majorée a un unique plus grand élément.

Démonstration. Point par point.

(1) **Pour (1)** C'est le lemme 1.149.

(2) **Pour (2)** Soit une partie A non vide dans $\mathbb{N}$. Si $0\in A$, nous avons fini.

(2a) **L'ensemble B** Nous supposons donc que A ne contient pas zéro et nous définissons

$$B=\{n\in\mathbb{N}\setminus A\text{ tel que }n\leqslant a,\forall a\in A\}.\tag{1.162}$$

(2b) **Un élément particulier dans B** L'ensemble B vérifie :

- $0\in B$

[57] Proposition 1.138(2).
[58] Définition 1.26.

- $B \neq \mathbb{N}$ parce que A est non vide.

La contraposée de la condition (3) de la définition 1.125 d'un triplet naturel implique que $s(B) \not\subset B$. Autrement dit, il existe $b \in B$ tel que $s(b) \notin B$.

(2c) **Deux fonctions sur A** Puisque $b \in B$, nous avons une application $c\colon A \to \mathbb{N}$ telle que $b + c(a) = a$. Nous avons $c(a) \neq 0$ parce que $c(a) = 0$ signifierait $b = a$, ce qui est impossible parce que $a \in A$ et $b \in B$.

Comme pour tout $a \in A$, l'élément $c(a)$ est non nul, il existe une fonction $d\colon A \to \mathbb{N}$ telle que $c(a) = d(a) + 1$.

(2d) $s(b) \in A$ Supposons que $s(b) \notin A$. Alors il existe $a \in A$ tel que $s(b) \leqslant a$ est faux. Puisque l'ordre est total (proposition 1.151), nous avons

$$a \leqslant s(b). \tag{1.163}$$

Comme $b \in B$ nous avons aussi

$$b \leqslant a. \tag{1.164}$$

Et enfin nous avons

$$b \neq a \tag{1.165}$$

parce que $a \in A$ et $b \in B$.

Les conditions (1.164) et (1.165) se résument en $b < a$. Le lemme 1.145(3) nous indique alors que $s(b) \leqslant a$. Cela mis à côté de (1.163) conclut que $a = s(b)$, et donc que $s(b)$ est dans A. Contradiction. Nous en concluons que $s(b) \in A$.

(2e) $s(b)$ **est un minimum de A** En utilisant la commutativité et l'associativité de la somme nous avons, pour tout $a \in A$:

$$a = b + c(a) = b + \big(d(a) + 1\big) = (b + 1) + d(a) = s(b) + d(a). \tag{1.166}$$

Donc $s(b) \leqslant a$ pour tout $a \in A$. Mais comme $s(b) \in A$, l'élément $s(b)$ est bien un minimum de A.

(2f) **Unicité** Si a et a' sont des minimums de A, alors $a \leqslant a'$ et $a' \leqslant a$. Nous en déduisons que $a = a'$.

(3) **Pour (3)** Si $M \in \mathbb{N}$ majore tous les éléments de $\mathbb{N}$, alors en particulier $M \geqslant s(M)$. Mais le lemme 1.143 nous indique que $M \leqslant s(M)$. Nous avons donc $s(M) = M$, c'est-à-dire $M = M + 1$. En utilisant la régularité de M[59], nous trouvons $0 = 1$, ce qui est impossible par le lemme 1.139.

(4) **Pour (4)** Soit A une partie non vide et majorée de $\mathbb{N}$.

(4a) **L'ensemble B** Nous posons

$$B = \{n \in \mathbb{N} \setminus A \text{ tel que } a \leqslant n, \forall a \in A\}. \tag{1.167}$$

(4b) **B est non vide** Soit un majorant M de A : pour tout $a \in A$ nous avons $a \leqslant M$. Nous avons $s(M) \notin A$, parce que si $s(M)$ était dans A, ce serait un élément de A strictement plus grand que tout $a \in A$. Donc B est non vide parce qu'il contient $s(M)$.

(5) **Minimum** Puisque B est non vide, il possède un plus petit élément que nous notons b. Nous savons que $b \neq 0$ parce que sinon A serait vide. Il existe donc $c \in \mathbb{N}$ tel que $b = s(c)$.

(6) $a \leqslant c$ **pour tout $a \in A$** Comme $s(c) \in B$ nous avons $a < s(c)$ pour tout $a \in A$. Donc, par le lemme 1.145(3) nous avons $s(a) \leqslant s(c)$, c'est-à-dire $a + 1 \leqslant c + 1$. Par régularité nous avons $a \leqslant c$.

Nous avons prouvé que $a \leqslant c$ pour tout $a \in A$.

(7) $c \in A$ Si c n'est pas dans A, alors il est dans B et il contredit la minimalité de b. Donc c est dans A.

(8) **Conclusion** L'élément c est dans A tout en étant plus petit que tout élément de A.

(9) **Unicité** Si x est un élément minium de A, alors nous avons $x \leqslant c$ parce que x est minimum et $c \leqslant x$ parce que c est minimum, et donc $x = c$.

□

[59] Dit plus simplement : en simplifiant par M.

PROPooTQDJooFQGFpC

Proposition 1.153 ([1]).
Soient $s, k \in \mathbb{N}$.

ITEMooPQETooJYjhUj

(1) Si $s > k$ alors $s - 1 \geqslant k$.

ITEMooZLXQooPRLNoN

(2) Si $s \geqslant k$ alors $s + 1 > k$.

Démonstration. En deux parties.

(1) **Pour (1)** Nous supposons que $s > k$. Il existe $x \in \mathbb{N}$ tel que $s + x = k$ et $x \neq 0$ parce que $s \neq k$. En utilisant la proposition 1.146 nous avons $k + (x - 1) = s - 1$, c'est-à-dire $k \geqslant s - 1$.

(2) **Pour (2)** Nous savons que $s + x = k$ pour un certain $x \in \mathbb{N}$. Nous avons alors

$$(s + 1) + x = k + 1 > k. \tag{1.168}$$

□

PROBooUCQFooTugfDl

¡¡ Avertissement/question au lecteur !! 1.154
Je ne suis pas certain qu'il y ait moyen de prouver le lemme 2.31 sans d'abord définir les naturels. Une raison est que la véracité de ce lemme est à peu près équivalente au théorème 1.131 qui donne l'existence de $\mathbb{N}$.

J'ai essayé un certain nombre de choses avec le lemme de Zorn sans succès.
Si vous avez une idée, n'hésitez pas à me la partager, ou à l'écrire ici :

https://math.stackexchange.com/questions/5019157/every-non-empty-dedekind-finite-totally-ordered-set-has-a-maximum-using-zorns

Dans la réponse de Asaf Karagila, il y a seulement le fait que $f : D \to D$ que je ne comprends pas. C'est d'ailleurs ma dernière question dans les commentaires.

LEMooYMRJooYIAhBb

Lemme 1.155 ([1]).
Quelques affirmations sur l'ordre dans $\mathbb{N}$.

ITEMooTLOIooTWNtod

(1) Il n'existe pas de $n \in \mathbb{N}$ tel que $n < 0$.

ITEMooPJKQooGfLCUM

(2) Si $a, b \in \mathbb{N}$ vérifient $a > b$, alors il n'existe pas de x dans $\mathbb{N}$ tel que $a + x = b$.

Démonstration. En deux parties.

(1) **Pour (1)** Nous savons par la proposition 1.152(1) que 0 est l'unique minimum de $\mathbb{N}$. Nous avons donc forcément $0 \leqslant n$. Si n vérifie de plus $n \leqslant 0$ alors nous avons $n = 0$ par symétrie de la relation d'ordre $\leqslant$. Il n'est donc pas possible d'avoir $n \neq 0$.

(2) **Pour (2)** Si $b \leqslant a$ il existe $c \in \mathbb{N}$ tel que $b + c = a$. Et comme $a \neq b$, c n'est pas nul et il existe $y \in \mathbb{N}$ tel que $c = s(y)$. Bref, nous avons

$$b + s(y) = a. \tag{1.169}$$

Si de plus il existe $x \in \mathbb{N}$ tel que $a + x = b$ nous aurions

$$a + x + s(y) = a. \tag{1.170}$$

Comme a est régulier pour l'addition[60], nous avons

$$x + s(y) = 0, \tag{1.171}$$

ce qui signifie, par le lemme 1.140 que $x = s(y) = 0$. Puisque s prend ses valeurs dans $\mathbb{N} \setminus \{0\}$, cela est impossible.

□

DEFooKBUFooLvMHrf

Définition 1.156.
Soient $a, b \in \mathbb{N}$ tels que $a \leqslant b$. Nous notons par $\{a, \dots, b\}$ l'ensemble

$$\{x \in \mathbb{N} \text{ tel que } a \leqslant x \leqslant b\}. \tag{1.172}$$

[60] Proposition 1.138(3).

PROPooFYMJooWihvhk

Proposition 1.157.
Toute application $\mathbb{N} \to \mathbb{N}$ strictement croissante est injective.

Démonstration. Soit une application strictement croissante $f : \mathbb{N} \to \mathbb{N}$. Soient $a, b \in \mathbb{N}$ tels que $f(a) = f(b)$. Puisque l'ordre est total[61], nous supposons que $a \leqslant b$. Si $a = b$ nous avons terminé. Nous supposons donc que $a \neq b$, c'est-à-dire que $a < b$. Par stricte croissance nous avons alors $f(a) < f(b)$ qui signifie $f(a) \leqslant f(b)$ et $f(a) \neq f(b)$. Contradiction. Il n'existe donc pas de $a \neq b$ tels que $f(a) = f(b)$. L'application f est donc injective. □

LEMooFKLPooPrmeUU

Lemme 1.158 ([1]).
Si S n'est pas majoré dans $\mathbb{N}$, alors il existe une bijection $\mathbb{N} \to S$.

Démonstration. Nous considérons l'application suivante :

$$\begin{aligned} g : S &\to S \\ n &\mapsto \min\{x \in S \text{ tel que } x > n\}. \end{aligned} \tag{1.173}$$

Cette application est bien définie parce que tout partie non vide de $\mathbb{N}$ a un plus petit élément[62]. Maintenant nous définissons $f : \mathbb{N} \to S$ par

$$\begin{cases} f(0) = \min(S) & \text{(1.174a)} \\ f(n+1) = g\big(f(n)\big). & \text{(1.174b)} \end{cases}$$

C'est le théorème 1.131 qui nous permet de le faire. Nous montrons que f est bijective.

(1) **Injective** Nous avons
$$f(n+1) \in \{x \in S \text{ tel que } x > f(n)\}. \tag{1.175}$$
Donc f est strictement croissante. Elle est donc injective.

(2) **Surjective** Soit $a \in S$. Nous allons voir que a est dans l'image de f. Pour cela nous posons
$$A = \{x \in \mathbb{N} \text{ tel que } f(x) < a\}. \tag{1.176}$$
Cet ensemble est majoré par a. En effet si $x \in A$ nous avons $x \leqslant f(x) < a$. La partie A de $\mathbb{N}$ possède un maximum. Nous notons $M = \max(A)$. Ce M a deux propriétés intéressantes.

(2a) **D'abord** Puisque $M \in A$, nous avons $f(M) < a$. Une autre façon de dire cela est de dire que
$$a \in \{x \in S \text{ tel que } x > f(M)\}. \tag{1.177}$$
Or $f(M+1) = \min\{x \in S \text{ tel que } x > f(M)\}$. Donc $f(M+1) \leqslant a$.

(2b) **Ensuite** Puisque M est le maximum de A, $M+1$ majore A, c'est-à-dire que $f(M+1) \geqslant a$.

(2c) **Les deux ensemble** Nous avons prouvé que $f(M+1) \leqslant a$ et $f(M+1) \geqslant a$. Nous en déduisons, par le lemme 1.150, que $f(M+1) = a$.

□

NORMooQXASooMXqhjI

1.159.
Durant la preuve du lemme 1.158, nous n'avons pas été loin de prouver que
$$\big(\min(S), S, g\big) \tag{1.178}$$
est un triplet naturel.

Toute partie non bornée de $\mathbb{N}$ donne lieu à un triplet naturel.

LEMooLDKQooSTiVlW

Lemme 1.160 ([1]).
Si $A \subset \mathbb{N}$, alors
$$\min\big(A \setminus \{\min(A)\}\big) > \min(A). \tag{1.179}$$

Démonstration. Soient $m = \min(A)$ et $m' = \min\big(A \setminus \{m\}\big)$. Il y a trois possibilités : $m > m'$, $m = m'$ et $m < m'$. Supposons que $m' \leqslant m$. Étant donné que $m' \in A$, nous avons $m \leqslant m'$. Et donc $m = m'$, ce qui est impossibe parce que $m' \in A \setminus \{m\}$. □

[61] Proposition 1.151.
[62] Proposition 1.152(2).

1.5.6 Multiplication dans les naturels

SUBooMultiplicationNaturels

Définition 1.161 ([1]).
Soit un ensemble muni d'une loi de composition interne $(A,+)$. Soit $n\in\mathbb{N}$ et $a\in A$. Nous définissons $n\times A$ par

$$\begin{cases} 0\times a=0 & \text{(1.180a)}\\ (n+1)\times a=n\times a+a. & \text{(1.180b)}\end{cases}$$

DEFooLCWLooYrToFv

Définition 1.162.
*Un ensemble totalement ordonné muni d'une loi de composition interne $(A,+,\leqslant)$ est **archimédien** si pour tout $x,y\in A$ avec $x>0$, il existe $n\in\mathbb{N}$ tel que $n\times x\geqslant y$ (voir la définition 1.161).*

PROPooBBQPooRgPOjf

Proposition-Définition 1.163.
Il existe une unique fonction $f\colon\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ telle que

ITEMooNTUUooDAUVsV

(1) $f(a,0)=0$ pour tout $a\in\mathbb{N}$

ITEMooPPZZooQQabwn

(2) $f\big(a,s(b)\big)=f(a,b)+a$ pour tout $a,b\in\mathbb{N}$.

*Cette fonction est la **multiplication** et nous notons $f(a,b)=a\times b$, voire ab quand il n'y a pas d'ambigüité. Le nombre $a\times b$ est nommé le **produit** de a par b.*

Démonstration. En deux parties.

(1) **Fonctions définies par récurrence** Soit $a\in\mathbb{N}$. Par le théorème 1.131, il existe une unique application $f_a\colon\mathbb{N}\to\mathbb{N}$ telle que [EQSooWVCTooNTVjKU]

$$\begin{cases} f_a(0)=0 & \text{(1.181a)}\\ f_a\big(s(b)\big)=f_a(b)+a & \text{(1.181b)}\end{cases}$$

(2) **Existence** Nous considérons, pour chaque $a\in\mathbb{N}$ la fonction f_a définie par les conditions (1.181). En posant $f(a,b)=f_a(b)$, nous avons une application qui vérifie toutes les conditions.

(3) **Unicité** Soient des applications f et g vérifiant les propriétés demandées. Soit $a\in\mathbb{N}$. Nous pouvons définir $f_a\colon\mathbb{N}\to\mathbb{N}$ et $g_a\colon\mathbb{N}\to\mathbb{N}$ par $f_a(n)=f(a,b)$ et $g_a(b)=g(a,b)$.

Les applications f_a et g_a vérifient toutes deux les conditions (1.181), et sont donc égales : $f_a=g_a$ pour tout a. Donc $f=g$.

□

NORMooPrioriteOperations

1.164.
Nous supposons que le lecteur connait déjà la priorité des opérations. Il saura donc interpréter des expressions comme $a\times b+c$ comme voulant dire $(a\times b)+c$ sans que nous ayons à ajouter des parenthèses.

PROPooGHDOooFYRmon

Proposition 1.165 ([39, 1]).
La multiplication dans $\mathbb{N}$ possède les propriétés suivantes.

ITEMooHFWRooDCEpjj

(1) $n\times 1=n$ pour tout $n\in\mathbb{N}$.

ITEMooRSYMooSUrRsl

(2) $1\times n=n$ pour tout $n\in\mathbb{N}$.

ITEMooWJPOooRUYjwQ

(3) La multiplication est commutative.

ITEMooNBYKooXnGRrf

(4) $0\times n=0$ pour tout $n\in\mathbb{N}$

ITEMooLJQBooVpUxUv

(5) L'élément 1 est neutre pour la multiplication.

ITEMooDYLIooETIBEL

(6) La multiplication est distributive par rapport à l'addition.

ITEMooQBFSooWGDQYX

(7) La multiplication est associative.

Démonstration. Point par point.

(1) **Pour (1)** Nous avons $n\times 1=n\times s(0)=(n\times 0)+n=0+n=n$. Donc $n\times 1=n$.

(2) **Pour (2)** Nous le faisons par récurrence. Par définition c'est vrai pour $n=0$. En ce qui concerne la récurrence, nous supposons que $1\times n=n$, et nous prouvons que $1\times s(n)=s(n)$:

$$1\times s(n)=(1\times n)+1=n+1=s(n). \tag{1.182}$$

(3) **Pour (3)** Soit $a \in \mathbb{N}$. Nous prouvons par récurrence sur $b \in \mathbb{N}$ que $a \times b = b \times a$. Pour $b = 0$ c'est bon. Pour la récurrence, nous supposons que $a \times b = b \times a$ et nous prouvons que $a \times s(b) = s(b) \times a$:

$$\begin{aligned}
a \times s(b) &= a \times b + a && && (1.183a)\\
&= b \times a + a && \text{récurrence} && (1.183b)\\
&= (b \times a) + (1 \times a) && \text{par (2)} && (1.183c)\\
&= (b + 1) \times a && \text{distributivité} && (1.183d)\\
&= s(b) \times a. && && (1.183e)
\end{aligned}$$

(4) **Pour (4)** C'est vrai pour $n = 0$ par la définition 1.163(1). En ce qui concerne $s(n)$, nous avons

$$0 \times s(n) = (0 \times n) + 0 = 0. \tag{1.184}$$

(5) **Pour (5)** C'est la combinaison de (1) et (2).

(6) **Pour (6)** Soient $a, b \in \mathbb{N}$. Nous prouvons par récurrence sur $c \in \mathbb{N}$ que[63]

$$(a + b) \times c = a \times c + b \times c. \tag{1.185}$$

Pour $c = 0$, nous avons $(a + b) \times 0 = 0$ ainsi que $a \times 0 = b \times 0 = 0$ en vertu des points précédents sur la multiplication par zéro. Pour la récurrence nous utilisons associativité et commutativité de la somme :

$$\begin{aligned}
(a + b) \times s(c) &= (a + b) \times c + (a + b) && (1.186a)\\
&= a \times c + b \times c + a + b && (1.186b)\\
&= (a \times c + a) + (b \times c + b) && (1.186c)\\
&= \big(a \times s(c)\big) + \big(b \times s(c)\big). && (1.186d)
\end{aligned}$$

On devrait aussi prouver que $c(a + b) = ca + cb$: c'est peu ou prou la même chose.

(7) **Pour (7)** Soient $a, b \in \mathbb{N}$. Nous démontrons par récurrence sur $c \in \mathbb{N}$ que $(a \times b) \times c = a \times (b \times c)$. Pour $c = 0$ l'égalité est triviale. Nous supposons que l'égalité est correcte pour c, et nous la prouvons pour $s(c)$:

$$\begin{aligned}
(a \times b) \times s(c) &= \big((a \times b) \times c\big) + a \times b && && (1.187a)\\
&= \big(a \times (b \times c)\big) + a \times b && \text{récurrence} && (1.187b)\\
&= \big((b \times c) \times a\big) + b \times a && \text{commutativité} && (1.187c)\\
&= (b \times c + b) \times a && \text{distributivité} && (1.187d)\\
&= \big(b \times s(c)\big) \times a && \text{définition 1.163(2)} && (1.187e)\\
&= a \times \big(b \times s(c)\big) && \text{commutativité.} && (1.187f)
\end{aligned}$$

□

LEMooCompatMultiplicationOrdre

Lemme 1.166 ([1])**.**
La multiplication est compatible avec l'ordre :

$$a \leqslant b \Rightarrow a \times n \leqslant b \times n \tag{1.188}$$

pour tout $n \in \mathbb{N}$.

Démonstration. Par la définition 1.141 de l'ordre, si $a \leqslant b$, il existe $c \in \mathbb{N}$ tel que $b = a + c$. En utilisant la distributivité[64], nous avons

$$b \times n = (a + c) \times n = a \times n + c \times n. \tag{1.189}$$

Nous en déduisons que $a \times n \leqslant b \times n$ parce que $c \times n \in \mathbb{N}$. □

LEMooEHYEooLDudfn

Lemme 1.167.
Si $a \times b = 0$, alors $a = 0$ ou $b = 0$ (ou les deux).

[63] Nous n'écrivons pas toutes les parenthèses parce que les règles de priorité des opérations sont supposées connues. J'invite cependant la lectrice à remarquer qu'une formalisation de ces règles n'est probablement pas facile. Pour que tout soit rigoureux, il faudrait un algorithme qui parcourt une suite de caractères et l'interprète en ajoutant correctement les parenthèses.

[64] Proposition 1.165(6).

Démonstration. Supposons que $a \neq 0$. Alors il existe $c \in \mathbb{N}$ tel que $a = s(c)$. Nous avons

$$0 = a \times b = s(c) \times b = c \times b + b. \tag{1.190}$$

Le lemme 1.140 nous dit alors que $c \times b = b = 0$. □

LEMooGUXGooBcKJdS

Lemme 1.168 ([1]).
Soit a, b, n trois entiers naturels. Si $a < b$ et si $n \neq 0$, alors

$$a \times n < b \times n. \tag{1.191}$$

Démonstration. L'hypothèse $a \leqslant b$ implique qu'il existe $c \in \mathbb{N}$ tel que $a + c = b$. De plus $c \neq 0$ parce que $a \neq b$. En utilisant la distributivité[65], nous avons

$$b \times n = (a + c) \times n = (a \times n) + (c \times n). \tag{1.192}$$

Cela prouve que $a \times n \leqslant b \times n$. Et comme c et n ne sont pas nuls, nous avons même[66] $c \times n \neq 0$ et donc $a \times n < b \times n$. □

REMooultiplicationNaturelsOrdreStrictZ

Remarque 1.169.
Une version du lemme 1.168 dans $\mathbb{Z}$ sera le lemme 1.203.

LEMooSFUKooBNAple

Lemme 1.170 ([1]).
Soient $a \neq 0$ et $b > 1$ dans $\mathbb{N}$. Alors

$$ab > a. \tag{1.193}$$

Démonstration. Il s'agit d'une application du lemme 1.168 en partant de l'inégalité $1 < b$ et en la « multipliant » par a. □

PROPooNaturelsReguliersMultiplication

Proposition 1.171 ([1]).
Tous les naturels non nuls sont réguliers par rapport à la multiplication. Autrement dit, si $a \neq 0$, alors nous avons

$$a \times x = a \times y \Rightarrow x = y. \tag{1.194}$$

Démonstration. Soit $a \neq 0$ dans $\mathbb{N}$. Nous supposons que $a \times x = a \times y$. Puisque l'ordre sur $\mathbb{N}$ est total (proposition 1.151), nous pouvons supposer que $y \geqslant x$; sinon il suffit de permuter les rôles de x et y dans tout ce qui suit.

Il existe $d \in \mathbb{N}$ tel que $y = x + d$. En utilisant l'hypothèse $a \times y = a \times x$ et la distributivité[67],

$$a \times x = a \times y = a \times (x + d) = (a \times x) + (a \times d). \tag{1.195}$$

Puisque $(a \times x)$ est régulier pour la somme[68] nous en déduisons que

$$0 = a \times d. \tag{1.196}$$

Le lemme 1.167 dit alors que $a = 0$ ou que $d = 0$. Étant donné que $a \neq 0$ par hypothèse, nous déduisons que $d = 0$, c'est-à-dire que $x = y$. □

1.5.7 Presque unicité des triplets naturels

NORooUEooUniciteTripletsNaturels

1.172.
Il existe de nombreux triplets naturels ; l'existence d'un triplet naturel est un théorème de la théorie des ensembles que nous avons accepté. Nous avons déjà à peu près montré que toute partie non bornée de $\mathbb{N}$ donne lieu à un nouveau triplet naturel. Voir 1.159.

Nous voyons maintenant que tous les triplets naturels sont équivalents au moins pour l'ordre.

THOooFUXMooJuigHK

Théorème 1.173 ([1]).
Soient des triplets naturels $(\mathcal{N}_1, o_1, s_1)$ et $(\mathcal{N}_2, o_2, s_2)$. Alors

(1) il existe une unique application $f : \mathcal{N}_1 \to \mathcal{N}_2$ telle que

(1a) $f(o_1) = o_2$

[65] Proposition 1.165(6).
[66] Lemme 1.167.
[67] Proposition 1.165(6).
[68] Proposition 1.138(3).

(1b) $f \circ s_1 = s_2 \circ f$.

(2) Une telle application est une bijection croissante.

Démonstration. En plusieurs points.

(1) **Existence** Nous voyons $(\mathcal{N}_1, o_1, s_1)$ comme un triplet naturel, et $\mathcal{N}_2$ comme un simple ensemble. Nous pouvons appliquer le théorème 1.131 à $(\mathcal{N}_1, o_1, s_1)$. L'élément o_1 va jouer le rôle de 0 alors que o_2 va jouer le rôle de b. L'application g est s_2. Bref, il existe une unique application $f: \mathcal{N}_1 \to \mathcal{N}_2$ telle que

(1a) $f(o_1) = o_2$

(1b) $f\big(s_1(n)\big) = s_2\big(f(n)\big)$

pour tout $n \in \mathcal{N}_1$.

(2) **Unicité** Le théorème 1.131 donne déjà l'unicité. Nous la faisons quand même, juste pour vous faire plaisir. Soit g, une autre application vérifiant les mêmes conditions. Pour faire la récurrence de façon très explicite, nous posons

$$\begin{aligned} P: \mathcal{N}_1 &\to \{0,1\} \\ x &\mapsto \begin{cases} 1 & \text{si } g(x) = f(x) \\ 0 & \text{sinon.} \end{cases} \end{aligned} \tag{1.197}$$

Notre but est de prouver que $P(x) = 1$ pour tout $x \in \mathcal{N}_1$, en utilisant la récurrence telle que décrite dans la proposition 1.130.

Nous avons $f(o_1) = o_2 = g(o_1)$. Donc $P(o_1) = 1$. Nous supposons que, pour un certain $a \in \mathcal{N}_1$, nous ayons $P(a) = 1$, et nous prouvons que $P\big(s_1(a)\big) = 1$.

Nous avons $g(a) = f(a)$, et nous prenons s_2 des deux côtés, nous avons successivement

$$(s_2 \circ g)(a) = (s_2 \circ f)(a) \tag{1.198a}$$
$$(g \circ s_1)(a) = (f \circ s_1)(a) \tag{1.198b}$$
$$g\big(s_1(a)\big) = f\big(s_1(a)\big). \tag{1.198c}$$

La dernière égalité signifie que $P\big(s_1(a)\big) = 1$. La proposition 1.130 implique que $P(x) = 1$ pour tout $x \in \mathcal{N}_1$.

(3) **Bijection, définir l'inverse** Nous allons trouver un inverse et le lemme 1.18 nous dit que c'est suffisant. La partie « existence », en inversant les rôles de $\mathcal{N}_1$ et $\mathcal{N}_2$ nous donne une application $g: \mathcal{N}_2 \to \mathcal{N}_1$ telle que

(3a) $g(o_2) = o_1$

(3b) $g \circ s_2 = s_1 \circ g$.

Nous allons prouver que g est un inverse de f.

(4) $f \circ g = \mathrm{Id}$ Nous posons $A = \{x \in \mathcal{N}_2 \text{ tel que } (f \circ g)(x) = x\}$. Nous avons

$$f\big(g(o_2)\big) = f(o_1) = o_2, \tag{1.199}$$

et donc $o_2 \in A$.

Supposons que $x \in A$. Alors

$$(f \circ g)\big(s_2(x)\big) = (f \circ \underbrace{g \circ s_2}_{s_1 \circ g})(x) \tag{1.200a}$$
$$= (\underbrace{f \circ s_1}_{= s_2 \circ f} \circ g)(x) \tag{1.200b}$$
$$= (s_2 \circ f \circ g)(x) \tag{1.200c}$$
$$= s_2\big((f \circ g)(x)\big) \tag{1.200d}$$
$$= s_2(x) \tag{1.200e}$$

Donc $s_2(x) \in A$. Nous en déduisons que $A = \mathcal{N}_2$ par le point (3) de la définition 1.125 d'un triplet naturel.

(5) $g \circ f = \mathrm{Id}$ J'imagine que c'est la même chose que dans l'autre sens (ci-dessus)[69].

□

PROPooCCVNooYUYcqG

Proposition 1.174.
L'ensemble structuré $(\mathbb{N}, +, \times, \leqslant)$ *est archimédien*[70]. *En d'autres termes, pour tout* $a, b \in \mathbb{N} \setminus \{0\}$, *il existe* $n \in \mathbb{N}$ *tel que*

$$b < n \times a. \tag{1.201}$$

Démonstration. Soient $a, b \in \mathbb{N}$ avec $a \neq 0$.

Si $a > b$, nous avons le résultat avec $n = 1$.

Si $a = b$, en prenant $n = s(1)$ nous avons le résultat. En effet $s(1) \times a = a + a$. Puisque $a \neq 0$, nous avons $a + a \geqslant a$ et $a + a \neq a$, donc $s(1) \times a > a$.

La vraie vie est avec $a < b$. Nous posons

$$X = \{x \in \mathbb{N} \text{ tel que } 1 \leqslant x \times a \leqslant b\} \tag{1.202}$$

et

$$B = \{x \times a \text{ tel que } x \in X\}. \tag{1.203}$$

L'ensemble X est non vide parce que $1 \in X$. L'ensemble B est alors également non vide, et majoré par b. La proposition 1.152(4) nous indique alors que B possède un plus grand élément que nous allons noter $x_0 \times a$ ($x_0 \in X$).

Nous posons $n = s(x_0)$, et nous avons

$$x_0 \times a < x_0 \times a + a = s(x_0) \times a = n \times a. \tag{1.204}$$

Nous en déduisons que $n \times a$ n'est pas dans B parce que $x_0 \times a$ est le plus grand élément de B. Donc x_0 n'est pas dans X ; nous n'avons donc pas les inégalités

$$1 \leqslant n \times a \leqslant b. \tag{1.205}$$

Laquelle des deux inégalités est fausse ? Puisque $n = s(x_0) \geqslant 1$ et que $a \geqslant 1$, nous avons $1 \leqslant n \times a$. Donc c'est la seconde inégalité qui est fausse. Nous avons donc $n \times a > b$. □

1.5.8 Cardinalité dans $\mathbb{N}$

NORMooEnsembleFiniEquivalenceDef

1.175.
La proposition suivante est à peu près prise comme définition d'un ensemble fini dans [43] qui donne également une preuve de l'équivalence avec notre définition.

PROPooBYKCooGDkfWy

Proposition 1.176.
L'ensemble $\mathbb{N}$ *est infini*[71].

Démonstration. Nous considérons la partie propre[72]

$$A = \{n \in \mathbb{N} \text{ tel que } n \geqslant 1\}. \tag{1.206}$$

Ensuite nous posons

$$\begin{aligned} \sigma\colon \mathbb{N} &\to A \\ x &\mapsto s(x). \end{aligned} \tag{1.207}$$

Le fait que σ prenne ses valeurs dans A est parce que s prend ses valeurs dans $\mathbb{N} \setminus \{0\} = A$.

(1) **σ est injective** Parce que s l'est.

(2) **σ est surjective** C'est dans la définition 1.125(2)

Nous avons donc une bijection entre $\mathbb{N}$ et un sous-ensemble strict. □

[69] Je n'ai pas fait les calculs ; écrivez-moi si ça pose un problème.
[70] Définition 1.162.
[71] Définition 1.74.
[72] Le fait que ce soit une partie propre est dû au fait que 0 n'est pas dedans d'une part parce que le lemme 1.143 dit que $0 \leqslant 1$, et d'autre part parce que le lemme 1.140 donne $0 \neq 1$.

LEMooYIWDooIQFSad

Lemme 1.177.
Si $a \leqslant b$ dans $\mathbb{N}$, alors la partie[73] *$\{a, \dots, b\}$ est finie.*

Démonstration. En deux parties.

(1) **Pour $a = 0$** Nous commençons par prouver que $\{0, \dots, b\}$ est fini. Par récurrence sur b. Avec $b = 0$, la partie $\{0\}$ est finie parce que son seul sous-ensemble propre est $\varnothing$ qui n'est pas en bijection avec $\{0\}$.

Supposons que $\{0, \dots, b\}$ est fini. Alors $\{0, \dots, b\} \cup \{b+1\}$ est fini par le lemme 1.78.

(2) **Cas général** Nous avons $\{a, \dots, b\} \subset \{0, \dots, b\}$. Donc $\{a, \dots, b\}$ est une partie d'un ensemble fini. Elle est finie par 1.76.

□

LEMooJDGOooHdyJnu

Lemme 1.178.
Si $p \neq q$, alors il n'existe pas de bijection entre $\{0, \dots, p\}$ et $\{0, \dots, q\}$.

Démonstration. Supposons pour fixer les idées que $p \leqslant q$. Dans ce cas $\{0, \dots, p\}$ est une partie stricte de $\{0, \dots, q\}$. Vu que $\{0, \dots, q\}$ est fini (lemme 1.177), il n'y a pas de bijection avec ses parties strictes. □

PROPooONYBooQuqAPR

Proposition 1.179 ([1])**.**
Il n'existe pas de suites strictement décroissantes[74] *dans $\mathbb{N}$.*

Démonstration. Une suite dans $\mathbb{N}$ est une application $f : \mathbb{N} \to \mathbb{N}$. Nous supposons qu'elle est strictement décroissante. Étant donné que $f(k) \leqslant f(0)$ pour tout k, nous avons

$$f(\mathbb{N}) \subset \{x \in \mathbb{N} \text{ tel que } x \leqslant f(0)\} = \{0, \dots, f(0)\} \tag{1.208}$$

par la proposition 1.148.

D'autre part, l'ensemble $\mathbb{N}$ est infini par 1.176, et la partie $\{0, \dots, f(0)\}$ est finie par 1.177. L'application f serait une injection d'un ensemble infini dans un ensemble fini, ce qui est impossible par la proposition 1.79. □

PROPooZLEXooGyjNRk

Proposition 1.180 ([39])**.**
Toute partie non vide de $\mathbb{N}$ contient un unique élément minimal.

Démonstration. Soit une partie non vide A de $\mathbb{N}$.

(1) **Unicité** Soient deux éléments minimaux m_1 et m_2. Si $m_1 \leqslant m_2$ alors $m_1 = m_2$ parce que m_2 est minimal. Et si $m_2 \leqslant m_1$ alors $m_1 = m_2$ parce que m_1 est minimal.

(2) **Existence** Supposons que A n'ait pas d'éléments minimaux. Vu qu'aucun élément de A est minimal, il existe une application $f : A \to A$ telle que $f(a) < a$ pour tout a. Nous considérons un élément $x_0 \in A$ et la suite définie par récurrence $x_{n+1} = f(x_n)$ (via 1.134).

Cela donne une suite strictement décroissante dans $\mathbb{N}$, ce qui n'est pas possible par la proposition 1.179.

□

1.5.9 Division euclidienne

THOooKDJVooRIJRHP

Théorème 1.181 (division euclidienne [39])**.**
Pour tout $a \in \mathbb{N}$, pour tout $b \in \mathbb{N} \setminus \{0\}$, il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ avec $0 \leqslant r < b$.

Démonstration. Existence puis unicité.

(1) **Existence**

Nous posons

$$A = \{bx \text{ tel que } x \in \mathbb{N}, bx \leqslant a\}. \tag{1.209}$$

[73] Définition 1.156.
[74] Croissance, définition 1.24.

L'ensemble A contient 0 (avec $x = 0$) et est majoré par a. Donc il possède un plus grand élément que nous notons bq. Puisque $bq \in A$, nous avons $bq \leqslant a$ et donc il existe $r \in \mathbb{N}$ tel que

$$bq + r = a. \tag{1.210}$$

EQooIUICooLenNBP

Il reste à montrer que $r < b$. Supposons que $r \geqslant b$. Il existerait alors un x tel que $b+x = r$. En mettant ça dans (1.210),

$$bq + b + x = a, \tag{1.211}$$

c'est-à-dire $b(q+1)+x = a$, qui signifierait $b(q+1) \leqslant a$, ce qui est faux parce que bq est le plus grand élément de A.

(2) **Unicité** Supposons que nous ayons

$$a = bq + r = bq' + r' \tag{1.212}$$

avec $0 \leqslant r < b$ et $0 \leqslant r' < b$. Il y a trois possibilités : $q' < q$, $q' = q$ et $q' > q$.

(2a) **Si $q' < q$** Alors il existe $x \in \mathbb{N}$ tel que $q' + x = q$, et nous avons

$$b(q' + x) + r = bq' + bx + r, \tag{1.213}$$

ce qui, après distribution et simplification, donne $r' = bx + r$. Puisque nous avons $x \geqslant 1$, il vient

$$r' = bx + r \geqslant b + r \geqslant b. \tag{1.214}$$

Cela n'est pas possible parce que $r' < b$. Le cas $q' < q$ n'est pas possible.

(2b) **Si $q' = q$** Nous avons alors immédiatement $bq + r = bq + r'$ et donc $r = r'$. Unicité.

(2c) **Si $q' > q$** En posant $q + x = q'$ nous trouvons la même impossibilité que dans le cas $q' < q$.

□

DEFooDivisibleNombrePairImpair

Définition 1.182.
Quelques définitions associées au théorème 1.181. Soit a et b deux entiers naturels.

(1) *Dans le couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ avec $0 \leqslant r < b$, fourni par ce théorème, q est appelé **quotient** et r est appelé **reste**.*

(2) *Si $r = 0$ (et donc s'il existe un $q \in \mathbb{N}$ tel que $a = bq$, nous disons que a est **divisible** par b.*

(3) *Si n est divisible par 2, alors nous disons qu'il est **pair**.*

ITEMooDLHHooTmWSnN

(4) *Si n n'est pas divisible par 2, alors nous disons qu'il est **impair**.*

1.6 Ensembles finis

Voir 1.124 pour comprendre le type de résultats que nous groupons ici.

LEMooKNKEooYQeDdo

Lemme 1.183 ([1]).
Soient un ensemble E de cardinal n.

(1) *si $a \in E$ alors $\text{Card}(E \setminus \{a\}) = n - 1$.*

ITEMooLAECooBLOpwZ

(2) *Si $a \notin E$ alors $\text{Card}(E \cup \{a\}) = n + 1$.*

LEMooNTVKooTfvHfA

Lemme 1.184 ([1]).
Si E est un ensemble fini, alors son ensemble des parties $\mathcal{P}(E)$ est fini.

Démonstration. Nous y allons par récurrence sur le cardinal[75] de E. Nous supposons que pour tout ensemble E' de cardinal n, l'ensemble $\mathcal{P}(E')$ est fini. Soit maintenant E de cardinal $n + 1$.

Soit $a \in E$. La partie $E' = E \setminus \{a\}$ est de cardinal n par le lemme 1.183, donc $\mathcal{P}(E')$ est fini. En posant

$$\mathcal{S} = \{A \cup \{a\} \text{ tel que } A \in \mathcal{P}(E')\}, \tag{1.215}$$

nous avons

$$\mathcal{P}(E) = \mathcal{P}(E') \cup \mathcal{S}. \tag{1.216}$$

[75] Voir 1.133.

De plus

$$\begin{aligned}\varphi\colon \mathcal{S} &\to \mathcal{P}(E')\\ B &\mapsto B\setminus\{a\}\end{aligned} \tag{1.217}$$

est une bijection. Donc $\mathcal{S}$ est fini et $\mathcal{P}(E)$ est fini comme union d'ensembles finis. □

PROPooGJLYooTQtlSV

Proposition 1.185 ([1, 38])**.**
Tout ensemble fini partiellement ordonné[76] *possède un élément maximal*[77].
Tout ensemble fini partiellement ordonné possède un élément minimal[78].

Démonstration. Nous prouvons la contraposée, c'est-à-dire que si $(E,\leqslant)$ n'a pas d'élément maximal, alors il est infini.

(1) **Axiome du choix, fonction s** Nous supposons que $(E,\leqslant)$ n'admet pas d'élément maximal. Donc pour tout $x\in E$ l'ensemble $A_x=\{y\in E \text{ tel que } x<y\}$ est non vide. L'axiome du choix[79] nous permet de choisir un élément dans chaque A_x et donc créer une application

$$s\colon E\to E \tag{1.218}$$

telle que $s(x)\in A_x$ pour tout x.

(2) **La partie S** Soit $x_0\in E$. Nous définissons la suite $(x_n)_{n\in\mathbb{N}}$ par récurrence[80] par $x_{n+1}=s(x_n)$.

(3) **$x_i<x_j$ si $i<j$** SPITEMooNUVJooDKCINE Nous fixons $i\in\mathbb{N}$ et nous prouvons par récurrence sur j que $x_i<x_j$ dès que $i<j$. La définition 1.141 de l'ordre sur $\mathbb{N}$ dit que si $j>i$ alors il existe $k\in\mathbb{N}$ tel que $j=i+k$. On y va par récurrence sur k. D'abord nous avons

$$x_{i+1}=s(x_i)>x_i, \tag{1.219}$$

donc $x_{i+1}\neq x_i$. En ce qui concerne la récurrence, si $x_{i+k}>x_i$, alors

$$x_{i+n+1}=s(x_{i+n})>x_{i+n}>x_i. \tag{1.220}$$

Nous avons le résultat par transitivité de l'inégalité.

(4) **L'application φ** Nous posons $X=\{x_i\}_{i\in\mathbb{N}}$, et nous posons

$$\begin{aligned}\varphi\colon E&\to E\\ x&\mapsto\begin{cases}s(x) & \text{si } s\in X\\ x & \text{sinon.}\end{cases}\end{aligned} \tag{1.221}$$

(5) **$\varphi(E)\subset E\setminus\{x_0\}$** D'abord notons que $x_0\in X$, donc $\varphi(x_0)=s(x_0)>x_0$, donc $\varphi(x_0)\neq x_0$. Si $y\in X$, alors il existe n tel que $y=x_n$. Dans ce cas $\varphi(y)=x_{n+1}>x_0$ par (3). Si au contraire $y\notin X$ alors $\varphi(y)=y\notin X$ et en particulier $y\neq x_0$.

(6) **$E\setminus\{x_0\}\subset\varphi(E)$** Si $y\in X\setminus\{x_0\}$ alors $y=x_n=s(x_{n-1})=\varphi(x_{n-1})$. Si au contraire y n'est pas dans X alors $y=\varphi(y)\in\varphi(E)$.

(7) **$E\setminus\{x_0\}=\varphi(E)$** Ce sont les deux inclusions que nous venons de prouver.

(8) **Conclusion** L'application $\varphi\colon E\to E\setminus\{x_0\}$ est une bijection entre E et le sous-ensemble propre $E\setminus\{x_0\}$. Donc E est infini.

En ce qui concerne l'énoncé à propos de l'existence d'un élément minimal, il suffit de prendre un élément maximal pour l'ensemble ordonné $(E,\geqslant)$ (proposition 1.28.) □

[76] Définition 1.23.
[77] C'est-à-dire un élément qui majore tous ceux avec qui il est comparable.
[78] C'est-à-dire un élément qui minore tous ceux avec qui il est comparable.
[79] Je suis certain qu'on peut réexprimer ça avec le lemme de Zorn ; ce serait plus conforme à ce qui est fait dans le Frido, mais on ne va pas plus se casser la tête. Si la lectrice se sent capable de faire l'adaptation, qu'elle m'emvoie la preuve adaptée.
[80] Théorème 1.131.

1.7 Les entiers relatifs

PROPooNbsEntiers

Proposition-Définition 1.186 ([39]).
Soient $a, b, a', b' \in \mathbb{N}$. Nous disons que $(a, b) \sim (a', b')$ si et seulement si

$$a + b' = b + a' \tag{1.222}$$

(1) $\sim$ est une relation d'équivalence sur $\mathbb{N}^2$.

ITEMooZQSHooSDfdvK

(2) Si $(a, b) \sim (a', b')$ et $(x, y) \sim (x', y')$ alors

$$(a + x, b + y) \sim (a' + x', b' + y'). \tag{1.223}$$

*L'ensemble des **entiers** est*

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim, \tag{1.224}$$

et nous notons $\overline{a, b} \in \mathbb{Z}$ la classe de $(a, b) \in \mathbb{N} \times \mathbb{N}$.

Démonstration. En plusieurs points.

(1) **Symétrie** C'est la commutativité de la somme dans $\mathbb{N}$, proposition 1.138(1).

(2) **Réflexive** Immédiat.

(3) **Transitive** Nous supposons que $(a, b) \sim (u, v)$ et que $(u, v) \sim (x, y)$. Alors nous avons

$$a + v = u + b \tag{1.225a}$$
$$u + y = v + x. \tag{1.225b}$$

En additionnant membre à membre,

$$a + v + u + y = u + b + v + x. \tag{1.226}$$

La commutativité nous permet de mettre u et v à droite dans chacun des deux membres. Ensuite la proposition 1.138(3) nous permet de simplifier par $u+v$. Il reste $a+y = b+x$, qui signifie $(a, b) \sim (x, y)$.

(4) **Pour (2)** L'hypothèse donne les égalités

$$a + b' = b + a' \tag{1.227a}$$
$$x + y' = y + x' \tag{1.227b}$$

En sommant, et en utilisant l'associativité,

$$(a + x) + (b' + y') = (b + y) + (a' + x'). \tag{1.228}$$

Cela signifie bien que $(a + x, b + y) \sim (a' + x', b' + y')$.

□

LEMooEntiersEquivalentsZero

Lemme 1.187.
Soient $a, b \in \mathbb{N}$. Nous avons $(a, b) \sim (0, 0)$ si et seulement si $a = b$.

Démonstration. Dire que $(a, b) \sim (0, 0)$ est équivalent à dire que $a + 0 = b + 0$, ou encore que $a = b$. □

PROPooDEFAdditionEntiersRelatifs

Proposition-Définition 1.188 ([39]).
Soient $a, b, x, y \in \mathbb{N}$. L'application

$$\begin{aligned} f\colon \overline{(a, b)} \times \overline{(x, y)} &\to \mathbb{Z} \\ \big((a', b'), (x', y')\big) &\mapsto (a' + x', b' + y') \end{aligned} \tag{1.229}$$

est constante.

Nous nommons sa valeur $\overline{(a, b)} + \overline{(x, y)}$.

Démonstration. Cela est une conséquence de la proposition 1.186(2). □

PROPooGroupeEntiersRelatifs

Proposition 1.189.
L'ensemble $\mathbb{Z}$, muni de l'addition telle que définie par la proposition 1.188, est un groupe commutatif admettant pour neutre l'élément $e = \overline{(0, 0)}$.

Démonstration. En plusieurs points.

(1) **Neutre** Pour tous entiers naturels $a,\ b$, on a

$$\overline{(a,b)}+\overline{(0,0)}=\overline{(a+0,b+0)}=\overline{(a,b)}. \tag{1.230}$$

De même $e+\overline{(a,b)}=\overline{(a,b)}$ par commutativité de la somme dans $\mathbb{N}$.

(2) **Inverse** Il faut vérifier que $\overline{(b,a)}$ est l'inverse de $\overline{(a,b)}$.

(3) **Associativité** Calcul direct en utilisant l'associativité dans $\mathbb{N}$.

□

PROPooVMGYooUWsbSr

Proposition 1.190.
L'application

$$\begin{aligned}\iota\colon\mathbb{N}&\to\mathbb{Z}\\ n&\mapsto\overline{(n,0)}\end{aligned} \tag{1.231}$$

est un morphisme[81] *injectif.*

Démonstration. Le fait que ce soit un morphisme est le calcul

$$\iota(a+b)=\overline{(a+b,0)}=\overline{(a,0)}+\overline{(b,0)}=\iota(a)+\iota(b). \tag{1.232}$$

Pour l'injectivité, supposons que $\iota(a)=\iota(b)$. Alors $\overline{(a,0)}=\overline{(b,0)}$, c'est-à-dire $a+0=b+0$. Donc $a=b$. □

1.7.1 Opposé

SUBooLEMooRAENaGYpDes

Lemme 1.191.
Tout élément de $\mathbb{Z}$ a un représentant de la forme $(a,0)$ ou $(0,b)$.

Démonstration. Soient $a,b\in\mathbb{N}$. Si $b\leqslant a$, alors nous avons

$$(a,b)\sim(a-b,0) \tag{1.233}$$

où la différence est calculée dans $\mathbb{N}$ et a un sens parce que nous avons supposé $b\leqslant a$. Si par contre $a\leqslant b$ alors

$$(a,b)\sim(0,b-a). \tag{1.234}$$

Puisque l'ordre sur $\mathbb{N}$ est total[82], tous les cas sont couverts. □

LEMooDEFRelatifOppose

Lemme-Définition 1.192.
Soit $z\in\mathbb{Z}$. L'application[83]

$$\begin{aligned}f\colon z&\to\mathbb{Z}\\ (a,b)&\mapsto\overline{(b,a)}\end{aligned} \tag{1.235}$$

est constante.
Nous nommons $-z$ sa valeur.

Démonstration. Soient (a,b) et (x,y) dans z. Nous avons successivement :

- $(a,b)\sim(x,y)$.
- $a+y=b+x$.
- $(b,a)\sim(y,x)$
- $\overline{(b,a)}=\overline{(y,x)}$
- $f(a,b)=f(x,y)$.

D'où la constance de f. □

[81] Certes $\mathbb{N}$ n'est pas un groupe, donc le mot « morphisme » est un peu abusé, mais vous voyez ce que je veux dire.
[82] Proposition 1.151.
[83] Pour rappel, z est une classe d'équivalence dans $\mathbb{N}\times\mathbb{N}$, c'est-à-dire une partie de $\mathbb{N}\times\mathbb{N}$. Ça a un sens de prendre z comme ensemble sur lequel on définit une fonction.

PROPooJMETooHQGwnv

Proposition 1.193 ([1]).
Soient $a, b \in \mathbb{Z}$. Nous avons

ITEMooWNYGooMopPcq

(1) $(-a)b = -(ab)$

LEMooEntiersRelatifsSigne

Lemme 1.194.
Nous avons

ITEMooSQFGooQPgIMu

(1) $\mathbb{Z} = \iota(\mathbb{N}) \cup -\iota(\mathbb{N})$

ITEMooHQUQooJeqULl

(2) $\iota(\mathbb{N}) \cap -\iota(\mathbb{N}) = \{0\}$.

Démonstration. Nous avons

SUBEQooVJGVooCUxtvk

$$\iota(\mathbb{N}) = \{\overline{(n,0)} \text{ tel que } n \in \mathbb{N}\} \tag{1.236a}$$

SUBEQooAPGRooQCkYRx

$$-\iota(\mathbb{N}) = \{\overline{(0,n)} \text{ tel que } n \in \mathbb{N}\}. \tag{1.236b}$$

Montrons à présent les deux points.

(1) **Pour (1)** Nous savons par le lemme 1.191 que tous les éléments de $\mathbb{Z}$ sont de la forme (1.236a) ou (1.236b).

(2) **Pour (2)** Si $z \in \iota(\mathbb{N}) \cap -\iota(\mathbb{N})$, il existe $n, m \in \mathbb{N}$ tels que $\overline{(n,0)} = \overline{(0,m)}$, ce qui signifie en particulier que $(n,0) \sim (0,m)$ ou encore que $n + m = 0$. Le lemme 1.140 dit alors que $n = m = 0$.

Nous avons donc $z = \overline{(0,0)} = 0$.

□

PROPooCHGRooRksGGO

Proposition 1.195.
L'application

$$\begin{aligned} \iota\colon \mathbb{N} &\to \mathbb{Z} \\ n &\mapsto \overline{(n,0)} \end{aligned} \tag{1.237}$$

est un morphisme injectif qui respecte l'ordre.

Démonstration. Le fait que ce soit un morphisme injectif est la proposition 1.190.

Il faut encore prouver que ça respecte l'ordre[84] □

PROPooORABooXRbVoz

Proposition 1.196 ([1]).
Soit G, un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$. Alors

ITEMooUZBJooUeVmmz

(1) La partie $\{x > 0$ tel que $x \in G\}$ est non vide.

ITEMooIXXFooOWkbPb

(2) En posant

$$p = \min\{x > 0 \in G\}, \tag{1.238}$$

nous avons $G = p\mathbb{Z}$.

Démonstration. Vu que G est un sous-groupe de $(\mathbb{Z}, +)$, si $x, y \in G$ nous avons $x + y \in G$, $-x \in G$, etc.

(1) **Pour (1)** Soit $x \neq 0$ dans G. Si $x > 0$ c'est bon. Sinon $-x \in G$ et $-x > 0$.

(2) **Pour (2)** Nous posons

$$p = \min\{x \in G \text{ tel que } x > 0\}. \tag{1.239}$$

Vu que $p \in G$ nous avons $p\mathbb{Z} \subset G$. Nous devons montrer l'inclusion inverse.

Soit $y \in G$. Par la division euclidienne 1.181, il existe $q \in \mathbb{Z}$ et $0 \leqslant r < p$ tels que $y = qp + r$. Vu que y et qp sont dans G nous avons $r = y - qp \in G$. Par minimalité de p, nous devons avoir $r = 0$, et donc $y = qp \in p\mathbb{Z}$.

□

[84] Faites-le en envoyez-moi la preuve.

1.7.2 Ordre sur $\mathbb{Z}$

NORMooEntierRelatifOrdre

1.197.
Si $z \in \mathbb{Z}$, nous disons que $z \in \mathbb{N}$ lorsque $z \in \iota(\mathbb{N})$. C'est un abus de notation qu'il est difficile de ne pas faire. Le même abus sera fait pour passer de $\mathbb{Z}$ à $\mathbb{Q}$ puis $\mathbb{R}$ puis $\mathbb{C}$.

DEFooYMRHooCyEKtr

Définition 1.198 (Positivité et ordre dans $\mathbb{Z}$[1])**.**
La positivité[85] *que nous considérons sur $\mathbb{Z}$ est $\mathbb{N}\setminus\{0\}$. Nous considérons alors la relation d'ordre*[86] *$\leqslant$ donnée par $a \leqslant b$ si et seulement si $b-a \in \mathbb{N}$.*

Nous disons que

(1) L'élément $z \in \mathbb{Z}$ est ***positif*** *si $z \geqslant 0$.*

(2) L'élément $z \in \mathbb{Z}$ est ***strictement positif*** *si $z \geqslant 0$ et $z \neq 0$. Nous notons $z > 0$.*

(3) L'élément $z \in \mathbb{Z}$ est ***négatif*** *si $z \leqslant 0$.*

(4) L'élément $z \in \mathbb{Z}$ est ***strictement négatif*** *si $z \leqslant 0$ et $z \neq 0$. Nous notons $z < 0$.*

DEFooRelatifsPositifs

Définition 1.199 (Éléments positifs de $\mathbb{Z}$)**.**
On dit qu'un élément $z \in \mathbb{Z}$ est ***positif*** *si $z \in \mathbb{N}$. On note dans ce cas $z \geqslant 0$.*

On dira qu'il est ***négatif*** *quand $-z \in \mathbb{N}$. On note ainsi $z \leqslant 0$.*

On dit qu'un entier relatif z est ***strictement positif*** *s'il est positif et non nul; on note $z > 0$. Il est* ***strictement négatif****orsqu'il est négatif et non nul, et cela est noté $z < 0$.*

PROPooMYYDooOABOdB

Proposition-Définition 1.200 (Relation d'ordre [39])**.**
La paire[87] *$(\mathbb{Z}, \leqslant)$ est un ensemble totalement ordonné.*

1.201.
Une version de la proposition 1.200 dans $\mathbb{R}$ sera le lemme 4.53.

PROPooADGIooTioqdu

Proposition 1.202 ([1])**.**
L'anneau $\mathbb{Z}$ est totalement ordonné[88]

LEMooSVDDooWsyxNP

Lemme 1.203.
Soient $a > 0$ et $b \geqslant 1$ (resp. $b > 1$ dans $\mathbb{Z}$. Nous avons

$$ab \geqslant a \qquad (\text{resp. } ab > a). \tag{1.240}$$

Démonstration. On la fait seulement pour l'inégalité stricte : il suffit de recopier pour l'inégalité large. Par récurrence sur a qui se trouve être dans $\mathbb{N}$. Lorsque $a = 1$, on lit simplement $1b > 1$ qui est correct.

Si la propriété est vraie pour un certain a, alors

$$\begin{aligned}(a+1)b &= ab + b && \text{(distributivité)} && (1.241)\\ &> a + b (\text{hyp. de réc.}) && && (1.242)\\ &> a + 1 (\text{hyp. sur } b). && && (1.243)\end{aligned}$$

Et le principe de récurrence permet de conclure. □

NORMooLienRelatifsAnnTotOrdonne

1.204.
Cette proposition est en partie similaire à 1.116 qui parle d'anneau totalement ordonné.

PROPooYFUBooJUZgwH

Proposition 1.205 ([1])**.**
Quelques propriétés de l'ordre dans $\mathbb{Z}$. Soit $a, b \in \mathbb{Z}$.

ITEMooULKWooLmKBse

(1) Si $a, b \geqslant 0$, alors $ab \geqslant 0$.

ITEMooSAJPooEDSgXJ

(2) Si $a, b > 0$, alors $ab > 0$.

ITEMooINGNooOgSGiF

(3) Si $a, b \leqslant 0$ alors $ab \geqslant 0$.

ITEMooOGFXooDvLKAE

(4) Si $a \geqslant 0$ et $b \leqslant 0$ alors $ab \leqslant 0$.

[85] Définition 1.107.
[86] De la proposition 1.108.
[87] Voir la définition 1.198 pour $\leqslant$.
[88] Définition 1.115.

ITEMooRelatifsOrdreOppose

(5) *Si $a > 0$, alors $-a < 0$.*

ITEMooRelatifsOrdreCarrePositif

(6) *Nous avons $a^2 \geqslant 0$ et $a^2 = 0$ si et seulement si $a = 0$.*

ITEMooBUHIooLJOSLQ

(7) *Si $ab \geqslant 0$ et si $a \geqslant 0$ alors $b \geqslant 0$.*

ITEMooGDFPooBbpBgn

(8) *Si $ab > 0$ alors soit $a, b > 0$, soit $a, b < 0$.*

LEMooMYEIooNFwNVI

Lemme 1.206.
Toute partie bornée de $\mathbb{Z}$ possède un plus grand élément.

PROPooRelatifsValAbs

Proposition 1.207.
Si $z \in \mathbb{Z}$, alors :

(1) *$|z|$ est bien définie et $|z| \in \mathbb{N}$;*

(2) *nous avons $|ab| = |a||b|$.*

Démonstration. C'est le fait que $\mathbb{Z}$ est un anneau totalement ordonné[89] : donc la proposition-définition 1.121 s'applique, y compris l'équation (1.102). □

DEFooRelatifsDiviseurParite

Définition 1.208.
Soit $a, b \in \mathbb{Z}$. On étend les notions de divisibilité et de parité de la définition 1.182 en disant que :

(1) *a est divisible par b si $|a|$ est divisible par $|b|$;*

(2) *a est pair si $|a|$ est pair ;*

(3) *b est impair si $|b|$ est impair.*

PROPooYJBMooZrzkNX

Proposition 1.209.
Soit $a, b \in \mathbb{Z}$ non nuls, tels que a soit divisible par b. Alors $|a| \geqslant |b|$.

Démonstration. a est divisible b dans $\mathbb{Z}$ revient à dire que $|a|$ est divisible $|b|$ dans $\mathbb{N}$, donc par la définition 1.182, il existe $q \in \mathbb{N}$ tel que $|a| = q\,|b|$. Comme a et b sont non nuls, $|a|$ et $|b|$ sont aussi non nuls, et donc $q \neq 0$: en effet, sinon, nous aurions $q\,|b| = 0 = |a|$ à cause de la proposition 1.165 point (4). Ainsi, $q \geqslant 1$, et grâce au lemme 1.203, on a $|a| = q\,|b| \geqslant |b|$. □

LEMooCMOEooSoeclk

Lemme 1.210 ([1])**.**
Soit $n \in \mathbb{Z}$.

(1) *Si n est impair*[90]*, alors $n-1$ et $n+1$ sont pairs.*

(2) *Si n est pair, alors $n-1$ et $n+1$ sont impairs.*

Démonstration. Selon que $n \geqslant 0$ ou que $n \leqslant 0$, on effectue la division euclidienne de n ou de $-n$ par 2.

(1) **Cas $n \geqslant 0$** Il existe $q \in \mathbb{N}$ et $r \in \{0, 1\}$ tel que $n = 2q + r$.

- Quand n est pair, on a $r = 0$. Alors $n+1 = 2q+1$ et $n-1 = 2(q-1)+2-1 = 2(q-1)+1$ sont impairs.
- Quand n est impair, on a $r = 1$. Alors $n+1 = 2q+2 = 2(q+1)$ et $n-1 = 2q+1-1 = 2q$ sont pairs.

(2) **Cas $n \leqslant 0$** Il existe $q \in \mathbb{N}$ et $r \in \{0, 1\}$ tel que $-n = 2q + r$.

- Quand n est pair, on a $r = 0$. Alors $-n+1 = 2q+1$ est impair, et $n-1 = -(-n+1)$ l'est aussi. De même, $-n-1 = 2(q-1)+2-1 = 2(q-1)+1$, et donc $n+1 = -(-n-1)$, sont impairs.
- Quand n est impair, on a $r = 1$. Alors $-n+1 = 2q+2 = 2(q+1)$ est pair, et $n-1 = -(-n+1)$ l'est aussi. De même, $-n-1 = 2q+1-1 = 2q$, et donc $n+1 = -(-n-1)$, sont pairs.

□

LEMooJNXIooBmdOVi

Lemme 1.211.
L'ensemble $\mathbb{Z}$ est infini dénombrable.

[89] Proposition 1.202.
[90] Définition 1.208.

Démonstration. Nous considérons l'application

$$\begin{aligned} f\colon \mathbb{N} &\to \mathbb{Z} \\ n &\mapsto \begin{cases} n/2 & \text{si } n \text{ est pair} \\ -(n+1)/2 & \text{si } n \text{ est impair,} \end{cases} \end{aligned} \tag{1.244}$$

et nous montrons qu'elle est bijective.

(1) **f est injective** Soient $x, y \in \mathbb{Z}$ tels que $f(x) = f(y)$. Il y a trois possibilités : $f(x) < 0$, $f(x) = 0$ et $f(x) > 0$.

(1a) **Si $f(x) = 0$** Nous supposons que $f(x) = 0$. Si x est pair, c'est que $x/2 = 0$ et donc que $x = 0$. Si x est impair, c'est que $x + 1 = 0$ et donc que $x = -1$ qui n'est pas possible parce que $x \in \mathbb{N}$. Bref, la seule possibilité pour $f(x) = 0$ est $x = 0$.

(1b) **Si $f(x) < 0$** Alors x est pair et $x = 2f(x)$. Même raisonnement pour y : $y = 2f(y) = 2f(x) = x$.

(1c) **Si $f(x) < 0$** Alors x est impair et

$$f(x) = -\frac{x+1}{2} = f(y) = -\frac{y+1}{2}, \tag{1.245}$$

et donc $x = y$.

(2) **f est surjective** Soit $n \in \mathbb{Z}$. Si $n > 0$, alors $n = f(2n)$. Si $n < 0$ alors $n = f(-2n - 1)$. Notez que $-2n - 1 > 0$, donc c'est valide.

□

LEMooILYLooTDRtYj

Lemme 1.212 ([1]).
Soit un anneau[91] *A. Si une application $f\colon \mathbb{Z} \to A$ vérifie*

(1) $f(x + y) = f(x) + f(y)$ *pour tout* $x, y \in \mathbb{Z}$,

(2) $f(1) = 1$,

alors

ITEMooUQKWooByNDTK

(1) $f(0) = 0$

ITEMooYOEPooKOQQPH

(2) $f(-x) = -f(x)$

ITEMooKTSDooExAJHd

(3) f est un morphisme d'anneaux, c'est-à-dire que

$$f(xy) = f(x)f(y). \tag{1.246}$$

Démonstration. En deux parties.

(1) **Pour (1)** Prenons un x quelconque. Nous avons $f(x) = f(x + 0) = f(x) + f(0)$. Donc $f(0) = 0$.

(2) **Pour (2)** L'inverse pour la somme de $f(-x)$ est $-f(x)$. En effet

$$f(-x) + f(x) = f(-x + x) = f(0) = 0. \tag{1.247}$$

(3) **Pour (3), si $y > 0$** Nous prouvons que $f(xy) = f(x)f(y)$ par récurrence sur y. D'abord pour $y = 1$ nous avons bien $f(xy) = f(x)f(y)$ parce que $f(1) = 1$. Ensuite nous avons :

$$\begin{aligned} f\big(x(y+1)\big) &= f(xy + x) && && \text{(1.248a)} \\ &= f(xy) + f(x) && \text{morph pour } + && \text{(1.248b)} \\ &= f(x)f(y) + f(x) && \text{hyp. rec.} && \text{(1.248c)} \\ &= f(x)\big(f(y) + 1\big) && && \text{(1.248d)} \\ &= f(x)\big(f(y) + f(1)\big) && && \text{(1.248e)} \\ &= f(x)f(y+1) && && \text{(1.248f)} \end{aligned}$$

(4) **Si $y < 0$** Nous posons $y' = -y$. Vu que $y' > 0$ nous avons

$$f(xy) = f(-xy') = -f(xy') = -f(x)f(y') = f(x)(-1)f(y') = f(x)f(-y') = f(x)f(y). \tag{1.249}$$

□

[91] Définition 1.100.

1.8 Corps

DefTMNooKXHUd

Définition 1.213 ([44]).
*Un **corps** est un anneau*[92] $(A,+,\times)$ *dans lequel tout élément non nul est inversible pour l'opération* $\times$ *(pour l'opération* $+$*, tous les éléments sont inversibles parce que* $(A,+)$ *est un groupe).*

1.214.
Dans le Frido, nous ne parlons que de corps commutatifs ; nous ne le répéterons pas toujours.

1.215.
Pour savoir ce qu'est un « *ring* » ou « *field* » en anglais, voir -1.3.

1.8.1 Définitions, morphismes

PROPooFQZYooWedmwl

Proposition 1.216.
L'anneau A *est un corps*[93] *si et seulement si* $U(A) = A^*$.

Démonstration. En deux parties.

(1) **Sens direct** Nous supposons que A est un corps. D'une part tous les éléments non nuls sont inversibles, c'est-à-dire $A^* \subset U(A)$.

Pour l'inclusion inverse, nous montrons qu'une élément inversible ne peut pas être nul. Cela n'est autre que le lemme 1.101 couplé à la proposition 1.102 : $a \cdot 0 = 0 \neq 1$ pour tout a.

(2) **Sens inverse** Si $U(A) = A^*$, nous avons immédiatement que tous les éléments non nuls sont inversibles et donc que A est un corps.

□

1.217.
Nous verrons dans la définition 2.5 qu'un morphisme de corps est juste un morphisme d'anneaux. Le lemme 2.6 dira pourquoi c'est une bonne idée.

[92] Définition 1.100.
[93] Définition 1.213.

Chapitre 2

Théorie des groupes (début)

2.1 Groupes

2.1.1 Définition, unicité du neutre

La définition d'un groupe est la définition 1.92.

LEMooECDMooCkWxXf

Lemme-Définition 2.1 (Unicités)**.**
Dans un groupe, l'inverse et le neutre sont uniques. Plus précisément, si G est un groupe nous avons :

(1) il existe un unique élément $e \in G$ tel que $eg = ge = g$ pour tout $g \in G$,

ITEMooOIWTooYqmMPP

(2) pour tout $g \in G$, il existe un unique élément $h \in G$ tel que $gh = hg = e$.

*Le e ainsi défini est nommé **neutre** de G. Le h tel que $gh = hg = e$ est nommé l'**inverse** de g et est noté g^{-1}.*

Démonstration. Chaque point séparément.

(1) Supposons que e_1 et e_2 vérifient la propriété. Nous avons pour tout $g \in G$: $e_1 g = g e_1 = g$. En particulier pour $g = e_2$ nous écrivons $e_1 e_2 = e_2 e_1 = e_2$. Mais en partant dans l'autre sens : $e_2 g = g e_2 = g$ avec $g = e_1$ nous avons $e_2 e_1 = e_1 e_2 = e_1$. En égalant ces deux valeurs de $e_2 e_1$ nous avons $e_1 = e_2$.

Pour la suite de la preuve nous écrivons e l'unique neutre de G.

(2) Supposons que k_1 et k_2 soient deux inverses de g. On considère alors le produit $k_1 g k_2$. Puisque $k_1 g = e$, on a $k_1 g k_2 = e k_2 = k_2$; mais, comme $g k_2 = e$, on a aussi $k_1 g k_2 = k_1 e = k_1$. Le produit est donc à la fois égal à k_1 et à k_2, et donc $k_1 = k_2$.

□

DEFooJNPIooMuzIXd

Définition 2.2 (groupe symétrique)**.**
*Soit un ensemble E. Une **permutation** de l'ensemble E est une bijection $E \to E$. Le **groupe symétrique** de E est le groupe des bijections $E \to E$; il est noté S_E.*

*Le **groupe symétrique** S_n est le groupe des permutations de l'ensemble $\{1, \dots, n\}$. C'est donc l'ensemble des bijections $\{1, \dots, n\} \to \{1, \dots, n\}$.*

LEMooWYLRooNOdZnp

Lemme 2.3 ([45])**.**
Soient deux groupes G et H. Si $\alpha : G \to H$ est un morphisme de groupes[1]*, alors*

(1) $\alpha(e_G) = e_H$.

(2) $\alpha(g^{-1}) = \alpha(g)^{-1}$.

Démonstration. Pour le premier point, soit $g \in G$. Nous avons

$$\alpha(g) = \alpha(ge) = \alpha(g)\alpha(e). \tag{2.1}$$

En multipliant les deux côtés par $\alpha(g)^{-1}$ nous trouvons $e = \alpha(e)$.

[1] Définition 1.95.

Pour le second point, nous vérifions que $\alpha(g^{-1})\alpha(g) = e$. C'est le cas parce que

$$\alpha(g^{-1})\alpha(g) = \alpha(g^{-1}g) = \alpha(e) = e. \tag{2.2}$$

□

LEMooBIBFooBHxFYC

Lemme 2.4.
Si G est un groupe et si $h \in G$, alors les applications

$$\begin{aligned} L_h : G &\to G \\ g &\mapsto hg \end{aligned} \tag{2.3}$$

et

$$\begin{aligned} R_h : G &\to G \\ g &\mapsto gh \end{aligned} \tag{2.4}$$

sont des bijections.

Démonstration. D'abord si $L_h(g_1) = L_h(g_2)$, alors $hg_1 = hg_2$ et en multipliant à gauche par h^{-1} nous avons $g_1 = g_2$; donc L_h est injective. Ensuite L_h est surjective parce que si $g \in G$, alors $g = L_h(h^{-1}g)$.

Pour l'application R_h, la preuve est une simple adaptation. □

2.1.2 Morphisme de corps

DEFooWGKFooJaakjf

Définition 2.5 (Morphisme de corps)**.**
*Un corps étant un anneau sans plus de structure, un **morphisme de corps** n'est qu'un morphisme des anneaux*[2].

Le lemme suivant montre que définir un morphisme de corps comme étant simplement un morphisme des anneaux est une bonne idée.

LEMooWBOPooZnsZgQ

Lemme 2.6.
Si $\varphi : \mathbb{K} \to \mathbb{K}'$ est un morphisme de corps, alors

(1) pour tout $a \in \mathbb{K}$ nous avons $\varphi(a^{-1}) = \varphi(a)^{-1}$;

(2) le morphisme φ est injectif.

Démonstration. Vu que $\varphi(1) = 1$, nous avons aussi

$$1 = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}). \tag{2.5}$$

Donc, par unicité de l'inverse[3], $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Pour l'injectivité nous supposons $\varphi(a) = \varphi(b)$. Étant donné que $\mathbb{K}'$ est un corps, nous pouvons multiplier par $\varphi(b)^{-1}$:

$$\varphi(a)\varphi(b)^{-1} = 1. \tag{2.6}$$

En utilisant le premier point nous avons $1 = \varphi(a)\varphi(b^{-1})$, puis le morphisme d'anneaux : $1 = \varphi(ab^{-1})$, et encore le morphisme d'anneaux nous permet de déduire $ab^{-1} = 1$ et donc $a = b$. □

2.1.3 Groupe ordonné

DEFooEUHFooYvhnLQ

Définition 2.7 ([46])**.**
*Soient un groupe $(G, +)$, ainsi qu'une relation d'ordre $\leqslant$ sur G. Nous disons que la relation d'ordre est **compatible** avec la structure de groupe si pour tout $x, y, z \in G$, si $x \leqslant y$ alors $x + z \leqslant y + z$ et $z + x \leqslant z + y$. Dans ce cas, le triple $(G, +, \leqslant)$ est un **groupe ordonné**.*

Si $(G, \leqslant)$ est totalement ordonné, nous disons que le groupe est totalement ordonné.

[2] Définition 1.106.
[3] Lemme 2.1 (2).

2.1.4 Classes de conjugaison

DEFooOLXPooWelsZV

Définition 2.8 (classe de conjugaison)**.**
*Soit un groupe G et un élément $g \in G$. La **classe de conjugaison** de g est la partie*

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\}. \tag{2.7}$$

LEMooQYBJooYwMwGM

Lemme 2.9.
Un groupe est commutatif si et seulement si ses classes de conjugaison sont des singletons.

Démonstration. Supposons que G soit commutatif. Alors

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\} = \{g\}. \tag{2.8}$$

Donc les classes de conjugaison sont des singletons.

Dans l'autre sens, si les classes sont des singletons, on a $kgk^{-1} = g$ pour tous $k, g \in G$. Cela signifie immédiatement que G est commutatif. □

defGroupeCentre

Définition 2.10 (centralisateur[47])**.**
*Soient un groupe G, un sous-groupe H et un élément $h \in H$. Le **centralisateur** de h dans G est l'ensemble des éléments de G qui commutent avec h :*

$$Z_G(h) = \{z \in G \text{ tel que } hz = zh\}. \tag{2.9}$$

Le centralisateur de H dans G est l'ensemble des éléments de G qui commutent avec tous les éléments de H :

$$Z_G(H) = \bigcap_{h \in H} Z_G(h). \tag{2.10}$$

*Le **centre** d'un groupe G est l'ensemble des éléments de G qui commutent avec tous les autres :*

$$Z_G = Z_G(G) = \{z \in G \text{ tel que } gz = zg, \forall g \in G\}. \tag{2.11}$$

DEFooUXXTooCCLmQe

Définition 2.11.
*Un sous-groupe H de G est un sous-groupe **caractéristique** si $\alpha(H) \subset H$ pour tout automorphisme[4] α de G.*

Lemme 2.12 ([48])**.**
Si H est un sous-groupe caractéristique de G, alors $\alpha(H) = H$ pour tout automorphisme α de G.

Démonstration. Si α est un automorphisme de G, alors α^{-1} est encore un automorphisme de G. En particulier $\alpha^{-1}(H) \subset H$.

Soit $h \in H$. Nous devons prouver que $h \in \alpha(H)$. Pour cela :

$$h = \alpha\big(\alpha^{-1}(h)\big) \in \alpha\big(\alpha^{-1}(H)\big) \subset \alpha(H). \tag{2.12}$$

□

2.2 Sous-groupe normal

DEFooNIIMooFkZgvX

Définition 2.13 (Sous-groupe normal)**.**
*Un sous-groupe N de G est **normal** ou **distingué** si pour tout $g \in G$ et pour tout $n \in N$, $gng^{-1} \in N$. Autrement dit lorsque $gNg^{-1} \subset N$.*

Lorsque N est normal dans G il est parfois noté $N \lhd G$.

DEFooZTSMooBislIy

Proposition-Définition 2.14 (normalisateur[47])**.**
*Soient un groupe G et un sous-groupe H. Le **normalisateur** de H dans G est*

$$\mathcal{N}_G(H) = \{g \in G \text{ tel que } gH = Hg\}. \tag{2.13}$$

Le groupe H est normal dans $\mathcal{N}_G(H)$.

[4] Automorphisme de groupe, définition 1.95.

Démonstration. Soit $g \in \mathcal{N}_G(H)$ et $h \in H$. Nous devons prouver que $ghg^{-1} \in H$. Pour cela nous savons que $gH = Hg$, donc il existe $h' \in H$ tel que $gh = h'g$. Nous avons alors

$$ghg^{-1} = h'gg^{-1} = h' \in H. \tag{2.14}$$

□

LEMooZJAQooARqTCG

Lemme 2.15 ([1]).
Si N est normal dans G et si $N \neq G$ alors $|G/N| \geqslant 2$.

Démonstration. Si $g \in G \setminus N$, alors $[g]_N \neq [e]_N$. Ce sont deux éléments différents de G/N. □

NORMooRIGBooJYzkza

2.16.
Si G est un groupe, et si H est un sous-groupe, nous notons $\mathrm{Sub}(G)$ l'ensemble des sous-groupes de G et $\mathrm{Sub}(G, H)$ l'ensemble des sous-groupes de G contenant H.

THOooWONFooXDjtFX

Théorème 2.17 (Théorème de correspondance[49]).
Soient un groupe G et un sous-groupe normal N. Nous ordonnons $\mathrm{Sub}(G, N)$ *et* $\mathrm{Sub}(G/N)$ *par inclusion.*

ITEMooSEWOooKwWYuS

(1) Si $K \in \mathrm{Sub}(G, N)$ alors $K/N \in \mathrm{Sub}(G/N)$

ITEMooCNVGooULzKvW

(2) L'application

$$\begin{aligned} f\colon \mathrm{Sub}(G, N) &\to \mathrm{Sub}(G/N) \\ K &\mapsto K/N \end{aligned} \tag{2.15}$$

est un isomorphisme d'ensembles ordonnés[5]

ITEMooGKTZooSglRTh

(3) Si $K, L \in \mathrm{Sub}(G, N)$ et si $K \leqslant L$ alors K est normal dans L si et seulement si $f(K)$ est normal dans $f(L)$.

Démonstration. En plusieurs parties.

(1) **Pour (1)** Soit $K \in \mathrm{Sub}(G, N)$; nous devons montrer que K/N est un sous-groupe de G/N. En effet soient $k, k' \in K$. Nous avons

$$[k]_N[k']_N = [kk']_N \in K/N. \tag{2.16}$$

(2) **Pour (2)** D'abord notons que f prend bien ses valeurs dans $\mathrm{Sub}(G/N)$ par le point (1). Ensuite nous travaillons un peu. Nous considérons la projection canonique

$$\begin{aligned} \rho\colon G &\to G/N \\ x &\mapsto [g]_N. \end{aligned} \tag{2.17}$$

(2a) **Si $L \in \mathrm{Sub}(G/N)$ alors $\rho^{-1}(L) \in \mathrm{Sub}(G, N)$** Déjà la proposition 1.98 nous dit que $\rho^{-1}(L)$ est un sous-groupe de G parce que ρ est un morphisme. Nous devons montrer que $N \subset \rho^{-1}(L)$. Vu que L est un sous-groupe de G/N nous avons $[e]_N \in L$. En prenant ρ^{-1} est deux côtés,

$$\rho^{-1}\big([e]_N\big) \subset \rho^{-1}(L). \tag{2.18}$$

Et comme $\rho^{-1}([e]_N) = N$, c'est bon.

(2b) **L'application g** Nous posons

$$\begin{aligned} g\colon \mathrm{Sub}(G/N) &\to \mathrm{Sub}(G, N) \\ L &\mapsto \rho^{-1}(L). \end{aligned} \tag{2.19}$$

Nous allons montrer que f et g sont réciproque. Mais avant cela, nous faisons un peu de travail préliminaire.

(2c) **Si $K \in \mathrm{Sub}(G, N)$ alors $\rho^{-1}\big(\rho(K)\big) = K$** Si $x \in \rho^{-1}\big(\rho(K)\big)$, alors il existe $k \in K$ tel que $\rho(x) = \rho(k)$, c'est-à-dire $[x]_n = [k]_N$. Il existe donc $n \in N$ tel que $x = kn$. Et comme $N \subset K$, cela donne $x = kn \in K$.

SIJBITEMooHUBJooTRnKAE

Dans l'autre sens, si $x \in K$, alors $\rho(x) = [x]_N \in \rho(K)$. Donc $\rho(x) \in \rho(K)$ et donc $x \in \rho^{-1}\big(\rho(K)\big)$.

[5] Définition 1.25 : bijection, croissante, d'inverse croissante.

(2d) **Si $L \in \mathrm{Sub}(G/N)$ alors $\rho\big(\rho^{-1}(L)\big) = L$** SUBITEMooAFBWooJURSYd Soit $\alpha \in \rho\big(\rho^{-1}(L)\big)$. Alors il existe $g \in \rho^{-1}(L)$ tel que $\alpha = \rho(g)$. Mais vu que $g \in \rho^{-1}(L)$, nous avons $\rho(g) \in L$. Donc

$$\alpha = \rho(g) \in L. \tag{2.20}$$

Dans l'autre sens, si $\alpha \in L$, alors par définition de $\rho^{-1}(\alpha)$, nous avons $\alpha \in \rho\big(\rho^{-1}(\alpha)\big)$, et même $\rho\big(\rho^{-1}(\alpha)\big) = \{\alpha\}$.

(2e) $\rho^{-1}\big(\mathrm{Sub}(G/N)\big) \subset \mathrm{Sub}(G,N)$ SUBITEMooZSPBooQHgtJL Étant donné que ρ est une morphisme, ρ^{-1} d'un sous-groupe est un sous-groupe. Nous devons montrer que si$L \in \mathrm{Sub}(G/N)$ alors $N \subset \rho^{-1}(L)$. Nous avons $L \in \mathrm{Sub}(G/N)$ et en particulier $[e]_N \in L$. Vu que $\rho^{-1}([e]_N) = N$, nous avons bien $N \subset \rho^{-1}(L)$.

(2f) $g \circ f = \mathrm{Id}$ Notons d'abord que ρ s'applique à tout élément de G et donc, par extension à toute partie de G. L'application f est en réalité la restriction de ρ aux parties de G qui sont dans $\mathrm{Sub}(G,N)$.
Donc si $K \in \mathrm{Sub}(G,N)$ alors

$$(g \circ f)(K) = g\big(f(K)\big) = g\big(\rho(K)\big) = \rho^{-1}\big(\rho(K)\big) = K \tag{2.21}$$

par le point (2c).

(2g) $f \circ g = \mathrm{Id}$ Soit $L \in \mathrm{Sub}(G/N)$. Alors

$$(f \circ g)(L) = f\big(\rho^{-1}(L)\big) = \rho\big(\rho^{-1}(L)\big) = L \tag{2.22}$$

où nous avons utilisé le point (2e) pour remplacer f par ρ et le point (2d) pour la dernière égalité.

(2h) **Conclusion pour (2)** Nous avons prouvé que f était une bijection. En ce qui concerne la croissance, toutes les applications sont croissantes pour l'inclusion : si $A \subset B$ alors $f(A) \subset f(B)$. Et en ce qui concerne la réciproque si $A \subset B$ alors $f^{-1}(A) \subset f^{-1}(B)$. En effet si $x \in f^{-1}(A)$ alors il existe $a \in A$ tel que $f(x) = a$. Mais alors $f(x) = a \in A \subset B$. Donc $x \in f^{-1}(B)$.
Notre application f est donc une bijection croissante d'inverse croissante : un isomorphisme d'ensembles ordonnés.

(3) **Pour (3)** En deux parties.

(3a) $\Rightarrow$ Soient $K, L \in \mathrm{Sub}(G,N)$ avec $K \subset L$ et supposons que K soit normal dans L. Un élément de $f(K)$ est de la forme $[k]_N$ avec $k \in K$; idem pour un élément de $f(L)$ qui est de la forme $[l]_N$ avec $l \in L$. Pour vérifier que $f(K)$ est normal dans $f(L)$, nous

$$[l]_N[k]_N[l]_N^{-1} = [lkl^{-1}]_N. \tag{2.23}$$

Étant donné que k est normal dans L, nous avons $lkl^{-1} = k' \in K$ et donc $[l]_N[k]_N[l]_N^{-1} = [lkl^{-1}]_N = [k']_N \in f(K)$.

(3b) $\Leftarrow$ Nous supposons maintenant que $f(K)$ est normal dans $f(L)$, et nous prouvons que K est normal dans L. Soient $k \in K$ et $l \in L$; par hypothèse

$$[l]_N[k]_N[l]_N^{-1} \in K/N \tag{2.24}$$

Donc il existe $k_N \in k$ tel que $[lkl^{-1}]_N = [k_1]_N$, c'est-à-dire qu'il existe $n \in N$ tel que

$$lkl^{-1} = k_1 n. \tag{2.25}$$

Mais $N \subset K$, donc $lkl^{-1} = k_1 n \in K$, ce qui signifie que K est normal dans L.

□

Pour rappel, la notion de groupe est définie en 1.92.

LEMooQYETooZsTFMg

Lemme 2.18 ([1]).
Soient un groupe G ainsi qu'une partie $S \subset G$. Nous notons $i\colon G \to G$ l'application $x \mapsto x^{-1}$. Si nous posons $W = A \cap i(A)$, alors $W = W^{-1}$.

Démonstration. Nous montrons que $W^{-1} \subset W$. Un élément de W^{-1} est de la forme x^{-1} avec $x \in W$. Nous avons

$$x \in W \Rightarrow x \in i(A) \Rightarrow x^{-1} \in A, \tag{2.26}$$

et

$$x \in W \Rightarrow x \in A \Rightarrow x^{-1} \in i(A). \tag{2.27}$$

Nous avons prouvé que $x^{-1} \in A \cap i(A) = W$. □

2.3 Théorèmes d'isomorphismes

DEFooWBIYooGNRYOp

Définition 2.19.
*Soient un groupe G, un ensemble X et une application $f\colon X \to G$. Le **noyau** de f est la partie*

$$\ker(f) = \{x \in X \text{ tel que } f(x) = e\} \tag{2.28}$$

où e est l'élément neutre de G.

Si G est un groupe et si N est un sous-groupe normal, alors l'ensemble G/N a une structure de groupe et la projection canonique $\pi\colon G \to G/N$ est un morphisme surjectif de noyau N.

ThoPremierthoisomo

Théorème 2.20 (Premier théorème d'isomorphisme)**.**
Soit $\theta\colon G \to H$ un morphisme de groupe. Alors

(1) $\ker(\theta)$ *est normal dans G,*

(2) $\operatorname{Image}\theta$ *est un sous-groupe de H*

ItemWLCLdk

(3) nous avons un isomorphisme

$$\frac{G}{\ker(\theta)} \simeq \operatorname{Image}\theta \tag{2.29}$$

Démonstration. Point par point.

(1) Le fait que $\ker(\theta)$ soit un sous-groupe de G est clair ; montrons qu'il est normal. Si $g \in G$ et $u \in \ker(\theta)$, alors $\theta(g^{-1}ug) = \theta(g^{-1})\theta(u)\theta(g) = \big(\theta(g)\big)^{-1}\theta(g) = 1_H$, et donc $g^{-1}ug \in \ker(\theta)$.

(2) Il suffit de remarquer que si $h = \theta(g)$ et $h' = \theta(g')$, alors $h^{-1}h' = \theta(g^{-1}g')$.

(3) Si $[g]$ représente la classe de g dans $G/\ker(\theta)$, l'isomorphisme est donné par $\varphi([g]) = \theta(g)$.

□

THOooURXUooQJvkjx

Théorème 2.21 (Deuxième théorème d'isomorphisme)**.**
Soient H et N deux sous-groupes de G et supposons que N soit normal[6]*. Alors*

(1) $NH = HN$ est un sous-groupe.

(2) Le groupe N est normal dans NH.

(3) Le groupe $N \cap H$ est normal dans H.

ItemjRPajc

(4) Nous avons l'isomorphisme

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}. \tag{2.30}$$

Démonstration. Point par point.

(1) Il est clair que $1_G \in NH$. Soient nh et $n'h'$ deux éléments de NH ; alors en tenant compte du fait que N est normal,

$$nhn'h' = n\underbrace{hn'h^{-1}}_{\in N}hh' \in NH. \tag{2.31}$$

Cela prouve que NH est un groupe.

De la même façon, nous prouvons que HN est un groupe par

$$hnh'n' = hh'\underbrace{h'^{-1}nh'}_{\in N}n' \in HN \tag{2.32}$$

Nous devons encore prouver que $HN = NH$. Pour cela, $nh \in HN$, car $nh = hh^{-1}nh$, les trois derniers facteurs formant un élément de N par normalité ; de même $hn \in NH$, montrant que $NH = HN$. Enfin, comme $(nh)^{-1} = h^{-1}n^{-1}$, les inverses de NH sont dans $HN = NH$.

(2) N est normal dans G, a fortiori dans l'un de ses sous-groupes.

[6] Si N n'est pas normal, il y aura la proposition 2.22.

(3) Il suffit de voir que, si $h \in H$ et $n \in N \cap H$, alors $hnh^{-1} \in N \cap H$. Or, $hnh^{-1} \in H$ puisque H est un sous-groupe ; et $hnh^{-1} \in N$ car N est un sous-groupe normal de G.

(4) Il faut d'abord remarquer que H et N étant des groupes et le produit NH étant un groupe, nous avons $NH = HN$. Soit le morphisme injectif

$$\begin{aligned} j\colon H &\to HN \\ h &\mapsto h \end{aligned} \tag{2.33}$$

et la surjection canonique

$$\sigma\colon HN \to HN/N \tag{2.34}$$

Nous considérons ensuite l'application composée

$$\begin{aligned} f\colon H &\to HN/N \\ h &\mapsto hN. \end{aligned} \tag{2.35}$$

(4a) f **est surjective** L'application f est surjective parce que l'élément $hnN \in HN/N$ est l'image de h, étant donné que $hnN = hN$.

(4b) $\ker(f) = H \cap N$ Si $a \in H \cap N$, nous avons $f(a) = aN = N$, et donc $H \cap N \subset \ker(f)$. D'autre part, si $h \in H$ vérifie $h \in \ker(f)$, alors $f(h) = hN = N$, ce qui est uniquement possible lorsque $h \in N$.

Le premier théorème d'isomorphisme[7] implique alors que $H/\ker(f) \simeq \text{Image}\, f$, c'est-à-dire

$$H/N \cap H \simeq HN/N. \tag{2.36}$$

□

PROPooVBGMooPTlyLF

Proposition 2.22 (Deuxième théorème d'isomorphisme (suite)[50])**.**
Soient N et H des sous-groupes de G. Si H normalise N, c'est-à-dire si $hNh^{-1} \in N$ pour tout $h \in H$, alors nous avons l'isomorphisme

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}. \tag{2.37}$$

Démonstration. Nous considérons le normalisateur[8] $G' = \{g \in G \text{ tel que } gN = Ng\}$, qui est normal dans G'. Nous considérons le morphisme naturel

$$\begin{aligned} \varphi\colon G' &\to G'/N \\ x &\mapsto [x]_N, \end{aligned} \tag{2.38}$$

et sa restriction $\psi\colon H \to G'/N$.

(1) $\ker(\psi) = H \cap N$ Si $h \in \ker(\psi)$, alors $h \in H$ parce que ψ n'est définie que sur H, et nous avons $[e]_N = \psi(h) = [h]_n$, ce qui signifie que qu'il existe $n, n' \in N$ tels que $hn = n'$, c'est-à-dire $h = n'n^{-1} \in N$. Dans l'autre sens, si $n \in N$ alors $\psi(n) = [n]_N = [e]_N$.

(2) $\ker(\psi)$ **est normal dans** H Soient $x \in H \cap N$ et $h \in H$. Vu que $x \in H$, nous avons $hxh^{-1} \in H$. De plus $x \in N$, et H normalise N, donc $hxh^{-1} \in N$. Cela prouve que $hxh^{-1} \in H \cap N = \ker(\psi)$.

(3) **Premier théorème d'isomorphisme** Nous appliquons le premier théorème d'isomorphisme 2.20 à $\psi\colon H \to G'/N$. Nous avons

$$\frac{H}{\ker(\psi)} = \frac{H}{H \cap N} \simeq \text{Image}(\psi). \tag{2.39}$$

EQooSNIIooKUuwjT

(4) $\text{Image}(\psi) = HN/N$ Soit $h \in H$. Nous avons $\psi(h) = [h]_N \in [HN]_N$. Donc $\text{Image}(\psi) \subset HN/N$. Dans l'autre sens, si $h \in H$ et $n \in N$ alors

$$[hn]_N = [h]_N = \psi(h) \in \text{Image}(\psi). \tag{2.40}$$

(5) **Conclusion** Il suffit de remplacer $\text{Image}(\psi)$ par HN/N dans (2.39) et c'est fait.

[7] Théorème 2.20.
[8] Définition 2.14.

□

ThoezgBep

Théorème 2.23 (Troisième théorème d'isomorphisme)**.**
Soient N et M deux sous-groupes normaux de G avec $M \subset N$. Alors N/M est normal dans G/M et

$$(G/M)/(N/M) \simeq G/N. \tag{2.41}$$

Démonstration. Afin de montrer que N/M est normal dans G/M, nous considérons $g \in G$, $nM \in N/M$ et nous calculons

$$gnMg^{-1} = gng^{-1}\underbrace{gMg^{-1}}_{=M} = \underbrace{gng^{-1}}_{\in N}M \in N/M. \tag{2.42}$$

Pour prouver l'isomorphisme nous considérons le morphisme

$$\begin{aligned} \varphi\colon G/M &\to G/N \\ gM &\mapsto gN. \end{aligned} \tag{2.43}$$

Ce morphisme est surjectif et son noyau est N/M, parce que $\varphi(gM) = N$ uniquement si $g \in N$. Nous pouvons appliquer le premier théorème d'isomorphisme à φ en écrivant

$$(G/M)/\ker(\varphi) \simeq \text{Image}\,\varphi, \tag{2.44}$$

c'est-à-dire

$$(G/M)/(N/M) \simeq G/N. \tag{2.45}$$

□

2.4 Quelques résultats de cardinalité

PROPooJLGKooDCcnWi

Proposition-Définition 2.24 (Cardinal d'un ensemble fini[1])**.**
Soit un ensemble non vide I.

ITEMooMNMTooEOIjdo

(1) L'ensemble I est fini[9] *si et seulement si il existe une bijection entre I et $\{0, \dots, N\}$ pour un certain $N \in \mathbb{N}$.*

ITEMooZJFUooSNUSIk

(2) Si I est fini, il existe un unique $N \in \mathbb{N}$ tel que I soit en bijection avec $\{0, \dots, N\}$.

*Dans ce cas, le nombre $N+1$ est le **cardinal** de I, et est noté* $\text{Card}(I)$*. Pour l'ensemble vide, nous définissons* $\text{Card}(\varnothing) = 0$.

Démonstration. En plusieurs parties.

(1) **(1), $\Leftarrow$** Soit un ensemble A en bijection avec $\{0, \dots, N\}$. Nous avons vu que $\{0, \dots, N\}$ est fini dans le lemme 1.177. Le lemme 1.80(2) conclut que A est fini.

(2) **(1), $\Rightarrow$** Le vrai sport est de faire l'implication inverse. Nous supposons que A est un ensemble fini, et nous allons prouver qu'il est en bijection avec $\{0, \dots, N\}$ pour un N bien choisi. Nous allons utiliser le lemme de Zorn. Soit

$$\mathcal{A} = \{(N, \varphi) \text{ tel que } \varphi\colon \{0, \dots, N\} \to A \text{ est injective}\}. \tag{2.46}$$

Nous mettons sur $\mathcal{A}$ la relation d'ordre donnée par $(N_1, \varphi_1) \leqslant (N_2, \varphi_2)$ lorsque

(2a) $N_1 \leqslant N_2$

(2b) φ_2 étend φ_1, c'est-à-dire que $\varphi_2 = \varphi_1$ sur $\{0, \dots, N_1\}$.

(2a) **$\mathcal{A}$ est inductif** Soit une partie $\mathcal{F}$ totalement ordonnée de $\mathcal{A}$. Nous considérons la partie suivante de $\mathbb{N}$:

$$S = \{n \in \mathbb{N} \text{ tel que } \exists \varphi \text{ tel que } (n, \varphi) \in \mathcal{F}\}. \tag{2.47}$$

Si S est majoré, alors il a un maximum (proposition 1.152(4)). Si M est le maximum de S, le (M, φ) de $\mathcal{F}$ qui correspond à ce maximum est un majorant de $\mathcal{F}$.

[9] Ensemble fini, définition 1.74.

Supposons –pour l'absurde– que $\mathcal{F}$ n'est pas majoré dans $\mathcal{A}$; en particulier S n'est pas majoré dans $\mathbb{N}$. Pour chaque $n \in S$, il existe une application φ_n telle que $(n, \varphi_n) \in \mathcal{F}$. Cela nous permet de définir

$$\begin{aligned} \phi\colon S &\to A \\ n &\mapsto \varphi_n(n). \end{aligned} \tag{2.48}$$

Montrons que ϕ est injective. Si $\phi(m) = \phi(n)$, alors $\varphi_m(m) = \varphi_n(n)$. Supposons pour fixer les idées que $n \leqslant m$. Vu que (n, φ_n) et (m, φ_m) sont dans $\mathcal{F}$ qui est totalement ordonné, φ_m prolonge φ_n ; en particulier $\varphi_n(n) = \varphi_m(n)$. Mais comme φ_m est injective, $m = n$.
Nous avons donc une injection $\phi\colon S \to A$. Mais S est non borné et donc infini[10]. La proposition 1.79 conclut que A est infini, ce qui est contraire aux hypothèses.
Donc $\mathcal{F}$ a un majorant et $\mathcal{A}$ est inductif.

(2b) **Lemme de Zorn** Le lemme de Zorn dit que $\mathcal{A}$ a un élément maximal.

(2c) **Conclusion** Soit (N, φ) un élément maximal de $\mathcal{A}$. Nous allons prouver que $\varphi\colon \{0, \dots, N\} \to A$ est une bijection. Que φ soit injective est une conséquence du fait que (N, φ) est dans $\mathcal{A}$.
Pour prouver que φ est surjective, nous supposons qu'elle ne l'est pas. Soit $a \in A$ qui n'est pas dans l'image de φ. En posant

$$\begin{aligned} \phi\colon \{0, \dots, N+1\} &\to A \\ x &\mapsto \begin{cases} \varphi(x) & \text{si } x \neq N+1 \\ a & \text{si } x = N+1, \end{cases} \end{aligned} \tag{2.49}$$

le couple $(N+1, \phi)$ majore strictement (N, φ). Ce qui est une contradiction.

(3) **(2) existence** L'existence est ce que nous venons de montrer ci-dessus.

(4) **(2) unicité** Supposons que I soit en bijection avec $\{0, \dots, M\}$ et avec $\{0, \dots, N\}$. Il existe donc une bijection entre $\{0, \dots, M\}$ et $\{0, \dots, N\}$. Par le lemme 1.178, cela implique que $M = N$.

□

Nous ne définissons pas ce qu'est le cardinal d'un ensemble infini ; c'est très compliqué et ça ne nous servira pas.

LEMooRWUDooTgoRXH

Lemme 2.25.
Si A est une partie infinie de $\mathbb{N}$, alors pour tout n, la partie $A \setminus \{0, \dots, n\}$ est non vide.

Démonstration. Si $A \setminus \{0, \dots, n\}$ était vide, cela signifierait que A est une partie de $\{0, \dots, n\}$. Or nous savons que $\{0, \dots, n\}$ est fini (lemme 1.177), et que toute partie d'un ensemble fini est finie (lemme 1.76). Donc nous aurions que A est fini, ce qui est contraire à l'hypothèse. □

2.26.
En termes de notations, si I et A sont des ensembles et si $\sigma\colon I \to A$ est une injection, nous notons souvent

$$\{a_i\}_{i \in I} \tag{2.50}$$

l'ensemble $\sigma(I)$ en écrivant a_i pour $\sigma(i)$.
La proposition 2.27 dira entre autres que $\text{Card}\big(\{a_1, \dots, a_n\}\big) = n$ ou que

$$\text{Card}\big(a_i \text{ tel que } i \in I\big) = \text{Card}(I) \tag{2.51}$$

pourvu que les a_i sont tous différents.
La proposition 2.28 permettra de dire, si $\text{Card}(A) = k$, que $A = \{a_1, \dots, a_k\}$.

PROPooTJVUooZDxMpU

Proposition 2.27 ([1]).
Si il existe une injection $\sigma\colon I \to E$ alors $\text{Card}\big(\sigma(I)\big) = \text{Card}(I)$.

Démonstration. L'application σ est une bijection entre I et son image $\sigma(I)$. □

PROPooFRKAooAnqKEh

Proposition 2.28 ([1]).
Soient un ensemble fini E tel que $\text{Card}(E) = n$ et une partie finie $A \subset E$ telle que $\text{Card}(A) = k$. Nous considérons une bijection $\sigma\colon \{1, \dots, n\} \to E$. Alors il existe $S \subset \{1, \dots, n\}$ tel que

[10] Le lemme 1.158 dit qu'il existe une bijection entre S et $\mathbb{N}$. De là nous concluons que S est infini parce qu'un ensemble en bijection avec un ensemble infini est infini par la proposition 1.79.

(1) $\text{Card}(S) = k$

(2) $A = \sigma(S)$.

Démonstration. Il suffit de poser $S = \sigma^{-1}(A)$. □

LEMooVFPNooVmdUXY

Lemme 2.29 ([1]).
Union d'ensembles finis.

ITEMooBUCZooYLCuIe

(1) *Si A et B sont des ensembles finis disjoints, alors $A \cup B$ est fini et*

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B). \tag{2.52}$$

ITEMooCCWOooYwgGBp

(2) *Si A et B sont des ensembles finis, alors $A \cup B$ est fini.*

ITEMooYJSZooXQXkOX

(3) *Si A est fini et si $B \subset A$ alors*

$$\text{Card}(A \setminus B) = \text{Card}(A) - \text{Card}(B). \tag{2.53}$$

ITEMooSWJCooEpBVkG

(4) *Si A et B sont des ensembles quelconques, alors*

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B). \tag{2.54}$$

ITEMooJDUUooVMvAOn

(5) *Si les $\{A_i\}_{i=1,\dots,n}$ sont des ensembles deux à deux disjoints, alors*

$$\text{Card}\Big(\bigcup_{i=1}^{n} A_i\Big) = \sum_{i=1}^{n} \text{Card}(A_i). \tag{2.55}$$

ITEMooNMFSooBvsNyq

(6) *Si I ou J est infini, alors $I \cup J$ est infini.*

Démonstration. Point par point.

(1) **Pour (1)** Puisque A et B sont finis, la proposition 2.24 nous dit qu'il existe des naturels N et M ainsi que des bijections $\varphi_A\colon \{0,\dots,N\} \to A$ et $\varphi_B\colon \{0,\dots,M\} \to B$. Maintenant l'application

$$\begin{aligned} \varphi\colon \{0,\dots,M+N+1\} &\to A \cup B \\ n &\mapsto \begin{cases} \varphi_A(n) & \text{si } n \leqslant N \\ \varphi_B(n-N-1) & \text{si } n > N \end{cases} \end{aligned} \tag{2.56}$$

est une bijection. Le fait que A et B soient disjoints est important pour l'injectivité. La proposition 2.24 nous dit qu'alors $A \cup B$ est fini. De plus, par définition le cardinal de $A \cup B$ est $N + M$.

(2) **Pour (2)** Nous ne supposons plus que A et B sont disjoints. Nous posons $I = A$ et $J = B \setminus A$. Avec ça, I et J sont disjoints et finis (comme parties des ensembles finis, lemme 1.76), et vérifient $I \cup J = A \cup B$. Le point (1) indique que $I \cup J$ est fini.

(3) **Pour (3)**
L'ensemble A peut être écrit sous la forme d'une union disjointe : $A = B \cup (A \setminus B)$. Les ensembles B et $A \setminus B$ étant disjoints, nous avons

$$\text{Card}(A) = \text{Card}(B) + \text{Card}(A \setminus B). \tag{2.57}$$

(4) **Pour (4)** Nous utilisons quelques égalités d'ensembles pour ramener $A \cup B$ à des cas déjà traités :

$$A \cup B = A \cup (B \setminus A) = A \cup \big(B \setminus (A \cap B)\big). \tag{2.58}$$

EQooSZDYooPBOdYv

Nous avons en particulier utilisé $B \setminus A = B \setminus (A \cap B)$. La chose intéressante dans (2.58) est que l'union est disjointe et que $A \cap B \subset B$. Nous pouvons donc écrire

$$\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}\big(B \setminus (A \cap B)\big) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B). \tag{2.59}$$

(5) **Pour (5)** Récurrence en utilisant le point (4).

(6) **Pour (6)** Toute partie d'un ensemble fini est finie (lemme 1.76). Donc si $I \cup J$ était fini, I et J devraient l'être.

□

2.4.1 Ordre d'un groupe

L'ordre d'un groupe et l'ordre d'un élément d'un groupe sont deux choses différentes.

DEFooKWBCooMImpCP

Définition 2.30 (Ordre d'un groupe)**.**
Soit un groupe G.

*(1) Si G est un ensemble fini, l'**ordre** de G est son cardinal*[11]*, et nous le notons $|G|$.*

(2) Si l'ensemble G est infini, nous disons que $|G| = \infty$ et qu'il est d'ordre infini.

Oui : nous pourrions simplement toujours dire « cardinalité » et écrire $\text{Card}(G)$*. Au lieu de ça, dans le cas particulier des groupes, il y a une tradition de dire « ordre » et d'écrire* $|G|$*.*

Note : l'ordre d'un élément n'a rien à voir, ce sera la définition 2.68. Le lien est qu'il divise l'ordre du groupe par le corolaire 2.74.

2.4.2 Minimum, maximum

Une démonstration sans utilisation des naturels est dans la proposition 1.77.

LEMooPCRFooXRGrUr

Lemme 2.31 ([51])**.**
Si E est un ensemble ordonné et si A est une partie finie non vide totalement ordonnée de E, alors A possède un unique minimum et un unique maximum[12]*.*

Démonstration. En plusieurs parties.

(1) **Existence maximum** Soit un ensemble E totalement ordonné. Nous faisons par récurrence[13] sur le cardinal de la partie finie (proposition 2.24 pour la définition du cardinal).

Si $\text{Card}(A) = 1$, alors nous avons $A = \{a\}$ pour un certain $a \in E$ et ce a est un maximum de A.

Sinon nous passons à la récurrence. Nous supposons que pour toute partie B totalement ordonné de cardinal n, il existe un $m_B \in B$ tel que $m_B \geqslant x$ pour tout $x \in B$. Soit une partie A totalement ordonnée de cardinal $n+1$. Nous prouvons que A possède un maximum.

Soit $a \in A$. La partie $B = A \setminus \{a\}$ est de cardinal $n-1$ (lemme 2.29(3)). Par hypothèse de récurrence, l'ensemble B admet un maximum que nous notons b. Il y a deux possibilités : $a > b$ ou $a < b$.

(1a) **Si $a > b$** Alors nous avons $a \geqslant x$ pour tout $x \in A = B \cup \{a\}$. En effet si $x \in B$ nous avons $x < b < a$. Et si $x = a$ nous avons $a = x$.

(1b) **Si $b > a$** Alors $b \geqslant x$ pour tout $x \in A = B \cup \{a\}$. En effet si $x \in B$ nous avons $b \geqslant x$ par définition de b et si $x = a$ nous avons $b > x$ par hypothèse.

(2) **Unicité maximum** En ce qui concerne l'unicité, si a et b sont des maximums d'une partie A, alors $a \geqslant b$ parce que $b \in A$ et $b \geqslant a$ parce que $a \in A$. La définition 1.23(2) de la relation d'ordre conclu que $a = b$.

Pour l'existence et l'unicité du minimum, nous adaptons juste ce que nous venons de faire[14]. □

LEMooOEJOooOgaxzi

Lemme-Définition 2.32 ([1])**.**
Si A est une partie non vide de $\mathbb{N}$, il existe un unique élément $m \in \mathbb{N}$ tel que

$$\begin{cases} m \in A & \text{(2.60a)} \\ m \leqslant x \; \forall x \in A. & \text{(2.60b)} \end{cases}$$

Cet élément est noté $\min(A)$ *et nommé **minimum de** A.*

Si A est majoré, il existe un unique élément $M \in \mathbb{N}$ tel que

$$\begin{cases} M \in A & \text{(2.61a)} \\ M \geqslant x \; \forall x \in A. & \text{(2.61b)} \end{cases}$$

Cet élément est noté $\max(A)$ *et nommé **maximum de** A.*

[11] Définition 2.24.
[12] Définition 1.33.
[13] Proposition 1.130.
[14] Je n'ai pas vérifié. Faites-le et écrivez-moi si ça pose un problème.

Démonstration. En plusieurs parties.

(1) **Existence minimum** Soit $a \in A$. Nous considérons $E = A \cap \{0, \dots, a\}$. C'est un en semble non vide (il contient a) et fini en tant que partie de $\{0, \dots, a\}$ (utilisation des lemmes 1.76 et de 1.177). Donc 2.31 dit que E possède un minimum. Soit m ce minimum.

Si $x \in A$ alors soit $x \in E$ (et alors $l \leqslant x$), soit x n'est pas dans E et alors $x \geqslant a \geqslant m$.

(2) **Existence maximum** Soit un majorant M de A. Si $M \in A$ alors on est bon. Sinon nous posons

$$E = \bigcap_{a \in A} \{a, \dots, M\}. \tag{2.62}$$

C'est un ensemble non vide parce qu'il contient M. Et il est fini parce qu'il est contenu dans $\{0, \dots, M\}$ qui est fini.

Nous considérons le minimum μ de E. Pour tout $a \in A$ nous avons $\mu \in \{a, \dots, M\}$ et donc $\mu \geqslant a$.

Nous devons encore prouver que $\mu \in A$. Supposons que ce ne soit pas le cas. Alors pour tout $a \in A$ nous avons $\mu \in \{a, \dots, M\}$. Mains $\mu \neq a$, donc $\mu \in \{a+1, \dots, M\}$. Autrement dit, $\mu \in \{a+1, \dots, M\}$. Donc

$$\mu - 1 \in \bigcap_{a \in A} \{a, \dots, M\} = E. \tag{2.63}$$

Contradiction à propos de la minimalité de μ.

(3) **Unicité minimum** Soient des minima m_1 et m_2. Nous avons $m_1 \leqslant m_2$ parce que $m_2 \in A$ et m_1 est une minimum de A. De même $m_2 \leqslant m_1$. Donc $m_1 = m_2$.

(4) **Unicité maximum** De même que l'unicité du minimum.

□

LEMooGQUWooYJQfJB

Lemme 2.33.
À propos de majorant, minorant et parties finies.

ITEMooOOOZooXTClck

(1) Toute partie finie non vide de $\mathbb{N}$ est majorée et minorée.

ITEMooKXLXooVVwpnj

(2) Une partie de $\mathbb{N}$ admet un maximum si et seulement si elle est finie.

Démonstration. Le point (1) est un cas particulier du lemme 2.31. Le point (2) dans un sens est le point (1) tandis que dans l'autre sens, c'est le lemme 2.31. □

DefEnsembleDenombrable

Définition 2.34.
*Un ensemble est **dénombrable** si il peut être mis en bijection avec $\mathbb{N}$. Il est **non dénombrable** si il est infini et ne peut pas être mis en bijection avec $\mathbb{N}$.*

Une chose vraiment amusante avec cette définition que l'on met en rapport avec la définition 1.74, c'est qu'un ensemble fini n'est ni dénombrable ni non dénombrable[15].

2.4.3 Dénombrabilité et ensemble des naturels

PROPooOBKMooWEGCvM

Proposition 2.35 ([1, 18])**.**
Toute partie infinie de $\mathbb{N}$ est dénombrable.

Démonstration. Soit A, une partie infinie de $\mathbb{N}$.

(1) **Définition de σ** Nous voulons construire une application $\sigma : \mathbb{N} \to A$ telle que

$$\begin{cases} \sigma(0) = \min(A) & \text{SUBEQooEIEMooZcTOWT} \quad (2.64a) \\ \sigma(k+1) = \min\Big(A \setminus \sigma\big(\{0, \dots, k\}\big)\Big) & \text{SUBEQooWWOAooAEfrPx} \quad (2.64b) \end{cases}$$

Les lâches, par prudence, diront juste que c'est défini par récurrence et n'insisteront pas. Nous, nous insistons.

[15] Beaucoup de sources disent qu'un ensemble est dénombrable lorsqu'il est en bijection avec une partie de $\mathbb{N}$. Cela laisse la porte ouverte aux ensembles finis. Par exemple Wikipédia[52].

Nous allons définir $\sigma(n)$ à l'aide du théorème 1.131. Pour cela nous posons $E = \mathcal{P}(A)$, $b = \varnothing$ et

$$\begin{aligned} g\colon E &\to E \\ Z &\mapsto \begin{cases} A & \text{si } Z = A \\ Z \cup \{\min(A \setminus Z)\} & \text{sinon.} \end{cases} \end{aligned} \tag{2.65}$$

Notons que la proposition 1.152(2) nous indique que toute partie non vide de $\mathbb{N}$ possède un minimum ; la définition de g a donc un sens. Le théorème 1.131 donne alors une application $f\colon \mathbb{N} \to E$ telle que

(1a) $f(0) = b = \varnothing$

(1b) $f(n+1) = g\big(f(n)\big)$ pour tout $n \geqslant 0$.

Prouvons par récurrence que $f(n)$ est un ensemble fini pour tout n. D'abord $f(0) = \varnothing$. Ensuite, si $n \geqslant 0$ est tel que $f(n)$ est fini, alors en particulier $f(n) \neq A$ et nous avons

$$f(n+1) = g\big(f(n)\big) = f(n) \cup \{\min\big(A \setminus f(n)\big)\}. \tag{2.66}$$

Dans ce cas, $f(n+1)$ est également fini comme union de deux ensembles finis.

Nous posons

$$\sigma(n) = \min\big(A \setminus f(n)\big). \tag{2.67}$$

EQooGHQHooBnXDdo

Avec $n = 0$, nous avons $\sigma(0) = \min\big(A \setminus \varnothing\big) = \min(A)$. La condition (2.64a) est donc déjà satisfaite.

Nous devons encore prouver (2.64b). Pour tout n, la relation entre $f(n)$ et $\sigma(n)$ est donnée par

$$\begin{cases} f(0) = \varnothing & \text{(2.68a)} \\ f(n+1) = f(n) \cup \sigma(n). & \text{(2.68b)} \end{cases}$$

Par récurrence nous avons alors

$$f(n) = \bigcup_{k=0}^{n-1} \{\sigma(k)\} = \sigma\big(\{0, \dots, n-1\}\big) \tag{2.69}$$

EQooPXFEooYzhtBe

pour tout $n \geqslant 1$. Nous avons alors la condition 2.64b en substituant (2.69) dans la définition (2.67) écrite avec $n+1$:

$$\sigma(n+1) = \min\big(A \setminus f(n+1)\big) = \min\Big(A \setminus \sigma\big(\{0, \dots, n\}\big)\Big). \tag{2.70}$$

(2) **σ est strictement croissante** Vu que $A \setminus \sigma\{0, \dots, k\} \subset A \setminus \sigma\{0, \dots, k-1\}$, le minimum est plus grand ou égal : $\sigma(k+1) \geqslant \sigma(k)$. Mais $\sigma(k+1)$ est sélectionné dans l'ensemble $A \setminus \sigma\{0, \dots, k\}$, qui ne contient justement pas $\sigma(k)$. Donc $\sigma(k+1) \neq \sigma(k)$.

(3) **σ est définie sur $\mathbb{N}$** Il faut montrer que pour tout k, l'ensemble $A \setminus \sigma\{0, \dots, k\}$ est non vide. Si il l'était, cela signifierait que $A \subset \sigma\{0, \dots, k\}$. Par le lemme 1.80(1), la partie $\sigma\{0, \dots, k\}$ est finie dans $\mathbb{N}$. Le lemme 1.76 dit alors qu'en tant que partie de $\sigma\{0, \dots, k\}$, l'ensemble A est fini. Mais comme les hypothèses disent que A est infini, nous avons une contradiction et nous concluons que σ est bien définie sur tout $\mathbb{N}$.

(4) **σ est injective** Une application $\mathbb{N} \to \mathbb{N}$ strictement croissante est injective par la proposition 1.157.

(5) **σ est surjective** Soit $a \in A$. Vu que σ est strictement croissante et que $\sigma(0) \geqslant 0$, nous avons $\sigma(a) \geqslant a$. Si $\sigma(a) = a$ nous avons terminé. Supposons $\sigma(a) > a$. Alors

$$\min\big(A \setminus \sigma\{0, \dots, a\}\big) > a. \tag{2.71}$$

EQooNHTBooQexzwV

Si $\sigma\big(\{0, \dots, a\}\big)$ ne contenait pas a, alors $A \setminus \sigma(\{0, \dots, a\})$ le contiendrait et nous n'aurions pas l'inégalité (2.71). Donc $a \in \sigma\big(\{0, \dots, a\}\big)$ et a est bien dans l'image de σ.

□

NORMooPartieDenombrableParCantorBernstein

2.36.
La proposition 2.35 pourrait être prouvée plus facilement en acceptant le théorème de Cantor-Schröder-Bernstein 1.84. Il existe une injection $A \to \mathbb{N}$ parce que A est une partie de $\mathbb{N}$. Mais puisque A est infini, il possède une partie dénombrable. Cela donne une surjection $A \to \mathbb{N}$ et donc une injection $\mathbb{N} \to A$. Le théorème de Cantor-Schröder-Bernstein conclut.

Cela dit, une telle preuve demanderait des outils plus complexes.

NORMooBijectionNNMadore

2.37.
La proposition suivante donne une bijection explicite entre $\mathbb{N}$ et $\mathbb{N}\times\mathbb{N}$. Elle n'a rien de transcendante, mais je ne résiste pas à la donner ici parce qu'elle est utilisée dans l'article *Un peu de programmation transfinie* de David Madore[16]. Son utilité est de pouvoir créer un langage de programmation pouvant traiter des paires d'entiers rien qu'en traitant des entiers.

PROPooLPKUooAlsYJg

Proposition 2.38 (Une bijection $\mathbb{N}\times\mathbb{N}\to\mathbb{N}$)**.**
La fonction

$$\begin{aligned} f\colon \mathbb{N}\times\mathbb{N}&\to\mathbb{N}\\ (x,y)&\mapsto\begin{cases} y^2+x & si\ x<y\\ x^2+x+y & si\ y\leqslant x.\end{cases}\end{aligned} \tag{2.72}$$

est une bijection.

Démonstration. Il s'agit de prouver qu'elle est injective et surjective. Dans la suite, tous les nombres sont des entiers positifs.

(1) **f est injective**

Pour $k\in\mathbb{N}$ donné, nous allons prouver que

(1a) l'équation $f(x,y)=k$ possède au maximum une solution avec $x<y$,

(1b) l'équation $f(x,y)=k$ possède au maximum une solution avec $y\leqslant x$,

(1c) si $k=y^2+x$ avec $x<y$ alors il est impossible que $k=x'^2+x'+y'$ avec $y'\leqslant x'$.

On y va.

(1a) Nous supposons $y^2+x=t^2+z$ avec $x<y$ et $z<t$. Pour fixer les idées, nous supposons $t>y$ et nous posons $t=y+s$ ($s\geqslant 1$). En substituant, et en isolant z,

$$\begin{aligned} z&=x-2sy-s^2 && \text{(2.73a)}\\ &<x-2sy && \text{(2.73b)}\\ &<x-2sx && \text{(2.73c)}\\ &=x(1-2s) && \text{(2.73d)}\\ &<0. && \text{(2.73e)}\end{aligned}$$

Impossible parce que $z\geqslant 0$.

(1b) De même nous supposons $x^2+x+y=z^2+z+t$ avec $y\leqslant x$ et $t\leqslant z$. Nous posons $z=x+s$, et nous déballons le même genre de calculs en isolant t.

(1c) Enfin nous supposons $y^2+x=z^2+z+t$ avec $x<y$ et $t\leqslant z$. Les plus courageux diviseront en trois cas : $y<z$, $y=z$ et $y>z$ et feront les calculs. Par exemple, pour le cas $y>z$ nous posons $y=z+s$ et nous substituons :

$$(y+s)^2+x=z^2+z+t \tag{2.74}$$

qui donne

$$x=z+t-2zs-s^2<2z-2zs-s^2=2z(1-s)-s^2\leqslant -s<0 \tag{2.75}$$

parce que $s\geqslant 1$, donc $1-s\leqslant 0$.

(2) **f est surjective**

Nous devons prouver que tous les éléments de $\mathbb{N}$ sont dans l'image de $\mathbb{N}\times\mathbb{N}$ par f. En premier lieu, $0=f(0,0)$. C'est un bon début. Soit $a\in\mathbb{N}$ non nul ; nous montrons que tous les nombres de a^2 à $(a+1)^2$ sont des images de f. D'abord $a^2=f(0,a)$, ensuite les nombres

$$f(1,a),f(2,a),\dots,f(a-1,a) \tag{2.76}$$

prennent les valeurs a^2+1, …, a^2+a-1. Enfin nous avons $f(a,0)=a^2+a$ et les nombres $f(a,1),\dots,f(a,a)$ prennent les valeurs de a^2+a+1 à $a^2+2a=(a+1)^2-1$.

□

[16] Et comme j'aime beaucoup cet article, il me fallait une excuse pour le placer ici.
http://www.madore.org/~david/weblog/d.2017-08-18.2460.html.

REMooBijectionNNOrdinaux

Remarque 2.39.
Sachez que cette fonction s'étend aux ordinaux (mais là ce n'est plus pour rigoler).

CORooNRPIooZPSmqa

Corolaire 2.40.
Il existe des parties $\{\mathbb{N}_i\}_{i\in\mathbb{N}}$ *telles que* $\bigcup_{i\in\mathbb{N}}\mathbb{N}_i=\mathbb{N}$ *et que chaque* $\mathbb{N}_i$ *soit en bijection avec* $\mathbb{N}$

Démonstration. Nous considérons la bijection $f\colon\mathbb{N}\to\mathbb{N}\times\mathbb{N}$ donnée par (l'inverse de celle donnée) par la proposition 2.38, et nous posons

$$\mathbb{N}_i=f^{-1}(i,\mathbb{N}). \tag{2.77}$$

L'application

$$f\colon\mathbb{N}_i\to\{(i,k)\}_{k\in\mathbb{N}} \tag{2.78}$$

est une bijection. Or l'ensemble $\{(i,k)\}_{k\in\mathbb{N}}$ est évidemment en bijection avec $\mathbb{N}$. Par composition nous avons le résultat. □

LEMooDLWFooNAJbbq

Lemme 2.41 ([1])**.**
Si il existe une surjection $\mathbb{N}\to A$*, alors* A *est fini ou dénombrable.*

Démonstration. Pour chaque $a\in A$, l'ensemble $f^{-1}(a)$ est une partie de $\mathbb{N}$.

(1) **Une application** La proposition 1.152(2) nous permet de poser

$$\begin{aligned}\sigma\colon A&\to\mathbb{N}\\ a&\mapsto\min\big(f^{-1}(a)\big).\end{aligned} \tag{2.79}$$

(2) **σ est injective** Supposons que $\sigma(a)=\sigma(b)$. Nous appelons x ce nombre :

$$x=\min\big(f^{-1}(a)\big)=\min\big(f^{-1}(b)\big). \tag{2.80}$$

Nous avons $x\in f^{-1}(a)\cap f^{-1}(b)$, ce qui implique que $f(x)=a$ et que $f(x)=b$; donc $a=b$.

Donc σ est une injection.

(3) **A est infini** Si A est fini, le lemme est prouvé. Donc à partir de maintenant nous supposons que A est infini. Le but est de prouver qu'il est dénombrable, c'est-à-dire de construire une bijection $A\to\mathbb{N}$.

(4) **$\sigma(A)$ est dénombrable** Puisque $\sigma\colon A\to\mathbb{N}$ est injective et que A est infini, la proposition 1.79 dit que $\sigma(A)$ est infini dans $\mathbb{N}$. La proposition 2.35 nous dit alors que $\sigma(A)$ est dénombrable.

Soit une bijection $\varphi\colon\sigma(A)\to\mathbb{N}$.

(5) **La candidate bijection** Nous posons

$$f=\varphi\circ\sigma\colon A\to\mathbb{N} \tag{2.81}$$

et nous allons prouver que c'est une bijection.

(6) **Injective** Puisque φ et σ sont injectives, l'égalité $(\varphi\sigma)(a)=(\varphi\sigma)(b)$ implique immédiatement $a=b$.

(7) **Surjective** Soit $k\in\mathbb{N}$. Puisque φ et σ sont des injections, nous pouvons poser $a=(\sigma^{-1}\varphi^{-1})(k)$. Il est alors immédiat que $f(a)=k$.

□

PROPooENTPooSPpmhY

Proposition 2.42 ([1, 52])**.**
Une union dénombrable d'ensembles finis ou dénombrables est finie ou dénombrable.

Démonstration. Soient A_i des ensembles finis ou dénombrables. Nous posons $A=\bigcup_{i\in\mathbb{N}}A_i$, et nous considérons les parties $\mathbb{N}_i$ du corolaire 2.40. Puisque A_i est dénombrable ou fini et que $\mathbb{N}_i$ est dénombrable, il existe une surjection $\varphi_i\colon\mathbb{N}_i\to A_i$.

Nous définissons $s\colon\mathbb{N}\to\mathbb{N}$ par $n\in\mathbb{N}_{s(n)}$, et nous posons enfin

$$\begin{aligned}\varphi\colon\mathbb{N}&\to A\\ n&\mapsto\varphi_{s(n)}(n).\end{aligned} \tag{2.82}$$

Nous prouvons que φ est surjective.

Soit $a \in A_i$. Il existe $n \in \mathbb{N}_i$ tel que $a = \varphi_i(n)$. Mais comme $n \in \mathbb{N}_i$, nous avons $s(n) = i$. Donc

$$a = \varphi_i(n) = \varphi_{s(n)}(n) = \varphi(n). \tag{2.83}$$

Donc $\varphi: \mathbb{N} \to A$ est surjective.

Le lemme 2.41 conclut que A est fini ou dénombrable. □

LEMooDTAEooIBdHyo

Lemme 2.43.
Si A est dénombrable et si il existe une surjection $f: A \to B$, alors B est fini ou dénombrable.

Démonstration. Étant donné que A est dénombrable, il existe une bijection $\varphi: \mathbb{N} \to A$. L'application $f \circ \varphi: \mathbb{N} \to B$ est donc une surjection de $\mathbb{N}$ vers B. Donc B est fini ou dénombrable par le lemme 2.41. □

LEMooSRZWooASgEfy

Lemme 2.44.
Si A est un ensemble fini ou dénombrable, alors il existe une surjection $\mathbb{N} \to A$.

LEMooKFBAooHxgOsg

Lemme 2.45 ([1]).
Si A est dénombrable, alors l'ensemble des parties finies de A est dénombrable.

LEMooRXSRooBUWOyb

Lemme 2.46 ([1]).
Si N est un ensemble dénombrable, alors il existe une bijection $g: \{1,2\} \times N \to N$.

Démonstration. D'abord nous définissons une bijection $\varphi: \{0,1\} \times \mathbb{N} \to \mathbb{N}$ par

$$\begin{aligned} \varphi: \{0,1\} \times \mathbb{N} &\to \mathbb{N} \\ (n,k) &\mapsto 2k + n. \end{aligned} \tag{2.84}$$

Ensuite si $f: \mathbb{N} \to N$ est une bijection, il suffit de poser $g(n,k) = f\big(\varphi(n,k)\big)$. □

PROPooDMZHooXouDrQ

Proposition 2.47 (Produit d'ensembles dénombrables[52]).
Deux résultats.

ITEMooWNBGooZjoIjZ

(1) Si A et B sont dénombrables, alors $A \times B$ est dénombrable.

(2) Si N est un ensemble dénombrable, alors pour tout $n \in \mathbb{N}$, l'ensemble N^n est dénombrable.

Démonstration. La proposition 2.38 donne une bijection $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Par hypothèse sur A et B nous avons des bijections $\varphi: A \to \mathbb{N}$ et $\sigma: B \to \mathbb{N}$. Nous posons

$$\begin{aligned} f: A \times B &\to \mathbb{N} \\ (a,b) &\mapsto f\big(\varphi(a), \sigma(b)\big) \end{aligned} \tag{2.85}$$

et nous prouvons que c'est une bijection.

(1) **Injectif** Supposons que $g(a,b) = g(x,y)$. Vu que f est une bijection, nous avons $\varphi(a) = \varphi(x)$ et $\sigma(b) = \sigma(y)$. Étant donné que φ et σ sont des bijections, ça donne $a = x$ et $b = y$. Donc $(a,b) = (x,y)$).

(2) **Surjectif** Soit $n \in \mathbb{N}$. Nous posons $(a,b) = f^{-1}(n)$ puis $x = \varphi^{-1}(a)$ et $y = \sigma^{-1}(b)$. Avec ça nous avons

$$n = f(a,b) = f\big(\varphi(x), \sigma(y)\big) = g(a,b). \tag{2.86}$$

Donc n est bien dans l'image de g.

En ce qui concerne le fait que A^n soit dénombrable, nous le faisons par récurrence. Pour $n = 1$, nous savons que $A^n = A$ est dénombrable. Si nous supposons que A^{n-1} est dénombrable, alors nous avons $A^n = A^{n-1} \times A$ qui est dénombrable en tant que produit cartésien de deux ensembles dénombrables. □

NORMooDenombrablesPlusPetitsInfinis

2.48.
Les ensembles dénombrables sont les plus petits ensembles infinis possibles, comme en témoigne la proposition suivante.

PROPooUIPAooCUEFme

Proposition 2.49.
Tout ensemble infini contient une partie en bijection avec $\mathbb{N}$.

Démonstration. Soient un ensemble infini E_0 et une partie propre E_1 en bijection avec E_0. Nous notons $\varphi: E_0 \to E_1$ une bijection.

Soit $x_0 \in E_0 \setminus E_1$ (axiome du choix et tout ça). Nous définissons

$$\begin{aligned} \psi: \mathbb{N} &\to \{\varphi^k(x_0)\} \\ n &\mapsto \varphi^n(x_0) \end{aligned} \tag{2.87}$$

et nous allons prouver que c'est une bijection. Que ce soit surjectif est immédiat. Pour l'injectivité, soit $\varphi^k(x_0) = \varphi^l(x_0)$ avec $k \neq l$. Supposons pour fixer les notations que $k > l$. Alors, vu que φ est inversible nous pouvons écrire

$$x_0 = \varphi^{k-l}(x_0) = \varphi\big(\varphi^{k-l-1}(x_0)\big) \tag{2.88}$$

où il est entendu que $\varphi^0(x_0) = x_0$. Cela signifie que x_0 est dans l'image de φ, c'est-à-dire dans E_1, ce que nous avons exclu par choix de x_0 dans $E_0 \setminus E_1$. Donc en réalité $\varphi^k(x_0) \neq \varphi^l(x_0)$ dès que $k \neq l$. □

PropQEPoozLqOQ

Proposition 2.50.
Toute partie d'un ensemble fini est finie, et toute partie d'un ensemble dénombrable est finie ou dénombrable.

Démonstration. Soient un ensemble E ainsi qu'une partie infinie $A \subset E$. Nous notons $\varphi: A \to A'$ une bijection entre A et une partie propre A' de A. Dans ce cas, l'application

$$\begin{aligned} \phi: E &\to (E \setminus A) \cup A' \\ x &\mapsto \begin{cases} x & \text{si } x \in E \setminus A \\ \varphi(x) & \text{si } x \in A \end{cases} \end{aligned} \tag{2.89}$$

est une bijection entre E et une partie propre de E. Donc E est infini.

Par contraposée nous déduisons que toute partie d'un ensemble fini est finie.

En ce qui concerne les parties d'ensembles dénombrables, soit une partie A d'un ensemble dénombrable E. Nous avons une bijection $t\varphi: E \to \mathbb{N}$. La restriction $\varphi: A \to \varphi(A)$ est une bijection entre A est une partie de $\mathbb{N}$.

- Si $\varphi(E)$ est infinie, elle est dénombrable (proposition 2.35). Dans ce cas A est en bijection avec un ensemble dénombrable. Il est donc dénombrable.
- Si $\varphi(E)$ est fini, alors le lemme 1.80(2) nous dit que A est fini.

□

LEMooGTOTooFbpvzU

Lemme 2.51.
Soit un ensemble E non dénombrable ainsi qu'une application $f: E \to F$ où F est un ensemble quelconque. Si $f(E)$ est dénombrable (ou fini), alors il existe $y \in f(E)$ tel que $f^{-1}(y)$ est indénombrable.

Démonstration. Nous avons

$$E = \bigcup_{y \in F} f^{-1}(y). \tag{2.90}$$

Si tous les $f^{-1}(y)$ sont dénombrables, alors E est une union dénombrable (F est dénombrable) d'ensembles dénombrables. Il serait donc dénombrable (proposition 2.42), ce qui est contraire à l'hypothèse. □

2.4.4 Ajouter ou soustraire des cardinalités

NOOOMooOperationsCardinaux

2.52.
Nous allons prouver une série de résultats que nous pourrions résumer en « ajouter ou retrancher des parties de cardinalité plus petite ne change pas la cardinalité ».

LEMooUFCAooSyZtZj

Lemme 2.53 ([1]).
Si A est infini et B est fini, alors $A \cup B \approx A$.

Démonstration. Nous supposons que A et B sont disjoints[17]. La proposition 2.24 nous permet de considérer une bijection $\psi: \{1, \dots, n\} \to B$.

Puisque A est infini, la proposition 2.49 nous permet de considérer $N \subset A$ et une bijection $\varphi: \mathbb{N} \to N$.

[17] Adaptez la démonstration au cas où l'intersection n'est pas vide.

Maintenant, il s'agit seulement d'insérer B dans A en le mettant « au début » de N et en décalant les autres éléments. La bijection est

$$\begin{aligned} f\colon A\cup B&\to A\\ x&\mapsto\begin{cases} x & \text{si } x\in A\setminus N\\ \varphi\big(\varphi^{-1}(x)+n\big) & \text{si } x\in N\\ \varphi\big(\psi^{-1}(x)\big) & \text{si } x\in B. \end{cases}\end{aligned} \tag{2.91}$$

□

LEMooXMVDooIWLWis

Lemme 2.54.
Si A est infini et si A est surpotent à B, alors $A\approx A\cup B$.

Démonstration. Il existe évidemment une injection $A\to A\cup B$. Donc le théorème de Cantor-Schröder-Bernstein 1.84 nous indique que trouver une injection $A\cup B\to A$ suffira pour la peine.

Nous allons utiliser le lemme de Zorn 1.42 avec l'ensemble

$$\mathcal{A}=\left\{(X,\varphi_X)\text{ tel que }\begin{cases}X\subset B\\ \varphi_X\colon A\cup X\to A\text{ est injective.}\end{cases}\right\} \tag{2.92}$$

muni de l'ordre de l'inclusion : $(X,\varphi_X)<(Y,\varphi_Y)$ si $X\subset Y$ et $\varphi_Y(x)=\varphi_X(x)$ pour tout $x\in A\cup X$.

(1) **$\mathcal{A}$ est inductif** Soit une famille $\mathcal{F}=\{(X_i,\varphi_i)\}_{i\in I}$ complètement ordonnée indexée par l'ensemble I. En posant $X=\bigcup_{i\in I}X_i$ et $\varphi(x)=\varphi_i(x)$ dès que $x\in A\cup X_i$, l'élément (X,φ) majore $\mathcal{F}$.

(2) **Un maximum** Le lemme de Zorn nous assure que $\mathcal{A}$ possède (au moins) un élément maximal. Soit un tel élément maximum (X,φ).

(3) **$X\approx B$** Ah oui, vous auriez aimé avoir $X=B$. Mais non ; il n'y a pas de garantie. Nous allons montrer que $X\approx B$, et ça suffira.

Vu que $X\subset B$, si X n'est pas équipotent à B, il est strictement inclus dans B. Nous pouvons donc considérer

$$b\in B\setminus X \tag{2.93a}$$
$$a\in A\setminus\varphi(X). \tag{2.93b}$$

Nous considérons alors l'élément $(Y,\psi)\in\mathcal{A}$ défini par

$$Y=X\cup\{b\} \tag{2.94a}$$
$$\psi(x)=\begin{cases}a & \text{si } x=b\\ \varphi(x) & \text{sinon .}\end{cases} \tag{2.94b}$$

Cet élément majore (X,φ).

Donc $X\approx B$.

(4) **Résumé de la situation** Nous avons $A\approx A\cup X$ ainsi qu'une injection $\varphi\colon A\cup X\to A$ et une bijection $\psi\colon B\to X$.

(5) **Conclusion si A est disjoint de B** Si A et B sont disjoints, nous avons une bijection

$$\begin{aligned} l\colon A\cup B&\to A\\ x&\mapsto\begin{cases}\varphi(x) & \text{si } x\in A\\ \varphi\big(\psi(x)\big) & \text{si } x\in B.\end{cases}\end{aligned} \tag{2.95}$$

(6) **Conclusion si A n'est pas disjoint de B** Il suffit de poser $C=B\setminus A$ et nous avons

$$A\cup B=[A\cup(A\cap B)]\cup C. \tag{2.96}$$

Cette union est disjointe, $A\cup(A\cap B)$ est surpotent à A et C est subpotent à B. La conclusion est donc encore valable.

□

NORMooBijectionApplicThMesure

2.55.
La proposition suivante sera utilisée en théorie de la mesure, dans l'exemple 16.75.

PropVCSooMzmIX

Proposition 2.56 ([53, 18])**.**
Si S est un ensemble infini alors il existe une bijection $\varphi\colon \{0,1\}\times S\to S$.

Démonstration. Nous posons $A=\{0\}\times S$ et $B=\{1\}\times S$. L'ensemble A est infini et surpotent à B (pas strictement, mais quand même).

Donc A est idempotent à $A\cup B$ par le lemme 2.54. Mais A est idempotent à S, donc

$$S\approx A\approx A\cup B=\{0,1\}\times S. \tag{2.97}$$

□

CORooJCSIooOeOICJ

Corolaire 2.57.
Si A est un ensemble infini, alors A possède deux sous-ensembles disjoints A_1 et A_2 qui sont tous deux en bijection avec A.

Démonstration. La proposition 2.56 donne une bijection $\varphi\colon\{0,1\}\times A\to A$. Il suffit de poser $A_1=\varphi(0,A)$ et $A_2=\varphi(1,A)$. □

NORMooInfiniteCopies

2.58.
Maintenant que nous pouvons mettre dans A deux copies disjointes de A, il n'est pas très étonnant que nous puissions en mettre une infinité dénombrable. Nous verrons ça dans 2.59.

PROPooFKBEooKXqujV

Proposition 2.59.
Si A est infini, alors $A\times\mathbb{N}\approx A$.

Démonstration. La démonstration se base sur le fait qu'à l'intérieur de A, nous pouvons construire autant de copies de A deux à deux disjointes que nous le voulons. La k^{e} « copie » sera naturellement l'image de $k\times A$.

Voyons tout cela en détail.

(1) **Ce que nous allons faire** Nous allons construire, pour tout $i\geqslant 1$ des parties $A_i,B_i\subset A$ telles que

- $A_i\cap B_i=\varnothing$,
- $A_i,B_i\subset B_{i-1}$,
- $A_i\approx B_i\approx A$,
- $A_i\cap A_j=\varnothing$ si $i\neq j$

(2) **La construction** Nous commençons à zéro en utilisant le corolaire 2.57 pour construire des parties disjointes A_0 et B_0 de A telles que $A_0\approx B_0\approx A$.

Ensuite, puisque $B_0\approx A$, il existe A_1 et B_1 dans B_0 tels que $A_1\cap B_1=\varnothing$ et $A_1\approx B_1\approx B_0\approx A$. Cela est notre construction pour $i=1$.

Pour la récurrence, puisque $A_i\approx B_i\approx A$, nous considérons A_{i+1} et B_{i+1} dans B_i tels que $A_{i+1}\cap B_{i+1}=\varnothing$ et $A_{i+1}\approx B_{i+1}\approx B_i\approx A$. C'est encore le corolaire 2.57 qui fait le travail.

(3) **Les propriétés** Nous avons $A_i\cap A_{i+1}=\varnothing$ parce que $A_i\cap A_{i+1}\subset A_i\cap B_i=\varnothing$.

Nous devons encore montrer que $A_i\cap A_j=\varnothing$ dès que $i\neq j$. Supposons que $j>i$. Nous avons les inclusions

$$A_j\subset B_{j-1}\subset B_{j-2}\subset\ldots\subset B_i. \tag{2.98}$$

Donc $A_j\cap A_i\subset B_i\cap A_i=\varnothing$.

(4) **Une injection** Nous pouvons à présent écrire une injection qui termine presque la preuve. Pour cela nous considérons pour tout i, une bijection $\psi_i\colon A\to A_i$. Ensuite nous posons

$$\begin{aligned}\varphi\colon A\times\mathbb{N}&\to A\\ (a,k)&\mapsto\psi_k(a).\end{aligned} \tag{2.99}$$

Si $\varphi(a,k)=\varphi(b,l)$, alors $\psi_k(a)=\psi_l(b)$. L'élément $\psi_k(a)$ est donc dans $A_k\cap A_l$; ce n'est possible que si $k=l$. Donc $\psi_l(a)=\psi_l(b)$. Cette dernière égalité n'est possible que si $a=b$ parce que ψ_l est une bijection.

Donc φ est une injection, et nous avons prouvé que $A\times\mathbb{N}\preceq A$.

(5) **La bijection** Nous venons de prouver que $A \times \mathbb{N} \preceq A$. La surpotence $A \times \mathbb{N} \succeq A$ étant évidente, le théorème de Cantor-Schröder-Bernstein 1.84 conclut que $A \times \mathbb{N} \approx A$.

□

LEMooDHWSooFqhano

Lemme 2.60 ([1]).
Soit un ensemble A muni de deux sous-ensembles B et B' équipotents et disjoints. Alors $A \setminus B$ est équipotent à $A \setminus B'$.

Démonstration. Soit une bijection $\psi\colon B' \to B$. L'application

$$\begin{aligned} \varphi\colon A \setminus B &\to A \setminus B' \\ x &\mapsto \begin{cases} x & \text{si } x \notin B' \\ \psi(x) & \text{si } x \in B'. \end{cases} \end{aligned} \tag{2.100}$$

est la bijection cherchée. □

LEMooIVCBooHWQiZB

Lemme 2.61 ([54]).
Si A est un ensemble infini et si $B \prec A$, alors $A \approx A \setminus B$.

Démonstration. Nous pouvons écrire

$$A = (A \setminus B) \cup B. \tag{2.101}$$

Le théorème de comparabilité cardinale 1.86 nous indique que soit $A \setminus B \preceq B$, soit $A \setminus B \succeq B$. Nous allons étudier les deux cas.

(1) **Si $A \setminus B \succeq B$** Dans ce cas, $(A \setminus B) \cup B \approx A \setminus B$ par le lemme 2.54. Alors, notre résultat est prouvé parce que $A = (A \setminus B) \cup B \approx A \setminus B$.

(2) **Si $A \setminus B \preceq B$** Dans ce cas, le lemme 2.54 nous indique que $A = (A \setminus B) \cup B \approx B$. Mais $A \approx B$ est exclu par l'hypothèse. Ce cas est donc impossible.

□

LEMooMRVQooUZSSyL

Lemme 2.62 ([1]).
Si A est infini et si B est une partie strictement subpotente de A, alors il existe $U \subset A$ disjoint de B et équipotent à B.

Démonstration. Le lemme 2.61 nous donne une bijection $\varphi\colon A \to A \setminus B$. Il suffit alors de poser $U = \varphi(B)$. Cette partie est disjointe de B parce que φ prend ses valeurs dans $A \setminus B$. □

Lemme 2.63 ([55]).
Soit un ensemble infini A ainsi qu'un sous-ensemble $B \subset A$. Nous supposons l'existence d'une fonction surjective $f\colon B \to B \times B$.
Alors $B \preceq B \times B \preceq B \preceq A$.

Démonstration. La première est l'hypothèse sur f. La seconde est l'existence (évidente) d'une surjection $B \times B \to B$. La troisième est le fait que B soit inclus dans A. □

LEMooPOEFooXaifhT

Lemme 2.64 ([55]).
Soit un ensemble infini A ainsi qu'un sous-ensemble strictement subpotent $B \subset A$. Nous supposons l'existence d'une fonction surjective $f\colon B \to B \times B$.
Alors f peut être étendue en une injection $f\colon D \to D \times D$ où $D \subset A$ contient strictement B.

Démonstration. Par le lemme 2.62, nous considérons une partie $U \subset A$ disjointe de B et équipotente à B. Nous pouvons écrire le développement

$$(B \cup U) \times (B \cup U) = (B \times B) \cup (B \times U) \cup (U \times B) \cup (U \times U). \tag{2.102}$$

Nous savons que B est surpotent à U (il est même équipotent) ; donc le lemme 2.54 nous dit que $B \cup U \approx B$. De plus il existe une bijection $B \to U$, donc

$$U \approx B \approx B \times B \approx B \times U \approx U \times B \approx U \times U. \tag{2.103}$$

Chacun des ensembles $U \times B$, $B \times U$ et $U \times U$ est équipotent à U. Leur union est donc équipotente[18] à U et nous avons une bijection

$$\varphi\colon U \to U \times B \cup (B \times U) \cup (U \times U). \tag{2.104}$$

[18] Lemme 2.54.

Et enfin nous définissons

$$\begin{aligned} g\colon B\cup U &\to (B\times U)\times(B\cup U)\\ x &\mapsto \begin{cases} f(x) & \text{si } x\in B\\ \varphi(x) & \text{si } x\in U. \end{cases} \end{aligned} \tag{2.105}$$

Cette définition est bonne parce que U et B sont disjoints, et g est injective. □

NORMooBijectionAA

2.65.
Le théorème suivant est une généralisation de la proposition 2.56. Elle implique, entre autres choses, qu'il existe une bijection entre $\mathbb{R}$ et $\mathbb{R}\times\mathbb{R}$. Pour le cas de $\mathbb{N}\times\mathbb{N}\approx\mathbb{N}$, il y a la proposition 2.38 qui donne une bijection explicite et donc sans axiome du choix et sans lemme de Zorn.

THOooDGOVooRdURVi

Théorème 2.66.
Si A est infini, alors $A\approx A\times A$.

Démonstration. Une fois de plus, ce sera le lemme de Zorn qui va s'y coller. Soit l'ensemble

$$\mathcal{A}=\left\{(X,\varphi)\text{ tel que }\begin{cases} X\subset A\\ \varphi\colon X\to X\times X\text{ est surjective.}\end{cases}\right\} \tag{2.106}$$

Cet ensemble est non vide parce que A est infini ; il contient donc une partie dénombrable N, et nous connaissons la surjection $\mathbb{N}\to\mathbb{N}\times\mathbb{N}$ du lemme 2.38.

Nous ordonnons $\mathcal{A}$ par l'inclusion : $(X,\varphi)\leqslant(Y,\phi)$ lorsque $X\subset Y$ et $\phi|_X=\varphi$. La tambouille usuelle montre que $\mathcal{A}$ est un ensemble inductif et le lemme de Zorn 1.42 donne l'existence d'un élément maximal que nous notons (B,φ).

Puisque B est subpotent à A (parce qu'il est inclus), soit il est strictement subpotent, soit il est équipotent. Nous commençons par montrer que B ne peut pas être strictement subpotent à A.

En effet, si nous avions une surjection $B\to B\times B$, alors que B est strictement subpotent à A. Le lemme 2.64 nous dit alors que φ peut être étendue, ce qui contredirait la maximalité de (B,φ).

Donc la partie B est équipotente à A : il existe une bijection $g\colon A\to B$. Mais nous avons une surjection $B\to B\times B$ et donc aussi une injection $B\times B\to B$. Vu que nous avons par ailleurs une injection $B\to B\times B$, le théorème de Cantor-Schröder-Bernstein 1.84 nous donne une bijection $\phi\colon B\times B\to B$. Avec ça, l'application

$$\begin{aligned} f\colon A\times A&\to A\\ (a,b)&\mapsto\phi\big(g(a),g(b)\big)\end{aligned} \tag{2.107}$$

est une bijection. Donc les ensembles A et $A\times A$ sont équipotents. □

LEMooNKKDooUvSYPO

Lemme 2.67.
Si A est infini, et si pour tout $i\in\mathbb{N}$ nous avons $A_i\approx A$, alors

$$\bigcup_{i\in\mathbb{N}}A_i\approx A. \tag{2.108}$$

Démonstration. Pour chaque $i\in\mathbb{N}$ nous avons une bijection $\varphi_i\colon A_i\to A$. Nous posons

$$\begin{aligned}\varphi\colon A\times\mathbb{N}&\to\bigcup_{i=0}^{\infty}A_i\\ (a,i)&\mapsto\varphi_i(a).\end{aligned} \tag{2.109}$$

EQooCHJAooRpHypV

Cette application est surjective mais peut-être pas injective parce que les A_i peuvent avoir des intersections non vides. Nous avons alors le calcul

$$\begin{aligned} A&\approx A\times\mathbb{N} && \text{(2.110a)}\\ &\succeq\bigcup_{i=0}^{\infty}A_i && \text{(2.110b)}\\ &\succeq A && \text{(2.110c)}\end{aligned}$$

SUBEQooICFEooTLuFHZ
SUBEQooRVPBooJJevkv
SUBEQooFJRGooJnervy

Justifications :

- Pour (2.110a), c'est la proposition 2.59.
- Pour (2.110b), c'est la surjection (2.109).
- Pour (2.110c), c'est le fait que seulement A_0 possède déjà une surjection vers A.

Donc $\bigcup_i A_i$ est à la fois surpotent et subpotent à A. Il est donc équipotent par le théorème 1.84. □

2.5 Indice d'un sous-groupe et ordre des éléments

2.5.1 Ordre d'un élément

DEFooKSTVooOObpgC

Définition 2.68 (Ordre d'un élément)**.**
*L'**ordre** d'un élément g de G est le naturel*[19]

$$\min\{n \in \mathbb{N} \setminus \{0\} \text{ tel que } g^n = e\}, \tag{2.111}$$

si il existe ; dans le cas contraire, nous disons que l'ordre de g est infini.

2.69.
Nous verrons que le corolaire 2.74 au théorème de Lagrange dira que l'ordre d'un élément divise l'ordre du groupe.

LEMooFNVRooRCkjLc

Lemme 2.70.
Lorsque H est normal dans G, alors la définition

EQooEUESooScUWHK

$$[a] \cdot [b] = [ab] \tag{2.112}$$

définit une loi de groupe sur l'ensemble G/H.

Démonstration. Le neutre est $[e]$ et l'associativité ne pose pas plus de problème que l'existence d'un inverse. Le point à vérifier est que la formule (2.112) est une bonne définition : $[ah] \cdot [bh'] = [ab]$ pour tout $h, h' \in H$. Nous avons :

$$[ah] \cdot [bh'] = [ahbh'] = [ahb]. \tag{2.113}$$

Pour montrer que c'est $[ab]$, l'astuce est d'introduire bb^{-1} à côté du a :

$$[ahb] = [abb^{-1}hb] = [ab] \tag{2.114}$$

parce que $b^{-1}hb \in H$ du fait que H soit normal dans G. □

EXooFNIKooHxePSs

Exemple 2.71 ([56])**.**
Il ne faudrait pas croire que le groupe quotient G/H est forcément un sous-groupe de G. Par exemple le quotient $\mathbb{Z}/2\mathbb{Z}$ est l'ensemble $\{0, 1\}$ muni de l'addition. En particulier $1+1 = 0$, ce qui est évidemment faux dans $\mathbb{Z}$. Le groupe $(\mathbb{Z}, +)$ ne possède aucun élément d'ordre[20] 2.

Il n'en est pas moins vrai que l'application

$$\begin{aligned} f\colon G &\to G/H \\ g &\mapsto [g] \end{aligned} \tag{2.115}$$

est un morphisme de groupes. △

DEFooMPIAooIeZNaR

Définition 2.72.
*Si H est un sous-groupe d'un groupe fini, l'**indice** de H dans G est le nombre $|G|/|H|$, souvent noté $|G : H|$.*

Le théorème de Lagrange dira en particulier que l'indice est toujours un nombre entier. C'est à ne pas confondre avec le degré d'une extension de corps (définition 8.61).

ThoLagrange

Théorème 2.73 (Théorème de Lagrange)**.**
Soit H un sous-groupe du groupe fini G. Alors

ITEMooDPKSooNpOusd

(1) L'ordre de H divise l'ordre de G.

(2) Les trois nombres suivants sont égaux :

- *le nombre de classes de H à gauche,*
- *le nombre de classes de H à droite,*
- *l'indice de H dans G.*

En particulier si H est distingué dans G, nous avons

$$|G/H| = \frac{|G|}{|H|}. \tag{2.116}$$

[19] Le minium d'une partie non vide de $\mathbb{N}$ est le lemme 2.32.
[20] ordre d'un élément, définition 2.68.

Démonstration. Nous commençons par montrer que les classes de H ont toutes le même nombre d'éléments que H. En effet pour chaque $g \in G$ nous avons la bijection

$$\begin{aligned} \varphi\colon H &\to gH \\ h &\mapsto gh. \end{aligned} \tag{2.117}$$

L'injectivité de φ est le fait que $gh = gh'$ implique $h = h'$. La surjectivité est par définition de la classe.

Les classes à gauche formant une partition de G, le cardinal de G est le produit de la taille des classes par le nombre de classes :

$$|G| = |H| \cdot \text{ nombre de classes.} \tag{2.118}$$

En particulier nous voyons que $|H|$ divise $|G|$.

La dernière formule exprime simplement que G/H est par définition le nombre de classes de H à gauche (ou à droite) dans G. □

CorpZItFX

Corolaire 2.74.
L'ordre d'un élément[21] *d'un groupe fini divise l'ordre du groupe. En particulier dans un groupe d'ordre n tous les éléments vérifient $g^n = e$.*

Démonstration. Soit G un groupe fini et considérons, à $g \in G$ fixé, le sous-groupe

$$H = \{g^k \text{ tel que } k \in \mathbb{N}\}. \tag{2.119}$$

Par le théorème de Lagrange 2.73, l'ordre de H divise $|G|$, mais l'ordre de H est le plus petit k tel que $g^k = e$, c'est-à-dire l'ordre de g. □

D'autres résultats à propos d'ordres et d'indices de groupes finis dans la proposition 3.168 et le lemme 3.170. En particulier le théorème de Cauchy 3.164 qui dit : si le groupe est cyclique et si p divise l'ordre du groupe G, alors G contient au moins un élément d'ordre p.

2.6 Groupe simple

DefGroupeSimple

Définition 2.75 (Groupe simple)**.**
*Un groupe est dit **simple** si il est non trivial et si les seuls sous-groupes normaux qu'il admet sont lui-même et le sous-groupe réduit à l'élément neutre.*

DEFooXUVOooRyJnbx

Définition 2.76 ([49])**.**
*Un sous-groupe normal N de G est **normal maximal** si il est différent de G et si il est maximal pour l'inclusion parmi tous les sous-groupes normaux contenant N.*

PROPooUWLHooVUxTHB

Proposition 2.77 ([49])**.**
Soient un groupe G et un sous-groupe normal N de G. Alors N est normal maximal[22] *de G si et seulement si G/N est simple.*

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que N est normal maximal dans G, et nous devons prouver que G/N est simple. Soit L normal dans G/N ; nous considérons l'application

$$\begin{aligned} f\colon \mathrm{Sub}(G,N) &\to \mathrm{Sub}(G/N) \\ K &\mapsto \rho(K) \end{aligned} \tag{2.120}$$

du théorème de correspondance 2.17, et nous posons $L' = f^{-1}(L) \in \mathrm{Sub}(G,N)$. Nous savons que L' sera normal dans G si et seulement si $f(L')$ est normal dans $f(G) = G/N$. Par hypothèse $f(L') = L$ est normal dans G/N, donc L' est normal dans G. Mais $L' \in \mathrm{Sub}(G,N)$ et N est maximal. Il y a deux possibilités : $L' = N$ ou $L' = G$.

Si $L' = N$, alors

$$L = f(L') = f(N) = \{[e]_N\}, \tag{2.121}$$

et donc L est trivial.

Si $L' = G$ alors $L = f(L') = f(G) = G/N$ et L est encore trivial.

[21] Ordre d'un élément, définition 2.68.
[22] Définition 2.76.

(2) $\Leftarrow$ Dans l'autre sens,nous supposons que G/N est simple, et nous prouvons que N est maximalement normal dans G. Nous prenons donc K : un sous-groupe normal de G contenant N, et nous montrons que soit $K = N$ soit $K = G$.

Vu que K est normal dans G, la partie $f(K)$ est normale dans $f(G) = G/N$ (théorème de correspondance encore). Étant donné que G/N est simple, nous en déduisons que $f(K)$ est soit $\{[e]_N\}$ soit G/N au complet.

Si $f(K) = \{[e]_N\}$ alors $K = N$. Pour l'autre possibilité, nous supposons que $f(K) = G/N$. Soit $g \in g$. Vu que $[g]_N \in G/N = f(K)$, il existe $k \in K$ tel que $[g]_N = \rho(k) = [k]_N$. Donc $g = kn$ pour un certain $n \in N$ mais comme $N \subset K$, nous avons $nk \in K$ de telle sorte que $g \in K$. Nous en déduisons que $G = K$.

□

2.7 Symbole de sommation

2.7.1 Sommation

PROPooDUSJooWNyqWm

Proposition-Définition 2.78 ([1, 3]).
Soit un groupe commutatif $(G, +)$. Soient un ensemble fini I et une application $f\colon I \to G$. Il existe une unique application

$$s\colon \mathcal{P}(I) \to G \tag{2.122}$$

telle que

(1) $s(\varnothing) = 0$,

(2) pour toute partie $K \subset I$ et pour tout $x \notin K$,

$$s(K \cup \{x\}) = s(K) + f(x). \tag{2.123}$$

Lorsque J est une partie de I, nous notons

$$\sum_{j \in J} f(j) = s(J). \tag{2.124}$$

EQooDVYXooEoNUiF

Démonstration. En deux parties.

(1) **Unicité** Soient $s, t\colon \mathcal{P}(I) \to G$ vérifiant les propriétés. Nous posons

$$\mathcal{A} = \{J \subset I \text{ tel que } s(J) \neq t(J)\}. \tag{2.125}$$

Vu que $\mathcal{A}$ est une partie de $\mathcal{P}(I)$ qui est fini[23], l'ensemble $\mathcal{A}$ est fini. Muni de l'inclusion, $\mathcal{A}$ est un ensemble partiellement ordonné par le lemme 1.27.

Vu que $s(\varnothing) = t(\varnothing) = 0$, nous savons que $\varnothing \notin \mathcal{A}$. Si $\mathcal{A} = \varnothing$, alors $s = t$ et c'est bon. Sinon, nous considérons un élément minimal[24] $J \in \mathcal{A}$.

Soit $a \in J$. Étant donné que J est minimal, l'ensemble $K = J \backslash \{a\}$ n'est pas dans $\mathcal{A}$. Donc $s(K) = s(J)$. Mais

$$s(J) = s(K \cap \{a\}) = s(K) + f(a) = t(K) + f(a) = t(K \cap \{a\}) = t(J). \tag{2.126}$$

Bref, $s(J) = t(J)$, contredisant le fait que $J \in \mathcal{A}$. Donc $\mathcal{A} = \varnothing$, et $s = t$.

(2) **Existence** Nous y allons par récurrence sur le cardinal de I. Nous supposons que pour tout triple (I, f, G) où I est un ensemble avec $\text{Card}(I) \leqslant n$, G est un groupe commutatif et $f\colon I \to G$ est une application, il existe une application $s\colon \mathcal{P}(I) \to G$ vérifiant les conditions.

Soit maintenant (I, f, G) avec $\text{Card}(I) = n + 1$. Soit $a \in I$, et posons $J = I \setminus \{a\}$. Le triple (J, g, G) où g est la restriction de f à J vérifie les hypothèses de récurrence, et il existe donc une application $s\colon \mathcal{P}(J) \to G$ vérifiant

(2a) $t(\varnothing) = 0$

(2b) $t\big(K \cup \{x\}\big) = t(K) + g(x)$ pour tout $x \in J = I \setminus \{a\}$.

[23] Par le lemme 1.184.
[24] Par la proposition 1.185.

Nous définissons ensuite l'application

$$s\colon \mathcal{P}(I) \to G$$
$$S \mapsto \begin{cases} t(S) & \text{si } a \notin S \\ t(S \setminus \{a\}) + f(a) & \text{si } a \in S. \end{cases} \tag{2.127}$$

Nous vérifions que ce s vérifie les condition. D'abord $s(\varnothing) = t(\varnothing) = 0$ parce que $a \notin \varnothing$. Ensuite nous considérons $K \subset I$ et $x \in I \setminus K$. Que vaut $s(K \cup \{x\})$? Il y a 4 possibilités selon que $a \in K$ ou $x = a$.

(2a) **Si $a \in K$ et $x = a$** Pas possible parce que $x \notin K$.

(2b) **Si $a \in K$ et $x \neq a$** Nous avons

$$\begin{aligned} s(K \cup \{x\}) &= t\big(K \cup \{x\} \setminus \{a\}\big) + f(a) && \text{(2.128a)} \\ &= t(K \setminus \{a\}) + f(x) + f(a) && \text{(2.128b)} \\ &= s(K \cup \{a\}) + f(x) && \text{(2.128c)} \\ &= s(K) + f(x). && \text{(2.128d)} \end{aligned}$$

(2c) **Si $a \notin K$ et $x = a$** Alors nous avons

$$\begin{aligned} s(K \cup \{x\}) &= s(K \cup \{a\}) && \text{(2.129a)} \\ &= t(K) + f(a) && \text{(2.129b)} \\ &= s(K) + f(x) && \text{(2.129c)} \end{aligned}$$

parce que $s(K) = t(K)$ et $f(a) = f(x)$.

(2d) **Si $a \notin K$ et $x \neq a$** Alors nous avons

$$\begin{aligned} s(K \cup \{x\}) &= t(K \cup \{x\}) && \text{(2.130a)} \\ &= t(K) + f(x) && \text{(2.130b)} \\ &= s(K) + f(x). && \text{(2.130c)} \end{aligned}$$

□

DEFooNEVNooJlmJOC

Proposition-Définition 2.79.
Soit A un ensemble muni d'une loi de composition interne[25] *notée $+$. Si nous avons une application $f\colon \mathbb{N} \to A$, alors il existe une unique application $t\colon \mathbb{N} \to A$ telle que* SUBEQSooKJOFooOOxDKH

$$\begin{cases} t(0) = f(0) & \text{SUBEQooCCBKooQTbwrQ} \quad \text{(2.131a)} \\ t(k) = t(k-1) + f(k). & \text{(2.131b)} \end{cases}$$

Cette fonction vérifie

$$t(k) = \sum_{i\{0,\dots,k\}} f(i) \tag{2.132}$$ EQooADXEooVshdnf

où la somme est celle de (2.124).

La valeur de $t(k)$ est notée $\sum_{i=0}^{k} \alpha(i)$.

Démonstration. Existence et unicité sont une application du théorème 1.131. En ce qui concerne l'égalité (2.132), il suffit de montrer qu'en posant $q(k) = s\big(\{0,\dots,k\}\big)$, la fonction q vérifie bien les conditions (2.131).

D'abord $q(0) = s(\{0\}) = s(\varnothing) + f(0) = f(0)$. Bien. Ensuite

$$\begin{aligned} q(k) &= s\big(\{0,\dots,k\}\big) && \text{(2.133a)} \\ &= s(\{0,\dots,k-1\} \cup \{k\}) && \text{(2.133b)} \\ &= s(\{0,\dots,k-1\}) + f(k) && \text{(2.133c)} \\ &= q(k-1) + f(k). && \text{(2.133d)} \end{aligned}$$

Bien aussi.

Par unicité, nous en déduisons que $q = t$. □

[25] Peut-être un anneau, mais comme nous avons l'intention, dans les propositions 2.82 et suivantes, de faire des sommes vers $(\mathbb{N}, +)$, plutôt un monoïde.

NORooNotationSommeNaturels

2.80.
Les équations de définition (2.131) signifient que nous définissons la notation $\sum_{i=0}^{N}\alpha(i)$ par récurrence par les conditions suivantes :

ITEMooIPDTooEhOxea

(1) $\sum_{i=0}^{0}\alpha(i)=\alpha(0)$,

ITEMooSommeNaturelsSucc

(2) $\sum_{i=0}^{k}\alpha(i)=\sum_{i=0}^{k-1}\alpha(i)+\alpha(k)$.

LEMooVFNOooZenJSl

Lemme 2.81 ([1])**.**
Si A est un ensemble fini, alors

$$\sum_{i\in I}1=\operatorname{Card}(I). \tag{2.134}$$

Démonstration. Si $\varphi\colon\{1,\dots,n\}\to I$ est une bijection, la somme à calculer est

$$\sum_{i=1}^{n}a_{\varphi(i)} \tag{2.135}$$

où $a_i=1$ pour tout i. Cette somme est définie par 2.79 (voir 2.80). Si $\operatorname{Card}(I)=1$, alors la somme est $\sum_{k=1}^{1}1=1$ par (2.131a).

Si la proposition est vraie pour tout ensemble de cardinal n, alors nous considérons un ensemble I de cardinal $n+1$, et nous devons calculer $\sum_{k=1}^{n+1}1=\sum_{k=1}^{n}1+1=n+1$. □

PROPooXXGHooLafGsI

Proposition 2.82 (La multiplication est une somme itérée[39])**.**
Pour tout $a,b\in\mathbb{N}$, nous avons

$$\sum_{i=1}^{n}a=a\times n. \tag{2.136}$$

Démonstration. Nous le faisons par récurrence en partant de $n=1$. Avec $n=1$ nous avons $\sum_{i=1}^{1}a=a$, et $a\times 1=a$. Donc c'est bon.

Pour la récurrence nous avons :

$$a\times s(n)=a\times n+a=\sum_{i=1}^{n}a+a=\sum_{i=1}^{n+1}a=\sum_{i=1}^{s(n)}a. \tag{2.137}$$

□

LEMooIETGooMyrilW

Lemme 2.83.
Soit $a>1$ dans $\mathbb{N}$. Pour tout $n\geqslant 1$ nous avons $na\leqslant a^n$.

Démonstration. Par récurrence. Avec $n=1$ nous avons bien $a\leqslant a$; pas de problème. Supposons que $na\leqslant a^n$, et montrons le pas de récurrence. Nous avons :

$$\begin{aligned}
(n+1)a&=na+a && && (2.138a)\\
&\leqslant na+na && \text{parce que } a\leqslant na && (2.138b)\\
&=2na && && (2.138c)\\
&\leqslant 2a^n && \text{récurrence} && (2.138d)\\
&\leqslant aa^n && \text{parce que } a\geqslant 2 && (2.138e)\\
&=a^{n+1}. && && (2.138f)
\end{aligned}$$

□

PROPooSuiteGeometriqueCroissante

Proposition 2.84 ([39])**.**
Soit $a>1$. Alors

(1) l'application $n\mapsto a^n$ est strictement croissante ;

(2) l'ensemble $\{a^n$ tel que $n\in\mathbb{N}\}$ n'est pas majoré.

Démonstration. Nous avons

$$a^{n+1} = a^n \times a \tag{2.139a}$$
$$> a^n \times 1 \qquad \text{lemme 1.170} \tag{2.139b}$$
$$= a^n. \tag{2.139c}$$

Cela prouve le premier point.

Pour le second point, soit $m \in \mathbb{N}$. Nous devons trouver $N \in \mathbb{N}$ tel que $a^N \geqslant m$. Puisque $\mathbb{N}$ est archimédien[26], nous pouvons considérer N tel que $Na > m$. Le lemme 1.140 nous assure alors que

$$m < Na \leqslant a^N. \tag{2.140}$$

□

2.7.2 Écriture d'un naturel dans une base

SOBooEcritureChiffres

2.85.
Nous avons déjà donné la notation $1 = s(0)$. Nous continuons avec $2 = s(1)$, $3 = s(2)$, $4 = s(3)$, $5 = s(4)$, $6 = s(5)$, $7 = s(6)$, $8 = s(7)$ et $9 = s(8)$.

Nous allons maintenant voir comment écrire des nombres plus grands.

NORooTuplesChiffres

2.86.
Si $b > 1$ et $N \in \mathbb{N}$ sont donnés, nous notons

$$C_{b,N} = \big\{u \in \{0, \dots, b-1\}^{N+1} \text{ tel que } u_N \neq 0\big\}. \tag{2.141}$$

où les u_i sont numérotés à partir de 0 ; donc dire $u_N \neq 0$ revient à dire que le *dernier* est non nul, et non l'avant dernier. Nous définissons[27]

$$\varphi_{b,N} : C_{b,N} \to \mathbb{N}$$
$$u \mapsto \sum_{i=0}^{N} u_i b^i. \tag{2.142}$$

EQooWWTUooHAnSEv

Cette application $\varphi_{b,N}$ sera encore bien étudiée pour la partie décimale d'un réel. Voir la définition 12.541.

LEMooJUGKooGsbrhi

Lemme 2.87 ([39]).
Soient $b > 1$, $N \geqslant 0$ ainsi que $u \in C_{b,N}$. Alors

$$b^N \leqslant \varphi_{b,N}(u) < b^{N+1}. \tag{2.143}$$

EQooYHTLooNvqIIq

Démonstration. En séparant la somme nous avons

$$\varphi_{b,N}(u) = u_N b^N + \sum_{i=0}^{N-1} u_i b^i. \tag{2.144}$$

Puisque $u_N \geqslant 1$ nous avons $b^N \leqslant u_N b^N$, et donc

$$b^N \leqslant u_N b^N \leqslant \varphi_{b,N}(u). \tag{2.145}$$

Voilà qui prouve la première inégalité de (2.143).

Pour prouver que $\varphi_{b,N}(u) < b^{N+1}$, nous faisons une récurrence sur N.

(1) **Pour $N = 0$** Nous devons prouver que $\varphi_{b,0}(u) < b$. Par définition $\varphi_{b,N}(u) = u_0 b^0$. Puisque $u \in \{0, \dots, b-1\}^{N+1}$, nous avons $u_0 \leqslant b - 1 < b$.

(2) **Récurrence** Nous supposons que pour tout $u \in C_{b,N}$ nous avons $\varphi_{b,N}(u) < b^{N+1}$. Et nous devons montrer que pour tout $v \in C_{b,N+1}$ nous avons $\varphi_{b,N+1}(v) < b^{N+2}$.

[26] Proposition 1.174.
[27] Le symbole de sommation est défini par 2.79.

Nous posons $u = (v_0, \dots, v_N)$; nous avons alors

$$\begin{aligned}
\varphi_{b,N+1}(v) &= v_{N+1}b^{N+1} + \sum_{i=0}^{N} v_i b^i && && (2.146a)\\
&= v_{N+1}b^{N+1} + \varphi_{b,N}(u) && && (2.146b)\\
&< v_{N+1}b^{N+1} + b^{N+1} && \text{récurrence} && (2.146c)\\
&= (v_{N+1}+1)b^{N+1} && && (2.146d)\\
&\leqslant bb^{N+1} && \text{parce que } v_{N+1} \leqslant b-1 && (2.146e)\\
&= b^{N+2}. && && (2.146f)
\end{aligned}$$

□

LEMooKDKJooSkhcJS

Lemme 2.88 ([1]).
Soient $x \in \mathbb{N}$ ainsi que $b \geqslant 2$. Nous posons

$$N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}. \tag{2.147}$$

Alors

(1) *Si $n > N$ alors $\varphi_{b,n}(u) > x$ pour tout $u \in C_{b,n}$.*

(2) *Si $n < N$ alors $\varphi_{b,n}(u) < x$ pour tout $u \in C_{b,n}$.*

Démonstration. En deux parties.

(1) **Si $n > N$** Nous avons, par définition de $C_{b,n}$ que $u_n \neq 0$, de telle sorte que

$$\varphi_{b,n}(u) \geqslant u_n b^n \geqslant b^n > x. \tag{2.148}$$

La dernière inégalité est due au fait que $n \notin \{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}$.

(2) **Si $n < N$** Nous avons

$$x \geqslant b^N > \varphi_{b,n}(u). \tag{2.149}$$

Le seconde inégalité est une conséquence du lemme 2.87.

□

THMooUniciteEcritureChiffres

Théorème 2.89 ([39]).
Soit $b \geqslant 2$. Si $x \in \mathbb{N}$, alors il existe un unique $N \in \mathbb{N}$ et un unique $u \in C_{b,N}$ tels que

$$x = \varphi_{b,N}(u). \tag{2.150}$$

Démonstration. Nous commençons par $x < b$. Dans ce cas, $N = 0$ parce que si $u_k \neq 0$ avec $k \neq 0$, nous avons

$$\sum_{i=0}^{N} u_i b^i \geqslant u_k b^k \geqslant b > x. \tag{2.151}$$

Donc $x = x_0 b^0 = u_0$. Bref, dans le cas $x < b$ nous avons obligatoirement $N = 0$ et $u_0 = x$.

Nous étudions à présent le cas $x \geqslant b$ que nous subdivisons en plusieurs étapes.

(1) $N \geqslant 1$ Si $N = 0$, alors $\varphi_{b,0}(u) = u_0 < b \leqslant x$. Donc $N \geqslant 1$.

Notons incidemment que nous pouvons parler de $N - 1$ à partir de maintenant.

(2) **Unicité, préambule** Le lemme 2.88 nous indique que si $x = \varphi_{b,N}(u)$ pour un certain $N \in \mathbb{N}$ et un certain $u \in C_{b,N}$, alors

$$N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}. \tag{2.152}$$

Nous posons

$$X_k = \sum_{i=k}^{N} u_i b^{i-k}, \tag{2.153}$$

et nous allons montrer que le couple (X_{k+1}, u_k) est le résultat de la division euclidienne[28] de X_k par b.

[28] Théorème 1.181.

D'abord, $u_k < b$, donc ça a bien la tête d'un reste. Ensuite, pour le quotient,

$$bX_{k+1} + u_k = b \sum_{i=k+1}^{N} u_i b^{i-(k+1)} + u_k \tag{2.154a}$$
$$= \sum_{i=k+1}^{N} u_i b^{i-k} + u_k \tag{2.154b}$$
$$= \sum_{i=k}^{N} u_i b^{i-k} \tag{2.154c}$$
$$= X_k. \tag{2.154d}$$

(3) **Unicité** En quoi cela fait-il avancer la choucroute ? Supposons que $\varphi_{b,N}(u) = \varphi_{b,M}(v)$. Alors nous avons déjà prouvé que

$$M = N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}. \tag{2.155}$$

Ensuite nous devons montrer que $u = v$. Nous posons $X_k = \sum_{i=k}^{N} u_i b^{i-k}$ et $Y_k = \sum_{i=k}^{N} v_i b^{i-k}$. Notez que

$$X_0 = Y_0 = x. \tag{2.156}$$

Si $X_k = Y_k$, alors par unicité de la division euclidienne nous avons $X_{k+1} = Y_{k+1}$ et $u_k = v_k$. Par récurrence nous avons $X_k = Y_k$ et $u_k = v_k$ pour tout k.

(4) **Existence** Soit $x \in \mathbb{N}$. Nous posons $y_0 = x$ et

$$y_k = by_{k+1} + u_k \tag{2.157}$$

avec $u_k < b$. Vus l'unicité dans la division euclidienne et le théorème[29] 1.131 permettant la définition par récurrence, ces conditions définissent deux suites (u_k) et (y_k) dans $\mathbb{N}$.

Montrons qu'il existe un $N \in \mathbb{N}$ tel que $y_n = 0$ pour tout $n \geqslant N + 1$. Nous avons :

$$2y_{k+1} \leqslant by_{k+1} \qquad \text{parce que } b \geqslant 2 \tag{2.158a}$$
$$\leqslant y_k \qquad \text{pcq } by_{k+1} + u_k = y_k. \tag{2.158b}$$

Bref : $2y_{k+1} \leqslant y_k$. Par récurrence[30] nous trouvons que

$$2^k y_k \leqslant x \tag{2.159}$$

parce que $y_0 = x$. Par le lemme 2.83, si k est assez grand,

$$2ky_k \leqslant 2^k y_k \leqslant x. \tag{2.160}$$

Puisque $\mathbb{N}$ est archimédien[31], nous pouvons considérer $s \in \mathbb{N}$ tel que $2s > x$. À ce moment nous avons

$$y_n = 0 \tag{2.161}$$

pour tout $n \geqslant s$. Nous posons

$$N = \max\{k \text{ tel que } y_k \neq 0\}. \tag{2.162}$$

Prouvons par récurrence sur l que

$$y_{N-l} = \sum_{i=N-l}^{N} u_i b^{(i+l)-N}. \tag{2.163}$$

EQooZBKQooEcckr

Notez que $i + l \geqslant N - l + l = N$, donc $(i + l) - N$ a un sens.

(4a) **Pour $l = 0$** Avec $l = 0$ nous avons $\sum_{i=N-l}^{N} u_i b^{(i+l)-N} = u_N$. Il faut donc voir que $y_N = u_N$. Nous avons

$$y_N = by_{N+1} + u_N. \tag{2.164}$$

En se rappelant que $y_{N+1} = 0$, nous avons le résultat.

[29] Nous ne citerons pas toujours ce théorème à chaque fois que nous définissons quelque chose par récurrence.
[30] Faut-il citer la proposition 1.130 et donner explicitement la fonction P ?
[31] Proposition 1.174.

(4b) **Pour $l+1$** Pour la récurrence nous avons le calcul suivant :

$$y_{N-l-1} = by_{N-l} + u_{N-l-1} \tag{2.165a}$$
$$= b\sum_{i=N-l}^{N} u_i b^{(i+l)-N} + u_{N-l-1} \tag{2.165b}$$
$$= \sum_{i=N-l}^{N} u_i b^{(i+l)-N+1} + u_{N-l-1} \tag{2.165c}$$
$$= \sum_{i=N-l-1}^{N} u_i b^{(i+l+1)-N}. \tag{2.165d}$$

La récurrence est prouvée. L'égalité (2.163) est validée pour tout l.

En posant $l = N$ dans (2.163) nous trouvons

$$y_0 = \sum_{i=0}^{N} u_i b^i. \tag{2.166}$$

Mais la définition de la suite (y_k) contient $y_0 = x$. Donc nous avons prouvé que

$$x = \sum_{i=0}^{N} u_i b^i = \varphi_{b,N}(u). \tag{2.167}$$

□

EXooEcritureDix

Exemple 2.90.
Comment écrire le nombre b en base b ? Nous devons trouver un N et une suite (u_i) tels que

$$b = \sum_{i=0}^{N} u_i b^i. \tag{2.168}$$

Il est facile de voir que le choix $N = 1$ et $u = (0, 1)$ fonctionne bien : $b = 1 \times b^1 + 0$. Nous avons donc

$$b = \varphi_{b,1}(1, 0). \tag{2.169}$$

Nous écrivons cela plus sobrement $b = 10$. △

NORooBaseStandardDix

2.91.
À part des cas très exceptionnels, nous utilisons toujours la base $b = s(9) = s^9(0)$. Nous nous permettons donc d'écrire « 64 » le nombre $\varphi_{s(9),2}(6, 4)$. Vous saviez que tout groupe simple d'ordre $\varphi_{s(9),2}(6, 0)$ est isomorphe au groupe alterné $A_{\varphi_{s(9),0}(5)}$? C'est la proposition 7.54.

PROPooComparaisonNaturelsParChiffres

Proposition 2.92 ([39])**.**
Soit $b > 2$ un entier naturel fixé, et $M > N$ deux entiers naturels. Si $u \in C_{b,N}$ et $v \in C_{b,M}$, alors $\varphi_{b,N}(u) < \varphi_{b,M}(v)$.

De manière plus intuitive : à base fixée, le nombre qui a le plus de chiffres est le plus grand.

Démonstration. Le lemme 2.87 nous dit que

$$b^N \leqslant \varphi_{b,N}(u) < b^{N+1} \tag{2.170}$$

et

$$b^M \leqslant \varphi_{b,M}(v) < b^{M+1}. \tag{2.171}$$

Puisque $M > N$ nous avons $b^{N+1} \leqslant b^M$ et donc

$$\varphi_{b,N}(u) < b^{N+1} \leqslant b^M \leqslant \varphi_{b,M}(v). \tag{2.172}$$

□

PROPooComparaisonNaturelsParChiffresIdentiques

Proposition 2.93.
Soient $u, v \in C_{b,N}$ tels que $u_i = v_i$ pour $i = r+1, \dots, N$. Si $u_r > v_r$ alors $\varphi_{b,N}(u) > \varphi_{b,N}(v)$.

De manière intuitive : avec le même nombre de chiffres, le plus grand est celui dont le premier chiffre différent est le plus grand.

Autrement dit, les nombres en écriture de position se classent par ordre lexicographique.

Démonstration. En découpant les sommes nous avons

$$\varphi_{b,N}(u) = \sum_{i=r+1}^{N} u_i b^i + u_r b^r + \sum_{i=0}^{r-1} u_i b^i \tag{2.173}$$

et

$$\varphi_{b,N}(v) = \sum_{i=r+1}^{N} u_i b^i + v_r b^r + \sum_{i=0}^{r-1} v_i b^i. \tag{2.174}$$

Puisque $b^r > \sum_{i=0}^{r-1} u_i b^i$ (lemme 2.87), nous avons aussi

$$b^r + \sum_{i=0}^{r-1} u_i b^i > \sum_{i=0}^{r-1} v_i b^i. \tag{2.175}$$

EQooTZPBooTeaubX

Et le calcul final :

$$\begin{aligned}
\varphi_{b,N}(v) &< \sum_{i=r+1}^{N} v_i b^i + v_r b^r + b^r + \sum_{i=0}^{r-1} u_i b^i && \text{pcq (2.175)} && \text{(2.176a)}\\
&= \sum_{i=r+1}^{N} u_i b^i + (v_r+1) b^r + \sum_{i=0}^{r-1} u_i b^i && && \text{(2.176b)}\\
&\leqslant \sum_{i=r+1}^{N} u_i b^i + u_r b^r + \sum_{i=0}^{r-1} u_i b^i && \text{pcq } u_r \geqslant v_r + 1 && \text{(2.176c)}\\
&= \sum_{i=0}^{N} u_i b^i && && \text{(2.176d)}\\
&= \varphi_{b,N}(u). && && \text{(2.176e)}
\end{aligned}$$

Et voilà. □

2.7.3 Symbole de produit

NORMooDBOFooQCwbOY

2.94.
Si $(G, \cdot)$ est un groupe et si $H \subset G$, nous notons le produit des éléments de H par

$$\prod_{g\in H} g = \sum_{g\in H} g \tag{2.177}$$

où à droite, c'est la somme déjà définie. La différence entre $\prod$ et $\sum$ est que nous utilisons $\prod$ pour les groupes notés « multiplicativement » comme $(G, \cdot)$ alors que nous utilisons $\sum$ lorsque le groupe est noté « additivement » comme $(G, +)$.

Dans le cas d'un anneau $(A, +, \cdot)$, la distinction est importante pour savoir quelle opération est sous-entendue.

La définition 2.79(1) signifie qu'une somme vide vaut zéro : $\sum_{x\in\varnothing} x = 0$. Vu que zéro est la façon usuelle de noter le neutre pour une opération notée « + », lorsque l'opération est notée $\cdot$ nous avons

$$\prod_{x\in\varnothing} x = 1 \tag{2.178}$$

EQooCSDSooTxdfzQ

parce que 1 est la façon usuelle de noter le neutre d'une opération notée « $\cdot$ ».

Notez que (2.178) n'est pas une nouvelle définition ou une nouvelle convention. C'est seulement l'égalité $\sum_{x\in\varnothing x} x = 0$, avec des notations adaptées à un groupe dont l'opération est notée multiplicativement.

2.8 Permutations, groupe symétrique

Nous donnons ici quelques éléments à propos du groupe symétrique. Beaucoup de choses supplémentaires sont reportées à la section 7.6. Voir aussi le thème 8.

La définition du groupe symétrique est 2.2.

DEFooSupportPermutation

Définition 2.95.
*Le **support** d'une permutation σ est l'ensemble constitué des éléments modifiés par σ :*

$$\operatorname{supp}\sigma = \{i \in \{1,\dots,n\} \text{ tel que } \sigma(i) \neq i\}.$$

DEFooMVFKooMpXMQy

Définition 2.96 ([57]).
*Soient une permutation $\sigma \in E$ ainsi que $a \in E$. La σ-**orbite** de a est l'ensemble*

$$\Omega_\sigma(a) = \{\sigma^i(a)\}_{i\in\mathbb{N}}. \tag{2.179}$$

LEMooSGWKooKFIDyT

Lemme 2.97 ([58]).
Le groupe symétrique S_n est un ensemble fini contenant $n!$ éléments :

$$\operatorname{Card}(S_n) = n!. \tag{2.180}$$

LEMooUPBOooWbwMTx

Lemme 2.98 ([59]).
Deux résultats.

(1) Tout groupe est isomorphe à un sous-groupe d'un groupe symétrique.

(2) Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

Démonstration. Soit, pour $g \in G$ donné, l'application

$$\begin{aligned}\tau_g\colon G &\to G\\ x &\mapsto gx.\end{aligned} \tag{2.181}$$

Commençons par prouver que cela est une bijection. D'une part, $\tau_g(x) = y$ pour $x = g^{-1}y$ (surjection) et, d'autre part, $\tau_g(x) = \tau_g(y)$ implique $gx = gy$ et donc $x = y$ (injection).

Nous avons donc $\tau_g \in S_G$. L'application

$$\begin{aligned}\varphi\colon G &\to S_G\\ g &\mapsto \tau_g\end{aligned} \tag{2.182}$$

est un morphisme de groupe[32] :

$$\varphi(gh)x = ghx = \varphi(g)(hx) = \varphi(g)\Big(\varphi(h)x\Big) = \Big(\varphi(g)\circ\varphi(h)\Big)x. \tag{2.183}$$

Elle est injective parce que si $\tau_g = \tau_h$ alors $gx = hx$ pour tout x. En particulier $g = h$. Donc $\varphi\colon G \to \text{Image}(\varphi)$ est un isomorphisme entre G et un sous-groupe de S_G (proposition 1.96).

Un groupe fini de cardinal n est isomorphe à un sous-groupe de S_G ; or S_G est isomorphe à un des S_n. □

2.8.1 Décomposition en cycles

DEFooRWYSooYmKwph

Définition 2.99 (cycle[57]).
*Soit E un ensemble de cardinal[33] n. Soit un entier $1 \leqslant k \leqslant n$. Un élément $\sigma \in S_E$ est un k-**cycle** si il ne possède qu'une seule orbite[34] non réduite à un élément et qu'elle est de cardinal[35] k.*

LEMooADNGooDZpdTb

Lemme 2.100 ([1]).
Soient un k-cycle σ et $a \in \Omega$. Alors

$$\Omega_\sigma(a) = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\} \tag{2.184}$$

et $\sigma^k(a) = a$.

En particulier, les éléments $\sigma^q(a)$ avec $q = 0,\dots,k-1$ sont tous distincts.

Démonstration. Soit l le plus grand entier tel que les $\sigma^i(a)$ avec $0 \leqslant i \leqslant l$ soient tous distincts, et notons $A = \{\sigma^i(a)\}_{i=0,\dots,l}$. Cet ensemble satisfait

[32] Définition 1.95.
[33] Définition 2.24.
[34] Définition 2.96.
[35] Cardinal d'un ensemble fini définition 2.24.

- $\text{Card}(A) = l + 1$
- $A \subset \Omega_\sigma(a)$, et donc $\text{Card}(A) \leqslant \text{Card}(\Omega_\sigma(a)) = k$ par le lemme 2.29(3).

Que vaut $\sigma^{l+1}(a)$? Par maximalité de l, $\sigma^{l+1}(a)$ est un des $\sigma^i(a)$ avec $i \leqslant l$. Par injectivité de σ, nous avons donc forcément $\sigma^{l+1}(a) = a$.

Donc pour tout $i > l$ il existe $j \leqslant l$ tel que $\sigma^i(a) = \sigma^j(a)$ (parce que $\sigma^i(a) = \sigma^{i-l-1}(a)$). Nous en déduisons que

$$\Omega_\sigma(a) = \{\sigma^i(a)\}_{0 \leqslant i \leqslant l} = A. \tag{2.185}$$

Le cardinal de $\Omega_\sigma(a)$ étant k par hypothèse nous avons $k = l + 1$, et donc $l = k - 1$. □

LEMooANVHooOQiTwY

Lemme 2.101.
Si σ est une cycle de longueur k, et si $b \in \Omega_\sigma(a)$, alors

$$\Omega_\sigma(a) = \Omega_\sigma(b) = \{\sigma^i(b)\}_{i=0,\dots,k-1}. \tag{2.186}$$

Démonstration. Comme $b \in \Omega_\sigma(a)$, il existe $l \leqslant k - 1$ tel que $b = \sigma^l(a)$. Pour tout i nous avons $\sigma^i(a) = \sigma^{k-l+1}(b)$, et donc $\Omega_\sigma(a) \subset \Omega_\sigma(b)$.

Mais pour tout i nous avons aussi $\sigma^i(b) = \sigma^{l+1}(a)$ et donc $\Omega_\sigma(b) \subset \Omega_\sigma(a)$.

Nous avons donc montré que $\Omega_\sigma(a) = \Omega_\sigma(b)$. La seconde égalité est le lemme 2.100 appliqué à b. □

LEMooMIHGooQfALbc

Lemme 2.102 ([1]).
Soient un ensemble fini E, une permutation $\sigma \in S_E$ ainsi que $a \in E$. Si $b \in \Omega_\sigma(a)$, alors $\Omega_\sigma(b) = \Omega_\sigma(a)$.

Démonstration. Nous supposons que $b \in \Omega_\sigma(a)$ et nous montrons que $\Omega\sigma(a) = \Omega_\sigma(b)$. Posons $b = \sigma^k(a)$ et allons-y pour la preuve.

(1) $\Omega_\sigma(b) \subset \Omega_\sigma(a)$ Soit $x \in \Omega_\sigma(b)$; nous avons $x = \sigma^l(a)$ pour un certain l et alors :

$$x = \sigma^l(b) = \sigma^l\big(\sigma^k(a)\big) = \sigma^{k+l}(a) \in \Omega_\sigma(a). \tag{2.187}$$

(2) $\Omega_\sigma(a) \subset \Omega_\sigma(b)$ Notons $H = \{\sigma^k \text{ tel que } k \in \mathbb{N}\}$ le groupe engendré par σ. Le groupe H est fini parce que $S(E)$ est fini (lemme 2.97 et le fait que toute partie d'un ensemble fini est fini, lemme 1.76). Le corolaire 2.74 nous dit qu'en posant $p = \text{Card}(H)$ nous avons $\sigma^p = \text{Id}$ et donc, en particulier, $\sigma^p(a) = a$.

Nous prouvons que $a \in \Omega_\sigma(b)$. Pour rappel : $b = \sigma^k(a)$ et $\sigma^p(a) = a$. En utilisant la division euclidienne (théorème 1.181), nous considérons $q \in \mathbb{N}$ et $r < p$ dans $\mathbb{N}$ tels que $k = qp + r$. Vu que $\sigma^{qp} = \text{Id}$ nous avons

$$b = \sigma^k(a) = \sigma^r(a). \tag{2.188}$$

Étant donné que $p > r$, nous pouvons appliquer σ^{p-r} des deux côtés et trouver

$$\sigma^{p-r}(b) = \sigma^{p-r}\big(\sigma^r(a)\big) = \sigma^p(a) = a. \tag{2.189}$$

Donc $a \in \Omega_\sigma(b)$. Et donc $\Omega_\sigma(a) \subset \Omega_\sigma(b)$.

□

LEMooGWZNooXFezrg

Lemme 2.103 ([57]).
Tout k-cycle est d'ordre[36] *k.*

Démonstration. Soit le cycle $\{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$. Tous les $\sigma^i(a)$ avec $i \leqslant k-1$ sont distincts et $\sigma^k(a) = a$. Donc σ^k est l'identité, et l'ordre de σ est plus petit ou égal à k.

Si $i \leqslant k - 1$, alors $\sigma^i(a) \neq a$ parce que les éléments du cycle sont distincts. Donc $\sigma^i \neq \text{Id}$ pour $i \leqslant k - 1$. Nous en déduisons que l'ordre de σ est k. □

LEMooWXXLooIzrwJT

Lemme 2.104 ([57]).
Deux cycles[37] *de support*[38] *disjoint commutent.*

Démonstration. Soient σ et θ deux cycles de support disjoints. Soit $x \in E$. Il y a trois possibilités : $x \in \text{supp}(\sigma)$, $x \in \text{supp}(\theta)$ et x hors des deux supports.

[36] Définition 2.68.
[37] cycle, définition 2.99.
[38] support, définition 2.95.

(1) **Si $x \in \text{supp}(\sigma)$** Alors $\sigma(x) \in \text{supp}(\sigma)$ parce que σ est une bijection. En effet si $\sigma\big(\sigma(x)\big) = \sigma(x)$, alors on aurait un problème d'injectivité. Bref, $\sigma(x) \in \text{supp}(\sigma)$ et donc $\sigma(x) \notin \text{supp}(\theta)$. Donc $\theta\big(\sigma(x)\big) = \sigma(x)$.

Vu qu'on a aussi $\theta(x) = x$, on a $(\sigma \circ \theta)(x) = \sigma(x)$. Donc oui pour qu'ils commutent.

(2) **Si $x \in \text{supp}(\theta)$** Idem.

(3) **Si x est hors des deux** Alors $\sigma(x) = \theta(x) = x$.

□

LEMooVVPWooMkRjyR

Lemme 2.105 ([60]).
Tout cycle de longueur r est le produit de $r-1$ transpositions.

Démonstration. Il suffit de vérifier que

$$(a_1, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2). \tag{2.190}$$

□

LEMooGGLUooUSzuAx

Lemme 2.106 ([1]).
Soit une permutation $\sigma \in S_E$. Soit un cycle c et une permutation s de supports disjoints telles que $\sigma = s \circ c$. Alors

LEMooUHWTooFptoZU

(1) Si $a \in \text{supp}(\sigma)$, alors pour tout $q \in \mathbb{N}$ nous avons $c^q(a) = \sigma^q(a)$.

ITEMooHSDLooIAKYZA

(2) Si $a \in \text{supp}(c)$, alors

$$\Omega_\sigma(a) = \Omega_c(a) = \text{supp}(c). \tag{2.191}$$

(3) Si $a \in \text{supp}(c)$, alors

$$c(x) = \begin{cases} \sigma(x) & \text{si } x \in \Omega_\sigma(a) \\ x & \text{sinon.} \end{cases} \tag{2.192}$$

Démonstration. En plusieurs parties.

(1) **Si $a \in \text{supp}(c)$, alors $c(a) = \sigma(a)$** Soit $a \in \text{supp}(c)$. Nous savons que $c(a) \neq a$, et vu que c est injective, nous devons aussi avoir $c\big(c(a)\big) \neq c(a)$. Donc a et $c(a)$ sont dans $\text{supp}(c)$. Étant donné que les supports de c et de s sont disjoints, nous déduisons que $c(a)$ n'est pas dans le support de s, et donc que

$$\sigma(a) = (s \circ c)(a) = s\big(c(a)\big) = c(a). \tag{2.193}$$

(2) $\sigma^q(a) = c^q(a)$ Juste une récurrence sur le point précédent : si $b \in \text{supp}(a)$, alors $\sigma(b) = c(b) \in \text{supp}(a)$.

(3) **Si $a \in \text{supp}(c)$, alors $\Omega_\sigma(a) = \Omega_c(a)$** Utilisant le point précédent, ainsi que la définition 2.96 d'une orbite,

$$\Omega_\sigma(a) = \{\sigma^q(a)\} = \{c^q(a)\} = \Omega_c(a). \tag{2.194}$$

(4) $\text{supp}(c) \subset \Omega_c(a)$ Comme toujours, a est un élément de $\text{supp}(c)$. Nous considérons $b \in \text{supp}(c)$ et nous montrons que $b \in \Omega_c(a)$. Étant donné que $b \in \text{supp}(c)$, nous avons $c(b) \neq b$, de telle sorte que $\Omega_c(b)$ contienne au moins deux éléments distincts.

Même chose pour a : l'ensemble $\Omega_c(a)$ contient au moins a et $c(a)$. Vu que c est un cycle, il n'existe qu'une seule orbite non triviale. Donc $\Omega_c(a) = \Omega_c(b)$. En particulier $b \in \Omega_c(b) = \Omega_c(a)$.

(5) $\Omega_c(a) \subset \text{supp}(c)$ Soit $b \in \Omega_c(a)$. Le lemme 2.101 nous permet de dire que $\Omega_c(a) = \Omega_c(b)$. Comme $\Omega_c(b)$ contient au moins deux éléments (parce qu'il est égal à $\Omega_c(a)$ et que a est dans le support de c), nous savons que $c(b) \neq b$ et donc que $b \in \text{supp}(c)$.

(6) **La formule pour $c(x)$** Si $x \in \Omega_{\sigma)}(a)$, alors $c(x) = \sigma(x)$ par le point (1). Si x n'est pas dans $\Omega_c(a) = \text{supp}(c)$, alors x n'est pas dans le support de c et donc $c(x) = x$.

□

PROPooSWEYooGRYvcM

Proposition 2.107 ([61]).
Soient un ensemble fini E, un élément $\sigma \in S(E)$ du groupe symétrique de E, et $a \in E$.

ITEMooSAMGooPDGCwF

(1) *Les orbites de σ forment une partition de E.*

ITEMooXPPWooOFqwBl

(2) *La partie $\{k \in \mathbb{N} \text{ tel que } \sigma^k(a) = a\}$ est non vide.*

ITEMooBOHSooJScjxU

(3) *Nous posons $l = \min\{k \in \mathbb{N} \text{ tel que } \sigma^k(a) = a\}$. Nous avons*[39]

$$\Omega_\sigma(a) = \{\sigma^k(a)\}_{k=0,\dots,l-1}. \tag{2.195}$$

ITEMooBWCKooZeKtyM

(4) *Si $0 \leqslant k < k' \leqslant l-1$, alors $\sigma^k(a) \neq \sigma^{k'}(a)$.*

Démonstration. En plusieurs étapes.

(1) **Pour (1)** Déjà l'union des orbites fait bien E parce que pour tout $x \in E$ nous avons $x \in \Omega_\sigma(x)$. Le fait que les orbites soient disjointes est le lemme 2.102 : si deux orbites ont une intersection, alors elles sont égales.

(2) **Pour (2)** C'est le corolaire 2.74 qui dit qu'avec $p = \text{Card}(H)$ nous avons $\sigma^p(a) = a$. Toute partie non vide de $\mathbb{N}$ possède un unique minimum (proposition 1.152(2)).

Cela pour dire que le l dont nous parlons dans le point (3) est bien défini.

(3) **Pour (3)** Nous posons $A = \{\sigma^k(a) \text{ tel que } 0 \leqslant k \leqslant l-1\}$, et nous prouvons que $A = \Omega_\sigma(a)$. Forcément, $A \subset \Omega_\sigma(a)$. Nous nous concentrons sur l'inclusion dans l'autre sens. Soit $x = \sigma^k(a) \in \Omega_\sigma(a)$. Si $k \leqslant l-1$, alors $x \in A$. Nous supposons que $k \geqslant l$.

Nous refaisons la division euclidienne $k = ql + r$, nous remarquons que $\sigma^l(a) = a$, et nous avons

$$x = \sigma^k(a) = \sigma^{ql+r}(a) = \sigma^r(a) \in A. \tag{2.196}$$

Donc $\Omega_\sigma(a) \subset A$.

(4) **Pour (4)** Soient k, k' tels que $0 \leqslant k < k' \leqslant l-1$. Supposons que $\sigma^k(a) = \sigma^{k'}(a)$. Nous savons que σ est une bijection, de telle sorte que nous pouvons appliquer $(\sigma^k)^{-1}$ des deux côtés :

$$a = \sigma^{k'-k}(a). \tag{2.197}$$

Or, par choix de k et k' nous avons

$$k' - k < k' \leqslant l-1. \tag{2.198}$$

En suivant la proposition 1.153(2) (et en adaptant un tout petit peu), nous en déduisons que $k' - k < l$. Cela contredit la minimalité de l.

□

Le théorème suivant dit que tout élément du groupe symétrique S_n peut être décomposé de façon unique en un nombre fini de cycles de supports disjoints.

THOooPGGLooInzSFo

Théorème 2.108 ([61]).
Soit un ensemble fini E de cardinal au moins deux. Soit une permutation $\sigma \in S_E$.

(1) *Il existe des cycles $c_1, \dots, c_m$ à support disjoints tels que $\sigma = c_1 \circ \dots \circ c_m$.*

(2) *Cette décomposition est unique à l'ordre près.*

Plus précisément, si σ est une permutation, alors il existe un unique ensemble fini $\{\omega_i\}_{i\in I}$ de cycles de supports disjoints tels que[40] *$\sigma = \prod_{i\in I} \omega_i$.*

Démonstration. Plusieurs points.

(1) **Existence** La proposition 2.107 nous permet de choisir éléments $\{a_i\}_{i=1,\dots,p}$ tels que les $\Omega_\sigma(a_i)$ forment une partition de E en sous-ensembles disjoints. Toujours avec la même proposition, en posant $l_k = \min\{r \text{ tel que } \sigma^r(a_k) = a_k\}$, nous avons

$$\Omega_\sigma(a_k) = \{\sigma^q(a_k)\}_{q=1,\dots,l_k-1} \tag{2.199}$$

[39] Ici $\Omega_\sigma(a)$ est l'orbite de a soit l'action des itérées de σ, définition 2.96.
[40] Ici I est un ensemble fini et vu que les supports sont disjoints, le produit est commutatif.

et tous les $\sigma^q(a_k)$ sont distincts pour $q = 1, \dots, l_k - 1$.

Posons

$$\begin{aligned} c_k \colon E &\to E \\ x &\mapsto \begin{cases} \sigma(x) & \text{si } x \in \Omega_\sigma(a_k) \\ x & \text{sinon.} \end{cases} \end{aligned} \tag{2.200}$$

Le lemme 2.106 dit que c_k est un cycle. Vu que $c(a_k) = \sigma(a_k)$, le cycle c est un l_k-cycle.

Nous montrons à présent que $\sigma = c_1 \circ \dots c_p$. Soit $x \in E$. Il existe un $k \in \{1, \dots, p\}$ tel que

$$x \in \Omega_\sigma(a_k) = \Omega_{c_k}(a_k) = \Omega_{c_k}(x), \tag{2.201}$$

la dernière égalité est parce que $x \in \Omega_{c_k}(a_k)$. Nous en déduisons que $c_k(x) \neq x$. D'autre part si $l \neq k$, alors x n'est pas dans $\Omega_\sigma(a_l)$, et donc $c_l(x) = x$. Au final[41],

$$(c_1 \circ \dots c_p)(x) = c_k(x) = \sigma(x). \tag{2.202}$$

(2) **Unicité** Nous supposons avoir $\sigma = c_1 \circ \dots \circ c_p = \gamma_1 \circ \gamma_q$ où les c_i et les γ_j sont deux ensembles de cycles de supports disjoints. Nous avons

$$\operatorname{supp}(\sigma) = \bigcup_{i=1}^{p} \operatorname{supp}(c_i) = \bigcup_{j=1}^{q} \operatorname{supp}(\gamma_j). \tag{2.203}$$

Montrons que si $\operatorname{supp}(c_i) \cap \operatorname{supp}(\gamma_j) \neq \varnothing$, alors $\operatorname{supp}(c_i) = \operatorname{supp}(\gamma_j)$. En effet si $a \in \operatorname{supp}(c_i) \cap \operatorname{supp}(\gamma_j)$, alors

$$\operatorname{supp}(c_i) = \Omega_{c_i}(a) = \Omega_\sigma(a) = \Omega_{\gamma_j}(a) = \operatorname{supp}(\gamma_j). \tag{2.204}$$

Et comme les $\operatorname{supp}(\gamma_j)$ sont disjoints, l'ensemble $\operatorname{supp}(c_i)$ n'a d'intersection qu'avec un et un seul des $\operatorname{supp}(\gamma_j)$. Cela définit donc une application

$$\begin{aligned} u \colon \{1, \dots, p\} &\to \{1, \dots, q\} \\ i &\mapsto \text{l'unique } j \text{ tel que } \operatorname{supp}(c_i) = \operatorname{supp}(\gamma_j). \end{aligned} \tag{2.205}$$

Autrement dit, l'application u permet d'écrire

$$\operatorname{supp}(c_i) = \operatorname{supp}\left(\gamma_{u(i)}\right). \tag{2.206}$$

L'application u est injective. En effet si $u(i) = u(l)$, nous avons

$$\operatorname{supp}(c_i) = \operatorname{supp}\left(\gamma_{u(i)}\right) \tag{2.207a}$$
$$\operatorname{supp}(c_l) = \operatorname{supp}\left(\gamma_{u(l)}\right) \tag{2.207b}$$
$$u(i) = u(l). \tag{2.207c}$$

Donc $\operatorname{supp}(c_i) = \operatorname{supp}(c_l)$. Et comme les supports sont disjoints, $i = l$.

L'application u est surjective. En effet, soit $j \in \{1, \dots, q\}$. Soit $a \in \operatorname{supp}(\gamma_j)$. Il existe un i tel que $a \in \operatorname{supp}(c_i)$. Nous avons alors $a \in \operatorname{supp}(\gamma_j) \cap \operatorname{supp}(c_i)$, autrement dit $u(i) = j$.

Maintenant l'application $u \colon \{1, \dots, p\} \to \{1, \dots, q\}$ est bijective. Nous en déduisons que $p = q$. Concluons en montrant que $c_i = \gamma_{u(i)}$. Soit $a \in \operatorname{supp}(c_i) = \operatorname{supp}\left(\gamma_{u(i)}\right)$.

Nous avons

$$c_i(x) = \begin{cases} \sigma(x) & \text{si } x \in \Omega_\sigma(a) \\ x & \text{sinon} \end{cases} \tag{2.208}$$

et

$$\gamma_j(x) = \begin{cases} \sigma(x) & \text{si } x \in \Omega_\sigma(a) \\ x & \text{sinon,} \end{cases} \tag{2.209}$$

et donc $c_i = \gamma_j$.

□

Le lemme suivant permet d'extraire le cycle de σ associé à un élément de E.

[41] La notation $a_1 \dots a_n$ est une notation « abrégée » pour ce qui est défini par $\prod_{i=1}^{n} a_i$, voir 2.94.

LEMooFFTBooCZsaFu

Lemme 2.109 ([1]).
Soient un ensemble fini E ainsi que $\sigma \in S_E$, et $a \in E$ tel que $\sigma(a) \neq a$. Nous posons

$$\begin{aligned} c\colon E &\to E \\ x &\mapsto \begin{cases} \sigma(x) & si\ x \in \Omega_\sigma(a) \\ x & sinon \end{cases} \end{aligned} \tag{2.210}$$

Alors

(1) Si $b \in \Omega_\sigma(a)$, nous avons $\Omega_c(b) = \Omega_\sigma(a)$.

(2) Si $b \notin \Omega_\sigma(a)$, nous avons $\Omega_c(b) = \{b\}$.

(3) c est un cycle.

Démonstration. Si $b \in \Omega_\sigma(a)$, alors $\sigma^q(b) \in \Omega_\sigma(a)$ pour tout $q \in \mathbb{N}$, et donc

$$c^q(b) = \sigma^q(b) \in \Omega_\sigma(a) \tag{2.211}$$

pour tout q. Donc nous avons

$$\Omega_c(b) = \{c^q(b) \text{ tel que } q \in \mathbb{N}\} = \{\sigma^q(b) \text{ tel que } q \in \mathbb{N}\} = \Omega_\sigma(b) = \Omega_\sigma(a). \tag{2.212}$$

La dernière égalité est le lemme 2.102.

Si $b \notin \Omega_\sigma(a)$, alors $c(b) = b$ et $\Omega_c(b) = \{b\}$.

Nous avons prouvé que c a une seule orbite de taille plus grands ou égale à 2. Donc c est un cycle. □

LemmvZFWP

Lemme 2.110 ([62]).
Soit $\sigma = (i_1, \dots, i_k) \in S_n$, un cycle de longueur k et $\theta \in S_n$. Alors

$$\theta\sigma\theta^{-1} = \big(\theta(i_1), \dots, \theta(i_k)\big). \tag{2.213}$$

Tous les cycles de longueur k sont conjugués entre eux.

PropEAHWXwe

Proposition 2.111 (Classes de conjugaison et structure en cycles[63]).
Une classe de conjugaison[42] dans S_n est formée des permutations ayant une décomposition en cycles disjoints de même structure. Autrement dit, deux permutations σ et σ' sont conjuguées si et seulement si le nombre k_i de cycles de longueur i dans σ est le même que le nombre k'_i de cycles de longueur i dans σ'.

Démonstration. Soit $\sigma = c_1 \dots c_m$ la décomposition de σ en cycles c_i de supports disjoints. Si τ est une permutation, alors

$$\sigma' = \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \dots (\tau c_m \tau^{-1}), \tag{2.214}$$

mais $\tau c_i \tau^{-1}$ est un cycle de même longueur que c_i, puisque le lemme 2.110 nous dit que si $\sigma = (a_1, \dots, a_k)$, alors $\tau c \tau^{-1} = \big(\tau(a_1), \dots, \tau(a_k)\big)$. Notons encore que les cycles $\tau c_i \tau^{-1}$ restent à support disjoints.

Donc tous les éléments de la classe de conjugaison de σ sont des permutations de même structure que σ.

Réciproquement, si $\sigma' = c'_1 \dots c'_m$ est une décomposition de σ' en cycles disjoints tels que la longueur des c_i est la même que la longueur des c'_i, alors il suffit de construire des permutations τ_i telles que $\tau_i c_i \tau_i^{-1} = c'_i$, à travers le lemme 2.110. Comme les supports des c_i et des c'_i sont disjoints, la permutation $\tau_1 \dots \tau_m$ conjugue σ et σ'. □

EXooQAXRooBsPURs

Exemple 2.112.
Voyons les classes de conjugaison de S_3. Étant donné que ce groupe agit par définition sur un ensemble à 3 éléments, aucun élément de S_3 ne possède un cycle de plus de 3 éléments. Il y a donc seulement des cycles de longueur deux ou trois (à part les triviaux). Aucun élément de S_3 n'a une décomposition en cycles disjoints contenant deux cycles de deux ou un cycle de deux et un de trois.

En résumé il y a trois classes de conjugaison dans S_3. La première est celle contenant seulement l'identité. La seconde est celle contenant les cycles de longueur deux et la troisième contient les cycles de longueur 3.

Ce sont donc

$$C_1 = \{\mathrm{Id}\} \tag{2.215a}$$
$$C_2 = \{(1,2), (1,3), (2,3)\} \tag{2.215b}$$
$$C_3 = \{(1,2,3), (2,1,3)\}. \tag{2.215c}$$

△

[42] Définition 2.8.

DEFooXNAFooGTbTTJ

Définition 2.113 (transposition)**.**
Une ***transposition*** *est une permutation*[43] *qui échange deux éléments de E. Plus précisément, une bijection $\sigma : E \to E$ est une transposition si il existe $a, b \in E$ tels que*

$$\sigma(x) = \begin{cases} a & si\ x = b \\ b & si\ x = a \\ x & sinon. \end{cases} \tag{2.216}$$

ExVYZPzub

Exemple 2.114.

△

PROPooQRZYooKVZTCJ

Proposition 2.115 ([1])**.**
Les classes de conjugaison de S_4 sont :

ITEMooZIYYooCqpicx

(1) Le cycle vide qui représente la classe constituée de l'identité seule.

ITEMooVDLGooFOkgzc

(2) Les transpositions (de type (a, b)) qui sont au nombre de 6.

ITEMooWKUIooTedZAA

(3) Les doubles transpositions (de type $(a, b)(c, d)$) qui sont au nombre de 6.

ITEMooMHRWooSkUveJ

(4) Les 3-cycles qui sont au nombre de 8.

ITEMooCBYNooZmFsBd

(5) Les 4-cycles qui sont au nombre de 6.

ITEMooGCMYooKZgFHX

(6) Les doubles transpositions, du type $(a, b)(c, d)$ qui sont au nombre de 3.

Démonstration. Nous savons que les classes de conjugaison dans S_4 sont caractérisées par la structure des décompositions en cycles (proposition 2.111). Avec 4 éléments, il n'y a pas des tonnes de cycles qu'on peut faire.

On peut faire des cycles de taille 1, 2, 3 ou 4. Les seules façons de faire 4 avec ces nombres sont :

(1) $1 + 1 + 1 + 1$

(2) $2 + 1 + 1$

(3) $2 + 2$

(4) $3 + 1$

(5) 4

Comptons combien il y a de possibilités dans chaque cas.

(1) **Pour (1)** À propos de la possibilité $1 + 1 + 1 + 1 = 4$. Il y a une seule possibilité de fixer tous les éléments.

(2) **Pour (2)** À propos de $2 + 1 + 1 = 4$. Il y a 4 possibilités pour a, et 3 pour b. Mais $(a, b) = (b, a)$, donc il faut diviser par deux. Donc 6 en tout.

(3) **Pour (3)** À propos de $2 + 2 = 4$. Nous cherchons les possibilités pour $(a, b)(c, d)$. Nous venons de voir qu'il y a 6 possibilités pour (a, b). Les deux autres sont fixés.

(4) **Pour (4)** Pour savoir quel est leur nombre nous commençons par remarquer qu'il y a 4 façons de prendre 3 nombres parmi 4 et ensuite 2 façons de les arranger. Il y a donc 8 éléments dans cette classe de conjugaison.

(5) **Pour (5)** Le premier est arbitraire (parce que c'est cyclique). Pour le second il y a 3 possibilités, et deux possibilités pour le troisième ; le quatrième est alors automatique. Cette classe de conjugaison contient donc 6 éléments.

(6) **Pour (6)** Dans ce cas, tous les nombres sont permutés, et l'image de 1 détermine la double transposition. Il y a 3 images possibles, et donc 3 éléments dans cette classe.

□

[43] Une permutation est une bijection, définition 2.2.

PropPWIJbu

Proposition 2.116.
Tout élément de S_n peut être écrit sous la forme d'un produit fini de transpositions.

Si E est un ensemble fini, tout élément de S_E pour être écrit sous forme d'un produit fini de transposition de E.

Démonstration. Un élément de S_n se décompose en un nombre fini de cycles par le théorème 2.108 et chacun des cycles peut être décomposé en un nombre fini de transpositions par le lemme 2.105. □

Cette décomposition n'est pas à confondre avec celle en cycles de support disjoints. Par exemple $(1,2,3) = (1,3)(1,2)$.

2.8.2 Parité d'une permutation, signature

La notion de parité d'une permutation est la clef pour savoir quelles positions du jeu de taquin sont possibles ou impossibles[64, 65].

DEFooYDUHooKIXGNW

Définition 2.117 ([66]).
Soit une permutation $\sigma \in S_E$ où $\text{Card}(E) = n$. Si k est le nombre de σ-orbites dans E, nous définissons la ***signature*** *par*

$$\epsilon(\sigma) = (-1)^{n-k}. \tag{2.217}$$

PROPooWCHBooTgMokj

Proposition 2.118 ([66]).
Soient une transposition τ et une permutation σ de l'ensemble fini E. Nous avons

$$\epsilon(\sigma\tau) = -\epsilon(\sigma). \tag{2.218}$$

Démonstration. Soient $a, b \in E$ tels que $\tau(a) = b$ et $\tau(b) = a$. Nous allons comparer la liste des orbites de σ avec celle de $\sigma\tau$. Il y a deux possibilités : soit a et b sont dans la même orbite de σ, soit ils sont dans des orbites séparées.

Nous notons[44]

(1) I l'ensemble des orbites de σ ne contenant ni a ni b.

(2) I' l'ensemble des orbites de $\tau\sigma$ ne contenant ni a ni b.

(3) $\mathcal{O}_a$ la σ-orbite de a, $\mathcal{O}_b$ la σ-orbite de b.

(4) $\mathcal{O}'_a$ la $\sigma\tau$-orbite de a, $\mathcal{O}'_b$ la $\sigma\tau$-orbite de b.

Il est tout à fait possible à priori d'avoir $\mathcal{O}_a = \mathcal{O}_b$ ou $\mathcal{O}'_a = \mathcal{O}'_b$. Je vous laisse méditer un instant sur le fait que $\text{Card}\{\mathcal{O}_a, \mathcal{O}_b\}$ vaut 1 ou 2 et que le nombre d'orbites de σ est $\text{Card}(I) + \text{Card}\{\mathcal{O}_a, \mathcal{O}_b\}$.

(1) $\underline{I = I'}$

Soit une orbite $\mathcal{O}$ de σ ne contenant ni a ni b. Alors pour tout $y \in \mathcal{O}$ nous avons $(\sigma\tau)(y) = \sigma(y)$, et donc $\mathcal{O}$ est également une orbite de $\sigma\tau$. Cela prouve que $I = I'$.

(2) $\underline{\textbf{Si } \mathcal{O}_a = \mathcal{O}_b}$ Nous supposons que a et b sont dans la même orbite de σ que nous écrivons

$$\mathcal{O} = \{a, x_1, \dots, x_r, b, x_{r+1}, \dots, x_s\} \tag{2.219}$$

avec $\sigma(x_s) = a$. Étudions la $\sigma\tau$-orbite de a. Nous avons $(\sigma\tau)(a) = \sigma(b) = x_{r+1}$, et $(\sigma\tau)(x_s) = \sigma(x_s) = a$, donc

$$\mathcal{O}'_a = \{a, x_{r+1}, \dots, x_s\} \tag{2.220}$$

ne contient pas b. De même la $(\sigma\tau)$-orbite de b est

$$\mathcal{O}'_b = \{b, x_1, \dots, x_r\} \tag{2.221}$$

et ne contient pas a. Autrement dit, $\mathcal{O}'_a \neq \mathcal{O}'_b$.

(3) $\underline{\textbf{Si } \mathcal{O}_a \neq \mathcal{O}_b}$ Disons que $\mathcal{O}_a = \{a, x_1, \dots, x_r\}$ et $\mathcal{O}_b = \{b, y_1, \dots, y_s\}$ avec $\sigma(y_s) = b$ et $\sigma(x_r) = a$. Nous étudions la $(\sigma\tau)$-orbite de a. Nous avons $(\sigma\tau)(a) = \sigma(b) = y_1$, et ensuite $(\sigma\tau)(y_1) = \sigma(y_1) = y_2$, et ainsi de suite jusqu'à $(\sigma\tau)(y_s) = \sigma(y_s) = b$, et $(\sigma\tau)(b) = \sigma(a) = x_1$. Bref nous avons

$$\mathcal{O}'_a = \{a, y_1, \dots, y_s, b, x_1, \dots, x_r\}, \tag{2.222}$$

et donc $\mathcal{O}'_a = \mathcal{O}'_b$.

[44] Parce que nous adorons à la fois les notations et les listes énumérées.

Nous avons prouvé que si $\text{Card}\{\mathcal{O}_a, \mathcal{O}_b\} = 1$, alors $\text{Card}\{\mathcal{O}'_a, \mathcal{O}'_b\} = 2$ et que si $\text{Card}\{\mathcal{O}_a, \mathcal{O}_b\} = 2$, alors $\text{Card}\{\mathcal{O}'_a, \mathcal{O}'_b\} = 1$. Donc $\sigma\tau$ a une orbite en plus ou une orbite en moins que σ suivant les cas. Dans les deux cas, $\epsilon(\sigma\tau) = -\epsilon(\sigma)$. □

THOooUILDooRUAZfW

Théorème 2.119 ([66])**.**
À propos de signature.

ITEMooOLVOooWJKSDY

(1) Soient des transpositions $\tau_1, \dots, \tau_s$. Nous avons

$$\epsilon(\tau_1 \dots \tau_s) = (-1)^s. \tag{2.223}$$

ITEMooWRONooJQkhzG

(2) L'application

$$\epsilon\colon S_E \to \big(\{-1, 1\}, \times\big) \tag{2.224}$$

est un morphisme de groupe surjectif.

Démonstration. En plusieurs parties.

(1) **Pour (1)** D'abord si τ est une transposition, alors $\epsilon(\tau) = -1$ parce que τ possède $n-1$ orbite dans $\{1, \dots, n\}$. Ensuite une récurrence en utilisant la proposition 2.118 donne le résultat.

(2) **Pour (2)** L'application ϵ est surjective parce que $\epsilon(\tau) = -1$ et $\epsilon(\text{Id}) = 1$. En ce qui concerne le morphisme, si $\sigma, \sigma' \in S_E$, ils peuvent être décomposés en transpositions[45] : $\sigma = \tau_1 \dots \tau_s$ et $\sigma' = \tau_{s+1} \dots \tau_{s+r}$. Nous avons alors

$$\epsilon(\sigma\sigma') = \epsilon(\tau_1 \dots \tau_s \tau_{s+1} \dots \tau_{s+r}) = (-1)^{s+r} = (-1)^s(-1)^r = \epsilon(\sigma)\epsilon(\sigma'). \tag{2.225}$$

□

PROPooKRHEooAxtmRv

Proposition-Définition 2.120 (parité d'une permutation)**.**
À propos de décomposition ne permutations.

(1) Si une permutation peut être écrite sous forme d'un produit d'un nombre pair de transpositions, alors toute décomposition en transpositions sera en quantité paire.

(2) Si une permutation peut être écrite sous forme d'un produit d'un nombre impair de transpositions, alors toute décomposition en transpositions sera en quantité impaire.

*Une permutation qui se décompose en une quantité paire de transpositions est une **permutation paire** (et **impaire** sinon).*

Démonstration. Si $\sigma = \tau_1 \dots \tau_s$ et $\sigma = \tau'_1 \dots \tau'_r$, alors le théorème 2.119(1) dit que $\epsilon(\sigma) = (-1)^s$ et $\epsilon(\sigma) = (-1)^r$, ce qui signifie que $(-1)^r = (-1)^s$ et donc que r et s ont la même parité. □

PROPooXIQOooCcoekP

Proposition 2.121.
La signature de $\sigma \in S_E$ est donné par

$$\begin{aligned} \epsilon\colon S_E &\to \{-1, 1\} \\ \sigma &\mapsto \begin{cases} 1 & \text{si } \sigma \text{ est paire} \\ -1 & \text{si } \sigma \text{ est impaire.} \end{cases} \end{aligned} \tag{2.226}$$

Démonstration. Si σ est paire, alors, par la définition 2.120, $\sigma = \tau_1 \dots \tau_s$ avec s pair. Dans ce cas[46], $\epsilon(\sigma) = (-1)^s = 1$. Même chose si σ est impaire. □

DEFooPXIVooXyYKAH

Définition 2.122.
*Nous disons qu'un élément $\sigma \in S_n$ est une **inversion** pour les nombres $i < j$ si $\sigma(i) > \sigma(j)$.*

LemhxnkMf

Lemme 2.123 ([57])**.**
Un k-cycle[47] est une permutation impaire si k est pair et paire si k est impair.

Démonstration. Il faut remonter à la définition 2.117 de la signature. Si σ est un k-cycle, alors il possède une orbite de cardinal k et $n-k$ orbites singleton. Donc $\epsilon(\sigma) = (-1)^{n-(n-k+1)} = (-1)^{k-1}$. Donc la parité de la signature est toujours opposée à la parité de k. □

[45] Par la proposition 2.116.
[46] Par le théorème 2.119(1)
[47] Définition 2.99.

ProphIuJrC

Proposition 2.124 ([62]).
Soit S_n le groupe symétrique.

ITEMooBQKUooFTkvSu

(1) L'application $\epsilon\colon S_n \to \{1,-1\}$ est l'unique homomorphisme[48] surjectif de S_n sur $\{-1,1\}$.

(2) Si $s = t_1 \cdots t_k$ est le produit de k transpositions, alors $\epsilon(s) = (-1)^k$.

Démonstration. La seule partie à prouver est l'unicité. Le reste est dans le théorème 2.119.

Soit un homomorphisme surjectif $\varphi\colon S_n \to \{-1,1\}$ et τ, une transposition telle que $\varphi(\tau) = -1$ (qui existe parce que sinon φ ne serait pas surjectif[49]). Si τ' est une autre transposition, il existe $\sigma \in S_n$ tel que $\tau' = \sigma\tau\sigma^{-1}$ (lemme 2.110). Dans ce cas, $\varphi(\tau') = \varphi(\tau) = -1$, et si $\sigma = (\tau_1 \dots \tau_k)$,

$$\varphi(\sigma) = (-1)^k = \epsilon(\sigma). \tag{2.227}$$

□

CORooZLUKooBOhUPG

Corolaire 2.125.
Si $\sigma \in S_n$, alors

$$\epsilon(\sigma) = \epsilon(\sigma^{-1}). \tag{2.228}$$

Démonstration. Comme énoncé par la proposition 2.124, ϵ est un homomorphisme, donc

$$\epsilon(\sigma)\epsilon(\sigma^{-1}) = \epsilon(\sigma\sigma^{-1}) = \epsilon(\mathrm{Id}) = 1. \tag{2.229}$$

Puisque $\epsilon(\sigma)$ et $\epsilon(\sigma^{-1})$ ne peuvent valoir que ± 1, ils doivent être tous les deux égaux à 1 ou tous les deux à -1 pour que le produit soit 1. □

2.8.3 Permutations un peu ordonnées

LEMooEOTGooPslULz

Lemme 2.126 ([1]).
Deux énoncés.

ITEMooQZDRooUYjcgX

(1) Soit $\pi \in S_k$ satisfaisant $\pi(1) = 1$. Nous définissons $\tau \in S_{k-1}$ par $\tau(i) = \pi(i+1) - 1$.
Alors $\epsilon(\tau) = \epsilon(\pi)$.

ITEMooBUGZooVCVhKz

(2) L'application

$$\begin{aligned}\varphi\colon \{\pi \in S_k \text{ tel que } \pi(1) = 1\} &\to S_{k-1}\\ \pi &\mapsto \Big[\tau(i) = \pi(i+1) - 1\Big]\end{aligned} \tag{2.230}$$

est une bijection.

Démonstration. Nous nommons π' la restriction de π à $\{2,\dots,k\}$. Cela est encore une bijection, de telle sorte que π' puisse être écrite sous forme d'un produit de n transpositions de $\{2,\dots,k\}$ (proposition 2.116) :

$$\pi = \sigma_1 \circ \dots \circ \sigma_n. \tag{2.231}$$

Les σ_i étant des transpositions de $\{2,\dots,k\}$, elles sont des transpositions de $\{1,\dots,k\}$. Tout cela pour dire que π peut être écrite comme produit de transpositions ne faisant pas intervenir 1.

Nous introduisons la bijection

$$\begin{aligned}\psi\colon \{2,\dots,k\} &\to \{1,\dots,k-1\}\\ i &\mapsto i-1.\end{aligned} \tag{2.232}$$

En termes de ψ, la définition de τ s'écrit $\psi(\pi) = \psi \circ \pi \circ \psi^{-1}$, et nous avons

$$\begin{aligned}\tau &= \psi \circ \pi \circ \psi^{-1} && \text{(2.233a)}\\ &= \psi \circ \sigma_1 \circ \dots \circ \sigma_n \circ \psi^{-1} && \text{(2.233b)}\\ &= \psi \circ \sigma_1 \circ \psi^{-1} \circ \psi \circ \sigma_2 \circ \dots \circ \psi \circ \sigma_n \circ \psi^{-1}. && \text{(2.233c)}\end{aligned}$$

Bref, en notant $\sigma'_i = \psi\sigma_i\psi^{-1}$ nous avons $\tau = \sigma'_1 \circ \dots \circ \sigma_n$.

Il suffit maintenant de remarquer que σ'_i est une transposition dans $\{1,\dots,k-1\}$. On vérifie pour cela que si $\sigma = (a,b)$ alors $\sigma' = \big(\psi(a),\psi(b)\big)$. En effet, pour $i = 1,\dots,k-1$, il y a trois possibilités : soit $i = \psi(a)$, soit $i = \psi(b)$ soit i n'est ni l'un ni l'autre.

[48] Voir -1.1.
[49] Nous utilisons ici le fait que tous les éléments de S_n sont des produits de transpositions, proposition 2.116.

Si $i = \psi(a)$, alors $\sigma'(i) = (\psi\sigma\psi^{-1})\big(\psi(a)\big) = \psi\sigma(a) = \psi(b)$. Même vérification pour montrer que $\sigma'\big(\psi(b)\big) = \psi(a)$. Si i n'est ni $\psi(a)$ ni $\psi(b)$, alors $\psi^{-1}(i)$ n'est ni a ni b et dans ce cas

$$(\psi\sigma\psi^{-1})(i) = \psi\sigma\big(\psi^{-1}(i)\big) = \psi\big(\psi^{-1}(i)\big) = i. \tag{2.234}$$

Donc la décomposition $\tau = \sigma'_1 \circ \ldots \circ \sigma'_n$ est une décomposition de τ en n transpositions. Autrement dit le nombre de transpositions est le même pour τ que pour π.

En particulier les signatures de τ et de π sont les mêmes. Cela finit la preuve du point (1).

Prouvons le point (2).

(1) **Injectif** Supposons que $\varphi(\pi) = \varphi(\sigma)$. Alors pour tout $i = 1, \ldots, k-1$ nous avons

$$\pi(i+1) - 1 = \sigma(i+1) - 1, \tag{2.235}$$

c'est-à-dire $\pi(j) = \sigma(j)$ pour tout $j = 2, \ldots, k$. Vu que $\pi(1) = \sigma(1)$ nous avons bien $\pi = \sigma$.

(2) **Surjectif** Soit $\tau \in S_{k-1}$. En posant

$$\pi(i) = \begin{cases} 1 & \text{si } i = 1 \\ \tau(i-1) + 1 & \text{sinon,} \end{cases} \tag{2.236}$$

nous avons bien $\tau = \varphi(\pi)$.

□

DEFooDFBEooFElghU

Définition 2.127 ([1, 67]).
Nous notons

$$S_{(k,l)} = \{\pi \in S_{k+l} \text{ tel que } \pi(1) < \ldots \pi(k), \pi(k+1) < \ldots < \pi(k+l)\}, \tag{2.237}$$

et

$$A_{(k,l)} = \{\pi \in S_{(k,l)} \text{ tel que } \pi(1) = 1\}. \tag{2.238}$$

LEMooCKJAooBIAyVs

Lemme 2.128 ([1]).
Deux énoncés.

ITEMooCNWMooIbnHnz

(1) Soit $\pi \in A_{(k,l)}$. En posant $\tau(i) = \pi(i+1) - 1$ nous avons $\tau \in S_{(k-1,l)}$.

ITEMooKNKRooWbLYrF

(2) L'application

$$\begin{aligned} \varphi\colon A_{(k,l)} &\to S_{(k-1,l)} \\ \pi &\mapsto \Big[\tau(i) = \pi(i+1) - 1\Big] \end{aligned} \tag{2.239}$$

est une bijection.

(3) En ce qui concerne la signature, $\epsilon\big(\varphi(\pi)\big) = \epsilon(\pi)$.

Démonstration. Pour prouver (1), soit d'abord $1 \leqslant i < j \leqslant k-1$. Nous avons

$$\tau(i) = \pi(i+1) - 1 < \pi(i+j) - 1 = \tau(j) \tag{2.240}$$

parce que $i+1$ et $j+1$ sont entre 1 et k. Le même raisonnement tient pour $k+1 \leqslant i < j \leqslant k+l$.

Pour (2). Même preuve que la partie correspondante du lemme 2.126. □

2.9 Somme à valeurs dans un groupe commutatif

Si S est un ensemble fini, nous savons de la proposition 2.24 qu'il existe un unique $N \in \mathbb{N}$ pour lequel il existe une bijection $\varphi\colon \{0, \ldots, N\} \to S$. Cette bijection n'est à priori pas unique.

DEFooLNEXooYMQjRo

Lemme-Définition 2.129 ([1]).
Soient un groupe commutatif $(G, +)$ ainsi qu'un ensemble fini I contenant n éléments. Soit une application $f\colon I \to G$. Si $\sigma_1, \sigma_2\colon \{1, \ldots, n\} \to I$ sont deux bijections, alors[50]

$$\sum_{i=1}^{n} f\big(\sigma_1(i)\big) = \sum_{i=1}^{n} f\big(\sigma_2(i)\big). \tag{2.241}$$

La valeur commune est notée

$$\sum_{i \in I} f(i) \tag{2.242}$$

EQooWTTJooIJEbrV

[50] Pour rappel, le symbole $\sum_{i=1}^{n}$ est défini par 2.79.

Démonstration. Nous commençons par considérer une transposition σ (qui permute k et l avec $k<l$). Nous avons

$$\sum_{i=1}^{n} f(i) = \sum_{i=1}^{k-1} f(i) + f(k) + \sum_{i=k+1}^{l-1} f(i) + f(l) + \sum_{i=l+1}^{n} f(i) \tag{2.243a}$$

$$= \sum_{i=1}^{k-1} f(i) + f(l) + \sum_{i=k+1}^{l-1} f(i) + f(k) + \sum_{i=l+1}^{n} f(i) \tag{2.243b}$$

$$= \sum_{i=1}^{n} f\big(\sigma(i)\big). \tag{2.243c}$$

Pour cela nous avons utilisé le fait que G est commutatif pour permuter $f(l)\in G$ et $f(k)\in G$ avec $\sum_{i=k+1}^{l-1} f(i)\in G$.

Une permutation quelconque est un produit de telles transpositions (proposition 2.116). Donc pour toute permutation σ nous avons

$$\sum_{i=1}^{n} f\big(\sigma(i)\big) = \sum_{i=1}^{n} f(i). \tag{2.244}$$

□

La définition 2.129 donne lieu à un certain nombre de remarques.

(1) Elle donne la somme sur un ensemble fini. Un problème avec les ensembles infinis (outre la convergence) est l'ordre de sommation. Si vous voulez sommer sur $\mathbb{Z}$, dans quel ordre le faire ?

(2) Pour aller plus loin, et sommer sur des ensembles infinis, rendez-vous dans le thème 53.

En ce qui concerne les produits[51], nous avons cette proposition.

PROPooQMUDooQQVRIe

Proposition 2.130.
Si E est un ensemble fini et si G est un groupe commutatif, alors pour toute fonction $f\colon E\to G$ et pour toute permutation[52] σ de E,

$$\prod_{i\in E} f(i) = \prod_{i\in E} f\big(\sigma(i)\big) \tag{2.245}$$

Démonstration. C'est exactement la proposition 2.129, sauf qu'ici la loi de groupe est notée multiplicativement au lieu d'additivement. □

PROPooJBQVooNqWErk

Proposition 2.131.
Soient un groupe commutatif $(G,+)$, un ensemble fini I, une application $f\colon I\to G$ et une bijection $\sigma\colon I\to I$. Alors

$$\sum_{i\in I} f(i) = \sum_{i\in I} f\big(\sigma(i)\big). \tag{2.246}$$

Démonstration. Par définition 2.129, si $\varphi\colon\{1,\dots,n\}\to G$ est une bijection, alors

$$\sum_{i\in I} f(i) = \sum_{i=1}^{n} (f\circ\varphi)(i) \tag{2.247}$$

et

$$\sum_{i\in I} (f\circ\sigma)(i) = \sum_{i=1}^{n} (f\circ\varphi\circ\sigma)(i). \tag{2.248}$$

Vu que φ et $\varphi\circ\sigma$ sont des bijections, les deux sont égaux par le lemme 2.129. □

Si nous avons une application $L\colon S\to S$, nous notons

$$\sum_{s\in S} f\big(L(s)\big) = \sum_{s\in S} (f\circ L)(s). \tag{2.249}$$

[51] Pour le symbole de produit, c'est juste le symbole de sommation, quand la loi de groupe est notée multiplicativement. Voir 2.94.

[52] Une permutation est une bijection, définition 2.2.

Cette façon d'écrire donne une interprétation pour la notation $\sum_{g\in G} f(hg)$ qui arrive dans la proposition 2.136. Il s'agit de considérer l'application L_h du lemme 2.4, de considérer[53]

$$\sum_{g\in G} f(hg) = \sum_{g\in G} (f\circ L_h)(g) \tag{2.250}$$

EQooQQBEooFDQBVG

et de faire tourner la définition 2.129. La même chose tient pour définir $\sum_{g\in G}(gh)$ à l'aide de R_h.

LEMooGAMAooOAFhrc

Lemme 2.132 (Changement de variables dans une somme[1])**.**
Soient deux ensembles finis I, J ainsi qu'une bijection $\varphi\colon I \to J$. Soient un groupe abélien G et une application $f\colon I \to G$. Alors

$$\sum_{i\in I} f(i) = \sum_{j\in J} f\big(\varphi^{-1}(j)\big). \tag{2.251}$$

LEMooQDFLooVTwJQq

Lemme 2.133 ([1])**.**
Soit un groupe G ainsi qu'une application $f\colon E \to G$. Soient deux parties $A, B \subset E$ telles que $A \cup B = E$ et $A \cap B = \varnothing$. Alors

$$\sum_{i\in E} f(i) = \sum_{i\in A} f(i) + \sum_{i\in B} f(i). \tag{2.252}$$

LEMooNDBYooAGEkmw

Lemme 2.134.
Soit un ensemble A fini pouvant être écrit comme une union disjointe $A = \bigcup_{k=1}^{n} A_k$; nous supposons que les A_i sont non vides. Soient un groupe commutatif $(G, +)$ et une application $f\colon A \to G$. Alors

$$\sum_{a\in A} f(a) = \sum_{k=1}^{n} \sum_{a\in A_k} f(a). \tag{2.253}$$

Démonstration. Le lemme 1.76 nous indique que les parties A_k sont des ensembles finis. Nous notons

(1) $N_0 = 0$, et $N_k = \mathrm{Card}(A_k)$,

(2) $S_k = \sum_{i=1}^{k} N_k$.

(3) $\varphi_k\colon \{1, \dots, N_k\} \to A_k$, une bijection (l'existence est dans la proposition 2.24).

Nous avons $\mathrm{Card}(A) = S_n$ par le lemme 2.29(4). Nous définissons une belle bijection comme il faut :

$$\begin{aligned} \alpha\colon \{1, \dots, S_n\} &\to A \\ i &\mapsto \varphi_{k+1}(i - S_k) \end{aligned} \tag{2.254}$$

pour $i \in]S_k, S_{k+1}]$.

(1) **α est bien définie** Puisque $i > S_k$ et $i \leqslant S_{k+1}$ nous avons $i - S_k \in \{1, \dots, N_{k+1}\}$, et donc φ_{k+1} s'applique bien à $i - S_k$.

(2) **α est injective** Supposons que $\alpha(i) = \alpha(j)$. Si $i \in]S_k, S_{k+1}]$ et $j \in]S_l, S_{l+1}]$, alors $\alpha(i) = \varphi_{k+1}(i - S_k) \in A_{k+1}$ et $\alpha(j) = \varphi_{l+1}(j - S_l) \in A_{l+1}$. Vu que les A_i sont disjoints, nous avons $k = l$, et donc

$$\varphi_{k+1}(i - S_k) = \varphi_{k+1}(j - S_k). \tag{2.255}$$

Étant donné que φ_{k+1} est injective, nous avons $i - S_k = j - S_k$, ce qui montre que $i = j$.

(3) **α est surjective** Soit $a \in A$. Il existe k tel que $a \in A_k$. Nous avons donc un $s \in \{1, \dots, N_k\}$ tel que $a = \varphi_k(s)$. En posant $i = s + S_k$, nous avons bien $a = \alpha(s + S_k)$ parce que $s + S_k \in]S_{k-1}, S_k]$.

Vu que α est une bijection, nous avons l'égalité

$$\sum_{a\in A} f(a) = \sum_{i=1}^{S_n} (f\circ\alpha)(i). \tag{2.256}$$

Nous avons encore besoin d'introduire une bijection. Nous posons

$$\begin{aligned} \beta_k\colon]S_{k-1}, S_k] &\to A_k \\ i &\mapsto \varphi_k(i - S_{k-1}). \end{aligned} \tag{2.257}$$

[53] Le fait que L_h soit une bijection n'a pas d'importance ici.

C'est une bijection parce que φ_k en est une, et que $i \mapsto i - S_{k-1}$ est une bijection de $]S_{k-1}, S_k]$.

Nous pouvons maintenant terminer :

$$\sum_{a\in A} f(a) = \sum_{i=1}^{S_n} (f\circ\alpha)(i) \tag{2.258a}$$
$$= \sum_{k=1}^{n} \left(\sum_{i=S_{k-1}-1}^{S_k} (f\circ\alpha)(i) \right) \tag{2.258b}$$
SUBEQooNVKWooZqBAau
$$= \sum_{k=1}^{n} \left(\sum_{i\in]S_{k-1},S_k]} f\big(\varphi_k(i - S_{k-1})\big) \right) \tag{2.258c}$$
$$= \sum_{k=1}^{n} \left(\sum_{i\in]S_{k-1},S_k]} f\big(\beta_k(i)\big) \right) \tag{2.258d}$$
$$= \sum_{i=1}^{n} \left(\sum_{a\in A_k} f(a) \right). \tag{2.258e}$$

Justifications :

- Pour (2.258b). Associativité de la somme.

□

LEMooUWMYooIHdoeZ

Lemme 2.135 ([1])**.**
Soit un anneau $(A, +, \cdot)$. Soit un ensemble fini I et pour chaque $i \in I$ un élément $x_i \in A$. Soit encore $s \in A$. Alors nous avons

ITEMooUVAIooETyzyc

(1)

$$\sum_{i\in I} sx_i = s\sum_{i\in I} x_i. \tag{2.259}$$

ITEMooQIILooDbRnRJ

(2)

$$\sum_{i\in I} 1 = \mathrm{Card}(I). \tag{2.260}$$

Démonstration. Nous commençons par prouver (1). Soit une bijection $\varphi\colon \{1,\dots,n\} \to I$; par définition,

$$\sum_{i\in I} sx_i = \sum_{k=1}^{n} sx_{\varphi(k)}. \tag{2.261}$$

Nous allons même écrire x_k pour $x_{\varphi(k)}$. Sinon on devient fou avec les notations. Nous faisons une récurrence sur n, c'est-à-dire sur le cardinal de I :

$$\sum_{k=1}^{n+1} sx_k = \Big(\sum_{k=1}^{n} sx_k\Big) + sx_{k+1} \qquad \text{def. de } \sum \tag{2.262a}$$
$$= s\sum_{k=1}^{n} x_k + sx_{k+1} \qquad \text{hyp.rec.} \tag{2.262b}$$
$$= s\big(\sum_{k=1}^{n} x_k + x_{k+1}\big) \qquad \text{assoc.} \tag{2.262c}$$
$$= s\sum_{k=1}^{n+1} x_k \qquad \text{def. de } \sum. \tag{2.262d}$$

Et nous passons à (2). Pour cela nous utilisons la définition 2.78 avec la fonction

$$\begin{aligned} f\colon I &\to \mathbb{N} \\ i &\mapsto 1. \end{aligned} \tag{2.263}$$

Il suffit de vérifier que l'application $s(A) = \mathrm{Card}(A)$ vérifie les conditions de 2.78. D'abord $\mathrm{Card}(\varnothing) = 0$. C'est bon. Et ensuite si $K \subset I$ et si $x \notin K$ alors en utilisant 1.183(2),

$$\mathrm{Card}(K \cap \{x\}) = \mathrm{Card}(K) + 1 = \mathrm{Card}(K) + f(x). \tag{2.264}$$

□

PROPooWJQQooFINSEc

Proposition 2.136 ([1]).
Soient un groupe fini G et une fonction $f\colon G\to A$ où A est un anneau commutatif. Alors

$$\sum_{g\in G} f(g)=\sum_{g\in G} f(gh)=\sum_{g\in G} f(hg) \tag{2.265}$$

pour tout $h\in G$.

Démonstration. Nous avons une bijection $\varphi\colon\{0,\dots,N\}\to G$ garantie par la proposition 2.24. Sa définition est

$$\sum_{g\in G} f(g)=\sum_{i=0}^{N} f\big(\varphi(i)\big). \tag{2.266}$$

Par ailleurs, le lemme 2.4 donne une bijection $L_h\colon G\to G$ et permet de considérer la composée

$$\begin{aligned}\varphi'\colon\{0,\dots,N\}&\to G\\ \varphi'&=L_h\circ\varphi.\end{aligned} \tag{2.267}$$

La proposition 2.129 nous permet d'utiliser la bijection φ' au lieu de φ pour exprimer la somme $\sum_{g\in G}$. Ensuite un jeu de notation utilisant (2.250) donne

$$\begin{aligned}\sum_{g\in G} f(g)&=\sum_{i=0}^{N} f\big(\varphi(i)\big)=\sum_{i=0}^{N} f\big(\varphi'(i)\big)=\sum_{i=0}^{N}(f\circ L_h\circ\varphi)(i)\\ &=\sum_{i=0}^{N}(f\circ L_h)\big(\varphi(i)\big)=\sum_{g\in G}(f\circ L_h)(g)=\sum_{g\in G} f(hg).\end{aligned} \tag{2.268}$$

En ce qui concerne $\sum_{g\in G} f(gh)$, c'est la même chose, en utilisant R_h au lieu de L_h. □

LEMooKSVWooIFsfwm

Lemme 2.137.
Soit un groupe totalement ordonné[54] *$(A,+,\leqslant)$. Soient deux suites (a_i) et (b_i) dans G telles que $a_i\leqslant b_i$ pour tout i. Alors pour tout n nous avons*

$$\sum_{i=0}^{n} a_i\leqslant\sum_{i=0}^{n} b_i. \tag{2.269}$$

Tout cela nous permet de définir une somme sympathique et bien connue.

LEMooAWEDooErkqZw

Lemme 2.138.
Soit $n\in\mathbb{N}$. Nous avons

$$\sum_{k=0}^{n} k=\frac{n(n+1)}{2}. \tag{2.270}$$

Démonstration. La preuve est pratiquement immédiate par récurrence. Nous allons donner une preuve plus « constructive », qui formalise l'idée classique d'écrire la somme à l'endroit et à l'envers.

Nous notons S la somme $\sum_{k=0}^{n} k$. Le lemme 2.129 dit que si les $\sigma_i\colon\{0,\dots,n\}\to\{0,\dots,n\}$ sont des bijections, alors $\sum_{k=0}^{n} f\big(\sigma_1(k)\big)=\sum_{k=0}^{n} f\big(\sigma_2(k)\big)$. Nous sommes intéressé au cas $f(i)=i$.

En prenant $\sigma_1(k)=k$ et $\sigma_2(k)=n-k$, nous avons

$$S=\sum_{k=0}^{n} k=\sum_{k=0}^{n}(n-k). \tag{2.271}$$

Donc

$$2S=\sum_{k=0}^{n}\big(k+(n-k)\big)=\sum_{k=0}^{n} n=n\sum_{k=0}^{n} 1=n(n+1). \tag{2.272}$$

En divisant par deux, nous obtenons le résultat annoncé. □

[54] Définition 2.7.

2.9.1 Cardinalité d'ensembles finis

PROPooOTHMooPzPzdW

Proposition 2.139 (Cardinalité d'ensembles finis[1]).
À propos d'ensembles finis.

ITEMooBQDUooOoYhnI

(1) Si A et B sont finis et vérifient $A \cap B = \varnothing$, alors $\operatorname{Card}(A \cup B) = \operatorname{Card}(A) + \operatorname{Card}(B)$.

ITEMooUCUFooBLByHz

(2) Si I est fini et si les $(A_i)_{i\in I}$ sont des ensembles disjoints, alors

$$\operatorname{Card}\left(\bigcup_{i\in I} A_i\right) = \sum_{i\in I} \operatorname{Card}(A_i). \tag{2.273}$$

ITEMooSXBMooFgAvyJ

(3) Si A et B sont finis, alors $A \cup B$ est fini.

ITEMooKYXFooWukErM

(4) Si A et B sont finis, alors $\operatorname{Card}(A \cup B) = \operatorname{Card}(A) + \operatorname{Card}(B) - \operatorname{Card}(A \cap B)$.

ITEMooFIEUooRmDcfo

(5) Si I est un ensemble fini et si $\{A_i\}_{i\in I}$ sont des ensembles finis, alors $\bigcup_{i\in I} A_i$ est fini.

ITEMooLVSVooHEwNWA

(6) Si A et B sont finis, alors $A \times B$ est fini et

$$\operatorname{Card}(A \times B) = \operatorname{Card}(A) \operatorname{Card}(B). \tag{2.274}$$

Démonstration. En plusieurs parties.

(1) **Pour (1)** Nous considérons des bijections $\varphi\colon \{1,\dots,n\} \to A$ et $\sigma\colon \{1,\dots,m\} \to B$. Puis nous posons

$$\begin{aligned} \alpha\colon \{1,\dots,n+m\} &\to A \cup B \\ s &\mapsto \begin{cases} \varphi(s) & \text{si } s \in \{1,\dots,n\} \\ \sigma(s-n) & \text{si } s \in \{n+1,\dots,n+m\}. \end{cases} \end{aligned} \tag{2.275}$$

(1a) **σ est injective** Si $\alpha(a) = \alpha(b)$, il y a 4 possibilités suivant que a et b soient dans $\{1,\dots,n\}$ ou dans $\{n+1,\dots,n+m\}$.

(1a.i) **Si $a, b \in \{1,\dots,n\}$** Alors $\alpha(a) = \varphi(a)$ et $\alpha(b) = \varphi(b)$. Donc $\varphi(a) = \varphi(b)$ et comme φ est injective, nous avons $a = b$.

(1a.ii) **Si $a \in \{1,\dots,n\}$ et $b \in \{n+1,\dots,m+n\}$** Alors $\alpha(a) = \varphi(a) \in A$ et $\alpha(b) = \sigma(b-n) \in B$. Donc $\alpha(a) = \alpha(b) \in A \cap B$. Mais comme $A \cap B = \varnothing$, ce cas est impossible.

(1a.iii) **Les deux autres cas ...** Sont laissés au lecteur.

(1b) **α est surjective** Soit $x \in A \cup B$. Si $x \in A$ alors $x = \alpha\big(\varphi^{-1}(x)\big)$ et si $x \in B$, alors $x = \alpha\big(\sigma^{-1}(x) + n\big)$.

(2) **Pour (3)** Si $A \cap B = X$, alors nous avons l'union disjointe $A \cup B = A \cup (B \setminus A)$. Par hypothèse A est fini et par 1.76, la partie $B \setminus A$ est finie. Donc par le point (1), l'union est finie.

(3) **Pour (4)**

(4) **Pour (5)** Nous y allons par récurrence sur $\operatorname{Card}(I)$. Si $\operatorname{Card}(I) = 2$, c'est déjà fait au point (1). Sinon on suppose que la proposition est vraie pour tout choix d'ensemble I et d'ensembles $(A_i)_{i\in I}$. Nous supposons que $\operatorname{Card}(I) = n+1$ et nous considérons une bijection $\varphi\colon \{1,\dots,n+1\} \to I$. Nous avons

$$\bigcup_{i\in I} A_i = \bigcup_{k=1}^{n+1} A_{\varphi(k)} \qquad \text{cf. 1.5} \tag{2.276a}$$

$$= \bigcup_{k=1}^{n} A_{\varphi(k)} \cup A_{\varphi(n+1)}. \tag{2.276b}$$

Le premier est fini par hypothèse de récurrence et le second par hypothèse.

(5) **Pour (6)** Nous écrivons le produit $A \times B$ sous la forme

$$A \times B = \bigcup_{a\in A} \left(\bigcup_{b\in B} \{(a,b)\} \right). \tag{2.277}$$

Fixons $a \in A$. Pour $b \in B$ nous notons $A_b = \{(a,b)\}$, de telle sorte à avoir $\text{Card}(A_b) = 1$ et

$$\begin{aligned}
\text{Card}\left(\bigcup_{b\in B}\{(a,b)\}\right) &= \text{Card}\left(\bigcup_{b\in B} A_b\right) && (2.278a)\\
&= \sum_{b\in B}\text{Card}\big(\{a,b\}\big) && \text{par (2)} \quad (2.278b)\\
&= \sum_{b\in B} 1 && (2.278c)\\
&= \text{Card}(B). && \text{lem. 2.81} \quad (2.278d)
\end{aligned}$$

En posant

$$X_a = \bigcup_{b\in B}\{(a,b)\}, \tag{2.279}$$

nous venons de voir que $\text{Card}(X_a) = \text{Card}(B)$. Et comme $A \times B = \bigcup_{a\in A} X_a$, nous avons

$$\begin{aligned}
\text{Card}(A\times B) &= \sum_{a\in A}\text{Card}(X_a) && (2.280a)\\
&= \sum_{a\in A}\text{Card}(B) && (2.280b)\\
&= \text{Card}(B)\sum_{a\in A} 1 && \text{lem. 2.135} \quad (2.280c)\\
&= \text{Card}(B)\,\text{Card}(A). && (2.280d)
\end{aligned}$$

□

LEMooRURDooRIGJnY

Lemme 2.140 ([1]).
Si $\text{Card}(A) = n$ *et si* $a \in A$ *alors* $\text{Card}(A \setminus \{a\}) = n-1$.

Démonstration. Soit une bijection $\varphi\colon \{1,\dots,n\} \to A$. Nous posons $k = \varphi^{-1}(a)$. Nous posons

$$\begin{aligned}
\psi\colon \{1,\dots,n-1\} &\to A\setminus\{a\}\\
s &\mapsto \begin{cases}\varphi(s) & \text{si } s<k\\ \varphi(s+1) & \text{si } <s\geqslant k.\end{cases}
\end{aligned} \tag{2.281}$$

(1) ψ **est injective** Soient s,t tels que $\psi(s) = \psi(t)$.
Si $s < k$ et $t \geqslant k$ alors $\psi(s) = \varphi(s)$ et $\psi(t) = \varphi(t+1)$. Mais $s < k \leqslant t < t+1$, donc $s \neq t+1$ et donc $\varphi(s) = \varphi(t+1)$ est impossible.
Si $s < k$ et $t < k$ alors $\psi(s) = \varphi(s)$ et $\psi(t) = \varphi(t)$. Donc $\varphi(t) = \varphi(s)$ et donc $s = t$.
Les deux derniers cas sont du même tonneau.

(2) ψ **est surjective** Si $b \in A\setminus\{a\}$, alors $b = \varphi(s)$ pour un certain $s \neq k$. Si $s < k$ alors $b = \varphi(s) = \psi(s)$. Si $s > k$ alors $b = \varphi(s) = \psi(s-1)$ parce que si$s > k$, alors $s - 1 \geqslant k$ (proposition 1.153).

(3) ψ **prend ses valeurs dans** $A\setminus\{a\}$ Supposons que $\psi(s) = a$, c'est-à-dire $\psi(s) = \varphi(k)$. Il y a deux possibilités : $s < k$ ou $s \geqslant k$.
Si $s < k$ alors on aurait $\psi(s) = \varphi(s) \neq \varphi(k)$ parce que $s \neq k$. Donc ce cas est impossible.
Si $s \geqslant k$ alors $\psi(s) = \varphi(s+1) = \varphi(k)$. Donc $s + 1 = k$, qui est également impossible parce que $s \geqslant k$ (encore la proposition 1.153).

□

2.10 Groupes

2.10.1 Sous-groupe engendré

DefooRDRXooEhVxxu

Définition 2.141 (Sous-groupe engendré).
Soit A une partie du groupe G. Le sous-groupe ***engendré*** *par A est l'intersection de tous les sous-groupes de G contenant A. Nous notons ce groupe* $\text{gr}_G(A)$.
Lorsque A est fini (disons $A = \{a_1,\dots,a_n\}$), on note aussi le sous-groupe engendré $\langle a_1,\dots,a_n\rangle$.

2.142.
Un sous-groupe engendré n'est jamais vide parce qu'il contient toujours au moins le neutre (parce que c'est un sous-groupe). Si G est un groupe, le sous-groupe $\mathrm{gr}_G(\varnothing)$ lui-même contient e[55].

2.143.
Dans de nombreux cas, le groupe « ambiant » G est entendu par le contexte et nous noterons $\mathrm{gr}(A)$ au lieu de $\mathrm{gr}_G(A)$.

Si par exemple A est la matrice $\begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix}$, le groupe $\mathrm{gr}(A)$ est à comprendre dans $\mathrm{GL}(2,\mathbb{R})$. Il faudrait être fou pour avoir en tête un autre groupe que $\mathrm{GL}(2,\mathbb{R})$ sans le préciser.

D'ailleurs, connaissez-vous un groupe contenant la matrice A et n'étant pas un sous-groupe de $\mathrm{GL}(2,\mathbb{C})$?

Lemme 2.144.
Si G est un groupe et A une partie de G, alors $\mathrm{gr}(A)$ est un sous-groupe de G.

Le sous-groupe engendré par A est le plus petit (pour l'inclusion) groupe de G contenant A. Plus formellement, nous avons le résultat suivant :

Lemme 2.145.
Tout sous-groupe de G contenant A contient $\mathrm{gr}(A)$.

Démonstration. Si H est un sous-groupe de G contenant A, alors $\mathrm{gr}(A)$ est l'intersection de H avec tous les autres sous-groupes de G contenant A. Il contient donc $\mathrm{gr}(A)$. □

LemFUIZooBZTCiy

Lemme 2.146 ([68]).
Si A est une partie du groupe G, alors le sous-groupe $\mathrm{gr}(A)$ engendré[56] *par A est l'ensemble de tous les produits finis d'éléments de A et de A^{-1} (l'identité est le produit à zéro éléments).*

C'est-à-dire que tout élément de $\mathrm{gr}(A)$ peut être écrit sous la forme[57]

$$\prod_{i=1}^{n} g_i^{a_i} \tag{2.282}$$

où $a_i \in \mathbb{Z}$ et $g\colon \mathbb{N} \to A$ n'est pas spécialement injective : il peut arriver que $g_i = g_j$.

Démonstration. Puisqu'un produit vide est égal à l'identité[58], le lemme est vrai (un peu trivialement) dans le cas où $A = \varnothing$. À partir de maintenant, nous supposons que A est non vide.

Nous nommons $\mathrm{gr}(A)$ le groupe engendré par A et H, l'ensemble

$$H = \{g_1 \dots g_n \text{ tel que } g_i \in A \cup A^{-1}\}. \tag{2.283}$$

Nous commençons par prouver que H est un groupe.

- Puisque A est non vide, nous considérons $a \in A$. Dans ce cas, $e = aa^{-1} \in H$. Donc $e \in H$.
- L'inverse de $g_1 \dots g_n$ est $g_n^{-1} \dots g_1^{-1}$ qui est également dans H.
- Le produit de $g_1 \dots g_n$ par $h_1 \dots h_n$, tous éléments de H, est également dans H[59].

Comme H est un groupe contenant A, nous avons $\mathrm{gr}(A) \subset H$ parce que $\mathrm{gr}(A)$ est une intersection dont un des éléments est H.

Par ailleurs tout groupe contenant A doit contenir les inverses et les produits finis, donc $H \subset \mathrm{gr}(A)$.

Au final, $H = \mathrm{gr}(A)$, ce qu'il fallait. □

LEMooCFTVooKvmyKN

Lemme 2.147.
Soit un groupe G et un sous-groupe $H = \mathrm{gr}(h_1, \dots, h_n)$. Si $\alpha \in G$, alors

$$\alpha H \alpha^{-1} = \mathrm{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1}). \tag{2.284}$$

Démonstration. Il s'agit d'une conséquence du lemme 2.146. Un élément de $\mathrm{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1})$ est un produit d'éléments de G de la forme $\alpha h_i \alpha^{-1}$ ou $(\alpha h_j \alpha^{-1})^{-1} = \alpha h_j^{-1} \alpha^{-1}$. Or nous avons

$$\alpha h_i \alpha^{-1} \alpha h_j \alpha^{-1} = \alpha h_i h_j \alpha^{-1} \in \alpha H \alpha^{-1}. \tag{2.285}$$

[55] Demandez-vous si il est possible que $\mathrm{gr}(\varnothing)$ contienne d'autres éléments que e.
[56] Définition 2.141.
[57] Les a_i négatifs correspondent aux inverses. Notons que si $g \in A$, il n'y a pas de garanties que g^{-1} soit également dans A.
[58] Voir 2.94.
[59] Et c'est ici qu'on se rend compte que la décomposition n'est probablement que rarement unique.

Donc

$$\mathrm{gr}(\alpha h_1\alpha^{-1},\dots,\alpha h_n\alpha^{-1})\subset \alpha H\alpha^{-1}. \tag{2.286}$$

L'inclusion dans l'autre sens est du même tonneau. □

DEFooWMFVooLDqVxR

Définition 2.148 (Partie génératrice, groupe monogène)**.**
*Soient un groupe G, et une partie $A\subset G$. Si $\mathrm{gr}(A)=G$, alors nous disons que A est une **partie génératrice** du groupe G.*

*Un groupe est **monogène** si il a une partie génératrice réduite à un seul élément.*

DefHFJWooFxkzCF

Définition 2.149 (Groupe cyclique)**.**
*Un élément $a\in G$ est un **générateur** de G si tous les éléments de G s'écrivent sous la forme a^n pour un certain $n\in\mathbb{Z}$. Un groupe fini et monogène est dit **cyclique**.*

2.150.
La différence entre un groupe monogène et un groupe cyclique est qu'un groupe cyclique est fini. Dans un groupe cyclique, à force d'itérer le générateur, nous finissons par tourner en rond – d'où le nom.

Exemple 2.151.
Soit le groupe $\big(\mathbb{Z}/10\mathbb{Z},+\big)$. L'élément $[2]_{10}$ n'est pas générateur parce que ses puissances[60] sont

$$\mathrm{gr}([2]_{10})=\{[2]_{10},[4]_{10},[6]_{10},[8]_{10},[0]_{10}\}. \tag{2.287}$$

Par contre l'élément $[3]_{10}$ est générateur : ses puissances sont dans l'ordre

$$[3]_{10},[6]_{10},[9]_{10},[2]_{10},[5]_{10},[8]_{10},[1]_{10},[4]_{10},[7]_{10},[0]_{10}. \tag{2.288}$$

△

Un exemple presque identique, mais un peu masqué sera l'exemple 20.168.

LEMooTHBIooJPjBlp

Lemme 2.152 ([1])**.**
Si $n=dr$, alors

(1) $r\mathbb{Z}/n\mathbb{Z}$ est un groupe.

LEMooSAAXooMezYui

(2) Le groupe $r\mathbb{Z}/n\mathbb{Z}$ est cyclique[61]*.*

ITEMooGCGQooIfZULt

(3) $\mathrm{Card}(r\mathbb{Z}/n\mathbb{Z})=d=n/r$.

2.11 Groupe dérivé

DEFooVHZAooUgmesE

Définition 2.153.
*Si G est un groupe et si $g,h\in G$, nous notons $[g,h]=ghg^{-1}h^{-1}$ le **commutateur** de g et h.*

L'élément neutre est toujours un commutateur : pour $g=h$, $[g,g]=ggg^{-1}g^{-1}=e$.

DEFooBNLPooShKYXa

Définition 2.154.
*Le **groupe dérivé** de G est le sous-groupe noté $D(G)$ ou $[G,G]$ engendré*[62] *par les commutateurs.*

Autrement dit, $D(G)$ est l'intersection de tous les sous-groupes de G contenant tous les commutateurs. Le groupe $D(G)$ contient toujours au moins le neutre parce que c'est un groupe.

En vertu du lemme 2.146, le groupe dérivé de G est l'ensemble des produits finis de commutateurs. C'est-à-dire que si S_m est l'ensemble des produits de m commutateurs, alors

$$D(G)=\bigcup_{m=1}^{\infty}S_m. \tag{2.289}$$

LemMMOCooDJJJhy

Lemme 2.155.
Le groupe dérivé est un sous-groupe caractéristique[63]*, et un sous-groupe normal*[64]*.*

[60] Attention aux notations ; en général on écrit la loi de groupe de façon multiplicative et on parle des puissances d'un élément, mais ici on écrit la loi de groupe additivement, donc les « puissances » sont en réalité les multiples.
[61] Définition 2.149.
[62] Définition 2.141.
[63] Définition 2.11.
[64] Définition 2.13.

Démonstration. Il est évident que si $\alpha \in \mathrm{Aut}(G)$ alors

$$\alpha\big([g,h]\big) = \big[\alpha(g),\alpha(h)\big], \tag{2.290}$$

c'est-à-dire que $D(G)$ est un sous-groupe caractéristique. En particulier si c est un commutateur, alors xcx^{-1} en est encore un, ce qui montre que $D(G)$ est normal dans G. Plus spécifiquement,

$$x(ghg^{-1}h^{-1})x^{-1} = (xgx^{-1})(xhx^{-1})(xg^{-1}x^{-1})(xh^{-1}x^{-1}) \tag{2.291a}$$
$$= (xgx^{-1})(xhx^{-1})(xgx^{-1})^{-1}(xhx^{-1})^{-1}. \tag{2.291b}$$

□

PropAPRGooHBkELf

Proposition 2.156.
Le groupe quotient $G/D(G)$ est abélien.

Démonstration. En ce qui concerne le fait que $G/D(G)$ soit abélien, nous savons que pour tout $g,h \in G$ nous avons $h^{-1}g^{-1}hg \in D(G)$ et donc

$$[g][h] = [gh] = [ghh^{-1}g^{-1}hg] = [hg] = [h][g]. \tag{2.292}$$

□

Le groupe quotient $G/D(G)$ est appelé l'**abélianisé** de G et est parfois noté G^{ab}.

Si $f\colon G \to A$ est un morphisme entre le groupe G et un groupe abélien A, alors $f\big(D(G)\big) = \{0\}$. Du coup f passe au quotient de G par $D(G)$, et il existe une unique application $\bar{f}\colon G/D(G) \to A$ telle que $f = \bar{f} \circ \pi$ où $\pi\colon G \to G/D(G)$ est la projection canonique.

2.12 Produit semi-direct de groupes

Définition 2.157.
*Une **suite exacte** est une suite d'applications comme suit :*

$$\cdots \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \cdots \tag{2.293}$$

où pour chaque i, les applications f_i et f_{i+1} vérifient $\ker(f_{i+1}) = \mathrm{Image}(f_i)$. Lorsque les ensembles A_i sont des groupes, alors nous demandons de plus que les f_i soient des morphismes.

Très souvent nous sommes confrontés à des suites exactes de la forme

$$1 \longrightarrow A \xrightarrow{f} G \xrightarrow{g} B \longrightarrow 1 \tag{2.294}$$

où G, A et B sont des groupes, 1 est l'identité. La première flèche est l'application $\{1\} \to A$ qui à 1 fait correspondre 1. La dernière est l'application $B \to 1$ qui à tous les éléments de B fait correspondre 1. Le noyau de f étant l'image de la première flèche (c'est-à-dire $\{1\}$), l'application f est injective. L'image de g étant le noyau de la dernière flèche (c'est-à-dire B en entier), l'application g est surjective.

DEFooKWEHooISNQzi

Définition 2.158.
*Soient N et H deux groupes et un morphisme de groupes $\phi\colon H \to \mathrm{Aut}(N)$. Le **produit semi-direct** de N et H relativement à ϕ, noté $N \times_\phi H$ est l'ensemble $N \times H$ muni de la loi (que l'on vérifiera être de groupe)*

$$(n,h)\cdot(n',h') = (n\phi_h(n'), hh'). \tag{2.295}$$

EqDBgbBI

NORMooTPBGooIdQskM

2.159.
Attention à l'ordre quelque peu contre-intuitif. Lorsque nous notons $N \times_\phi H$, c'est bien $\phi\colon H \to \mathrm{Aut}(N)$, c'est-à-dire H qui agit sur N et non le contraire.

Lorsque N et H sont des sous-groupes d'un même groupe, le plus souvent ϕ est l'action adjointe définie en 5.18.

Le théorème suivant permet de reconnaitre un produit semi-direct lorsqu'on en voit un.

THOooZNYTooPhnIdE

Théorème 2.160 ([16]).
Soit une suite exacte de groupes

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{s} H \longrightarrow 1 \tag{2.296}$$

Si il existe un sous-groupe $\tilde{H}$ de G à partir duquel s est un isomorphisme, alors

$$G \simeq i(N) \times_\sigma \tilde{H} \tag{2.297}$$

où σ est l'action adjointe[65] *de $\tilde{H}$ sur $i(N)$.*

Démonstration. Nous posons $\tilde{N} = i(N)$ et nous allons subdiviser la preuve en petits pas.

(1) $\tilde{N}$ est normal dans G. En effet étant donné que la suite est exacte nous avons $\tilde{N} = \ker(s)$. Le noyau d'un morphisme est toujours un sous-groupe normal.

(2) $\tilde{N} \cap \tilde{H} = \{e\}$. L'application s étant un isomorphisme depuis $\tilde{H}$, il n'y a pas d'éléments de $\tilde{H}$ dans $\ker(s)$ autre que e. ItemzIaXGM

(3) $G = \tilde{N}\tilde{H}$. Nous considérons $g \in G$ et $h \in \tilde{H}$ tel que $s(g) = s(h)$. L'existence d'un tel h est assurée par le fait que s est surjective depuis $\tilde{H}$. Du coup nous avons $e = s(gh^{-1})$, c'est-à-dire $gh^{-1} \in \ker(s) = \tilde{N}$. Nous avons donc bien la décomposition $g = (gh^{-1})h$, et donc $G = \tilde{N}\tilde{H}$. ItemUGFjle

(4) L'écriture $g = nh$ avec $n \in \tilde{N}$ et $h \in \tilde{H}$ est unique. Si $nh = n'h'$, alors $n = n'h'h^{-1}$, ce qui signifierait que $h'h^{-1} \in \tilde{N}$. Mais étant donné que $\tilde{H} \cap \tilde{N} = \{e\}$, nous obtenons $h = h'$ et par suite $n = n'$. ItemUZlrKo

(5) L'application
$$\begin{aligned} \phi\colon G &\to \tilde{N} \times \tilde{H} \\ nh &\mapsto (n, h) \end{aligned} \tag{2.298}$$
est une bijection. C'est une conséquence des points (3) et (4).

(6) Si sur $\tilde{N} \times \tilde{H}$ nous mettons le produit
$$(n, h) \cdot (n', h') = (n\sigma_h n', hh') \tag{2.299}$$
où σ est l'action adjointe du groupe sur lui-même, c'est-à-dire $\sigma_x(y) = xyx^{-1}$, alors ϕ est un isomorphisme. Si $g, g' \in G$ s'écrivent (de façon unique par le point (5)) $g = nh$ et $g' = n'h'$ alors

$$\begin{aligned} \phi(nhn'h') &= \phi(n \underbrace{hn'h^{-1}}_{\in\tilde{N}} hh') && \text{(2.300a)} \\ &= \phi\big((nhn'h^{-1})(hh')\big) && \text{(2.300b)} \\ &= (nhn'h^{-1}, hh') && \text{(2.300c)} \\ &= (n, h) \cdot (n', h') && \text{(2.300d)} \\ &= \phi(nh)\phi(n'h'). && \text{(2.300e)} \end{aligned}$$

□ CoroGohOZ

Corolaire 2.161.
Soit G un groupe, et N, H des sous-groupes de G tels que

(1) H normalise N (c'est-à-dire que $\sigma_h(n) = hnh^{-1} \in N$ pour tout $h \in H$ et $n \in N$[66]*),*

(2) $H \cap N = \{e\}$,

(3) $HN = G$.

Alors l'application

$$\begin{aligned} \psi\colon N \times_\sigma H &\to G \\ (n, h) &\mapsto nh \end{aligned} \tag{2.301}$$

est un isomorphisme de groupes.

Démonstration. En plusieurs parties.

[65] Le fait que H agisse sur $i(N)$ fait partie du théorème.
[66] Ou encore que H agit sur N par automorphismes internes.

(1) **ψ est un morphisme** Simple calcul en utilisant la formule (2.295) du produit dans $N \times_\sigma H$:

$$\psi\big((n,h)(n',h')\big) = \psi\big(n\sigma_h(n'), hh'\big) \tag{2.302a}$$
$$= nhn'h^{-1}hh' \tag{2.302b}$$
$$= nhn'h' \tag{2.302c}$$
$$= \psi(n,h)\psi(n',h'). \tag{2.302d}$$

(2) **ψ est injective** Supposons que $\psi(n,h) = \psi(n',h')$. Alors $nh = n'h'$ et

$$n = n'h'h^{-1}. \tag{2.303}$$

En multipliant par $(n')^{-1}$ nous trouvons

$$h'h^{-1} = (n')^{-1}n \in N. \tag{2.304}$$

Donc $h'h^{-1} \in H \cap N = \{e\}$. Nous en déduisons que $h = h'$ et donc que $n = n'$.

(3) **ψ est surjective** Nous savons que $HN = G$. Soit $g \in G$. Il existe $h \in H$ et $n \in N$ tel que $g^{-1} = h^{-1}n^{-1}$. Avec ces éléments nous avons

$$g = nh = \psi(n,h). \tag{2.305}$$

□

Dans les hypothèses, l'ordre entre N et H est important lorsqu'on dit que c'est N qui agit sur H ; mais l'hypothèse $NH = G$ est équivalente à $HN = G$ (passer à l'inverse pour s'en assurer).

Insistons encore un peu sur la notation : dans $N \times_\sigma H$, c'est H qui agit sur N par σ.

2.13 Groupe de torsion

Soit G un groupe. Un élément $g \in G$ est un **élément de torsion** si il est d'ordre fini. La **torsion** de G est l'ensemble de ses éléments de torsion. Nous disons qu'un groupe est un **groupe de torsion** si tous ses éléments sont de torsion.

Exemple 2.162.
Le groupe additif $\mathbb{Q}/\mathbb{Z}$ est un groupe de torsion parce que si $[x] = [p/q]$, alors $q[x] = [p] = [0]$. △

2.14 Famille presque nulle

Soit $(G,+)$ un groupe abélien et $\mathcal{F} = \{g_i\}_{i\in I}$ une famille d'éléments de G indicés par un ensemble I. Le **support** de $\mathcal{F}$ est l'ensemble $\{i \in I \text{ tel que } g_i \neq 0\}$. La famille est dite **presque nulle** si le support est fini.

Nous disons que $\mathcal{F}$ est une **suite** si $I = \mathbb{N}$.

Chapitre 3

Anneaux

Attention aux conventions. Dans le Frido, un corps peut être réduit à $\{0\}$ et un idéal premier ne peut pas être $\{0\}$. Ces conventions ont une série de conséquences un peu partout, par exemple dans la proposition 3.90 où nous parlons d'idéal maximum propre. Comparez par exemple avec [69]. Soyez attentif.

En cas de doutes, nous suivons les conventions de Wikipédia.

3.1 Anneaux

Nous avons déjà parlé d'anneaux dans la définition 1.100.

DEFooKWKGooIOwGTA

Définition 3.1.
*Un **isomorphisme d'anneaux** est un morphisme d'anneaux*[1]*, bijectif.*

Soit X un ensemble et un anneau $(A, +, \times)$. Nous considérons $\mathrm{Fun}(X, A)$ l'ensemble des applications $X \to A$. Cet ensemble devient un anneau avec les définitions

$$(f + g)(x) = f(x) + g(x) \tag{3.1a}$$
$$(fg)(x) = f(x)g(x). \tag{3.1b}$$

C'est la **structure canonique** d'anneau sur $\mathrm{Fun}(X, A)$.

Définition 3.2.
*Le **centralisateur** de $x \in A$ dans A est l'ensemble*

$$\{y \in A \text{ tel que } xy = yx\}, \tag{3.2}$$

*le **centre** de A est*

$$\{y \in A \text{ tel que } xy = yx, \forall x \in A\}. \tag{3.3}$$

3.1.1 Idéal dans un anneau

DefooQULAooREUIU

Définition 3.3 (Idéal dans un anneau)**.**
*Un sous-ensemble $I \subset A$ est un **idéal à gauche** si*

(1) I est un sous-groupe pour l'addition,

(2) pour tout $a \in A$, $aI \subset I$.

*De même nous disons que $I \subset A$ est une **idéal à droite** lorsque I est un sous-groupe pour l'addition et $Ia \subset I$ pour tout $a \in A$.*

*Lorsqu'un ensemble est idéal à gauche et à droite, nous disons que c'est un **idéal bilatère**. Lorsque nous parlons d'idéal sans précision, nous parlons d'idéal bilatère.*

DEFooZFYSooJGZndS

Définition 3.4 (Idéaux premiers entre eux[70])**.**
Deux définitions.

*(1) Deux idéaux I et J de l'anneau A sont **premiers entre eux** si $I + J = A$.*

*(2) Des idéaux I_1,..., I_n sont **premiers dans leur ensemble** si $I_1 + \ldots + I_n = A$.*

[1] Définition 1.106.

LEMooMAHXooXSowdn

Lemme 3.5.
Les seuls idéaux d'un corps sont $\{0\}$ et le corps lui-même.

3.1.2 Idéal engendré

Démonstration. Soient un corps $\mathbb{K}$ et un idéal I dans A. Si $I = \{0\}$, c'est un idéal, pas de problèmes. Si $I \neq \{0\}$, alors $0 \in I$ parce qu'un idéal doit contenir le neutre de l'addition.

Soit $x \neq 0$ dans I. Alors pour tout $a \in \mathbb{K}$ nous avons $ax \in I$. En particulier avec $a = x^{-1}$ nous voyons que $1 \in I$. De là, $I = \mathbb{K}$ parce que si $x \in \mathbb{K}$, nous avons $x = x \cdot 1 \in xI \subset I$. □

DefSKTooOTauAR

Proposition-Définition 3.6 (Idéal engendré par un élément)**.**
Soit un anneau A et une partie $S \subset A$. Nous notons (S) l'intersection de tous les idéaux de A contenant S. C'est un idéal.

*Nous nommons (S) l'**idéal engendré** par S,*

Démonstration. Nous prouvons que (S) est un idéal. En deux parties.

(1) **Somme** Soient $a, b \in (S)$. Nous devons prouver que $a + b \in (S)$ c'est-à-dire que que si I est un idéal de A, alors $a + b \in I$. Soit donc un idéal I. Vu que $(S) \subset I$ nous avons $a, b \in I$. Et comme I est un idéal, $a + b \in I$.

(2) $a(S) \subset (S)$ Soit $a \in A$. Nous prouvons que $a(S) \subset (S)$. Soit $x \in (S)$ et un idéal I de A. Nous avons $x \in (S) \subset I$. Donc $ax \in I$.

□

PROPooDTYUooJPzPZV

Proposition 3.7 ([71, 1])**.**
Soient un anneau A et une partie $S \subset A$. L'idéal engendré par S est la partie

$$P = \{\sum_{i=1}^{r} a_i s_i b_i \text{ tel que } a_i, b_i \in A, s_i \in S\}. \tag{3.4}$$

Démonstration. Nous commençons par remarquer que P est un idéal. Ensuite nous prouvons

(1) $P \subset (S)$ Il faut montrer que P est inclus dans tous les idéaux contenant S. Soit I un tel idéal. Soit un élément $\sum_{i=1}^{r} a_i s_i b_i$ dans P. Vu que $s_i \in S \subset I$, nous avons $s_i \in I$ et donc $a_i s_i b_i \in I$.

(2) $(S) \subset P$ Nous savons que P est un idéal contenant S. Comme (S) est l'intersection de tous les idéaux contenant S, en particulier $(S) \subset P$.

□

PROPooFDJXooYbXEpo

Proposition 3.8 ([1])**.**
Soient un anneau A ainsi que $a, b, x \in A$.

ITEMooVFXMooPljoHf

(1) La partie $(a) + (b)$ est un idéal.

ITEMooMXHAooHPnAdu

(2) Si $a \in (x)$, alors $(a) \subset (x)$.

Démonstration. En deux parties.

(1) **Pour (1)** Soient $u, v \in (a) + (b)$. Nous avons $u = u_1 + u_2$ et $v = v_1 + v_2$ avec $u_1, v_1 \in (a)$ et $u_2, v_2 \in (b)$. Donc

$$u + v = (u_1 + v_1) + (u_2 + v_2) \in (a) + (b) \tag{3.5}$$

parce que $u_1 + v_1 \in (a)$ du fait que (a) est un idéal.

(2) **Pour (2)** Si $s =\in (x)$, alors la proposition 3.7 dit qu'il existe $a, b \in A$ tels que $s = axb$. Donc un élément général de (s) est de la forme $\alpha s \beta$ avec $\alpha, \beta \in A$. Mais $\alpha s \beta = \alpha a x b \beta \in (x)$.

□

LEMooSEIAooYVIvPK

Lemme 3.9 ([])**.**
Soit un anneau A.

(1) Toute union d'idéaux est un idéal.

(2) Une somme finie d'idéaux est un idéal.

LEMooHSVYooRjhGUU

Lemme 3.10 ([1]).
Soient un anneau commutatif A ainsi que $S \subset A$. Les parties

$$I = \bigcap_{s\in S} sA \tag{3.6}$$

et

$$J = \bigcup_{\alpha \text{ fini dans } S} \sum_{s\in\alpha} sA \tag{3.7}$$

sont des idéaux.

Démonstration. Nous faisons pour J. Soient $x, y \in J$. Il existe α, β finis dans S et des élements $a_s, b_s \in A$ pour chaque $s \in \alpha \cup \beta$ tels que $x = \sum_{s\in\alpha} sa_s$ et $y = \sum_{s\in\beta} sb_s$.

Nous posons $a_s = 0$ quand $s \notin \alpha$ et $b_s = 0$ lorsque $s \notin \beta$ et ensuite $\gamma = \alpha \cup \beta$. Nous avons alors

$$x + y = \sum_{s\in\gamma} s(a_s + b_s) \in J. \tag{3.8}$$

De plus si $a \in A$, alors $xa = \sum_{s\in\alpha} sAa \subset \sum_{s\in A} sA$. □

PROPooMMHPooZYzvdK

Proposition 3.11 ([72, 1]).
Soit un anneau commutatif A. Soit une partie S de A.

ITEMooJKGMooCqWYOq

(1) Un élément μ est un ppcm de S si et seulement si il est générateur de l'idéal[2] *$I = \bigcap_{s\in S} sA$.*

ITEMooZUCVooRIpnhU

(2) Si δ est un générateur de l'idéal $J = \bigcup_{\alpha \text{ fini dans } S} \sum_{s\in\alpha} sA$, alors $\delta \in \text{pgcd}(S)$.

Démonstration. En plusieurs parties.

(1) **Pour (1)** En deux parties.

(1a) $\Rightarrow$ Soit $m \in \text{ppcm}(S)$. Nous allons montrer que $\mu A = I$, et ce sera suffisant par la proposition 3.7 et le fait que A est commutatif.

(1a.i) $\mu A \subset I$ Vu que $\mu \in \text{ppcm}(S)$, pour tout $s \in S$, il existe $a_s \in A$ tel que $\mu = sa_s$. Donc $\mu A \subset sA$ pour tout $s \in S$. Autrement dit, $\mu A \subset \bigcup_{s\in S} sA = I$.

(1a.ii) $I \subset \mu A$ Soit $m \in I$. Donc m est un multiple de tout élément de S. Vu que μ est un ppcm de S, il existe $a \in A$ tel que $m = \mu a$. Et donc $m \in \mu A$, et donc $I \subset \mu A$.

(1b) $\Leftarrow$ Soit un générateur μ de I, c'est-à-dire que $\mu A = I$.

(1b.i) $S \mid \mu$. Soit $s \in S$. Vu que $\mu \in I$, nous avons $\mu \in \bigcap_{s\in S} sA$, et donc il existe $a \in A$ tel que $\mu = sa$, c'est-à-dire que $s \mid \mu$. Bref, tout élément de S divise μ.

(1b.ii) **Si $S \mid m$, alors $\mu \mid m$** Nous supposons que m est un multiple de tout élément de S. Donc pour tout $s \in S$, il existe a_s tel que $m = sa_s$. Donc $m \in I$, et donc μ divise m.

(2) **Pour (2)** Nous considérons un générateur δ de J, et nous prouvons que $\delta \in \text{pgcd}(S)$.

(2a) **δ divise S** Soit $s \in S$. Nous avons $s \in J$ et donc il existe $a_s \in A$ tel que $\delta a_s = s$. Donc $\delta \mid s$.

(2b) **Si $d \mid S$ alors $d \mid \delta$** Vu que $\delta \in J$, il existe une partie fine $\alpha \subset S$ et des $b_s \in A$ tels que $\delta = \sum_{s\in\alpha} sb_s$. En même temps, nous savons que $s = da_s$. Donc

$$\delta = \sum_{s\in\alpha} sb_s = \sum_{s\in\alpha} da_s b_s = d \sum_{s\in\alpha} a_s b_s, \tag{3.9}$$

c'est-à-dire que d divise δ.

□

[2] Lemme 3.10.

3.1.3 Autres trucs sur les idéaux

PROPooGXMRooTcUGbi

Proposition-Définition 3.12.
Soit A, un anneau, I un idéal bilatère[3] de A. Nous considérons la relation d'équivalence $x \sim y$ si et seulement si $x - y \in I$. Sur le quotient[4]

$$A/\sim = A/I, \tag{3.10}$$

nous mettons les opérations

(1) $[x] + [y] = [x + y]$

(2) $[x][y] = [xy]$.

Nous avons alors les résultats suivants :

ITEMooEJPEooRKAqmS

(1) Les opérations sont bien définies,

ITEMooYBEGooTlHgNz

(2) l'ensemble A/I, muni de ces opérations, est un anneau. Le neutre pour l'addition est $[0]$, l'inverse de $[a]$ est $[-a]$ que nous noterons $-[a]$.

ITEMooLNRLooMkoWXZ

(3) la surjection canonique $\pi : A \to A/I$ est un morphisme.

Cet anneau est appelé ***anneau quotient****.*

Démonstration. En plusieurs parties.

(1) **Pour (1)** Nous savons que, par définition,

$$\bar{x} = \{x + i \text{ tel que } i \in I\}. \tag{3.11}$$

Calculons le produit de représentants génériques de $\bar{x}$ et de $\bar{y}$:

$$(x + i_1)(y + i_2) = xy + xi_2 + yi_1 + i_1i_2. \tag{3.12}$$

Puisque I est un idéal, nous avons $xi_2 + yi_1 + i_1i_2 \in I$ et donc bien

$$(x + i_1)(y + i_2) \in \overline{xy}. \tag{3.13}$$

(2) **Pour (2)** Il s'agit de vérifier les conditions de la définition 1.100.

D'abord A/I est un groupe de neutre $[0]$. En effet, vu que $(A, +)$ est un groupe commutatif de neutre 0, nous avons

(2a) Neutre : $[a] + [0] = [a + 0] = [a]$.

(2b) Associativité : $[a] + ([b] + [c]) = [a] + [b + c] = [a + b + c] = [a + b] + [c] = \big([a] + [b]\big) + [c]$.

(2c) Inversibilité : l'inverse de $[a]$ est $[-a]$ parce que $[a] + [-a] = [a - a] = [0]$.

Nous pouvons noter $-[a]$ l'élément $[-a]$. Le groupe A/I est commutatif :

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]. \tag{3.14}$$

Donc $(A/I, +)$ est un groupe commutatif de neutre $[0]$.

L'associativité de A donne l'associativité dans A/I :

$$\big([a][b]\big)[c] = [ab][c] = [abc] = [a][bc] = [a]\big([b][c]\big). \tag{3.15}$$

Et enfin pour la distributivité,

$$[a]\big([b] + [c]\big) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]. \tag{3.16}$$

Nous avons prouvé que A/I est un anneau de neutre $[0]$ et d'unité $[1]$.

(3) **Pour (3)** Nous devons vérifier les trois conditions de la définition 1.106. Cela est immédiat parce que $\pi(x) = [x]$.

□

[3] Définition 3.3.
[4] Définition 1.56.

3.1.4 Élément irréductible et premier

DEFooZCRQooWXRalw

Définition 3.13 ([73]).
*Soit un anneau commutatif A. Un élément $p \in A$ est **premier** si il est*

(1) non nul,

(2) non inversible,

ITEMooPMTTooCVHPIm

(3) si p divise un produit ab, alors il divise soit a soit b (ou les deux).

DeirredBDhQfA

Définition 3.14 (Élément irréductible[74]).
*Un élément d'un anneau commutatif est **irréductible** si il n'est ni inversible, ni le produit de deux éléments non inversibles.*

3.15.
Nous allons voir dans la section 3.14 que le concept d'élément irréductible n'est vraiment utile que dans le cas des anneaux intègres.

Exemple 3.16.
Un corps n'a pas d'élément irréductible parce qu'à part zéro, tous les éléments sont inversibles. Mais 0 n'est pas irréductible parce qu'il peut être écrit comme produit d'éléments non inversibles : $0 = 0 \cdot 0$. △

LEMooJBUJooScsiGc

Lemme 3.17 ([1]).
Si p est irréductible et si u est inversible, alors pu est irréductible.

Démonstration. D'abord pu n'est pas inversible parce que p ne l'est pas.

Ensuite supposons que $pu = ab$. Vu que u est inversible, nous avons $p = a(bu^{-1})$. Comme p est irréductible, soit a, soit bu^{-1} est inversible.

Si c'est a, c'est gagnée. Sinon, soit k un inverse de bu^{-1} : $bu^{-1}k = 1$. Nous voyons que $u^{-1}k$ est un inverse de b. Donc b est inversible. □

PROPooKDWQooTtScrN

Proposition 3.18.
Les éléments irréductibles de l'anneau $\mathbb{Z}$ sont les nombres premiers[5].

Démonstration. Les seuls inversibles de $\mathbb{Z}$ sont ± 1.

Si p est premier et $p = ab$ avec $a, b \in \mathbb{Z}$, alors nous avons soit $a = \pm 1$ soit $b = \pm 1$. Donc p n'est pas le produit de deux éléments non inversibles.

Dans le sens inverse, supposons que p soit irréductible dans $\mathbb{Z}$. D'abord p ne peut pas être ± 1 parce que ± 1 sont inversibles. Ensuite supposons que $p = ab$. Vu que p est irréductible, nous avons $a = \pm 1$ ou $b = \pm 1$. Autrement dit, dans $p = ab$, soit a soit b est un inversible. □

3.1.5 Anneau intègre

DEFooHRRYooTmbUTH

Définition 3.19 (Éléments nilpotents, unipotents).
*On dit que $a \in A$ est **nilpotent** si il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Il est dit **unipotent** si $a - 1$ est nilpotent, c'est-à-dire si $(a-1)^n = 0$ pour un certain $n \in \mathbb{N}$.*

DEFooCIHVooAhpJxy

Définition 3.20 (Éléments inversibles).
*Un élément $a \in A$ est dit **inversible** si il existe $b \in A$ tel que $ab = 1$.*

L'ensemble $U(A)$ des éléments inversibles de A est un groupe pour la multiplication. Nous notons $A^* = A \setminus \{0\}$.

Conformément à la définition 1.109 de diviseur, nous posons la définition suivante pour les diviseurs de zéro.

DEFooCIYLooFkhVOc

Définition 3.21 (diviseur de zéro[75]).
*Un élément $a \neq 0$ est un **diviseur de zéro à gauche** si il existe $x \neq 0$ tel que $ax = 0$. L'élément a est un diviseur de zéro **à droite** si il existe $y \neq 0$ tel que $ya = 0$.*

*Nous disons que a est un **diviseur de zéro** si il est un diviseur de zéro à gauche ou à droite.*

DEFooTAOPooWDPYmd

Proposition-Définition 3.22 (Anneau intègre[1]).
Soit A un anneau non réduit à $\{0\}$. Les assertions suivantes sont équivalentes :

[5] Nombre premier, définition 3.13.

ITEMooMXMKooXMYpkN

(1) *A ne possède pas de diviseurs de zéro*[6].

ITEMooLAJCooFwxXrV

(2) *La règle du produit nul s'applique dans A : pour tous $a, b \in A$, si $ab = 0$, alors $a = 0$ ou $b = 0$.*

ITEMooQNTFooSRrVPK

(3) *On peut simplifier par un même élément non-nul, deux expressions produit dans A qui sont égales : pour tous $a, b, c \in A$ avec $a \neq 0$, si $ab = ac$, alors $b = c$.*

*Un anneau non réduit à $\{0\}$ qui vérifie ces propriétés est dit **intègre**.*

Démonstration. En trois implications.

(1) **(1) implique (2)**
Si $ab = 0$ avec $b \neq 0$ alors a est un diviseur de zéro. Vu que nous supposons que A n'a pas de diviseurs de zéros, a est nul. De même, si $a \neq 0$ b devrait être nul.

(2) **(2) implique (3)**
Si $ab = ac$, alors $a(b - c) = 0$ et l'hypothèse dit que soit $a = 0$, soit $b - c = 0$. Donc si $a \neq 0$, alors $b - c = 0$.

(3) **(3) implique (1)** Si $A = \{0\}$, le point (3) n'est pas applicable.
Si $a \neq 0$ et $ax = 0$, alors nous avons aussi $ax = a \times 0$. Par propriété de simplification, $x = 0$. Donc a n'est pas un diviseur de zéro à gauche. Nous prouvons de la même façon qu'il n'y a pas de diviseurs de zéro à droite.

□

LEMooIKNMooMfvQnu

Lemme 3.23.
Un corps est un anneau intègre[7]*. Tout corps satisfait la règle du produit nul.*

Démonstration. Nous vérifions la définition 3.22, et nous nommons $\mathbb{K}$ le corps considéré.

(1) **Pour (1)** Soit $a \in \mathbb{K}$. Si $ax = 0$ avec $x \neq 0$ alors en multipliant par x^{-1} nous trouvons $a = 0$. Donc a n'est pas un diviseur de zéro non nul.

(2) **Pour (2)** Idem à ce que nous venons de faire. Si dans $ab = 0$ l'un des deux est non nul, en multipliant par son inverse, nous trouvons que l'autre est nul.

(3) **Pour (3)** Si $ab = ac$ avec $a \neq 0$, alors il suffit de multiplier à gauche par a^{-1} (qui existe parce que nous sommes dans un corps) pour obtenir $b = c$.

□

Conséquence : dans un corps nous avons toujours la règle du produit nul, et l'élément nul n'est jamais inversible.

LEMooJNIBooAURhrt

Lemme 3.24.
Si $\mathbb{K}$ est un corps et si $a \in \mathbb{K}$ vérifie $a^2 = 1$, alors $a = \pm 1$.

Démonstration. Soit $a \in \mathbb{K}$ tel que $a^2 = 1$. Alors $a^2 - 1 = 0$. Il est facile de vérifier[8] que $(a+1)(a-1) = a^2 - 1$. Bref, on a le produit nul

$$(a + 1)(a - 1) = 0. \tag{3.17}$$

Le lemme 3.23 dit que tout corps respecte la règle du produit nul. Donc soit $a + 1 = 0$ soit $a - 1 = 0$. Donc $a \in \{1, -1\}$. □

PROPooZBTIooRhAhvg

Proposition 3.25 ([72])**.**
Soit un anneau unitaire et intègre A. Soit $p \in A$.

ITEMooJWRYooHndNpV

(1) *p est premier si et seulement si l'idéal pA est premier.*

ITEMooGHGCooRkJilg

(2) *p est irréductible si et seulement si il n'existe pas d'idéal principal I tel que $pA \subsetneq I \subsetneq A$.*

Démonstration. En plusieurs parties.

[6] Définition 3.21.
[7] Définition 3.22.
[8] Parce que tous les corps du Frido sont commutatifs.

(1) **(1)⇒**
Supposons que p est premier. Soient $a, b \in A$ tels que $ab \in pA$. En particulier $p \mid ab$, et p étant premier[9], nous avons soit $p \mid a$ soit $p \mid b$. Supposons que $p \mid a$. Il existe $k \in A$ tel que $pk = a$, et donc

$$a = pk \in pA. \tag{3.18}$$

De même si $p \mid b$ nous avons $b \in pA$.

(2) **(1)⇐**
Nous supposons que l'idéal pA est premier, et nous prouvons que p est premier. Soient $a, b \in A$ tels que $p \mid ab$. Il existe $k \in A$ tel que $pk = ab$. Donc $ab \in pA$. L'idéal pA étant premier, nus avons soit $a \in pA$ soit $b \in pA$. Donc soit $a \mid a$ soit $b \mid p$.

(3) **(2)⇒**
Supposons que p est irréductible. Soit un idéal principal I vérifiant $pA \subset I$. Nous allons montrer que soit $I = pA$ soit $I = A$. Vu que I est principal, il existe $a \in A$ tel que $I = aA$. Nous avons $pA \subset aA$, et en particulier $p \in aA$. Notons $b \in A$ un élément tel que $ab = p$.

Vu que p est irréductible, il n'est pas le produit de deux non inversibles. Donc soit a soit b est inversible.

Si a est inversible, alors $I = A$.

Si b est inversible, alors $a = pb^{-1}$, de telle sorte que $a \in pA$. De ce fait $I = pA$.

(4) **(2)⇐**
Enfin, nous supposons qu'il n'existe pas d'idéal principal I tel que $pA \subsetneq I \subsetneq A$, et nous montrons que p est irréductible. Soient $a, b \in A$ tels que $p = ab$.

Nous avons $p \in aA$ et donc $pA \subset aA$. Donc soit $aA = pA$ soit $aA = A$.

Si $aA = pA$, alors il existe $k \in A$ tel que $pk = a$. En multipliant l'égalité $ab = p$ par k nous trouvons $abk = pk = a$. Vu que A est intègre, nous pouvons simplifier par a et trouver $bk = 1$, de telle sorte que b soit inversible.

Si $aA = A$, alors a est inversible parce que $1 \in A = aA$.

□
LEMooSFHMooQoKsPV

Lemme 3.26 ([1])**.**
Soient un anneau intègre A, et une partie $S \subset A$. Si un des pgcd *de S est inversible*[10]*, alors ils le sont tous.*

Démonstration. Pour rappel, les pgcd d'une partie de A sont définis dans 1.113. Soit un pgcd inversible de S, ainsi qu'un autre pgcd que nous nommons δ'. Vu que δ' divise tous les éléments de S, il est divisé par δ : $\delta \mid \delta'$. Réciproquement, $\delta' \mid \delta$.

Soient x et y définis par $\delta = x\delta'$ et $\delta' = y\delta$. Nous avons

$$\delta = x\delta' = xy\delta. \tag{3.19}$$

Comme l'anneau A est intègre, nous pouvons simplifier par δ et voir $xy = 1$, ce qui signifie que x et y sont inversibles. Donc si δ est inversible, alors $\delta' = y\delta$ est inversible. □
LEMooMHZQooIcSNSf

Lemme 3.27 ([1, 76])**.**
Soient un anneau intègre, A, une partie $S \subset A$ et un élément $a \in A$. Nous avons[11]

$$\operatorname{pgcd}(aS) = a \operatorname{pgcd}(S). \tag{3.20}$$

Démonstration. Deux inclusions à prouver.

(1) $\operatorname{pgcd}(aS) \subset a \operatorname{pgcd}(S)$ Soit un pgcd δ de aS. Nous devons trouver un $\delta' \in \operatorname{pgcd}(S)$ tel que $\delta = a\delta'$. En termes de notations, nous notons $S = \{s_i\}_{i \in I}$. Pour chaque i nous avons $\delta \mid as_i$: il existe $x_i \in A$ tel que

$$\delta x_i = as_i. \tag{3.21}$$

Vu que a divise tous les éléments de aS, il divise n'importe quel pgcd de aS, et en particulier $a \mid \delta$: il existe $\delta' \in A$ tel que $\delta = a\delta'$. Nous montrons que $\delta' \in \operatorname{pgcd}(S)$.

[9] Définition 3.13.
[10] Définition 3.20.
[11] Définition du pgcd : 1.113.

Nous savons que $\delta x_i = as_i$. En remplaçant δ par $a\delta'$, $a\delta' x_i = as_i$. Vu que nous sommes dans un anneau intègre, nous pouvons simplifier par a (définition 3.22(3)) :

$$\delta' x_i = s_i. \tag{3.22}$$

Donc δ' divise tous les éléments de S, et vérifie la première condition pour être un pgcd de S. Pour la seconde condition, nous supposons que d divise tous les éléments de S. Nous avons $d \mid S$, donc $ad \mid aS$. Et comme δ est un pgcd de aS, nous déduisons que ad divise δ. Il existe $y \in A$ tel que

$$ady = \delta. \tag{3.23}$$

Nous remplaçons δ par sa valeur $a\delta'$: $ady = a\delta'$. Encore une fois nous simplifions par a et nous trouvons $dy = \delta'$, c'est-à-dire que δ divise δ'.

(2) $a\,\mathrm{pgcd}(S) \subset \mathrm{pgcd}(aS)$

Soit un pgcd δ de S. Nous voulons que $a\delta \in \mathrm{pgcd}(aS)$. Vu que $\delta \in \mathrm{pgcd}(S)$ nous avons $\delta x_i = s_i$ pour tout i, et donc aussi $a\delta x_i = as_i$, de telle sorte que $a\delta$ divise tous les éléments de aS.

Soit maintenant $d \in A$ divisant tous les éléments de aS. Nous devons prouver que $d \mid a\delta$.

(2a) **Travail préliminaire**

Nous considérons $\delta' \in \mathrm{pgcd}(aS)$. Vu que $\delta \mid s$ pour tout $s \in S$, nous avons aussi $a\delta \mid as$ pour tout $s \in S$. Comme δ' est un est un pgcd de aS, nous avons donc

$$a\delta \mid \delta'. \tag{3.24}$$

Soit $u \in A$ tel que $\delta' = a\delta u$.

En utilisant la première partie de la preuve, nous avons

$$\delta' \in \mathrm{pgcd}(aS) \subset a\,\mathrm{pgcd}(S). \tag{3.25}$$

Donc il existe $\delta_1 \in \mathrm{pgcd}(S)$ tel que $\delta' = a\delta_1$. En écrivant l'égalité $\delta' = a\delta u$ avec cette valeur de δ', nous trouvons

EQooVHSSooDdVUeW

$$a\delta_1 = a\delta u, \tag{3.26}$$

et donc $\delta_1 = \delta u$ parce que A est intègre. Vu que $\delta_1 \in \mathrm{pgcd}(S)$, nous avons aussi $\delta u \in \mathrm{pgcd}(S)$. En particulier δu divise tous les éléments de S, et donc divise δ qui est un pgcd de S : $\delta u \mid \delta$. En multipliant par a,

$$\delta' = a\delta u \mid a\delta. \tag{3.27}$$

(2b) **Résumé** Nous avons considéré $\delta \in \mathrm{pgcd}(S)$ et nous sommes en train de prouver que $a\delta \in \mathrm{pgcd}(aS)$. Nous avons déjà prouvé que si $\delta' \in \mathrm{pgcd}(aS)$, alors nous avons $\delta' \mid a\delta$.

Nous posons $y \in A$ tel que $\delta' y = a\delta$.

(2c) **Et enfin** Soit d divisant tous les éléments de $a\delta$. Donc $d \mid \delta'$: il existe $x \in A$ tel que $dx = \delta'$. En multipliant par y,

$$dxy = \delta' y = a\delta. \tag{3.28}$$

Nous avons montré que d divise $a\delta$, ce qu'il nous fallait.

□

LEMooZSUNooUmYmgt

Lemme 3.28 ([77]).
Soient un anneau intègre A et une partie $S \subset A$. Si $\delta \in \mathrm{pgcd}(S)$, alors $\mathrm{pgcd}(S/\delta)$ ne contient que des inversibles.

Démonstration. En utilisant le lemme 3.27, nous avons

$$\mathrm{pgcd}(S) = \mathrm{pgcd}\big(\delta(S/\delta)\big) = \delta\,\mathrm{pgcd}(S/\delta). \tag{3.29}$$

Soit $d \in \mathrm{pgcd}(S/\delta)$. Notre but est de montrer que d est inversible. D'abord

$$\delta d \in \delta\,\mathrm{pgcd}(S/\delta) = \mathrm{pgcd}(S). \tag{3.30}$$

Donc δd divise tous les éléments de S. Étant donné que δ est un pgcd de S, la définition 1.113(2) nous dit que δd divise δ. Il existe donc $d' \in A$ tel que $\delta dd' = \delta$, c'est-à-dire

$$\delta(dd' - 1) = 0. \tag{3.31}$$

Étant donné que $\delta \neq 0$ et que A est intègre nous avons $dd' - 1 = 0$ (définition 3.22(2)), c'est-à-dire $dd' = 1$. Cela montre que d' est un inverse de d, et donc que d est inversible. □

LEMooZKASooKstTuK

Lemme 3.29 ([1]).
Soit un anneau intègre A. Si $\delta \in \text{pgcd}(S)$ et si $u \in A$ est inversible, alors $\delta u \in \text{pgcd}(S)$.

Démonstration. Soit $s \in S$. Si $\delta x = s$, alors $u\delta(u^{-1}x) = s$. Donc $u\delta$ divise tous les éléments de S. De plus si $d \mid S$, alors $d \mid \delta$. Dans ce cas il existe y tel que $dy = \delta$. Nous avons alors aussi

$$dxu = \delta u, \tag{3.32}$$

de telle sorte que d divise δu. □

3.1.6 Fonction puissance

Voici une première définition de la fonction puissance. Il y en aura d'autres, de plus en plus générales. Voir le thème 52.

DEFooGVSFooFVLtNo

Définition 3.30.
Si A est un anneau, si $a \in A$ et si $n \in \mathbb{N}$, nous définissons a^n par récurrence :

ITEMooOUIPooGjAgQb

(1) $a^0 = 1$ *(l'unité pour la multiplication dans A),*

(2) $a^{k+1} = a \cdot a^k$.

Si vous n'êtes pas sûr de vous, ne citez pas le théorème 1.131. Il est indispensable pour faire fonctionner cette définition, mais vous pouvez faire comme si vous n'avez rien vu.

Le lemme suivant dit que le point (2) de la définition 3.30 aurait pu être écrit $a^k \cdot a$ au lieu de $a \cdot a^k$.

LEMooWPARooYLZlzr

Lemme 3.31 ([1]).
Si A est un anneau, si $a \in A$ et si $n \in \mathbb{N}$, alors

$$a^n = a \cdot a^{n-1} = a^{n-1} \cdot a. \tag{3.33}$$

Démonstration. Cela se prouve par récurrence. Pour $n = 1$ c'est l'égalité $a = a^0 a$ qui est correcte parce que par définition $a^0 = 1$.

Supposons que le résultat soit bon pour n et voyons ce que ça donne pour $n + 1$:

$$\begin{aligned}
a^{n+1} &= aa^n && \text{Définition de } a^{n+1} && \text{(3.34a)}\\
&= a(a^{n-1}a) && \text{hypothèse de récurrence pour } a^n && \text{(3.34b)}\\
&= (aa^{n-1})a && \text{associativité} && \text{(3.34c)}\\
&= a^n a && \text{Définition de } a^n. && \text{(3.34d)}
\end{aligned}$$

□

PROPooPLLSooUpiLKa

Proposition 3.32 ([1]).
Soit un naturel $b \in \mathbb{N} \setminus \{0\}$. Soit un naturel $m > 0$. Il existe $n \in \mathbb{N}$ tel que $b^n > m$.

3.1.7 Anneau euclidien

DefAXitWRL

Définition 3.33 (Wikipédia).
Soit A un anneau intègre[12]*. Un **stathme euclidien** sur A est une application $\alpha\colon A \setminus \{0\} \to \mathbb{N}$ tel que*

ITEMooLVJAooLpjgEz

(1) $\forall a, b \in A \setminus \{0\}$, *il existe $q, r \in A$ tel que*

$$a = qb + r \tag{3.35}$$

et $\alpha(r) < \alpha(b)$.

(2) Pour tout $a, b \in A \setminus \{0\}$, $\alpha(b) \leqslant \alpha(ab)$.

*Un anneau est **euclidien** si il accepte un stathme euclidien.*

Le stathme est la fonction qui donne le « degré » à utiliser dans la division euclidienne. La contrainte est que le degré du reste soit plus petit que le degré du dividende.

[12] Défnition 3.22.

LEMooFUSTooDCcBDb

Lemme 3.34.
L'ensemble $\mathbb{Z}$ avec les opérations usuelles est un anneau intègre[13].

ExwqlCwvV

Exemple 3.35.
Le stathme de $\mathbb{N}$ pour la division euclidienne usuelle est $\alpha(n) = n$. Si $a, b \in \mathbb{N}$ nous écrivons

$$a = qb + r \tag{3.36}$$

où q est l'entier le plus proche *inférieur* à a/b (on veut que le reste soit positif) et $r = a - qb$. Nous avons donc

$$r - b = a - b(q + 1) < a - b\frac{a}{b} = 0, \tag{3.37}$$

ce qui montre que $r < b$. △

Cet exemple ne fonctionne pas avec $\mathbb{Z}$ au lieu de $\mathbb{N}$ parce que le stathme doit avoir des valeurs dans $\mathbb{N}$. Cela ne veut cependant pas dire qu'il n'existe pas de stathme sur $\mathbb{Z}$; cela veut seulement dire que $\alpha(x) = x$ ne fonctionne pas.

3.1.8 Anneau principal et idéal premier

DEFooMZRKooBPLAWH

Définition 3.36 (Idéal principal[78])**.**
Soit un idéal[14] *I dans A.*

*(1) Il est **principal à gauche** si il existe $a \in I$ tel que $I = Aa$.*

*(2) Il est **principal à droite** si il existe $a \in I$ tel que $I = aA$.*

*(3) Nous disons qu'il est **principal** bilatère si il existe $a \in I$ tel que*

$$I = \{\sum_{i=1}^{r} x_i a y_i \text{ tel que } x_i, y_i \in A\}. \tag{3.38}$$

DEFooGWOZooXzUlhK

Définition 3.37.
*Un anneau est **principal** si*

(1) il est commutatif et intègre

(2) tous ses idéaux[15] *sont principaux*[16].

Souvent pour prouver qu'un anneau est principal, nous prouvons qu'il est euclidien (définition 3.33) et nous utilisons la proposition 3.38 qui dit qu'un anneau euclidien est principal.

Une manière de prouver qu'un anneau n'est pas principal est de prouver qu'il n'est pas factoriel, théorème 3.209.

Propkllxnv

Proposition 3.38 ([79])**.**
Tout anneau euclidien[17] *est principal*[18].

Démonstration. Soit A un anneau euclidien et α un stathme sur A. Nous considérons un idéal I non nul de A. Nous devons montrer que I est généré par un élément. En l'occurrence nous allons montrer qu'un élément $a \in I \setminus \{0\}$ qui minimise $\alpha(a)$ va générer[19] I.

Soit $x \in I$. Par construction, il existe $q, r \in A$ tels que $x = aq + r$ avec $r = 0$ ou $\alpha(r) < \alpha(a)$. Étant donné que $x, a \in I$, $r \in I$. Si $r \neq 0$, alors r contredirait la minimalité de $\alpha(a)$. Donc $r = 0$ et $x = aq$, ce qui signifie que I est principal. □

PROPooPJGLooQSrJTU

Proposition 3.39.
L'anneau $\mathbb{Z}$ est principal[20] *et euclidien*[21].

[13] Anneau intègre, définition 3.22.
[14] Idéal, définition 3.3.
[15] Idéal, définition 3.36.
[16] Définition 3.36.
[17] Euclidien, définition 3.33.
[18] Principal, définition 3.36
[19] Un tel élément existe…
[20] Définition 3.37.
[21] Définition 3.33.

Démonstration. Nous allons seulement montrer que $\alpha(x) = |x|$ est un stathme euclidien. Ainsi $\mathbb{Z}$ sera euclidien et donc principal par la proposition 3.38.

D'abord $\mathbb{Z}$ est intègre, c'est le lemme 3.34.

La condition $\alpha(b) \leqslant \alpha(ab)$ est immédiate : $|a| \leqslant |ab|$ pour tout $a, b \in \mathbb{Z}$.

Soient maintenant $a, b \in \mathbb{Z}$. Nous définissons $q_0, r_0 \in \mathbb{N}$ tels que

$$|a| = q_0|b| + r_0 \tag{3.39}$$

avec $r_0 < |b|$. Cela existe parce que $\alpha(x) = x$ est un stathme sur $\mathbb{N}$ par l'exemple 3.35.

(1) **Si $a > 0$ et $b > 0$**
Alors $a = q_0 b + r_0$ et le couple (q_0, r_0) vérifie les conditions de la définition 3.33(1).

(2) **Si $a > 0$ et $b < 0$**
Alors $a = -q_0 b + r_0$, et le couple $(-q_0, r_0)$ vérifie les conditions de la définition 3.33(1).

(3) **Si $a < 0$ et $b > 0$** Alors $a = -q_0 b - r_0$, et le couple $(-q_0, -r_0)$ vérifie les conditions de la définition 3.33(1) parce que

$$\alpha(-r_0) = r_0 < |b| = \alpha(b). \tag{3.40}$$

(4) **Si $a < 0$ et $b < 0$** Alors $a = q_0 b - r_0$, et le couple $(q_0, -r_0)$ vérifie les conditions de la définition 3.33(1).

□

3.2 Le groupe et anneau des entiers

Certes $(\mathbb{Z}, +)$ est un groupe mais en ajoutant la multiplication, $(\mathbb{Z}, +, \times)$ devient un anneau[22].

3.2.1 Division euclidienne

ThoDivisEuclide

Théorème-Définition 3.40 (Division euclidienne[80])**.**
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$, avec $0 \leqslant r < b$, tel que

$$a = bq + r. \tag{3.41}$$

*L'opération $(a, b) \mapsto (q, r)$ ainsi définie est la **division euclidienne**. Le nombre q est le **quotient** et r est le **reste** de la division de a par b.*

Démonstration. Remarquons que $r = a - bq$, et donc, une fois l'existence et l'unicité de q établie, celle de r suivra.

(1) **Unicité** Nous supposons avoir $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que

$$\begin{cases} 0 \leqslant r < b & \text{(3.42a)} \\ a = qb + r. & \text{(3.42b)} \end{cases}$$

Ce système implique que

$$0 \leqslant a - qb < b. \tag{3.43}$$

En ajoutant qb dans les trois membres de cette inégalité,

$$qb \leqslant a < (q + 1)b. \tag{3.44}$$

Cela implique que

$$q = \max\{k \in \mathbb{Z} \text{ tel que } kb \leqslant a\}. \tag{3.45}$$

Donc q est unique et la relation $a = bq + r$ implique que r est également unique.

Soit

$$E = \{q \in \mathbb{Z} | bq \leqslant a\}.$$

La partie E est non vide (parce qu'elle contient $-|a|$) et admet un majorant : l'élément $|a|$. Elle admet donc un maximum q par le lemme 1.206. Ce maximum vérifie

$$bq \leqslant a < b(q + 1). \tag{3.46}$$

Cela donne $0 \leqslant a - bq < b$ et le résultat, en posant $r = a - qb$.

[22] Définition 1.100.

□

Le lemme suivant est souvent pris pour la définition d'un nombre premier lorsqu'on parle de $\mathbb{N}$ ou $\mathbb{Z}$.

Lemme 3.41 ([81, 1]).
Dans $\mathbb{N}$, un nombre est premier si et seulement si il admet exactement deux diviseurs entiers distincts.

Démonstration. En deux parties.

(1) $\Rightarrow$ Soit un élément premier $p \in \mathbb{N}$. Il y a trois possibilités : $p = 0$, $p = 1$ et $p > 1$.

Le nombre $p = 0$ n'est pas premier parce qu'il est nul. Le nombre $p = 1$ n'est pas premier parce qu'il est inversible. Donc nous savons que si p est premier, alors $p > 1$.

Un élément $p > 1$ dans $\mathbb{N}$ a toujours au moins deux diviseurs distincts : 1 et p. Soit un diviseur k de p. Il existe $l \in \mathbb{N}$ tel que $p = kl$. Vu que p est premier et divise le produit kl, il divise k ou l. Disons que p divise k. De cette façon p divise k et k divise p.

Il existe donc $n \in \mathbb{N}$ tel que $k = np$. En y substituant $p = kl$, on trouve $k = np = nkl$. En simplifiant par k, il vient

$$1 = nl, \tag{3.47}$$

ce qui prouve que $n = l = 1$ et donc que $k = p$ et donc que p n'a pas d'autres diviseurs que 1 et p.

(2) $\Leftarrow$ Nous supposons que $p \in \mathbb{N}$ ait exactement deux diviseurs entiers distincts. Nous vérifions que p vérifie les trois conditions de la définition 3.13.

(2a) $p \neq 0$ parce que 0 a nettement plus que deux diviseurs distincts.

(2b) $p \neq 1$ parce que 1 a exactement un diviseur. Donc p n'est pas inversible dans $\mathbb{N}$.

(2c) Soit p admettant exactement deux diviseurs distincts. Soit p divisant le produit ab' pour certains a et b' dans $\mathbb{N}$. Nous supposons que p ne divise pas a, et nous allons prouver que p divise b' en supposant d'abord que p ne divise pas b'.

(2c.i) **Un ensemble** Pour cela nous posons

$$E = \{x \in \mathbb{N} \text{ tel que } p \mid ax, p \nmid x\}. \tag{3.48}$$

Nous posons $b = \min(E)$. Nous avons pour hypothèse que E est non vide ; en particulier $0 < b$.

(2c.ii) $b < p$ On vérifie que si $p + k \in E$ alors $k \in E$. Donc b ne peut pas être plus grand que p. Vu que p lui-même n'est pas dans E, nous avons $b < p$.

(2c.iii) **Division euclidienne** Nous effectuons la division euclidienne du théorème 3.40 :

$$p = mb + r. \tag{3.49}$$

En multipliant par a, $ar = ap - mab$. Vu que ab est un multiple de p $ap - mab$ est un multiple de p. En particulier ar est divisible en p.

(2c.iv) **La contradiction** Nous avons donc $r \in E$, alors que $r < b$. Impossible.

□

PROPooWMNPooZdvOBt

Proposition 3.42 ([82]).
Dans un anneau intègre[23] tout élément premier est irréductible[24].

Démonstration. Soit p, un élément premier dans un anneau intègre A.

(1) p **n'est pas inversible** Cela fait partie de la définition d'un élément premier.

(2) p **n'est pas un produit d'inversibles** Soient $a, b \in A$ tels que $p = ab$. Par le point (3) de la définition 3.13, p divise soit a soit b. Supposons que p divise a. Alors il existe $x \in A$ tel que $a = px$. En remettant dans $p = ab$ nous avons :

$$p = pxb. \tag{3.50}$$

EQooPYBGooLFHMJZ

Mais l'anneau est intègre et permet donc des simplifications par tout élément non nul. La relation 3.50 donne donc

$$1 = xb, \tag{3.51}$$

ce qui signifie que b est inversible.

Un travail similaire montre que a est inversible si p divise b.

[23] Si pas intègre, voir l'exemple 3.44.
[24] Toutes les définitions dans le thème 6.

□

Exemple 3.43.
Si nous avons l'égalité $7 = ab$ dans $\mathbb{Z}$, alors soit a soit b vaut 1. Mettons $a = 1$. Dans ce cas, $b = 7$ et n'est donc pas inversible. △

Sur un anneau non intègre, la notion d'élément premier n'est pas aussi intéressante que sur un anneau intègre. Par exemple la proposition 3.42 devient fausse.

EXooEIUEooCZCPMC

Exemple 3.44.
Soit l'anneau $\mathbb{Z}^2$. L'élément $(1,0)$ est premier mais pas irréductible.

(1) $(1,0)$ **est premier** L'élément $(1,0)$ est non nul ; ça c'est pas cher. Pour qu'il soit inversible, il faudrait $(1,0)(x,y) = (1,1)$. Entre autres, $0 \times y = 1$, ce qui est impossible. Donc il n'est pas inversible.

Supposons que $(1,0)$ divise le produit $(a,b)(c,d) = (ac,bd)$. Alors il existe (x,y) tel que $(1,0)(x,y) = (ac,bd)$. Cela signifie que $x = ac$ et $0 \times y = bd$. En particulier, soit $b = 0$ soit $d = 0$. Si $b = 0$, nous avons $(a,b) = (a,0)$ et effectivement, $(1,0)$ le divise.

(2) $(1,0)$ **n'est pas irréductible** Nous avons $(1,0) = (1,0)(1,0)$. Donc l'élément $(1,0)$ est le produit de deux éléments non inversibles.

△

3.2.2 Sous-groupes de $(\mathbb{Z},+)$

PropSsgpZestnZ

Proposition 3.45 (liste des sous groupes de $\mathbb{Z}$)**.**
À propos de sous-groupes de $\mathbb{Z}$.

(1) Une partie H du groupe $(\mathbb{Z},+)$ est un sous-groupe si et seulement si il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.
ITEMooOWNZooUsYRok

(2) Si H est un sous-groupe de $(\mathbb{Z},+)$, il existe un unique n tel que $H = n\mathbb{Z}$.

Démonstration. Soit $H \neq \{0\}$ un sous-groupe de $\mathbb{Z}$. L'ensemble $H \cap \mathbb{N}^*$ contient un élément minimum que nous notons n. Nous avons certainement $n\mathbb{Z} \subset H$ parce que H est un groupe (donc $n+n$ et $-n$ sont dans H dès que n est dans H). Nous devons prouver que $H \subset n\mathbb{Z}$.

Si $x \in H$, par le théorème de division euclidienne 3.40, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$, uniques, tels que $x = nq + r$ et $0 \leqslant r < n$. Nous savons déjà que $nq \in H$, donc $r = x - nq \in H$. Le nombre r est donc un élément de H strictement plus petit que n. Mais nous avions décidé que n serait le plus petit élément de $H \cap \mathbb{N}^*$. Par conséquent $r = 0$ et $x = nq \in n\mathbb{Z}$.

En ce qui concerne l'unicité, supposons que $n\mathbb{Z} = m\mathbb{Z}$. Le nombre n divise m (parce que $m \in m\mathbb{Z} \subset n\mathbb{Z}$) et le nombre m divise n parce que $n \in m\mathbb{Z}$. Par conséquent $n = m$. □

3.2.3 Théorème de Bézout

Une généralisation de Bézout 3.46 à plus de 2 variables et dans un anneau principal : proposition 3.200.

ThoBuNjam

Théorème 3.46 (Théorème de Bézout[25][83], thème 3)**.**
Si $\{a_i\}_{i=1,\dots,N}$ sont des entiers non nuls. Nous avons $\operatorname{pgcd}(a1,\dots,a_N) = 1$ *si et seulement si il existe $u_1,\dots,u_N$ tels que*

$$\sum_i a_i u_i = 1. \tag{3.52}$$

Démonstration. En deux parties.

(1) $\Rightarrow$ Soit $E = \{\sum_{i=1}^N a_i u_i \text{ tel que } u_i \in \mathbb{Z}\}$. Cet ensemble est non vide. Il contient par exemple a_1. Nous posons $m = \min\big(E \setminus \{0\}\big)$, et nous considérons des $v_i \in \mathbb{Z}$ tels que

$$m = \sum_j a_j v_j. \tag{3.53}$$
EQooQSJLooOGbTzx

Nous prouvons à présent que m divise tous les a_i. Nous nous fixons $i \in \{1,\dots,N\}$ et nous considérons la division euclidienne[26] $a_i = mq + r$ avec $0 \leqslant r < m$. En remplaçant dedans la valeur de m de (3.53)

[25] Il y a une super application ici : https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/mauvais_prix.pdf.
[26] Théorème 1.181.

nous trouvons $a_i = \sum_j a_j v_j q + r$, et en isolant r :

$$r = a_i - \sum_j a_j v_j q = a_i(1 - v_i q) - \sum_{j \neq i} a_j v_j q \in E. \tag{3.54}$$

Mais comme $0 \leqslant r < m$ et $r \in E$ et $m = \min(E \setminus \{0\})$ nous avons $r = 0$, ce qui signifie que m divise a_i.

Donc $m = 1$ parce que 1 est le seul diviseur commun des tous les a_i. Donc $1 \in E$, ce qu'il fallait démontrer.

(2) $\Leftarrow$ Supposons qu'il existe des nombres u_i tels que $\sum_i a_i u_i = 1$. Si δ divise tous les a_i, alors il existe v_i tels que $a_i = \delta v_i$ et donc tels que

$$\sum_i a_i u_i = \sum_i \delta v_i u_i = \delta \sum_i v_i u_i, \tag{3.55}$$

ce qui montre que $\delta \mid 1$ et donc que $\delta = 1$. Nous avons démontré que 1 est le seul diviseur commun des tous les a_i.

□

CorgEMtLj

Corolaire 3.47.
Soient p et q deux entiers premiers entre eux. Alors

$$p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}; \tag{3.56}$$

en particulier, pour tout $x \in \mathbb{Z}$, il existe u_x, v_x entiers tels que $u_x p + v_x q = x$.

Démonstration. Soit $x \in \mathbb{Z}$. Le théorème de Bézout nous donne k et l tels que $kp + lq = 1$. Alors, $(xk)p + (xl)q = x$. □

Notons que l'application $p\mathbb{Z}+q\mathbb{Z}$ vers $\mathbb{Z}$ n'est évidemment pas injective : les u_x et v_x ne sont pas uniques à x fixé, car si $\alpha p + \beta q = x$, alors $(\alpha + kq)p + (\beta - kp)q = x$ pour tout $k \in \mathbb{Z}$.

CORooLINXooBlUKPG

Corolaire 3.48.
Les groupes quotients du groupe $(\mathbb{Z}, +)$ sont $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Tous les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$. En effet en vertu de la proposition 3.45, les seuls sous-groupes de $\mathbb{Z}$ (en tant que groupe additif) sont les $n\mathbb{Z}$. Tous les idéaux sont donc de cette forme. De plus les $n\mathbb{Z}$ sont effectivement tous des idéaux[27] : si $a \in n\mathbb{Z}$ et si $k \in \mathbb{Z}$ alors $ak \in n\mathbb{Z}$. □

PropZpintssiprempUzn

Proposition 3.49.
Soient $n \geqslant 2$ un entier et $\phi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. Nous noterons $\overline{a} = \phi(a)$. Alors l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donné par

$$U(\mathbb{Z}/n\mathbb{Z}) = \phi(P_n) = \{\overline{x} \text{ tel que } 0 \leqslant x \leqslant n \text{ tel que } \operatorname{pgcd}(x, n) = 1\}. \tag{3.57}$$

où P_n est l'ensemble $P_n = \{x \in \{0, \dots, n-1\} \text{ tel que } \operatorname{pgcd}(x, n) = 1\}$.
De plus,

$$\operatorname{Card}\big(U(\mathbb{Z}/n\mathbb{Z})\big) = \phi(n). \tag{3.58}$$

Démonstration. Soit $0 \leqslant x \leqslant n$ tel que $\operatorname{pgcd}(x, n) = 1$. Il existe donc[28] $u, v \in \mathbb{Z}$ tels que $ux + vn = 1$. En passant aux classes,

$$\overline{ux} = \overline{1}, \tag{3.59}$$

donc $\overline{u}$ est l'inverse de $\overline{x}$. Cela prouve que $\phi(P_n) \subset U(\mathbb{Z}/n\mathbb{Z})$.

Nous prouvons maintenant l'inclusion inverse. Soient $\overline{x}$ et $\overline{y}$ inverses l'un de l'autre : $\overline{xy} = \overline{1}$. Il existe donc $q \in \mathbb{Z}$ tel que $xy - qn = 1$, ce qui prouve[29] que $\operatorname{pgcd}(x, n) = 1$. □

[27] Définition 3.3.
[28] Théorème de Bézout 3.46
[29] À nouveau avec le Théorème de Bézout.

3.2.4 PGCD, PPCM

Puisque $\mathbb{Z}$ est un anneau intègre, nous avons la définition 1.113 de pgcd et de ppcm.

PROPooAVRGooUfhjwF

Proposition 3.50 (PPCM et PGCD)**.**
Soient $p, q \in \mathbb{Z}^*$.

(1) Le pgcd de p et q est le plus grand diviseur commun de p et q.

(2) Le ppcm de p et q est leur plus petit multiple commun.

Démonstration. Démontrons le premier point. Notons δ le pgcd de p et q. Si d est un diviseur commun de p et q, alors d divise δ. Dans $\mathbb{Z}$, $d \mid \delta$ implique $d \leqslant \delta$ (proposition 1.209). □

Lemme 3.51.
Soient $p, q \in \mathbb{Z}^*$. Les entiers $\operatorname{ppcm}(p,q)$ *et* $\operatorname{pgcd}(p,q)$ *fournissent les isomorphismes de groupes suivants :*

$$p\mathbb{Z} \cap q\mathbb{Z} = \operatorname{ppcm}(p,q)\mathbb{Z} \tag{3.60a}$$
$$p\mathbb{Z} + q\mathbb{Z} = \operatorname{pgcd}(p,q)\mathbb{Z}. \tag{3.60b}$$

DEFooXSPFooPumQSy

Définition 3.52.
Nous disons que deux éléments d'un anneau principal[30] *sont* ***premiers entre eux*** *si leurs diviseurs communs sont inversibles.*

Vu que $\mathbb{Z}$ est un anneau principal (proposition 3.39), la définition 3.52 d'éléments premiers entre eux s'applique.

LEMooLKLTooXUdsgB

Lemme 3.53.
Dans $\mathbb{Z}$, les nombres p et q sont premiers entre eux si et seulement si $\operatorname{pgcd}(p,q) = 1$.

DefZHRXooNeWIcB

Définition 3.54.
Soit un anneau A. Nous disons que les éléments $a_1, \dots, a_n$ sont Si nous avons un ensemble d'entiers a_i, nous disons qu'ils sont premiers ***dans leur ensemble*** *si*

$$\operatorname{pgcd}(a_1, \dots, a_n) = 1. \tag{3.61}$$

Les nombres 2, 4 et 7 ne sont pas premiers deux à deux (à cause de 2 et 4), mais ils sont premiers dans leur ensemble parce qu'il n'y a pas de diviseurs communs plus grand que 1, au triplet $(2, 4, 7)$.

La proposition suivante établit que si x est assez grand, alors il peut même être écrit comme une combinaison de p et q à coefficients positifs. Elle sera utilisée pour démontrer que les états apériodiques d'une chaine de Markov peuvent être atteints à tout moment (assez grand), voir la définition 40.33 et ce qui suit.

PropLAbRSE

Proposition 3.55.
Soient a et b deux éléments de $\mathbb{N}$ premiers entre eux. Il existe $N > 0$ tel que tout $x > N$ appartient à $a\mathbb{N} + b\mathbb{N}$.

Démonstration. Soient a et b, premiers entre eux, et $x \in \mathbb{N}$. Disons tout de suite, pour éviter les cas triviaux et pénibles, que x, a et b sont strictement positifs.

(1) **Une décomposition pour x**

On applique le théorème 3.40 de division euclidienne à x et $a+b$: il existe des entiers p_x, r_x, uniques, tels que

$$\begin{cases} x = (p_x - 1)(a+b) + r_x & \text{(3.62a)} \\ 0 \leqslant r_x < a + b. & \text{(3.62b)} \end{cases}$$

En d'autres termes, $p_x(a+b)$ est le premier multiple de $a+b$ supérieur ou égal à x. De plus, p_x est strictement positif car x l'est. Il existe alors des entiers u et v tels que

$$ua + vb = p_x(a+b) - x \tag{3.63}$$

EQooXYSZooJqxPui

par le corolaire 3.47. Ainsi, x peut s'écrire

$$x = (p_x - u)a + (p_x - v)b. \tag{3.64}$$

[30] Anneau principal, définition 3.37.

(2) **Des maximums**

Il s'agit maintenant de savoir si nous pouvons être assuré d'avoir $p_x > u$ et $p_x > v$ dès que x est assez grand. Pour cela, grâce au corolaire 3.47, nous considérons les nombres u_i et v_i définis par

$$u_i a + v_i b = i \tag{3.65}$$

pour $i = 1, \ldots, a + b$. Nous posons $u^* = \max\{u_i\}$, $v^* = \max\{v_i\}$, et $p^* = \max\{u^*, v^*\}$. Nous posons alors $N = p^*(a + b)$, et considérons $x > N$.

(3) **Nouvelle décomposition pour x**

Nous voulons écrire

$$x = (p_x - u_k)a + (p_x - v_k)b \tag{3.66}$$

EQooIKNWooBKJtYz

pour un certain k. Cela demande $u_k a + v_k b = ua + vb = p_x(a + b) - x$ par l'équation (3.63). Vu que $p_x(a + b) - x > 0$, les nombres u_k et v_k existent : il suffit de prendre $k = p_x(a + b) - x$.

(4) **Conclusion**

Avec tous ces choix, nous avons d'abord $x > p^*(a + b)$ et donc

$$x = (p_x - 1)(a + b) + r_x > p^*(a + b), \tag{3.67}$$

ce qui donne

$$(p_x - 1)(a + b) > p^*(a + b) - r_x > (p^* - 1)(a + b). \tag{3.68}$$

ou encore $p_x > p^*$. Nous avons finalement

$$p_x \geqslant p^* \geqslant u^* \geqslant u_k \tag{3.69}$$

et

$$p_x \geqslant p^* \geqslant v^* \geqslant v_k. \tag{3.70}$$

De ce fait, la décomposition (3.66) est celle que nous voulions.

□

3.56.
Une méthode pour obtenir les entiers naturels u et v qui permettent la décomposition $x = au + bv$ est d'abord de choisir u_0 et v_0 tels que au_0 et bv_0 soient les plus proches possibles de $x/2$, puis de décomposer le nombre (relativement petit) $x - au_0 - bv_0$ en $au_1 + bv_1$. Deux nombres u et v qui fonctionnent sont alors $u = u_0 + u_1$ et $v = v_0 + v_1$.

Exemple 3.57.
Écrivons $1000 = u \cdot 7 + v \cdot 5$ avec $u, v \in \mathbb{N}$. D'abord $72 \cdot 7 = 504$ et $100 \cdot 5 = 500$. Nous avons donc

$$1004 = 72 \cdot 7 + 100 \cdot 5. \tag{3.71}$$

Ensuite $4 = 25 - 21 = -3 \cdot 7 + 5 \cdot 5$. Au final,

$$1000 = 75 \cdot 7 + 95 \cdot 5. \tag{3.72}$$

△

3.2.5 Décomposition en facteurs premiers

LemPRuUrsD

Lemme 3.58 (Lemme de Gauss)**.**
Soient $a, b, c \in \mathbb{Z}$ tels que a divise bc. Si a est premier avec c, alors a divise b.

Démonstration. Puisque a est premier avec c, nous avons $\text{pgcd}(a, c) = 1$ et le théorème de Bézout 3.46 nous donne donc $s, t \in \mathbb{Z}$ tels que $sa + tc = 1$. En multipliant par b, nous avons $sab + tbc = b$. Mais les deux termes du membre de gauche sont multiples de a parce que a divise bc. Par conséquent b est somme de deux multiples de a et donc est multiple de a. □

Il y a une généralisation du lemme de Gauss pour les anneaux principaux dans 3.201.

LemAXINooOeuMJZ

Lemme 3.59 (Lemme d'Euclide[84])**.**
Soient $a, b \in \mathbb{Z}$. Si le nombre premier p divise le produit ab, alors p divise a ou b.

Démonstration. Comme p est premier, si il ne divise pas a c'est que $\text{pgcd}(a,p)=1$. Dans ce cas le lemme de Gauss 3.58 implique que p divise b. □

LEMooSRFMooHgEMwj

Lemme 3.60.
Soient $a,b\in\mathbb{N}$ tels que a divise b et b divise a. Alors $a=b$.

LEMooFVSJooRysGAm

Lemme 3.61 ([1])**.**
Soient $k,n,p\in\mathbb{Z}$. Le nombre kp divise kn si et seulement si p divise n.

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que $kp\mid kn$. Il existe $l\in\mathbb{Z}$ tel que $kpl=kn$. On peut simplifier par k : $pl=n$, ce qui signifie que $p\mid n$.

(2) $\Leftarrow$ Si $p\mid n$, alors il existe l tel que $lp=n$. Avec ça, $kn=klp$, et donc $kp\mid kn$.

□

Le théorème fondamental de l'arithmétique permet de décomposer des nombres en facteurs premiers.

ThoAJFJooAveRvY

Théorème 3.62 (Décomposition en facteurs premiers[85])**.**
Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

En d'autres termes, pour tout entier $n>1$, il existe une unique suite finie unique $(p_1,k_1),\ldots(p_r,k_r)$ telle que :

(1) les p_i sont des nombres premiers tels que, si $i<j$, alors $p_i<p_j$;

(2) les k_i sont des entiers naturels non nuls ;

(3) $n=\prod_{i=1}^{r}p_i^{k_i}$.

Démonstration. Soit n un entier positif. Nous prouvons l'existence d'une décomposition en facteurs premiers par récurrence. Le nombre $n=1$ est le produit d'une famille finie de nombres premiers : la famille vide[31].

Supposons que tout entier strictement inférieur à un certain entier $n>1$ est produit de nombres premiers. Deux possibilités apparaissent pour n : il est premier ou non. Si n est premier, et donc produit d'un unique entier premier, à savoir lui-même, le résultat est vrai. Si n n'est pas premier, il se décompose sous la forme kl avec k et l strictement inférieurs à n. Dans ce cas, l'hypothèse de récurrence implique que les entiers k et l peuvent s'écrire comme produits de nombres premiers. Leur produit aussi, ce qui fournit une décomposition de n en produit de nombres premiers. Par application du principe de récurrence, tous les entiers naturels peuvent s'écrire comme produit de nombres premiers.

Nous prouvons maintenant l'unicité. Prenons deux produits de nombres premiers qui sont égaux. Prenons n'importe quel nombre premier p du premier produit. Il divise le premier produit, et, de là, aussi le second. Par le lemme d'Euclide 3.59, p doit alors diviser au moins un facteur dans le second produit. Mais les facteurs sont tous des nombres premiers eux-mêmes, donc p doit être égal à un des facteurs du second produit. Nous pouvons donc simplifier par p les deux produits. En continuant de cette manière, nous voyons que les facteurs premiers des deux produits coïncident précisément. □

LEMooDTQQooYoJABt

Lemme 3.63 ([1])**.**
Nous notons $\mathcal{P}$ l'ensemble des nombres premiers dans $\mathbb{N}$. Soient des suites finies $(a_p)_{p\in\mathcal{P}}$ et $(b_p)_{p\in\mathcal{P}}$. Nous posons

$$a=\prod_{p\in\mathcal{P}}p^{a_p}\qquad\text{et}\qquad b=\prod_{p\in\mathcal{P}}p^{b_p}.\tag{3.73}$$

Alors $a\mid b$ si et seulement si $a_p\leqslant b_p$ pour tout p.

Démonstration. Dire que $a\mid b$ signifie qu'il existe $s\in\mathbb{N}$ tel que $as=b$; le théorème 3.62 nous permet de décomposer s en $s=\prod_{p\in\mathcal{P}}p^{s_p}$. Puisque le produit dans $\mathbb{N}$ est commutatif et associatif,

$$b=as=\prod_{p\in\mathcal{P}}p^{s_p+a_p}.\tag{3.74}$$

Par unicité de la décomposition de b (toujours le théorème 3.62), nous en déduisons que $b_p=s_p+a_p\geqslant a_p$.

[31] Voir 2.94.

Dans l'autre sens, l'hypothèse $a_p \leqslant b_p$ implique l'existence de $s_p \geqslant 0$ tels que $b_p = a_p + s_p$. En posant $s = \prod_{p\in\mathcal{P}} p^{s_p}$, nous avons

$$as = \prod_{p\in\mathcal{P}} p^{s_p+a_p} = \prod_{p\in\mathcal{P}} p^{b_p} = b. \tag{3.75}$$

Donc $a \mid b$. □

LEMooGLZHooUcRNgu

Lemme 3.64.
Soient un nombre premier q ainsi que $a \in \mathbb{Z}$. Soit un entier $n \geqslant 1$. Le nombre q divise a si et seulement si il divise a^n.

Démonstration. Nous numérotons les nombres premiers p_i pour que p_1 soit q. La décomposition en nombre premiers du théorème 3.62 nous dit que

$$a = q^{a_1} \prod_{i\neq 1} p_i^{a_i} \tag{3.76}$$

et

$$a^n = q^{na_1} \prod_{i\neq 1} p_i^{na_i} \tag{3.77}$$

Nous avons équivalence entre les énoncés suivants :

- q divise a
- $a_1 \neq 0$
- $na_1 \neq 0$ (parce que $n \neq 0$)
- q divise a^n.

□

CORooWBSQooQOEmaC

Corolaire 3.65.
Si $n \in \mathbb{N}$ n'est pas une puissance d'un nombre premier, alors il existe $a, b \in \mathbb{N}$ tels que $\text{pgcd}(a, b) = 1$ et $n = ab$.

Démonstration. Si n n'est pas une puissance d'un nombre premier, alors le théorème 3.62 de décomposition en nombres premiers dit que

$$n = \prod_{i=1}^{r} p_i^{k_i} \tag{3.78}$$

avec au moins $r = 2$, et les k_i non nuls. En prenant $a = p_1^{k_1}$ et $b = \prod_{i=2}^{r} p_i^{k_i}$ nous avons bien $n = ab$. Montrons que a et b n'ont pas de diviseurs communs. Soit, par l'absurde, q un diviseur premier commun à a et b.

Vu que q divise $p_1^{k_1}$, le nombre q divise p_1 par le lemme 3.64. Étant donné que q divise $\prod_{i=2}^{r} p_i^{k_i}$, il divise au moins un des facteurs (lemme d'Euclide 3.59). Disons que q divise $p_i^{k_i}$. Dans ce cas q divise p_i.

Donc q divise p_i et p_1 et donc $q = 1$ parce que p_i et p_1 sont des nombres premiers distincts. □

3.2.6 Double comptage

Lorsqu'on veut compter le nombre d'éléments d'un ensemble, il arrive souvent d'entendre « nous partitionnons cet ensemble en telles parties, mais ce faisant nous avons compté chaque élément 3 fois. Donc on doit diviser par 3 ». Cela arrive très souvent en combinatoire et dans les problèmes de dénombrement. La proposition suivante est ce qui se cache derrière ce raisonnement.

PROPooURPFooYSdyKW

Proposition 3.66 ([1])**.**
Soit un ensemble $A = \{a_1, \dots, a_n\}$. Nous considérons des parties $A_j \subset A$ $(j = 1, \dots, s)$ telles que

(1) $\bigcup_{j=1}^{s} A_j = A$,

(2) Pour chaque $a \in A$, nous avons $\text{Card}\{j \text{ tel que } a \in A_j\} = k$, c'est-à-dire que chaque élément de A se trouve dans exactement k des parties A_j.

Alors

$$\text{Card}(A) = \frac{1}{k} \sum_{j=1}^{s} \text{Card}(A_j). \tag{3.79}$$

Démonstration. Nous allons mettre les éléments de A un par un dans un ensemble E et les retirer au fur et à mesure des différents A_j. Nous commençons par poser

$$\begin{cases} E_0 = \varnothing & (3.80a) \\ A_j^{(0)} = A_j. & (3.80b) \end{cases}$$

Ensuite, pour chaque $i = 1, \dots, n$ nous posons

$$\begin{cases} E_i = \{a_1, \dots, a_i\} & (3.81a) \\ A_j^{(i)} = A_j^{(i-1)} \setminus \{a_i\}. & (3.81b) \end{cases}$$

Première remarque facile : $\text{Card}(E_i) = i$.

Ensuite fixons nous un i pour voir comment évoluent les cardinaux des $A_j^{(i)}$ avec i. Nous posons $S = \{j = 1, \dots, s \text{ tel que } a_i \in A_j\}$. Par hypothèse $\text{Card}(S) = k$. Le lemme 2.133 nous permet de couper la somme sur $j = 1, \dots, n$ en une somme sur $j \in S$ et une sur $j \neq S$:

$$\begin{aligned} \sum_{j=1}^{n} \text{Card}(A_j^{(i)}) &= \sum_{j\in S} \text{Card}\left(A_j^{(i-1)} \setminus \{a_i\}\right) + \sum_{j\notin S} \text{Card}\left(A_j^{(i-1)} \setminus \{a_i\}\right) && (3.82a) \\ &= \sum_{j\in S} \Big(\text{Card}\left(A_j^{(i-1)}\right) - 1\Big) + \sum_{j\notin S} \text{Card}(A_j^{(i-1)}) \qquad \text{prop. 2.140} && (3.82b) \\ &= \sum_{j=1}^{n} \text{Card}(A_j^{(i-1)}) - k. && (3.82c) \end{aligned}$$

Avec une récurrence sur i nous trouvons cette intéressante formule :

$$\sum_{j=1}^{s} \text{Card}(A_j^{(i)}) = \sum_{j=1}^{s} \text{Card}(A_j) - ki. \tag{3.83}$$

Nous évaluons cela en $i = n$:

$$\sum_{j=1}^{s} \text{Card}(A_j^{(n)}) = \sum_{j=1}^{s} \text{Card}(A_j) - kn. \tag{3.84}$$

EQooGWBXooDqXwTW

Mais $A_j^{(n)} = A_j \setminus \{a_1, \dots, a_n\} = \varnothing$. Donc le membre de gauche de (3.84) est nul. Donc

$$n = \frac{1}{k} \sum_{j=1}^{s} \text{Card}(A_j), \tag{3.85}$$

c'est-à-dire ce que nous voulions. □

3.2.7 Binôme de Newton

DEFooHXNFooOBKgqD

Définition 3.67 (Coefficient binomial)**.**
Soient des entiers n et k avec $k \leqslant n$. Nous définissons ***coefficients binomiaux*** *par*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{3.86}$$

EQooJJYGooTxmSAt

Lorsque α est un multiindice, la factorielle $\alpha!$ et les coefficients binomiaux sont définis en 3.177.

LEMooHWMNooIINsxu

Lemme 3.68.
Un formule pour les coefficients binomiaux :

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \tag{3.87}$$

Démonstration. Simple mise au même dénominateur :

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!(n-k+1)+n!k}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n+1-k)!}. \tag{3.88}$$

□

LEMooUFXEooUaFGjD

Lemme 3.69 (Formule d'itération de Pascal[86]).
Nous avons

$$\sum_{k=p}^{n}\binom{k}{p}=\binom{n+1}{p+1}. \tag{3.89}$$

LEMooUTDTooXAmvdF

Lemme 3.70 ([1]).
Deux énoncés de dénombrement.

(1) Soit un ensemble E de cardinal n. Nous posons

$$B_k=\{\text{parties de cardinal } k \text{ dans } E\}. \tag{3.90}$$

(2) Soit $A_k=\{I=(i_1,\dots,i_k)\in\{0,\dots,n\}^k \text{ tel que } 1\leqslant i_1<\dots<i_k\leqslant n\}$.

(3) Soit $C_k=\{s\in\{0,1\}^n \text{ tel que } \sum_i s_i=k\}$.

Alors

$$\operatorname{Card}(A_k)=\operatorname{Card}(B_k)=\operatorname{Card}(C_k)=\binom{n}{k}. \tag{3.91}$$

Démonstration. Nous faisons en détail la démonstration pour B_k, en utilisant la proposition 3.66. Nous fixons n et nous faisons une récurrence sur k.

(1) **Le partitionnement de B_{k+1}** D'abord nous posons

$$\begin{aligned}f\colon B_k&\to\mathcal{P}(B_{k+1})\\ A&\mapsto\{A\cup\{a\}\text{ tel que }a\in E\setminus A\}.\end{aligned} \tag{3.92}$$

où $\mathcal{P}$ désigne l'ensemble des parties. Notez que

$$B_{k+1}=\bigcup_{A\in B_k}f(A). \tag{3.93}$$

(2) **Combien de multi-compatage (1)** Prouvons que

$$\{A\in B_k\text{ tel que }S\in f(A)\}=\{S\setminus\{a\}\text{ tel que }q\in S\}. \tag{3.94}$$

Pour prouver la première inclusion, nous considérons $A\in B_k$ tel que $S\in f(A)$. Alors $S=A\cup\{a\}$ pour un certain $a\in E\setminus A$ et donc $S\setminus\{a\}=A$.

Pour l'inclusion dans l'autre sens, nous considérons $a\in S$. Alors $S\setminus\{a\}\in B_k$, ce qui fait que $a\in E\setminus\big(S\setminus\{a\}\big)$ et donc $S\in f\big(S\setminus\{a\}\big)$.

(3) **Combien de multi-compatage (2)** Nous avons donc

$$\operatorname{Card}\big(\{A\in B_k\text{ tel que }S\in f(A)\}\big)=\operatorname{Card}\{S\setminus\{a\}\text{ tel que }a\in S\}=\operatorname{Card}(S)=k+1 \tag{3.95}$$

(4) **Le cardinal recherché** La proposition 3.66 nous donne alors

$$\operatorname{Card}(B_{k+1})=\frac{1}{k+1}\sum_{A\in B_k}\operatorname{Card}\big(f(A)\big). \tag{3.96}$$

Mais $\operatorname{Card}\big(f(A)\big)=n-k$ et par hypothèse de récurrence $\operatorname{Card}(B_k)=\binom{n}{k}$ Donc

$$\operatorname{Card}(B_{k+1})=\binom{n}{k}\frac{n-k}{k+1} \tag{3.97a}$$

$$=\frac{n!}{k!(n-k)!}\frac{(n-k)}{k+1} \tag{3.97b}$$

$$=\frac{n!}{(k+1)!(n-k-1)!} \tag{3.97c}$$

$$=\frac{n!}{(k+1)!\big(n-(k+1)\big)!} \tag{3.97d}$$

$$=\binom{n}{k+1}. \tag{3.97e}$$

En ce qui concerne la démonstration pour A_k, c'est du même tonneau. Si $I \in A_k$, alors pour chaque $l \in \{0,\dots,n\} \setminus I$ nous avons un élément de A_{k+1} en l'insérant « au bon endroit » dans I. Je te laisse te débrouiller pour construire la fonction f correspondante et pour vérifier que tout va bien[32].

Maintenant nous montrons que $\text{Card}(C_k) = \binom{n}{k}$ en donnant une bijection entre C_k et B_k. Il existe une bijection

$$\sigma\colon \{1,\dots,n\} \to E \tag{3.98}$$

et nous considérons l'application

$$\begin{aligned} \varphi\colon C_k &\to \mathcal{P}(E) \\ s &\mapsto \{\sigma(i) \text{ tel que } s_i = 1\}. \end{aligned} \tag{3.99}$$

Nous allons voir que $\varphi(C_k) \subset B_k$ et que $\varphi\colon C_k \to B_k$ est une bijection.

(1) $\varphi(C_k) \subset B_k$ Soit $s \in C_k$. Vu que σ est une bijections, $\text{Card}(U) = \text{Card}\left(\sigma^{-1}(U)\right)$ pour tout $U \subset E$. En particulier

$$\text{Card}\big(\{\sigma(i) \text{ tel que } s_i = 1\}\big) = \text{Card}\big(\{i \text{ tel que } s_i = 1\}\big). \tag{3.100}$$

Nous posons $S = \{i \text{ tel que } s_i = 1\}$ et nous calculons

$$\begin{aligned} k = \sum_{i=1}^{n} s_i &= \sum_{i\in\{1,\dots,n\}} s_i && \text{not. (2.242)} && (3.101a)\\ &= \sum_{i\in S} s_i + \sum_{i\notin S} s_i && \text{lem. 2.133} && (3.101b)\\ &= \sum_{i\in S} 1 && && (3.101c)\\ &= \text{Card}(S) && \text{lem. 2.81} && (3.101d) \end{aligned}$$

En remettant avec (3.100) nous avons prouvé que

$$k = \text{Card}(S) = \text{Card}\big(\{\sigma(i) \text{ tel que } s_i = 1\}\big) = \text{Card}\big(\varphi(s)\big) \tag{3.102}$$

(2) φ **est injective** Si $\varphi(s) =^v p(t)$ alors

$$\{\sigma(i) \text{ tel que } s_i = 1\} = \{\sigma(i) \text{ tel que } t_i = 1\}, \tag{3.103}$$

et en prenant σ^{-1} des deux côtés,

$$\{i \text{ tel que } s_i = 1\} = \{i \text{ tel que } t_i = 1\}, \tag{3.104}$$

c'est-à-dire $s = t$.

(3) φ **est surjective** Soit $A \in B_k$. Nous considérons $s\colon \{1,\dots,n\} \to \{0,1\}$ donnée par

$$s(i) = \begin{cases} 1 & \text{si } \sigma(i) \in A \\ 0 & \text{sinon.} \end{cases} \tag{3.105}$$

(3a) $\varphi(s) = A$ Nous devons prouver que $\{\sigma(i) \text{ tel que } s_i = 1\} = A$. En deux inclusions.
D'abord soit $x \in \{\sigma(i) \text{ tel que } s_i = 1\}$. Alors il existe $i \in \{1,\dots,n\}$ tel que $x = \sigma(i)$ et $s_i = 1$. Mais $s_i = 1$ implique $\sigma(i) \in A$. Donc $x \in A$.
Dans l'autre sens, soit $a \in A$. Alors en prenant $i = \sigma^{-1}(a)$, nous avons $\sigma(i) = a \in A$ et donc $s_i = 1$. Donc $a \in \{\sigma(j) \text{ tel que } s_j = 1\}$.

(3b) $s \in C_k$ Nous devons voir que pour l'application s définie en (3.105), $\sum_{i=1}^{n} s_i = k$. Posons $S = \sigma^{-1}(A)$. Vu que σ est une bijection, $\text{Card}(S) = \text{Card}(A) = k$. Nous avons

$$\sum_{i=1}^{n} s_i = \sum_{i\in S} s_i + \sum_{i\notin S} s_i. \tag{3.106}$$

Mais si $i \in \sigma^{-1}(A)$ alors $s_i = 1$ et si $i \notin \sigma^{-1}(A)$ alors $s_i = 0$. Bref, la somme (3.106) vaut

$$\sum_{i=1}^{n} s_i = \sum_{i\in S} 1 + 0 = \text{Card}\left(\sigma^{-1}(A)\right) = \text{Card}(A) = k. \tag{3.107}$$

[32] Moi j'ai pas vérifié ni même essayé. Donc écrivez-moi si ça bloque réellement quelque part.

□

PROPooRBMVooIGkctj

Proposition 3.71 ([3]).
Soient $n, k \in \mathbb{N}$. Nous considérons

$$\Lambda_k^{(n)} = \{\alpha \in \mathbb{N}^n \text{ tel que } \sum_{i=1}^{n} \alpha_i = k\}. \tag{3.108}$$

EQooEHSRooUnhFsl

Alors

$$\text{Card}(\Lambda_k^{(n)}) = \binom{n+k-1}{n-1}. \tag{3.109}$$

Démonstration. Nous nommons $\Lambda_{k,i}$ la partie de Λ_k telle que $\alpha_n = i$, c'est-à-dire

$$\Lambda_{k,i}^{(n)} = \{(\beta, i) \text{ tel que } \beta \in \Lambda_{k-1}^{(n-1)}\}. \tag{3.110}$$

Vu que tous les éléments de $\Lambda_k^{(n)}$ ont une dernière composante entre 0 et k, nous avons

$$\text{Card}(\Lambda_k^{(n)}) = \sum_{i=0}^{k} \text{Card}(\Lambda_{k-i}^{(n-1)}). \tag{3.111}$$

Voilà déjà une belle relation de récurrence.

Nous prouvons que la relation (3.108) tient pour tout k par récurrence sur n en partant de $n = 1$. Pour $n = 1$ nous avons $\text{Card}(\Lambda_k^{(1)}) = 1$ pour tout k et en même temps,

$$\binom{k}{0} = \frac{k!}{0!(k!)} = 1. \tag{3.112}$$

Ok pour $n = 1$. Ensuite nous supposons avoir un n tel que (3.108) est correcte pour tout k. Et nous calculons

$$\begin{aligned}
\text{Card}(\Lambda_k^{(n+1)}) &= \sum_{i=0}^{k} \text{Card}(\Lambda_{k-i}^{(n)}) && \text{(3.113a)}\\
&= \sum_{i=0}^{k} \binom{n+(k-i)-1}{n-1} && \text{(3.113b)}\\
&= \sum_{j=0}^{k} \binom{n-1+j}{n-1} && \text{(3.113c)}\\
&= \sum_{l=n-1}^{n-1+k} \binom{l}{n-1} && \text{(3.113d)}\\
&= \binom{n+k}{n} && \text{prop. 3.69.} \quad \text{(3.113e)}
\end{aligned}$$

□

3.2.8 Divisibilité des coefficients binomiaux

LEMooYBOIooEtVfDQ

Lemme 3.72 (Formule du pion[87]).
Soient n et k deux nombres entiers tels que $1 \leqslant k \leqslant n$. Nous avons

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{3.114}$$

EQooDNBYooZfJEAc

PROPooVPOYooNNugWU

Proposition 3.73 ([88, 89]).
Un entier $n \geqslant 2$ est premier si et seulement si il divise $\binom{n}{k}$ pour tout $k = 1, \dots, n-1$.

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que n est un nombre premier. La formule du pion (3.114) nous dit que

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{3.115}$$

Donc n divise le produit $k\binom{n}{k}$; vu que n est premier, le lemme d'Euclide 3.59 dit qu'il divise un des deux facteurs. Le nombre n ne peut pas diviser k parce que $k < n$. Donc il divise l'autre. C'est-à-dire que n divise $\binom{n}{k}$.

(2) $\Leftarrow$ Nous allons à la contraposée : nous supposons que n n'est pas premier, et nous allons montrer qu'il y a (au moins) un des $\binom{n}{k}$ que n ne divise pas.

Posons $n = lp$ où p est premier. Nous montrons que n ne divise pas $\binom{n}{p}$. Pour cela nous utilisons encore la formule du pion :

$$\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = l\frac{(n-1)\dots(n-p+1)}{(p-1)!}. \tag{3.116}$$

Le lemme 3.61 dit que le tout est divisible par lp si et seulement si

$$\frac{(n-1)\dots(n-p+1)}{(p-1)!} \tag{3.117}$$

EQooIHXGooIOorMC

est divisible par p. Vu que p divise n, il ne divise aucun des nombres $n-1$,...,$n-p+1$. Et comme p est premier, il ne peut pas diviser le produit sans diviser aucun des facteurs. Et vlan, p ne divise pas (3.117).

□

3.2.9 Coefficients binomiaux et polynômes

NORMooROXXooXOybXN

3.74.
Une convention d'écriture. Si A est un anneau, et si $\lambda \in \mathbb{N}$ alors nous notons

$$\lambda a = \sum_{i=1}^{\lambda} a. \tag{3.118}$$

Et nous posons également $0a = 0$. À gauche : le 0 de $\mathbb{N}$ et à droite celui de A.

Si $\lambda \in \mathbb{Z}$, alors lorsque $\lambda < 0$ nous posons $\lambda a = -(-\lambda a)$

PropBinomFExOiL

Proposition 3.75 (Formule binomiale[90])**.**
Soit un anneau commutatif A. Pour tout $x, y \in A$ et $n \in \mathbb{N}$, nous avons

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k \tag{3.119}$$

EqNewtonB

où les coefficients binomiaux sont donnés dans la définition 3.67, et où nous utilisons les conventions d'écriture de 3.74.

Démonstration. La preuve se fait par récurrence. La vérification pour $n = 0$ et $n = 1$ se fait aisément pour peu que l'on se rappelle que $x^0 = 1$ et que $0! = 1$, ce qui donne entre autres $\binom{0}{0} = 1$.

Supposons que la formule (3.119) soit vraie pour $n \geqslant 1$, et prouvons la pour $n+1$. Nous avons

EqBinTrav

$$(x+y)^{n+1} = (x+y)\cdot\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \tag{3.120a}$$

SUBEQooBEUCooHSBtug

$$= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} \tag{3.120b}$$

SUBEQooRURMooGVIbbL

$$= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k + \sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} + y^{n+1}. \tag{3.120c}$$

Notez le passage de (3.120a) à (3.120b) qui demande la commutativité de la multiplication. La formule binomiale ne se généralise pas de façon directe à un anneau non commutatif.

La seconde grande somme peut être transformée en posant $i = k+1$:

$$\sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} = \sum_{i=1}^{n}\binom{n}{i-1}x^{n-(i-1)}y^{i-1+1}, \tag{3.121}$$

dans lequel nous pouvons immédiatement renommer i par k. En remplaçant dans la dernière expression de (3.120), nous trouvons

$$(x+y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n-k+1} y^k. \tag{3.122}$$

La thèse découle maintenant de la formule du lemme 3.68. □

LEMooLPCXooYIzJsD

Lemme 3.76 ([1]).
Si $n \geqslant k$ nous avons

$$\frac{n!}{k!(n-k)!} \leqslant \frac{n^{k-1}}{k!}. \tag{3.123}$$

Démonstration. Nous décomposons le produit définissant $n!$ en les facteurs entre 1 et $n-k$ et ceux entre $n-k+1$ et n :

$$n! = (n-k)! \prod_{i=n-k+1}^{n} i \leqslant n^{k-1}(n-k)!. \tag{3.124}$$

Donc

$$\frac{n!}{k!(n-k)!} \leqslant \frac{n^{k-1}}{k!}. \tag{3.125}$$

□

Tant que nous sommes à démontrer des égalités, en voici une.

LEMooLPOQooICJYdV

Lemme 3.77 ([91]).
Pour $a, b \in \mathbb{R}$ et $n \in \mathbb{N}$ nous avons

$$a^n + (-1)^{n-1} b^n = (a+b) \sum_{k=0}^{n-1} (-1)^k a^{n-1-k} b^k. \tag{3.126}$$

Démonstration. C'est un simple calcul :

$$(a+b) \sum_{k=0}^{n-1} (-1)^k a^{n-1-k} b^k = \sum_{k=0}^{n-1} (-1)^k a^{n-k} b^k + \sum_{k=0}^{n-1} (-1)^k a^{n-k-1} b^{k+1} \tag{3.127a}$$

$$= a^n + \sum_{k=1}^{n-1} (-1)^k a^{n-k} b^k + \sum_{k=0}^{n-2} (-1)^k a^{n-k-1} b^{k+1} + (-1)^{n-1} b^n \tag{3.127b}$$

SUBEQooUCIBooKsuEbb

$$= a^n + (-1)^{n-1} b^n \tag{3.127c}$$

SUBEQooLTIHooZPMwVF

Justifications.

- Pour (3.127b). Dans la première somme, nous avons séparé le terme $k = 0$ et dans la seconde nous avons séparé le terme $k = n-1$
- Pour (3.127c). Dans la seconde somme, décaler les termes pour sommer de 1 à $n-1$ et remarquer que ce qu'on obtient annule la première somme.

□

3.3 Idéal dans un anneau

La définition d'un idéal dans un anneau est la définition 3.3.

DefAJVTPxb

Définition 3.78.
*Un sous-ensemble $B \subset A$ d'un anneau est un **sous anneau** si*

(1) $1 \in B$

(2) *B est un sous-groupe pour l'addition*

(3) *B est stable pour la multiplication.*

Remarque 3.79.
Un idéal n'est pas toujours un anneau parce que l'identité pourrait manquer. Un idéal qui contient l'identité est l'anneau complet.

LEMooQAYSooCYJXkC

Lemme 3.80.
La partie $2\mathbb{Z}$ est un idéal[33] *de $\mathbb{Z}$. On peut aussi le noter (2).*

PROPooPZGFooEbSBXD

Proposition 3.81 ([92] Premier théorème d'isomorphisme)**.**
Soit des anneaux A et B ainsi qu'un idéal bilatère[34] *I. Nous considérons la projection canonique $\pi\colon A\to A/I$.*

Soit un morphisme d'anneaux[35] *$f\colon A\to B$ vérifiant $f(I)=\{0\}$. Alors il existe un unique morphisme $\tilde{f}\colon A/I\to B$ tel que $\tilde{f}\circ\pi=f$.*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\pi}\downarrow & \nearrow_{\tilde{f}} & \\ A/I & & \end{array} \tag{3.128}$$

Démonstration. Soient $a,b\in A$ tels que $\pi(a)=\pi(b)$. Alors $a-b\in I$ et donc $f(a-b)=0$. Vu que f est un morphisme nous en déduisons que $f(a)=f(b)$. La proposition 1.58 dit qu'il existe alors une unique application $\tilde{f}\colon A/I\to B$ telle que

$$\tilde{f}\big(\pi(a)\big)=f(a) \tag{3.129}$$

pour tout $a\in A$.

Nous devons prouver que cette application est un morphisme d'anneaux. Le neutre de A/I est la classe $[1]$ et nous avons $\tilde{f}([1])=1$. En ce qui concerne la somme, soient $\alpha,\beta\in A/I$. Si $a\in\alpha$ et $b\in\beta$ nous avons

$$\begin{aligned}\tilde{f}(\alpha+\beta)&=\tilde{f}([a+b]) && \text{(3.130a)}\\ &=f(a+b) && \text{(3.130b)}\\ &=f(a)+f(b) && \text{(3.130c)}\\ &=\tilde{f}([a])+\tilde{f}([b]) && \text{(3.130d)}\\ &=\tilde{f}(\alpha)+\tilde{f}(\beta). && \text{(3.130e)}\end{aligned}$$

Pour la multiplication c'est le même genre de vérifications. □

PROPooJALPooHFIObB

Proposition 3.82 (Premier théorème d'isomorphisme pour les anneaux)**.**
Soient A et B des anneaux et un morphisme $f\colon A\to B$. Nous considérons l'injection canonique $j\colon f(A)\to B$ et la surjection canonique $\phi\colon A\to A/\ker f$. Alors il existe un unique isomorphisme

$$\tilde{f}\colon A/\ker f\to f(A) \tag{3.131}$$

tel que $f=j\circ\tilde{f}\circ\phi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\phi}\downarrow & & \uparrow{\scriptstyle j} \\ A/\ker f & \xrightarrow[\tilde{f}]{} & f(A)\subset B \end{array} \tag{3.132}$$

Démonstration. Il s'agit d'appliquer la proposition 3.81 au cas particulier $I=\ker(f)$. Vérifions que $\tilde{f}$ est alors bien injective. Supposons que $\alpha,\beta\in A/\ker(f)$ vérifient $\tilde{f}(\alpha)=\tilde{f}(\beta)$. Soient $a\in\alpha$ et $b\in\beta$. Nous avons

$$f(a)=\tilde{f}(\alpha)=\tilde{f}(\beta)=f(b). \tag{3.133}$$

Donc $f(a-b)=0$, ce qui signifie $a-b\in\ker(f)$ et donc $\alpha=\beta$. □

PropIJJIdsousphi

Proposition 3.83.
Soient I un idéal de A et la projection canonique

$$\phi\colon A\to A/I. \tag{3.134}$$

[33] Idéal, définition 3.3.
[34] Définition 3.3.
[35] Morphisme d'anneaux, définition 1.106.

C'est une bijection entre les idéaux de A contenant I et les idéaux de A/I.

Dit de façon imagée :

$$\{\text{idéaux de } A \text{ contenant } I\} \simeq \{\text{idéaux de } A/I\}. \tag{3.135}$$

EqKbrizu

Démonstration. Si $I \subset J$ et si J est un idéal de A, alors $\phi(J)$ est un idéal dans A/I. En effet un élément de $\phi(J)$ est de la forme $\phi(j)$ et un élément de A/I est de la forme $\phi(i)$. Leur produit vaut

$$\phi(i)\phi(j) = \phi(ij) \in \phi(J). \tag{3.136}$$

Soit maintenant K un idéal dans A/I et soit $J = \phi^{-1}(K)$. Étant donné qu'un idéal doit contenir 0 (parce qu'un idéal est un groupe pour l'addition), $[0] \in K$ et par conséquent $I \subset \phi^{-1}(K)$. □

PROPooUOAmGZpAMd

Proposition 3.84 ([1]).
Si A est un anneau, nous avons les équivalences

ITEMooLAAVooXhTcMe

(1) A est un corps[36].

ITEMooDGZIooRopYGx

(2) A est non nul et ses seuls[37] *idéaux à gauche sont $\{0\}$ et A.*

ITEMooLPWHooDJpTbR

(3) A est non nul et ses seuls idéaux à droite sont $\{0\}$ et A.

Démonstration. Nous allons montrer que le point (1) est équivalent aux deux autres.

(1) **(1) implique (2)** Si I est un idéal à gauche différent de $\{0\}$, alors il contient un certain $a \neq 0$. Puisque A est un corps, il contient un inverse a^{-1}, et comme I est un idéal, $a^{-1}I \subset I$. En particulier $a^{-1}a \in I$. Donc $1 \in I$ et $I = A$.

(2) **(2) implique (1)** Supposons que les seuls idéaux de A soient $\{0\}$ et A. Soit $a \in A$. Si a est non nul, alors aA est un idéal de a. Vu qu'il contient $a \neq 0$, nous avons $aA = A$ (par hypothèse, un idéal qui n'est pas $\{1\}$ est A). En particulier, $1 \in aA$, c'est-à-dire qu'il existe $b \in A$ tel que $ab = 1$. L'élément a est donc inversible.

(3) **(1) implique (3)** Comme pour (1) implique (2).

(4) **(3) implique (1)** Comme pour (2) implique (1).

Notez que je n'ai pas vérifié les deux derniers points. Donc vous devriez le vérifier et m'écrire si il y a un problème. □

DEFIdealMax

Définition 3.85 ([69]).
*Soit un anneau A. Un idéal $I \neq A$ est dit **idéal maximal** si il n'existe pas d'idéal $J \neq A$ contenant strictement I.*

PROPooSHHWooCyZPPw

Proposition 3.86 (Thème 18).
Un idéal I dans un anneau A est maximum si et seulement si A/I est un corps.

Démonstration. Soit un idéal maximum $I \subset A$. Alors les idéaux contenant I sont A et I. L'application ϕ de la proposition 3.83 est une bijection, donc l'ensemble des idéaux de A/I ne contient que deux éléments. Les seuls idéaux de A/I sont donc $\{0\}$ et A/I ; donc A/I est un corps par la proposition 3.84.

Dans l'autre sens, c'est la même chose : si A/I est un corps, il possède exactement deux idéaux, donc A ne contient que deux idéaux contenant I. Donc I est un idéal maximum. □

THOooFWYLooOofaPa

Théorème 3.87 (Théorème de Krull[93]).
Pour tout idéal propre I d'un anneau commutatif A, il existe au moins un idéal maximal de A contenant I.

DEFooAQSZooVhvQWv

Définition 3.88.
*Nous disons qu'un idéal I dans A est **premier** si I est strictement inclus dans A et si pour tout $a, b \in A$ tels que $ab \in I$ nous avons $a \in I$ ou $b \in I$.*

LEMooYRPBooYxXXsi

Lemme 3.89.
L'idéal nul (réduit à $\{0\}$) est premier si et seulement si A est intègre[38].

Démonstration. En deux sens.

[36] Définition 1.213.
[37] Je vous laisse vous poser de grandes questions sur le fait que le vide est un idéal ou non.
[38] Définition 3.22 d'anneau intègre.

(1) **Si $\{0\}$ est premier** Alors $A \neq \{0\}$ parce que $I = \{0\}$ est propre (définition d'idéal premier).

De plus, si $ab = 0$, alors $ab \in I$ qui est un idéal premier. Donc soit a soit b est dans I, c'est-à-dire que soit a soit b est nul. Donc A est intègre.

(2) **Si A est intègre** Alors $A \neq \{0\}$ et l'idéal $I = \{0\}$ est strictement inclus dans A. Si $ab \in I$, alors $ab = 0$ et comme A est intègre, soit a soit b est nul, c'est-à-dire appartient à I.

□

PROPooRUQKooIfbnQX

Proposition 3.90 ([69]).
Soit un anneau commutatif[39] *et un idéal I dans A.*

ITEMooUGBTooOGrnWl

(1) I est un idéal premier[40] *si et seulement si A/I est un anneau intègre.*

ITEMooGLXSooUjINqR

(2) I est un idéal maximal[41] *si et seulement si A/I est un corps.*

ITEMooTFFQooOUajFw

(3) Tout idéal maximal propre est premier.

Démonstration. En plein d'étapes.

(1) **(1), $\Rightarrow$** Évacuons le cas trivial pour être sûr. Si $I = \{0\}$ alors A est intègre par le lemme 3.89. Donc $A/I = A/\{0\} = A$ est intègre également.

Soient $a, b \in A$ tels que $[a][b] = [0]$. Donc $[ab] = [0]$, c'est-à-dire $ab \in I$. Puisque I est un idéal premier nous avons $a \in I$ ou $b \in I$, c'est-à-dire $[a] = 0$ ou $[b] = 0$; nous en déduisons que A/I est un anneau intègre.

(2) **(1), $\Leftarrow$**

Soit $ab \in I$. Alors $[ab] = 0$, ce qui signifie que $[a][b] = 0$ donc que $[a] = 0$ ou que $[b] = 0$ parce que A/I est intègre. Mais la condition $[a] = 0$ signifie $a \in I$, et $[b] = 0$ signifie $b \in I$. Nous avons donc prouvé que soit a soit b est dans I, c'est-à-dire que I est premier.

(3) **(2), $\Rightarrow$**

Nous devons montrer que tout élément non nul de A/I est inversible. Un élément non nul de A/I est $[x]$ avec $x \in A \setminus I$.

Nous considérons $J = Ax + I$, qui est un idéal parce que pour tout $a \in A$, $aAx + aI \in Ax + I$. Mais comme I est maximal, $J = I$ ou $J = A$.

Si $J = I$, nous aurions que pour tout $a \in A$ et pour tout $i \in I$, $ax + i \in I$. En particulier pour $a = 1$ et $i = 0$ nous aurions $x \in I$, ce qui est contraire à l'hypothèse faite sur x.

Donc $J = A$. En particulier, $1 \in J$, c'est-à-dire qu'il existe $a \in A$ et $i \in I$ tels que $ax + i = 1$. En passant aux classes, $[ax] = 1$, c'est-à-dire $[a][x] = 1$ qui signifie que $[a]$ est un inverse de $[x]$ dans A/I.

Nous avons prouvé que A/I est un corps.

(4) **(2), $\Leftarrow$** Si $x \in A \setminus I$, il faut prouver que tout idéal contenant I et x est A.

Un idéal contenant I et x doit contenir l'idéal $J = Ax + I$. Comme $x \notin I$, nous avons $[x] \neq 0$ dans A/I. Donc $[x]$ est inversible et il existe $a \in A$ tel que $[ax] = [1]$. C'est-à-dire que $ax - 1 \in I$. Nous avons alors

$$1 = ax + \underbrace{(1 - ax)}_{\in I}. \tag{3.137}$$

C'est-à-dire que $1 \in Ax + I$ et donc $Ax + I = A$.

Enfin nous prouvons que tout idéal maximal propre est premier.

Si I est maximal, A/I est un corps par le point (2), et vu que I est propre, le corps A/I n'est pas réduit à $\{0\}$. Donc le lemme 3.23 dit que A/I est un anneau intègre. Le point (1) dit alors que I est un idéal premier. □

Remarque 3.91.
Puisqu'un corps peut être réduit à $\{0\}$, dans (2), l'idéal peut être A. Mais pas dans (3), parce qu'un idéal premier est propre, ça fait partie de la définition 3.88.

[39] Tous les anneaux du Frido sont commutatifs
[40] Idéal premier, définition 3.88.
[41] Idéal maximal, définition 3.85.

PROPooHABIooBZZQMj

Proposition 3.92 ([94]).
Si A est un anneau commutatif intègre, alors un idéal I dans A est premier si et seulement si A/I est intègre.

Démonstration. Supposons que I soit un idéal premier. Si $[a], [b] \in A/I$ sont tels que $[a][b] = 0$, alors $[ab] = 0$, ce qui signifie que $ab \in I$. Mais alors, puisque I est premier, soit a soit b est dans I. Cela signifie que soit $[a]$ soit $[b]$ est nul dans A/I. Cela prouve que A/I est un anneau intègre.

Dans l'autre sens, nous supposons que A/I est intègre. Cela implique immédiatement que $I \neq A$ parce que A/A n'est pas un anneau intègre (tout le monde est évidemment diviseur de zéro).

Soient donc $a, b \in A$ tels que $ab \in I$. Alors $[a][b] = [ab] = 0$ dans A/I, mais comme A/I est intègre, cela implique que soit $[a]$ soit $[b]$ est nul. Autrement dit, soit a soit b est dans I. □

PROPooSGLNooBYKNyo

Proposition 3.93.
Dans un idéal principal, les conditions suivantes sont équivalentes :

(1) *L'élément p est premier.*

(2) *L'élément p est irréductible.*

(3) *L'idéal pA est un idéal maximal.*

3.4 Module sur un anneau

DEFooHXITooBFvzrR

Définition 3.94 (module sur un anneau[95]).
*Soit un anneau A. Un **module à gauche** sur A est la donnée d'un triplet $(M, +, \cdot)$ où*

(1) *$+$ est une loi de composition interne à M, c'est-à-dire $+ : M \times M \to M$,*

(2) *$\cdot$ est une loi de composition externe, c'est-à-dire $\cdot : A \times M \to M$*

telles que

(1) *$(M, +)$ est un groupe*[42].

(2) *$a \cdot (x + y) = a \cdot x + a \cdot y$,*

(3) *$(a + b) \cdot x = a \cdot x + b \cdot x$,*

(4) *$(ab) \cdot x = a \cdot (b \cdot x)$*

(5) *$1 \cdot x = x$.*

pour tout $a, b \in A$ et $x, y \in M$.

*Si M et N sont des A-modules, un **morphisme** de M vers N est une application $f : M \to N$ qui*

(1) *est un morphisme de groupes entre $(M, +)$ et $(N, +)$*

(2) *vérifie $f(a \cdot x) = a \cdot f(x)$ pour tout $a \in A$, $x \in M$.*

L'ensemble des morphismes entre M et N est noté $\mathrm{Hom}_A(M, N)$. Si B est un sous-anneau de A, nous parlons de $\mathrm{Hom}_B(M, N)$ pour parler des morphismes de groupes qui ne vérifient $f(a \cdot x) = a \cdot f(x)$ que pour $a \in B$.

PROPooGARGooDiMqtN

Proposition 3.95.
Si M est un module sur un anneau, alors $(M, +)$ est un groupe commutatif.

Démonstration. Il suffit de calculer $(1 + 1) \cdot (x + y)$ de deux façons différentes :

$$(1 + 1) \cdot (x + y) = 1 \cdot (x + y) + 1 \cdot (x + y) = x + y + x + y \tag{3.138}$$

d'une part et

$$(1 + 1) \cdot (x + y) = (1 + 1) \cdot x + (1 + 1) \cdot y = x + x + y + y, \tag{3.139}$$

d'autre part. En égalant les deux expressions, il vient

$$x + y + x + y = x + x + y + y, \tag{3.140}$$

qui se simplifie (nous sommes dans un groupe) en $y + x = x + y$. □

[42] Nous verrons dans la proposition 3.95 qu'il est forcément commutatif.

DEFooKHWZooIfxdNc

Définition 3.96.
*Un **espace vectoriel** est un module*[43] *sur un corps commutatif*[44].

DEFooRUKVooLnXxdS

Définition 3.97 ([96]).
*Soient un A-module M et un ensemble I. Une famille $\{m_i\}_{i\in I}$ est **libre** si les m_i sont **linéairement indépendants**, c'est-à-dire si pour tout choix d'une partie finie J dans I et d'éléments $(a_j)_{j\in J}$ dans A, si nous avons*

$$\sum_{j\in J} a_j m_j = 0, \tag{3.141}$$

alors $a_j = 0$ pour tout j.

DEFooWBOBooJNyyBF

Définition 3.98 ([97]).
*Soit S, une partie du A-module M. Le **sous-module engendré** par S est l'ensemble des éléments de M qui sont des combinaisons linéaires finies d'éléments de S, c'est-à-dire de sommes de la forme*

$$\sum_{t\in T} a_t t \tag{3.142}$$

où T est fini dans S et $a_t \in A$.

3.4.1 Module produit

DEFooLCJEooBvVmkV

Lemme-Définition 3.99 ([96]).
*Soient un anneau A et un ensemble I. Le A-**module produit** A^I est l'ensemble des applications $I \to A$.*

En termes de notations, nous écrivons ceci :

$$A^I = \{(a_i)_{i\in I}, a_i \in A\}. \tag{3.143}$$

L'ensemble A^I devient un module par les définitions, pour $x, y \in A^I$ et $a \in A$:

$$ax = (ax_i)_{i\in I} \tag{3.144a}$$

EQooPLBSooFuQXrj

$$x + y = (x_i + y_i)_{i\in I}. \tag{3.144b}$$

EQooODBMooQKLUgd

En d'autres termes, $A^I = \mathrm{Fun}(I, A)$.

Démonstration. Il faut vérifier toutes les conditions de la définition 3.94. En guise d'exemple, nous vérifions la distributivité. Soient $a \in A$ et $x, y \in A^I$. Nous avons

$$\begin{aligned}
\big[a \cdot (x + y)\big]_i &= a(x + y)_i && (3.144a) && (3.145a)\\
&= a(x_i + y_i) && (3.144b) && (3.145b)\\
&= ax_i + ay_i && \text{distrib. dans } A && (3.145c)\\
&= (ax + ay)_i && (3.144b). && (3.145d)
\end{aligned}$$

□

Lemme 3.100.
Pour chaque $i \in I$ nous considérons l'élément $e_i \in A^I$ donné par

$$\begin{aligned}
e_i \colon I &\to A\\
j &\mapsto \begin{cases} 1 & \text{si } j = i\\ 0 & \text{sinon.} \end{cases}
\end{aligned} \tag{3.146}$$

La famille $\{e_i\}_{i\in I}$ est libre[45] *dans A^I.*

Démonstration. Soient J fini dans I ainsi que des éléments $a_j \in A$ ($j \in J$). Nous supposons que[46] $\sum_{j\in J} a_j e_j = 0$. Calculons un peu :

$$\sum_{j\in J} a_j e_j = \sum_{j\in J} (a_j \delta_{ji})_{i\in I} = \left(\sum_{j\in J} a_j \delta_{ji}\right)_{i\in I}. \tag{3.147}$$

[43] Définition 3.94.
[44] La condition de commutativité n'est pas indispensable, mais comme nous ne parlerons que de corps commutatifs…
[45] Définition 3.97.
[46] Pour rappel, les sommes finies sont définies par 2.129.

Pour que le tout soit nul dans A^I, il faut que

$$\sum_{j\in J} a_j\delta_{ji} \tag{3.148}$$

soit nul pour tout $i\in I$. Si nous fixons $i\in I$, la somme sur j possède un seul terme non annulé par δ_{ji}, et c'est le terme $j=i$. Nous avons donc $a_i=0$. □

DEFooBMEPooFsCHgb

Définition 3.101.
Nous notons $A^{(I)}$ le sous-module de A^I engendré[47] *par les e_i.*

Lemme 3.102 ([1]).
L'ensemble $A^{(I)}$ est l'ensemble des applications $I\to A$ de support fini.

Démonstration. En deux sens.

(1) **Si $x\in A^{(I)}$** Pour rappel, la définition 3.99 nous dit que x est une application $I\to A$. Vu que x est dans le sous-module engendré par les e_i, il existe une partie finie $J\subset I$ telle que

$$x=\sum_{j\in J} x_je_j. \tag{3.149}$$

Pour $i\in I$ nous avons

$$x(i)=\sum_{j\in J} x_j\delta_{ij}=\begin{cases} x_i & \text{si } i\in J\\ 0 & \text{sinon.}\end{cases} \tag{3.150}$$

Donc le support de x est dans J qui est fini. Vu que toute partie d'un ensemble fini est fini (lemme 1.76), le support de x est fini.

(2) **Si x est de support fini** Supposons que le support de $x\colon I\to A$ soit la partie finie $J\subset I$. En notant $x_j=x(j)$ pour tout $j\in J$, nous avons

$$x=\sum_{j\in J} x_je_j. \tag{3.151}$$

□

THOooPDZCooJnHbOd

Théorème 3.103 (Propriété universelle de $A^{(I)}$[96]).
Soient un anneau A ainsi qu'un A-module P. Pour $\phi\in \mathrm{Hom}_A(A^{(I)},P)$, nous considérons

$$\begin{aligned}\phi|_I\colon I&\to P\\ i&\mapsto \phi(e_i).\end{aligned} \tag{3.152}$$

(1) L'application

$$\begin{aligned}f\colon \mathrm{Hom}_A(A^{(I)},P)&\to \mathrm{Fun}(I,P)\\ \phi&\mapsto \phi|_I\end{aligned} \tag{3.153}$$

est une bijection.

(2) L'application inverse est $g\colon \mathrm{Fun}(I,P)\to \mathrm{Hom}_A(A^{(I)},P)$ donnée par

$$g(\psi)\big(\sum_{j\in J} a_je_j\big)=\sum_{j\in J} a_j\psi(j) \tag{3.154}$$

pour tout J fini dans I et choix de $a_j\in A$.

Démonstration. Nous allons montrer que $g\big(f(\phi)\big)=\phi$ et que $f\big(g(\psi)\big)=\psi$ pour tout $\phi\in\mathrm{Hom}_A(A^{(I)},P)$ et pour tout $\psi\in\mathrm{Fun}(I,P)$.

Dans un premier sens nous avons :

$$\begin{aligned} g\big(f(\phi)\big)\big(\sum_j a_je_j\big)&=\sum_j a_jf(\phi)(j) && \text{(3.155a)}\\ &=\sum_j a_j\phi(e_j) && \text{(3.155b)}\\ &=\phi\big(\sum_j a_je_j\big). && \text{(3.155c)}\end{aligned}$$

SUBALIGNooBWPLooHelbOs

SUBALIGNooUOQPooCwIgZo

Justifications :

[47] Définition 3.98.

- Pour (3.155b), nous avons utilisé le fait que $f(\phi)(i) = \phi|_I(i) = \phi(e_i)$.
- Pour (3.155c), nous utilisons le fait que ϕ est un morphisme de modules.

Et pour l'autre sens,

$$f\big(g(\psi)\big)(i) = g(\psi)(e_i) = \psi(i). \tag{3.156}$$

Vérifions que cela est suffisant pour que f soit une bijection.

(1) **Surjectif** Soit $\psi \in \mathrm{Fun}(I, P)$. Nous avons $f\big(g(\psi)\big) = \psi$, ce qui prouve que ψ est dans l'image de f.

(2) **Injectif** Supposons que $f(\phi_1) = f(\phi_2)$. Alors en appliquant g des deux côtés, il vient $\phi_1 = \phi_2$.

□

3.4.2 Sous-module

Soient M un A-module et $x = (x_i)_{i\in I}$ une famille d'éléments de M paramétrée par l'ensemble I. Nous considérons l'application

$$\begin{aligned} \mu_x\colon A^{(I)} &\to M \\ (a_i)_{i\in I} &\mapsto \sum_{i\in I} a_i x_i. \end{aligned} \tag{3.157}$$

Ici $A^{(I)}$ désigne l'ensemble de toutes les applications $I \to A$ de support fini (définition 3.101).

DefBasePouyKj

Définition 3.104.
À l'instar des espaces vectoriels, les modules ont une notion de partie libre, génératrice et de bases :

*(1) Si μ_x est surjective, nous disons que x est une partie **génératrice**.*

*(2) Si μ_x est injective, nous disons que la partie x est **libre**.*

*(3) Si μ_x est bijective, nous disons que la partie x est une **base**.*

Définition 3.105.
*Un sous-ensemble $N \subset M$ est un **sous-module** si $(N, +)$ est un sous-groupe de $(M, +)$ et si $a \cdot x \in N$ pour tout $x \in N$ et pour tout $a \in A$.*

Exemple 3.106.
Un anneau A est lui-même un A-module et ses sous-modules sont les idéaux. △

DEFooZACWooWydFDp

Définition 3.107 (Projecteur)**.**
*Soit M un module sur un anneau commutatif A. Un **projecteur** est une application linéaire $p\colon M \to M$ telle que $p^2 = p$.*

*Une famille $(p_i)_{i\in I}$ sur M est **orthogonale** si $p_i \circ p_j = 0$ pour tout $i \neq j$. La famille est **complète** si $\sum_{i\in I} p_i = \mathbb{1}$.*

ThoProjModpAlsUR

Théorème 3.108.
Soient des sous-modules $M_1, \dots, M_n$ du module M tels que $M = M_1 \oplus \dots \oplus M_n$. Les applications p_i définies par

$$p_i(x_1 + \dots + x_n) = x_i \tag{3.158}$$

forment une famille orthogonale de projecteurs et $p_1 + \dots + p_n = \mathrm{Id}$.

Inversement, si $(p_1, \dots, p_n)$ est une famille orthogonale de projecteurs dans un module $\mathcal{E}$ tel que $\sum_{i=1}^n p_i = \mathrm{Id}$, alors

$$M = \bigoplus_{i=1}^{n} p_i(M). \tag{3.159}$$

Démonstration. En deux parties.

(1) **Première partie** Les p_i sont des projecteurs parce que $p_i^2(x_1 + \dots + x_n) = p_i(x_i) = x_1 = p_i(x_1 + \dots + x_n)$. Ils sont orthogonaux parce que

$$(p_i \circ p_j)(x_1 + \dots + x_n) = p_i(x_j) = 0 \tag{3.160}$$

lorsque $i \neq j$. De plus nous avons

$$(p_1 + \dots + p_n)(x_1 + \dots + x_n) = x_1 + \dots + x_n, \tag{3.161}$$

donc la somme est l'identité.

(2) **L'autre sens** Tout élément de M doit pouvoir être écrit de façon unique comme somme d'éléments des $p_i(M)$. Avant de nous lancer dans la preuve proprement dite, notons que que si $i \neq j$, alors $p_j(x_i) = 0$. En effet il existe $m \in M$ tel que $x_i = p_i(m)$; donc $p_j(x_i) = (p_j \circ p_i)(m) = 0$.

Pour l'existence, soit $x \in M$. Nous avons

$$x = (p_1 + \ldots + p_n)(x) = p_1(x) + \ldots + p_n(x). \tag{3.162}$$

En ce qui concerne l'unicité, si $x_1 + \ldots + x_n = y_1 + \ldots + y_n$ avec $x_i, y_i \in p_i(M)$, en prenant p_i des deux côtés, nous obtenons

$$x_i = p_i(x_1 + \ldots + x_n) = p_i(y_1 + \ldots + y_n) = y_i. \tag{3.163}$$

Donc $x_i = y_i$ pour tout i et nous avons l'unicité.

□

Définition 3.109.
*Un module est **simple** ou **irréductible** si il n'a pas d'autres sous-modules que $\{0\}$ et lui-même. Un module est **indécomposable** si il ne peut pas être écrit comme somme directe de sous-modules.*

Un module simple est a fortiori indécomposable. L'inverse n'est pas vrai comme le montre l'exemple suivant.

Exemple 3.110.
Soit $\mathcal{E} = \mathbb{C}[X]/(X^2)$ vu comme $\mathbb{C}[X]$-module. C'est le $\mathbb{C}[X]$-module des polynômes de la forme $aX + b$ avec $a, b \in \mathbb{C}$. L'ensemble des polynômes de la forme aX est un sous-module. Le module $\mathcal{E}$ n'est donc pas simple. Il est cependant indécomposable parce que $\{aX\}$ est le seul sous-module non trivial. En effet si $\mathcal{F}$ est un sous-module de $\mathcal{E}$ contenant $aX + b$ avec $b \neq 0$, alors $\mathcal{F}$ contient $X(aX + b) = bX$ et donc contient tout $\mathcal{E}$. △

DefAEbnJqI

Définition 3.111 (Algèbre[98]).
*Si $\mathbb{K}$ est un corps commutatif[48], une $\mathbb{K}$-**algèbre** A est un espace vectoriel[49] muni d'une opération bilinéaire $\times : A \times A \to A$, c'est-à-dire telle que pour tout $x, y, z \in A$ et pour tout $\alpha, \beta \in \mathbb{K}$,*

(1) $(x + y) \times z = x \times z + y \times z$

(2) $x \times (y + z) = x \times y + x \times z$

(3) $(\alpha x) \times (\beta y) = (\alpha\beta)(x \times y)$.

*Si A et B sont deux $\mathbb{K}$-algèbres, une application $f : A \to B$ est un **morphisme d'algèbres** entre A et B si pour tout $x, y \in A$ et pour tout $\alpha \in \mathbb{K}$,*

(1) $f(xy) = f(x)f(y)$

(2) $f(x + \alpha y) = f(x) + \alpha f(y)$

où nous avons noté xy pour $x \times y$.

LEMooVKLKooSAHmpZ

Lemme 3.112 ([1]).
Soient une algèbre A et une famille $(X_i)_{i \in I}$ de sous-algèbres de A (ici I est un ensemble quelconque). Alors la partie $X = \bigcap_{i \in I} X_i$ est une sous-algèbre de A.

Démonstration. Nous devons prouver que si x et y sont dans X et $\lambda \in \mathbb{K}$, alors xy, $x + y$ et λx sont dans X. Pour tout $i \in I$ nous avons $x, y \in X_i$ et donc $xy \in X_i$, $x + y \in X_i$ et $\lambda x \in X_i$ (parce que X_i est une algèbre). Donc xy, $x + y$ et λx sont dans X_i pour tout I, et donc dans X. □

DefkAXaWY

Définition 3.113.
*L'**algèbre engendrée** par X est l'intersection de toutes les sous-algèbres de A contenant X (qui est une algèbre par le lemme 3.112).*

[48] Définition 1.213
[49] Définition 3.96.

3.5 Caractéristique d'un anneau

LEMDEFooVEWZooUrPaDw

Lemme-Définition 3.114.
Soit l'application

$$\begin{aligned}\mu\colon \mathbb{Z} &\to A\\ n &\mapsto n\cdot 1_A\end{aligned} \tag{3.164}$$

où $n\cdot 1_A$ est expliqué dans 3.74.

ITEMooPBWYooAWaCKJ

(1) C'est un morphisme d'anneaux.

ITEMooOQWMooFYcmFf

(2) Le noyau est un sous-groupe de $\mathbb{Z}$

ITEMooWDWEooMSMxfN

(3) Il existe un unique $p\in\mathbb{Z}$ tel que $\ker(\mu)=p\mathbb{Z}$.

*Ce p est la **caractéristique** de A.*

Démonstration. En plusieurs parties.

(1) **Pour (1)** Nous avons $\mu(1)=1$ et $\mu(0)=0$. De plus

$$\mu(n+m)=\sum_{i=1}^{n+m}1_A=\sum_{i=1}^{n}1_A+\sum_{i=n+1}^{n+m}1_A=\mu(n)+\sum_{i=1}^{m}1_A=\mu(n)+\mu(m). \tag{3.165}$$

Notez le passage délicat de $\sum_{i=n+1}^{n+m}1_A=\sum_{i=1}^{m}1_A$. Vu que ce qui est dans la somme sur i ne dépend pas de i, seul le cardinal de l'ensemble parcouru par i compte.

Nous avons donc $\mu(m+n)=\mu(n)+\mu(m)$. Notez que c'est également valide pour les négatifs grâce aux différentes conventions prises.

Le lemme 1.212 conclu que μ est un morphisme.

(2) **Pour (2)** Nous avons $\mu(0)=0$ et donc $0\in\ker(\mu)$. Si $k,l\in\ker(\mu)$, alors

$$\mu(k+l)=\mu(k)+\mu(l)=0+0=0, \tag{3.166}$$

donc $k+l\in\ker(\mu)$.

(3) **Pour (3)** La proposition 1.196 montre que tout sous-groupe de $\mathbb{Z}$ est de la forme $p\mathbb{Z}$.

□

Par exemple la caractéristique de $\mathbb{Q}$ est zéro parce qu'aucun multiple de l'unité n'est nul.
À propos de diagonalisation en caractéristique 2, voir l'exemple 10.224.

Lemme 3.115.
Si A est de caractéristique nulle, alors A est infini.

Démonstration. En effet, $\ker\mu=\{0\}$ implique que $n1_A\neq m1_A$ dès que $n\neq m$ et par conséquent A contient $\mathbb{Z}1_A$, et est infini. □

LemHmDaYH

Lemme 3.116.
Soit un anneau A de caractéristique p.

ITEMooPKSEooPKChGM

(1) Si $p>0$, alors nous avons l'isomorphisme d'anneaux

$$\mathbb{Z}1_A\simeq\mathbb{Z}/p\mathbb{Z}. \tag{3.167}$$

ITEMooBTUIooYzOycc

(2) Si $p=0$, alors nous avons l'isomorphisme d'anneaux

$$\mathbb{Z}1_A\simeq\mathbb{Z} \tag{3.168}$$

Démonstration. Pour (1), l'isomorphisme est donné par l'application $n1_A\mapsto\phi(n)$ si ϕ est la projection canonique $\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$.

Pour (2), la preuve est encore à faire. Écrivez-moi. □

PropGExaUK

Proposition 3.117.
La caractéristique d'un anneau fini divise son cardinal.

Démonstration. Si A est un anneau, le groupe $\mathbb{Z}$ agit sur A par

$$n \cdot a = a + n1_A. \tag{3.169}$$

Chaque orbite de cette action est de la forme

$$\mathcal{O}_a = \{a + n1_A \text{ tel que } n = 0, \dots, p-1\} \tag{3.170}$$

où p est la caractéristique de A. Les orbites ont p éléments et forment une partition de A, donc le cardinal de A est un multiple de p. □

LEMooJQIKooQgukqn

Lemme 3.118 ([99]).
Un anneau totalement ordonné est de caractéristique nulle.

Démonstration. Le morphisme $\mu\colon \mathbb{Z} \to A$, $n \mapsto n1_A$ est strictement croissant, en particulier $\mu(x) \neq \mu(y)$ dès que $x \neq y$. Donc $\ker(\mu) = \{0\}$. □

L'ensemble typique de caractéristique p est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3.5.1 Endomorphisme de Frobenius

PropFrobHAMkTY

Proposition 3.119 (Endomorphisme de Frobenius[100]).
Soit A un anneau commutatif unitaire dont la caractéristique est un nombre premier p. L'application

$$\begin{aligned} \text{Frob}_A\colon A &\to A \\ x &\mapsto x^p \end{aligned} \tag{3.171}$$

est un automorphisme d'anneau unitaire.

En particulier nous avons

$$(a+b)^p = a^p + b^p. \tag{3.172}$$

Cet automorphisme est nommé ***morphisme de Frobenius****. Nous utiliserons aussi les itérés du morphisme de Frobenius :* $\text{Frob}^k\colon x \mapsto x^{p^k}$.

Démonstration. Nous utilisons la formule du binôme de la proposition 3.75 :

$$\text{Frob}_A(x,y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} b^k. \tag{3.173}$$

Nous savons par le lemme 3.114 que si $\lambda \in p\mathbb{Z}$ et $x \in A$, alors $\lambda x = 0$ (attention aux notations, c'est expliqué dans 3.74). La proposition 3.73 dit que tous les termes de la somme (sauf le premier et le dernier) sont de la forme λx avec $\lambda \in p\mathbb{Z}$ et $x \in a$. Bref, tous ce coefficients sont divisibles par p et donc les éléments de A correspondants sont nuls :

$$\text{Frob}_A(x,y) = x^p + y^p = \text{Frob}_A(x) + \text{Frob}_A(y) \tag{3.174}$$

Le lemme 3.114 conclu que Frob_A est un morphisme. □

Exemple 3.120.
Soit à factoriser $X^p - 1$ dans $\mathbb{F}_p$. Grâce au morphisme de Frobenius, nous avons immédiatement

$$X^p - 1 = (X-1)^p. \tag{3.175}$$

△

3.5.2 Caractéristique deux

Beaucoup de résultats demandent une caractéristique différente de deux. Qu'a donc de particulier la caractéristique deux ?

Si $\mathbb{K}$ est un corps de caractéristique 2, alors l'égalité $x = -x$ n'implique pas $x = 0$, puisque $2x = 0$ est vérifiée pour tout x. Cela se répercute sur un certain nombre de résultats. Par exemple, en caractéristique deux, une forme antisymétrique n'est pas toujours alternée : voir le lemme 10.7.

3.6 Anneau intègre

LEMSEZSMEeuUnhXgMeZ

Lemme 3.121.
Un corps[50] *est un anneau intègre.*

Démonstration. En effet, soient un corps $\mathbb{K}$ et deux éléments $x, y \in \mathbb{K}$ tels que $xy = 0$. Si y est inversible, alors nous pouvons multiplier par y^{-1} pour trouver $x = 0$. Cela prouve que $\mathbb{K}$ est un anneau intègre. □

Exemple 3.122.
L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre parce que $3 \cdot 2 = 0$ alors que ni 3 ni 2 ne sont nuls. △

Nous verrons au théorème 3.260 que l'anneau A est intègre si et seulement si $A[X]$ est intègre.

CorZnInternprem

Corolaire 3.123.
L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

Démonstration. Supposons que n soit premier. La proposition 3.49 donne les inversibles de $\mathbb{Z}/n\mathbb{Z}$ par

$$U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \text{ tel que } 0 \leqslant x \leqslant n \text{ tel que } \operatorname{pgcd}(x, n) = 1\}. \tag{3.176}$$

Mais comme n est premier, $\operatorname{pgcd}(x, n) = 1$ pour tout x, et donc tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles. Donc $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Si n n'est pas premier, alors $n = pq$ avec $1 < p \leqslant q < n$. Alors

$$[p]_n[q]_n = [pq]_n = [0]_n. \tag{3.177}$$

Donc lorsque n n'est pas premier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ possède des diviseurs de zéro et n'est alors pas intègre. □

LemCaractIntergernbrcartpre

Lemme 3.124.
La caractéristique[51] *d'un anneau intègre est zéro ou un élément premier*[52].

Démonstration. Si A est intègre, alors $\mathbb{Z}1_A$ est a fortiori intègre. Notons p la caractéristique de A. Si $p = 0$, la preuve est finie ; supposons donc que $p \neq 0$. Alors, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à $\mathbb{Z}1_A$, et est donc intègre. Or, la proposition 3.123 dit que $\mathbb{Z}/p\mathbb{Z}$ est intègre si et seulement si p est premier, ce qui conclut la preuve. □

Exemple 3.125.
Il existe des corps dont la caractéristique n'est pas égale au cardinal (contrairement à ce que laisserait penser l'exemple des $\mathbb{Z}/p\mathbb{Z}$). En effet les matrices $n \times n$ inversibles sur $\mathbb{F}_3$ forment un corps qui n'est pas de cardinal trois alors que la caractéristique est 3 :

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = 0. \tag{3.178}$$

△

PropomqcGe

Proposition 3.126 (Thème 18, [1])**.**
Soit A un anneau principal[53] *qui n'est pas un corps. Pour un idéal propre I de A, les conditions suivantes sont équivalentes :*

ITEMooNOVFooEHtcwE

(1) I est un idéal maximal[54] *;*

ITEMooMQWVooNocVEU

(2) I est un idéal premier non nul[55] *;*

ITEMooJBXGooEISNuW

(3) il existe p irréductible[56] *dans A tel que $I = (p)$.*

Démonstration. En plusieurs implications.

[50] Définition 1.213.
[51] Définition 3.114.
[52] Définition 3.13.
[53] Définition 3.37.
[54] Définition 3.85.
[55] Définition 3.88.
[56] Définition 3.14.

(1) **(1) implique (2)** Par hypothèse, I est un idéal propre, de plus il n'est pas égal à $\{0\}$, parce que lorsque A et $\{0\}$ sont les seuls idéaux, nous avons un corps (proposition 3.84). Étant donné que I est un idéal maximal, le quotient A/I est un corps par la proposition 3.86.

Soient maintenant, pour entrer dans le vif du sujet, des éléments $a, b \in A$ tels que $ab \in I$. Dans le corps A/I nous avons $[ab] = 0$, et par définition du produit dans le quotient, $[a][b] = 0$. Par intégrité de l'anneau A/I (un corps est un anneau intègre, lemme 3.121) nous avons soit $[a] = 0$, soit $[b] = 0$, soit les deux en même temps. Dans tous les cas, soit a soit b est dans I.

(2) **(2) implique (3)** Maintenant I est un idéal premier non réduit à $\{0\}$. Puisque A est un anneau principal, il existe $x \in A$ tel que $I = (x)$. Nous devons prouver que x peut être choisi irréductible ; et nous allons faire plus : nous allons prouver que x ne peut être que irréductible[57].

Supposons que x ne soit pas irréductible. Alors il existe $a, b \in A$ non inversibles tels que $x = ab$. Si $a \in (x)$ alors il existe $k \in A$ tel que $a = xk$, et en particulier, $a = abk$, c'est-à-dire $1 = bk$ (parce que A est principal et donc intègre). Cela signifie que b est inversible alors que nous avions dit qu'il ne l'était pas. Nous en déduisons que a n'est pas dans (x). On montre de manière similaire que b n'est pas dans (x) non plus.

Nous nous retrouvons donc avec $a, b \in A$ tel que $ab \in I$ sans que ni a ni b ne soient dans I. Cela contredit le fait que I soit un idéal premier. En conclusion, x est irréductible.

(3) **(3) implique (1)** Nous avons $I = (p)$ avec p irréductible dans A. Supposons que J est un idéal différent de A contenant I. Comme A est principal, il existe $y \in A$ tel que $J = (y)$. En particulier $p \in J$, donc $p = ay$ pour un certain $a \in A$. Mais p est irréductible, donc soit a est inversible, soit y est inversible. Si y est inversible, alors $J = A$, ce qui est exclu. Si a est inversible, alors $(y) = (p)$, et $I = J$.

□

3.127.
Dans la proposition 3.126, l'hypothèse d'idéal propre est importante. En effet dans le cas $I = A$, nous avons évidemment que I est un idéal maximum. Mais A n'est d'abord pas un idéal premier parce qu'un idéal premier doit être strictement inclus dans l'anneau. Et ensuite, A est en général loin d'être garanti d'être égal à (p) pour un de ses éléments p.

PropoTMMXCx

Proposition 3.128.
Soit A un anneau principal, et soit $p \in A$ un élément irréductible. Alors

(1) (p) est un idéal maximum.

ITEMooKPJQooWuPZXS

(2) $A/(p)$ est un corps.

Démonstration. Nous notons $I = (p)$. Soit un idéal J contenant I. Comme A est principal, J est monogène : $J = (q)$. Mais comme p est dans I qui est dans J, il existe $a \in A$ tel que $p = qa$.

Puisque p est irréductible, soit q, soit a est inversible. Si q est inversible, alors $J = A$. Si a est inversible, alors nous avons $p = qa$, donc $q = pa^{-1}$, ce qui signifie que $q \in (p)$ et donc que $J = I$.

Cela prouve que (p) est un idéal maximum.

Le fait que $A/(p)$ soit un corps est maintenant la proposition 3.86. □

Exemple 3.129.
L'anneau $\mathbb{Z}$ est principal parce qu'il est intègre et que ses seuls idéaux sont les $n\mathbb{Z}$ qui sont principaux : $n\mathbb{Z}$ est engendré par n. △

EXooCJRPooYkWdyr

Exemple 3.130 (Les idéaux de $\mathbb{Z}/n\mathbb{Z}$)**.**
Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux, mais l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal lorsque n n'est pas premier. Nous allons voir ça.

(1) **Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux** Soit un idéal S dans $\mathbb{Z}/n\mathbb{Z}$. Nous considérons la projection canonique $\phi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. La proposition 3.83 dit que $S = \phi(J)$ où J est un idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Mais le corolaire 3.48 nous dit qu'alors $J = m\mathbb{Z}$ pour un certain m. Pour que $m\mathbb{Z}$ contienne $n\mathbb{Z}$, il faut que m divise n.

Bref, $S = \phi(m\mathbb{Z})$ avec $m \mid n$. Nous montrons maintenant que S est engendré par $[m]_n$. D'abord, l'élément $[m]_n$ est bien dans $\phi(m\mathbb{Z})$. Ensuite un élément de $\phi(m\mathbb{Z})$ est de la forme

$$[km]_n = k[m]_n \in ([m]_n). \tag{3.179}$$

[57] ça me semble un peu trop facile. Lisez attentivement, et écrivez-moi pour dire si vous êtes d'accord ou pas.

Donc $S \subset ([m]_n)$. Et l'inclusion dans l'autre sens est tout aussi immédiate : un élément de $([m]_n)$ est de la forme

$$k[m]_n = [km]_n = \phi(km) \in \phi(m\mathbb{Z}). \tag{3.180}$$

(2) **Si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal** Le fait est que lorsque n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre (corolaire 3.123).

(3) **Moralité** Un anneau comme $\mathbb{Z}/6\mathbb{Z}$ est un anneau dont tous les idéaux sont principaux, mais qui n'est pas principal.

△

Exemple 3.131.
Nous verrons dans la proposition 28.70 que l'anneau des fonctions holomorphes sur un compact de $\mathbb{C}$ est principal. △

3.7 Théorèmes chinois et idéaux

PROPooFGDKooPiDCAE

Proposition 3.132 ([70]).
Soit un anneau A. Soient des idéaux $I_1, \dots, I_n$ premiers deux à deux[58]*. Nous posons*

$$J_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j. \tag{3.181}$$

Alors les idéaux J_i sont premiers dans leur ensemble.

Démonstration. Nous y allons par récurrence. Pour $n = 2$ c'est facile parce que $J_1 = I_2$ et $J_2 = I_1$. Donc $J_1 + J_2 = I_2 + I_1 = A$.

Supposons que la propriété soit vraie pour n, et voyons pour $n + 1$. Soient donc des idéaux I_1,..., I_{n+1} premiers deux à deux. Pour $i = 1, \dots, n$ nous posons

$$K_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j. \tag{3.182}$$

Par hypothèse de récurrence les K_i sont premiers dans leur ensemble. Il existe $(k_1, \dots, k_n) \in K_1 \times \dots \times K_n$ tels que

$$k_1 + \dots + k_n = 1. \tag{3.183}$$

Par ailleurs I_i est premier avec I_{n+1}, donc il existe $a_i \in I_i$ et $b_i \in I_{n+1}$ tels que $a_i + b_i = 1$. Nous avons donc l'égalité

$$k_1(a_1 + b_1) + \dots + k_n(a_n + b_n) = 1 \tag{3.184}$$

que nous réarrangeons en

EQooDOFHooQUWtss

$$(k_1a_1 + \dots + k_na_n) + k_1b_1 + \dots + k_nb_n = 1. \tag{3.185}$$

Vu que $k_i \in K_i$ et $a_i \in I_i$ et vu que les idéaux sont absorbants,

$$k_ia_i \in I_i \cap \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j = \bigcap_{j=1}^{n} I_j = \bigcap_{\substack{j=1 \\ j\neq n+1}}^{n+1} I_j = J_{n+1}. \tag{3.186}$$

Vu que cela est vrai pour chaque i, et vu que les idéaux sont stables par somme, nous avons

$$k_1a_1 + \dots + k_na_n \in J_{n+1}. \tag{3.187}$$

De même pour chaque i nous avons $k_i \in I_i$ et $b_i \in I_{n+1}$, et donc

$$k_ib_i \in K_1 \cap I_{n+1} = I_{n+1} \cap \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j = \bigcap_{\substack{j=1 \\ j\neq i}}^{n+1} I_j = J_i. \tag{3.188}$$

[58] Définition 3.4.

Nous pouvons revenir à l'équation (3.185) :

$$\underbrace{(k_1a_1+\ldots+k_na_n)}_{\in J_{n+1}}+\underbrace{k_1b_1}_{\in J_1}+\ldots+\underbrace{k_nb_n}_{\in J_n}=1. \tag{3.189}$$

Nous avons donc démontré que $1\in J_1+\ldots+J_{n+1}$ et donc que ces idéaux sont premiers dans leur ensemble. □

PROPooKWZLooCHhSjs

Proposition 3.133 (Théorème des restes chinois version congruence[70])**.**
Soit un anneau A. Soient $a_1,\ldots,a_n\in A$. Soient des idéaux premiers entre eux $I_1,\ldots,I_n$. Nous considérons l'ensemble

$$S=\{x\in A \text{ tel que } x\in[a_i]_{I_i}\ \forall i\}. \tag{3.190}$$

Alors

ITEMooTGOEooZfsiKG

(1) S est non vide.

ITEMooCECDooQzGovx

(2) Si $x\in S$ alors $S=[x]_{I_1\cap\ldots\cap I_n}$.

Démonstration. En deux parties.

(1) **Pour (1)** Nous commençons par poser

$$J_i=\bigcap_{\substack{j=1\\ j\neq i}}^{n}I_j \tag{3.191}$$

qui sont des idéaux premiers dans leur ensemble par 3.132. Il existe donc $(j_1,\ldots,j_n)\in J_1\times J_n$ tel que $j_1+\ldots+j_n=1$. Nous posons alors

$$x=a_1j_1+\ldots+a_nj_n, \tag{3.192}$$

et nous vérifions que $x\in S$. Pour cela nous fixons un i et nous calculons un petit peu :

$$\begin{aligned}x-a_i&=a_1j_1+\ldots+a_nj_n-(a_ij_1+\ldots+a_ij_n) &(3.193a)\\ &=(a_1-a_i)j_1+\ldots+(a_n-a_i)j_n. &(3.193b)\end{aligned}$$

SUBEQooKDVXooKfVntq

Notez que dans la dernière somme, le coefficient de j_i est $(a_i-a_i)=0$. Pour les autres termes $(k\neq i)$ nous avons

$$(a_k-a_i)j_k\in J_k=\bigcup_{\substack{l=1\\ l\neq k}}^{n}I_l\subset I_i. \tag{3.194}$$

La dernière inclusion est parce que $i\neq k$, donc il y a un terme $l=i$ dans l'intersection. Nous avons démontré que chaque terme de la somme (3.193b) est dans I_i.

Donc $x-a_i\in I_i$. Cela étant valable pour tout i, nous avons bien prouvé que $x\in S$.

(2) **Pour (2)** Soit $x\in S$. Nous prouvons les deux inclusions.

(2a) $S\subset[x]_{I_1\cap\ldots\cap I_n}$ Soit $s\in S$. Vu que x et s sont dans S, pour chaque i nous avons

$$\begin{aligned}s-a_i&=e_i &(3.195a)\\ x-a_i&=f_i &(3.195b)\end{aligned}$$

pour certains éléments $e_i,f_i\in I_i$. En soustrayant, $s-x=e_i-f_i\in I_i$. Un tel calcul étant valable pour chaque I, nous avons $s-x\in I_1\cap\ldots\cap I_n$, c'est-à-dire $s\in[x]_{I_1\cap\ldots\cap I_n}$.

(2b) $[x]_{I_1\cap\ldots\cap I_n}\subset S$ Nous posons $s=x+e$ avec $e\in I_1\cap\ldots\cap I_n$, et nous prouvons que $s\in S$. Nous avons

$$s-a_i=\underbrace{x-a_i}_{\in I_i}-\underbrace{e}_{\in I_i}\in I_i. \tag{3.196}$$

Donc $s\in[a_i]_{I_i}$ pour chaque i. Donc $s\in S$.

□

THOooCBWWooEGjeSV

Théorème 3.134 (Théorème des restes chinois version anneaux quotients, thème 3[70, 101])**.**
Soient un anneau A et des idéaux $I_1,\ldots,I_n$ premiers entre eux deux à deux.

ITEMooPNFZooInhOQo

(1) *Il existe une unique application* $f\colon A/I_1\cap\ldots\cap I_n\to A/I_1\times\ldots\times A/_n$ *vérifiant*

$$f\big([x]\big)=\big([x]_{I_1},\ldots,[x]_{I_n}\big) \tag{3.197}$$

pour tout $x\in A$.

ITEMooYSDNooSpMVcB

(2) *Cette application est un isomorphisme d'anneaux.*

Démonstration. En plusieurs points.

(1) **Existence et unicité** Nous considérons l'application

$$\begin{aligned} g\colon A&\to A/I_1\times\ldots\times A/I_n\\ x&\mapsto\big([x]_{I_1},\ldots,[x]_{I_n}\big).\end{aligned} \tag{3.198}$$

Afin d'utiliser la proposition 1.58 nous vérifions que si $u\in[x]_{I_1\cap\ldots\cap I_n}$ alors $g(x)=g(y)$. En effet dire $y\in[x]$ signifie $x-y\in I_1\cap\ldots\cap I_n$ et donc pour tout j nous avons $x-y\in I_j$. Du coup pour tout j nous avons $[x]_{I_j}=[y]_{I_j}$. Voilà. Donc la proposition 1.58 prouve le point (1).

(2) **Injective** Soient $\alpha,\beta\in A/I_1\cap\ldots\cap I_n$ tels que $f(\alpha)=f(\beta)$. Nous considérons $x\in\alpha$ et $y\in\beta$. Nous avons

$$f(\alpha)=\big([x]_{I_1},\ldots,[x]_{I_n}\big) \tag{3.199a}$$
$$f(\beta)=\big([y]_{I_1},\ldots,[y]_{I_n}\big). \tag{3.199b}$$

Donc $[x]_{I_i}=[y]_{I_i}$ pour tout i. Pour chaque i, il existe un $e_i\in I_i$ tel que $x-y=e_i$. Forcément tous les e_i sont égaux et nous avons donc $x-y\in I_1\cap\ldots\cap I_n$. Cela prouve que $\alpha=\beta$ et donc que f est injective.

(3) **Surjective** Soient $\alpha_i\in A/I_i$. Nous avons besoin de trouver $\alpha\in A/I_I\cap\ldots\cap I_n$ tel que $f(\alpha)=(\alpha_1,\ldots,\alpha_n)$. Pour chaque α_i nous considérons $a_i\in\alpha_i$ et nous cherchons $x\in A$ tel que

$$x\in[a_i]_{I_i} \tag{3.200}$$

pour tout i. La version congruence du théorème chinois (proposition 3.133) dit qu'un tel x existe. En prenant $\alpha=[x]_{I_1\cap\ldots\cap I_n}$ nous avons bien $f(\alpha)=(\alpha_1,\ldots,\alpha_n)$.

(4) **Morphisme** L'application f est un morphisme d'anneaux parce que si $\alpha,\beta\in A/I_1\cap\ldots\cap I_n$ et si $x\in\alpha$ et $y\in\beta$, alors

$$f(\alpha+\beta)=f([x]+[y])=f([x+y])=\big([x+y]_1,\ldots,\big)=\big([x]_1+[y]_1,\ldots,\big)=f(\alpha)+f(\beta). \tag{3.201}$$

Le même genre de vérification marche pour le produit.

□

Pour la suite nous rappelons que $[x]_a$ est la classe de x pour le quotient par l'idéal (a). Donc

$$[x]_a=\{y\in A\text{ tel que }x-y\in(a)\}. \tag{3.202}$$

Notez au passage que

$$[xa]_a=[0]_a \tag{3.203}$$

EQooJAAQooJCcmVE

Nous avons vu dans 3.39 que $\mathbb{Z}$ est principal ; le lemme suivant nous dit que $\mathbb{Z}[X]$ n'est lui, pas principal.

LEMooDJSUooJWyxCL

Lemme 3.135 ([102]).
Si A *est un anneau intègre*[59] *qui n'est pas un corps, alors* $A[X]$ *n'est pas principal.*

Démonstration. Soit un élément non nul $a\in A$.

[59] Définition 3.22.

(1) **Un idéal principal contenant a et X est A[X]**

Soit (P) un idéal principal contenant a et X. Puisque $a \in (P)$, il existe Q tel que $a = QP$. Donc P divise a dans $\mathbb{Z}[X]$. L'égalité des degrés indique que P est un polynôme constant, c'est-à-dire en réalité un élément de A. Soit $P = k \in A$.

Comme P divise X, nous avons aussi $X = kQ$ pour un certain $Q \in \mathbb{Z}[X]$. L'égalité des degrés dit qu'il existe $k' \in A$ tel que $Q = k'X$ et donc $Q = k'X = k'kQ$, ce qui implique que $kk' = 1$. L'idéal engendré par k contient donc en particulier $kk' = 1$ et donc contient $A[X]$ en entier :

$$1 = k'k \in k'(P) = (P). \tag{3.204}$$

(2) **Si $(a, X) = A[X]$ alors a est inversible**

Si $(a, X) = A[X]$, en particulier, $1 \in (a, X)$, ce qui signifie qu'il existe des polynômes $U, V \in A[X]$ tels que

$$1 = UX + Va. \tag{3.205}$$

Nous évaluons cette égalité en 0 : comme $(UX)(0) = 0$, nous avons $1 = V(0)a$, ce qui signifie que $V(0)$ est un inverse de A. Donc a est inversible.

(3) **Si a n'est pas inversible alors (a, X) n'est pas principal**

Si (a, X) était principal, alors nous aurions, par ce qui est dit plus haut, $(a, X) = A[X]$. Mais cette dernière égalité impliquerait que a soit inversible.

En conclusion, si A n'est pas un corps, il possède un élément ni nul ni inversible. Dans ce cas, l'idéal (a, X) n'est pas principal dans $A[X]$ et nous en déduisons que $A[X]$ n'est pas un anneau principal. □

Nous verrons dans le lemme 3.266 que si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est principal.

3.8 Sous-groupe normal

propGroupeNormal

Proposition 3.136.
Soit N un sous-groupe de G. Les propriétés suivantes sont équivalentes :

ITEMooDYEUooOuKEqQ

(1) N est normal[60] dans G.

ITEMooPYTEooZhvrUa

(2) N est une union de classes de conjugaison[61] de G,

ITEMooJWTLooBRmriQ

(3) $gNg^{-1} \subseteq N$ pour tout $g \in G$,

ITEMooVRZIooAorhRY

(4) $gNg^{-1} = N$ pour tout $g \in G$,

ITEMooJGUOooYshOZa

(5) $gN = Ng$ pour tout $g \in G$,

ITEMooMRYRooZifCCe

(6) Le normalisateur[62] de N est G : $\mathcal{N}_G(N) = G$.

Démonstration. En plusieurs parties.

(1) **(1) implique (3)** C'est la définition de sous-groupe normal.

(2) **(3) implique (4)** Soit $g \in G$. Nous avons $gNg^{-1} \subset N$, mais aussi (en appliquant l'hypothèse à g^{-1}) $g^{-1}Ng \subset N$. En combinant nous avons

$$N \subset g(g^{-1}Ng)g^{-1} \subset gNg^{-1}. \tag{3.206}$$

Nous avons l'inclusion dans les deux sens. Donc l'égalité.

(3) **(4) implique (5)** Soit $g \in G$. Un élément général de gN est de la forme gn avec $n \in N$. Nous devons trouver un $n' \in N$ tel que $gn = n'g$. En posant $n' = gng^{-1}$ nous avons

$$n' = gng^{-1} \in gNg^{-1} \subset N. \tag{3.207}$$

Il est immédiat de prouver que $gn = n'g$. Cela prouve que $gN \subset Ng$.

Le même raisonnement donne $Ng \subset gN$.

[60] Définition 2.13.
[61] Définition 2.8.
[62] Définition 2.14.

(4) **(5) implique (3)** Un élément de gNg^{-1} est $a = gng^{-1}$ avec $n \in N$. Nous devons prouver que $a \in N$. Puisque $gn \in gN$, par hypothèse il existe n' tel que $gn = n'g$. En remplaçant dans la définition de a,

$$a = gng^{-1} = n'gg^{-1} = n' \in N. \tag{3.208}$$

(5) **(5) implique (2)** Pour chaque $a \in G$ nous notons C_a la classe de conjugaison de a dans G :

$$C_a = \{gag^{-1} \text{ tel que } g \in G\}. \tag{3.209}$$ EQooJIEVooCAshfe

Comme $a \in C_a$ (prendre $g = e$ dans (3.209).) nous avons forcément

$$N \subset \bigcup_{n \in N} C_n. \tag{3.210}$$

Prouvons maintenant l'inclusion inverse. Nous avons déjà prouvé que (5) implique (3). Donc si $n \in N$, alors $gng^{-1} \in N$. Nous avons alors

$$C_n = \{gng^{-1} \text{ tel que } g \in G\} \subset N. \tag{3.211}$$

Donc il est vrai que $N = \bigcup_{n \in N} C_n$.

(6) **(2) implique (1)** Nous supposons que $N \subset G$ est un sous-groupe de la forme

$$N = \bigcup_{a \in I} C_a \tag{3.212}$$

où I est une partie de G. Nous devons montrer que pour tout $g \in G$ et pour tout $n \in N$ nous avons $gng^{-1} \in N$. Puisque $n \in N$, il existe $a \in I$ tel que $n \in C_a$ et donc il existe $k \in G$ tel que $n = kak^{-1}$. Nous avons donc

$$gng^{-1} = g(kak^{-1})g^{-1} = (gk)a(gk)^{-1} \in C_a \subset N. \tag{3.213}$$

Le lecteur attentif aura remarqué l'utilisation de l'axiome du choix. La prudence l'incitera à ne pas le faire remarquer au jury.

(7) **(6) si et seulement si (5)** C'est la définition du normalisateur.

□

Définition 3.137.
Soit $g \in G$ et $n \in \mathbb{Z}$. Nous définissons g^n par

(1) $g^0 = e$ et $g^n = gg^{n-1}$ si n est positif.

(2) si $n < 0$, nous posons $g^n = (g^{-1})^{-n}$.

LemHUkMxp

Lemme 3.138 ([57, 18])**.**
Soient un groupe G et deux sous-groupes normaux[63] H et K tels que $H \cap K = \{e\}$. Alors : ITEMooDFVBooSnnlgR

(1) Tout élément de H commute avec tout élément de K. ITEMooVVBGooZSJqjp

(2) HK est un sous-groupe de G. IMTEooPCBZooQoZFOD

(3) L'application

$$\begin{aligned} \varphi\colon H \times K &\to HK \\ (h,k) &\mapsto hk \end{aligned} \tag{3.214}$$

est un isomorphisme de groupes.

Démonstration. Point par point.

(1) **(1)** Soient $h \in H$ et $k \in K$. Nous voulons montrer que $hk = kh$. Pour cela nous considérons l'élément $a = hkh^{-1}k^{-1}$. Comme H est normal dans G, nous avons

$$kh^{-1}k^{-1} \in H \tag{3.215}$$

et donc $a \in H$. De même K étant normal dans G, nous avons $hkh^{-1} \in K$ et donc $a \in K$. Au final $a \in H \cap K = \{e\}$. Nous avons prouvé que

$$hkh^{-1}k^{-1} = e, \tag{3.216}$$

et donc que $hk = kh$.

[63] Sous-groupe normal, définition 2.13.

(2) **(2)** Puisque H et K sont des sous-groupes, $\{e\}$ est dans les deux, de telle sorte que $e \in HK$. De plus si $h_i \in H$ et $k_i \in K$, la commutativité du point (1) donne

$$(h_1k_1)(h_2k_2) = h_1h_2k_1k_2 \in HK. \tag{3.217}$$

Donc le produit de deux éléments de HK est dans HK.

(3) **(3)** En trois sous-parties.

(3a) **Morphisme** Soient $h_i \in H$ et $k_i \in K$. En utilisant la commutativité du point (1) nous avons

$$\begin{aligned}\varphi\big((h_1,k_1)(h_2,k_2)\big) &= \varphi(h_1h_2,k_1k_2) && (3.218a)\\ &= (h_1h_2)(k_1k_2) && (3.218b)\\ &= (h_1k_1)(h_2k_2) && (3.218c)\\ &= \varphi(h_1,k_1)\varphi(h_2,k_2). && (3.218d)\end{aligned}$$

(3b) **Injectif** Si $\varphi(h_1,k_1) = \varphi(h_2,k_2)$ nous avons successivement

$$\begin{aligned}h_1k_1 &= h_2k_2 && (3.219a)\\ h_1k_1h_2^{-1} &= k_2 && (3.219b)\\ h_1k_1h_2^{-1}k_1^{-1} &= k_2k_1^{-1} && (3.219c)\\ h_1h_2^{-1} &= k_2k_1^{-1}. && (3.219d)\end{aligned}$$

Le membre de gauche est un élément de H et le membre de droite un élément de K. Comme $H \cap K = \{e\}$ nous avons $h_1h_2^{-1} = e$ et $k_2k_1^{-1} = e$, c'est-à-dire $h_1 = h_2$ et $k_1 = k_2$.

(3c) **Surjectif** Un élément général de HK est hk avec $h \in H$ et $k \in K$, c'est-à-dire $\varphi(h,k)$.

□

DefvtSAyb

Définition 3.139.
*L'**exposant** du groupe G est le plus petit entier non nul n tel que $g^n = e$ pour tout $g \in G$. S'il n'existe pas un tel n, nous disons que l'exposant du groupe est infini.*

PROPooSWHHooOzqWkw

Proposition 3.140.
À propos d'exposant de groupe et de ppcm.

ITEMooFIPBooFOaPkU

(1) Si l'ensemble des ordres de tous les éléments d'un groupe est majoré, alors l'exposant du groupe est le plus petit commun multiple des ordres des éléments du groupe.

ITEMooLIREooYEtcdL

(2) Pour un groupe fini, l'exposant est le ppcm *des ordres des éléments du groupe.*

Démonstration. En deux parties.

(1) **Pour (1)** Soit p le ppcm des ordres de tous les éléments du groupe. Si g est d'ordre a, il existe $k \in \mathbb{N}$ tel que $p = ak$. Avec ça nous avons $g^p = (g^a)^k = e^k = e$. Donc p a bien la propriété $g^p = e$ pour tout $g \in G$.

Si $q < p$, nous montrons que q ne peut pas avoir cette propriété. Il existe un élément g dont l'ordre a ne divise pas q. Par la division euclidienne 3.40, nous avons des entiers u et v tels que $q = ua + v$ avec $v < a$. Nous avons alors

$$g^q = g^{ua}g^v = g^v \neq e \tag{3.220}$$

parce que $v < a$ et que a est le plus petit n tel que $g^n = e$.

(2) **Pour (2)** Même chose. Pour un groupe fini, le ppcm existe toujours.

□

Le théorème de Burnside 10.314 nous donnera un bon paquet d'exemples de groupes d'exposant fini dans $\mathrm{GL}(n,\mathbb{C})$.

PropSRMJooIDPBoW

Proposition 3.141.
Soit un groupe G. Nous considérons un sous-groupe normal H de G ainsi qu'un morphisme $\psi\colon G \to H$. Alors

(1) $\psi(H)$ est normal dans $\psi(G)$

(2) Si G/H est abélien alors $\psi(G)/\psi(H)$ est abélien.

Démonstration. Soient $h \in H$ et $g \in G$. Alors $\psi(g)\psi(h)\psi(g)^{-1} = \psi(ghg^{-1}) \in \psi(H)$. Donc $\psi(H)$ est normal dans $\psi(G)$.

Pour la seconde partie nous notons $[\dots]$ les classes par rapport à $\psi(H)$ et $\overline{\dots}$ celles par rapport à H. Nous avons

$$\begin{aligned}
[\psi(g_1)][\psi(g_2)] &= \big[\psi(g_1)\psi(g_2)\big] && (3.221a)\\
&= \big[\psi(g_1g_2)\big] && (3.221b)\\
&= \{\psi(g_1g_2)\psi(h) \text{ tel que } h \in H\} && (3.221c)\\
&= \{\psi(g_1g_2h) \text{ tel que } h \in H\} && (3.221d)\\
&= \psi\Big(\{g_1g_2h \text{ tel que } h \in H\}\Big) && (3.221e)\\
&= \psi\big(\overline{g_1g_2}\big) && (3.221f)\\
&= \psi(\overline{g_2g_1}) && (3.221g)\\
&= \text{refaire à l'envers} && (3.221h)\\
&= [\psi(g_2)][\psi(g_1)]. && (3.221i)
\end{aligned}$$

Par conséquent $\psi(G)/\psi(H)$ est abélien. □

3.9 Inversibles et nilpotents

Le concept d'anneau est la définition 1.100.

LEMooOYZEooLivKWI

Lemme 3.142.
Si a et b commutent, nous avons, pour tout $r \in \mathbb{N}$ et $r > 0$, la formule

$$a^{r+1} - b^{r+1} = (a-b)\left(\sum_{k=0}^{r} a^{r-k}b^k\right). \tag{3.222}$$

Eqazpurmkbk

Démonstration. Démontrons cela par récurrence. Le cas $r = 0$ est évident. Pour un r donné, si (3.222) est vraie, alors

$$\begin{aligned}
a^{r+2} - b^{r+2} &= a^{r+1}a - a^{r+1}b + a^{r+1}b - b^{r+1}b\\
&= a^{r+1}(a-b) + (a^{r+1} - b^{r+1})b\\
&= a^{r+1}(a-b) + (a-b)\left(\sum_{k=0}^{r} a^{r-k}b^k\right)b\\
&= (a-b)\left(a^{r+1} + \left(\sum_{k=0}^{r} a^{r-k}b^k\right)b\right)\\
&= (a-b)\left(a^{r+1} + \sum_{k=0}^{r} a^{r-k}b^{k+1}\right)\\
&= (a-b)\left(a^{r+1} + \sum_{k'=1}^{r+1} a^{(r+1)-k'}b^{k'}\right)\\
&= (a-b)\left(\sum_{k'=0}^{r+1} a^{(r+1)-k'}b^{k'}\right).
\end{aligned}$$

□

Proposition 3.143.
Si a est un élément nilpotent de l'anneau A, alors $1-a$ est inversible. Si a est nilpotent non nul, alors il est diviseur de zéro.

Démonstration. Soit n le minimum tel que $a^n = 0$. En vertu de la formule (3.222) nous avons

$$1 = 1 - a^n = (1-a)(1 + a + \cdots + a^{n-1}) = (1 + a + \cdots + a^{n-1})(1-a). \tag{3.223}$$

La somme $1 + a + \cdots + a^{n-1}$ est donc un inverse de $(1-a)$. □

PROPooQMZMooBrQhhr

Proposition 3.144 ([1]).
Soit un anneau (pas spécialement commutatif) A. Si $a_i \in A$, alors

$$\sum_i \sum_j a_i a_j = \sum_i a_i^2 + 2\sum_{i<j} a_i a_j = (\sum_i a_i)^2 + \sum_{i<j} [a_i a_j] \tag{3.224}$$

où $[x, y]$ signifie $xy - yx$.

3.10 PGCD, PPCM et éléments inversibles

La définition de pgcd et ppcm dans un anneau commutatif est la définition 1.113. Dans la plus grande tradition, elle a été introduite sans motivation, et utilisée par-ci par-là. Nous revenons maintenant dessus.

Commençons par donner une autre vision de la divisibilité dans les anneaux intègres.

PropDiviseurIdeaux

Proposition 3.145.
Dans un anneau intègre[64] *A, on a l'équivalence suivante concernant deux éléments $a, b \in A$:*

$$a \mid b \Leftrightarrow (b) \subset (a). \tag{3.225}$$

Donc la divisibilité devient en réalité une relation d'ordre dont nous pouvons chercher un maximum et un minimum. Si S est une partie de A, nous notons $a \mid S$ pour exprimer que $a \mid x$ pour tout $x \in S$; de la même façon, $S \mid b$ signifie que $x \mid b$ pour tout $x \in S$.

Nous rappelons également la définition 1.106 de morphisme d'anneaux. Remarquons que si f est un morphisme, nous avons $f(0) = 0$ et $f(x)^{-1} = f(x^{-1})$.

Lemme 3.146 ([103]).
Les éléments inversibles d'un anneau sont diviseurs de tous les éléments.

Démonstration. Soit k inversible d'inverse k' : $kk' = 1$; soit aussi $a \in A$. Alors $a = k(k'a)$, ce qui montre que k divise a. □

Lemme 3.147 ([103]).
Dans un anneau, 1 est un pgcd de a et b si et seulement si les seuls diviseurs communs sont les inversibles.

Démonstration. Supposons pour commencer que 1 est un pgcd de a et b. Un diviseur commun de a et b doit donc diviser 1. Or un diviseur de 1 est forcément inversible.

Dans l'autre sens, les diviseurs communs de a et b sont tous inversibles et donc diviseurs de 1. Donc 1 est un pgcd de a et b. □

3.10.1 Calcul effectif du PGCD et théorème de Bézout

subSecIpmnhO

Soient a et b, deux entiers que nous allons prendre positifs. Nous allons voir maintenant l'algorithme de **Euclide étendu** qui est capable, pour a et b donnés, de calculer le PGCD de a et b, et un couple de Bézout (u, v) tel que $ua + vb = \text{pgcd}(a, b)$. Ce calcul est indispensable si on veut implémenter RSA (21.2).

3.148.
Cette vidéo de numberphile en parle : https://www.youtube.com/watch?v=6Y3jHHE_hbA (Euclid's algorithm).

Cela se base sur le lemme suivant.

LemiVqita

Lemme 3.149.
Soient $a, b \in \mathbb{N}$ et des nombres q et r tels que $a = qb + r$. Alors $\text{pgcd}(a, b) = \text{pgcd}(r, b)$.

Démonstration. Il suffit de voir que les diviseurs communs de a et b sont diviseurs de r et que les diviseurs communs de r et b divisent a.

Si s divise a et b, alors dans l'équation

$$\frac{a}{s} = \frac{qb}{s} + \frac{r}{s}$$

les termes a/s et qb/s sont entiers, donc r/s est aussi entier, et s divise r.

Inversement, si s divise r et b, alors il divise $qb + r$ et donc a. □

[64] Définition 3.22.

Remarque 3.150.
Ce lemme est surtout intéressant lorsque $a = qb + r$ est la division euclidienne de a par b : en effet, dans ce cas $r < b$, et le calcul du PGCD de deux nombres (a et b) est ramené à un calcul de PGCD de deux nombres plus petits (b et r).

L'algorithme pour calculer $\text{pgcd}(a, b)$ consiste à écrire des divisions euclidiennes successives de la manière suivante :

$$a = q_2 b + r_2 \qquad r_2 < b \tag{3.226a}$$
$$b = q_3 r_2 + r_3 \qquad r_3 < r_2 \tag{3.226b}$$
$$\vdots \tag{3.226c}$$

en remarquant que $\text{pgcd}(a, b) = \text{pgcd}(b, r_2) = \text{pgcd}(r_2, r_3)$. Étant donné que les inégalités $r_2 < b$ et $r_3 < r_2$ sont strictes, en continuant ainsi nous finissons sur zéro, c'est-à-dire qu'il existera un n pour lequel $r_{n+1} = 0$; et donc

$$r_{n-1} = q_{n+1} r_n,$$

et à ce moment nous avons $\text{pgcd}(a, b) = \text{pgcd}(r_{n-1}, r_n) = r_n$.

3.10.1.1 Algorithme d'Euclide pour le PGCD

SUBSECooAEBLooFGJRkg

Écrivons l'algorithme[104] en détail (parce que Bézout, ça va être la même chose en cinq fois plus compliqué). On pose

$$r_0 = a \tag{3.227a}$$
$$r_1 = b \tag{3.227b}$$

(ce qui explique que nous n'ayons pas utilisé r_0 et r_1 précédemment). Ensuite on écrit la division euclidienne $a = q_2 b + r_2$, c'est-à-dire $r_0 = q_2 r_1 + r_2$. Cela donne r_2 et q_2 en termes de r_0 et r_1 :

$$r_2 = r_0 - q_2 r_1. \tag{3.228}$$

Ensuite, sachant r_2 nous pouvons continuer :

$$r_1 = q_3 r_2 + r_3 \tag{3.229}$$

donne q_3 et $r_3 = r_1 - q_3 r_2$. On continue avec $r_2 = q_4 r_3 + r_4$. Tout cela pour poser la suite

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_k &= q_{k+2} r_{k+1} + r_{k+2} \end{aligned} \tag{3.230}$$

SUBEQooDYUEooYNQnIJ

où la troisième équation définit r_{k+2} et q_{k+2} en fonction de r_k et r_{k+1}, à l'aide du théorème de la division euclidienne. La suite (r_k) ainsi construite est strictement décroissante et à chaque étape le lemme 3.149 et le principe de l'algorithme d'Euclide nous donnent

$$\begin{cases} \text{pgcd}(r_k, r_{k+1}) = \text{pgcd}(r_{k+1}, r_{k+2}) = \text{pgcd}(a, b) & \text{(3.231a)} \\ 0 \leqslant r_{k+1} < r_k. & \text{(3.231b)} \end{cases}$$

La suite étant strictement décroissante, nous prenons r_n, le dernier non nul : $r_{n+1} = 0$. Dans ce cas, en prenant $k = n - 1$ dans la la dernière équation (3.230) devient :

$$r_{n-1} = q_{n+1} r_n \tag{3.232}$$

avec $\text{pgcd}(a, b) = \text{pgcd}(r_n, r_{n-1}) = r_n$.

Exemple 3.151.
Calculons le PGCD de 18 et 231. Pour cela nous écrivons les divisions euclidiennes en chaine :

$$231 = 18 \cdot 12 + 15 \tag{3.233a}$$
$$18 = 1 \cdot 15 + 3 \tag{3.233b}$$
$$15 = 5 \cdot 5 + 0. \tag{3.233c}$$

Donc le PGCD est 3 (le dernier reste non nul). △

3.10.1.2 Algorithme étendu : calcul effectif des coefficients de Bézout

SUBSECooRHSQooEuBWbd

La difficulté est de construire la suite qui donne des coefficients de Bézout. Elle va être construite à l'envers. Nous supposons déjà connaitre la liste complète des r_k jusqu'à $r_n = \text{pgcd}(a, b)$, ainsi que la liste complète des divisions euclidiennes

$$r_k = q_{k+2}r_{k+1} + r_{k+2}. \tag{3.234}$$

Nous voulons trouver les couples (u_k, v_k) de telle façon à avoir à chaque étape

$$r_n = u_k r_k + v_k r_{k-1}. \tag{3.235}$$

Notons que c'est à chaque fois r_n que nous construisons. La première équation de type Bézout à résoudre est

$$r_n = u_n r_n + v_n r_{n-1}, \tag{3.236}$$

sachant que $r_{n-1} = q_{n+1}r_n$. On pose $v_n = 0$ et $u_n = 1$ et c'est bon. Pour la récurrence, supposons les coefficients u_k et v_k connus, et déterminons les coefficients u_{k-1} et v_{k-1}. Pour ce faire, nous égalons les deux expressions pour r_n :

$$r_n = u_k r_k + v_k r_{k-1} = u_{k-1}r_{k-1} + v_{k-1}r_{k-2}; \tag{3.237}$$

dans laquelle nous substituons $r_{k-2} = q_k r_{k-1} + r_k$:

$$\begin{aligned} u_k r_k + v_k r_{k-1} &= u_{k-1}r_{k-1} + v_{k-1}(q_k r_{k-1} + r_k) && (3.238)\\ &= (u_{k-1} + q_k v_{k-1})r_{k-1} + v_{k-1}r_k && (3.239) \end{aligned}$$

et nous égalons les coefficients de r_k et r_{k-1} pour obtenir

$$\begin{cases} v_{k-1} = u_k & (3.240a)\\ u_{k-1} = v_k - v_{k-1}q_k. & (3.240b) \end{cases}$$

Dès que u_k et v_k ainsi que q_k sont connus, on peut calculer u_{k-1} et v_{k-1}.

La dernière équation, celle avec $k = 1$, est

$$r_n = u_1 r_1 + v_1 r_0, \tag{3.241}$$

c'est-à-dire

EqNDMLooDyaiAc

$$\text{pgcd}(a, b) = u_1 b + v_1 a. \tag{3.242}$$

Nous avons ainsi trouvé des coefficients de Bézout pour a et b.

3.10.2 Générateurs

3.152.
Les éléments de $\mathbb{Z}/n\mathbb{Z}$ ne sont pas des éléments de $\mathbb{Z}$; ce sont des parties de $\mathbb{Z}$. Pour rappel :

$$[a]_n = \{a + kn \text{ tel que } k \in \mathbb{Z}\}. \tag{3.243}$$

Pour écrire les éléments de $\mathbb{Z}/n\mathbb{Z}$, nous pouvons écrire

$$\{[i]_n\}_{i=1,\dots,n} \tag{3.244}$$

ou

$$\{[i]_n \text{ tel que } 1 \leqslant i \leqslant n\}. \tag{3.245}$$

Mais attention : l'ensemble

$$\bigcup_{i=1}^{n} [i]_n \tag{3.246}$$

est très différent. Ce dernier ensemble est $\mathbb{Z}$.

PROPooEWREooUOSMsE

Proposition 3.153 ([105]).
Soit $n \geqslant 2$.

ITEMooHTRHooDWgXlk

(1) L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ contient n éléments

(2) Nous avons $\mathbb{Z}/n\mathbb{Z} = \{[k]_n\}_{k=0,\dots,n-1}$.

Démonstration. Nous montrons que

$$\begin{aligned}\varphi\colon \{1,\dots,n\} &\to \mathbb{Z}/n\mathbb{Z}\\ k &\mapsto [k]_n\end{aligned} \tag{3.247}$$

est une bijection.

(1) **Injective** Supposons que $\varphi(k)=\varphi(l)$ pour $k,l\in\{1,\dots,n\}$. Il existe $t\in\mathbb{Z}$ tel que $l=l+tn$. Si $t>0$, alors nous avons

$$l+tn\geqslant 1+n>n, \tag{3.248}$$

ce qui est impossible parce que $k\in\{0,\dots,n\}$. Nous montrons de même que $t<0$ est impossible. Nous en déduisons que $t=0$ et donc que $k=l$.

(2) **Surjective** Soit $l\in\mathbb{Z}$. Nous allons montrer que $[l]_n$ est dans l'image de φ. Par la division euclidienne 3.40, il existe $q\in\mathbb{Z}$ et $r<n$ (dans $\mathbb{N}$) tels que $l=qn+r$. Nous venons de prouver que $[l]_n=[r]_n=\varphi(r)$.

Pour le point (2), c'est juste l'image de φ. □

PROPooMTWGooEMbvDi

Proposition 3.154 ([105]).
Soit $n\geqslant 2$ et $m\in\mathbb{Z}$. Nous avons équivalence entre

ITEMooMCIJooItgSHc

(1) $\operatorname{pgcd}(n,m)=1$,

ITEMooMNKCooPnpyye

(2) $[m]_n$ *engendre le groupe* $(\mathbb{Z}/n\mathbb{Z},+)$

ITEMooBPWLooFLdJfr

(3) $[m]_n$ *est inversible dans* $\big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big)$.

Démonstration. En trois parties.

(1) **(1) implique (2)**

Si $\operatorname{pgcd}(m,n)=1$, le théorème de Bézout 3.46 donne des $u,v\in\mathbb{Z}$ tels que $um+vn=1$, autrement dit $u[m]_n=[1]_n$. Si k est quelconque, nous avons

$$[k]_n=uk[m]_n, \tag{3.249}$$

ce qui signifie que $[k]_n$ est bien un multiple de $[m]_n$ qui est donc générateur.

(2) **(2) implique (3)**

Si $[m]_n$ engendre $\big(\mathbb{Z}/n\mathbb{Z},+\big)$, il existe en particulier un multiple de $[m]_n$ qui vaut $[1]_n$: il existe $k\in\mathbb{Z}$ tel que $k[m]_n=[1]_n$.

Nous voyons que $[k]_n$ est un inverse de $[m]_n$ dans $\big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big)$.

(3) **(3) implique (1)**

Nous supposons que $[m]_n$ est inversible dans $\big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big)$. C'est-à-dire qu'il existe $k\in\mathbb{Z}$ tel que $[k]_n[m]_n=[1]_n$. Cela signifie qu'il existe $l\in\mathbb{Z}$ tel que

$$km=1+ln. \tag{3.250}$$

Par le théorème de Bézout (pris dans l'autre sens), cela signifie que $\operatorname{pgcd}(m,n)=1$.

□

3.10.3 pgcd, ppcm dans $\mathbb{N}$

LEMooBJVJooFyuFeN

Lemme 3.155 ([1]).
Dans $\mathbb{N}$, le pgcd[65] *et le ppcm sont uniques.*

Démonstration. Supposons que δ_1 et δ_2 soient des pgcd de la partie S. Puisque $\delta_1\mid S$, nous avons $\delta_1\mid\delta_2$ parce que δ_2 est un pgcd. Le même raisonnement, inversant δ_1 et δ_2 montre que $\delta_2\mid\delta_1$. Si (a_p) sont les éléments de la décomposition de δ_1 et (b_p) ceux de δ_2, alors le lemme 3.63 nous indique que $a_p\leqslant b_p$ et $b_p\leqslant a_p$, ce qui implique que $a_p=b_p$.

La démonstration pour le ppcm s'effectue selon le même principe. □

[65] Le pgcd et ppcm sont définis dans 1.113.

LEMooWMZWooCmkOoD

Lemme 3.156.
Si $d \mid \delta$ dans $\mathbb{N}$ alors $d \leqslant \delta$.

Démonstration. Nous avons $k \in \mathbb{N}$ tel que $kd = \delta$. Le lemme 1.203 dit qu'alors $\delta \geqslant d$. □

NORMooNAMKooCKKZMc

3.157.
Rappel de ce que nous disions dans 1.114. Dans $\mathbb{Z}$, le pgcd n'est pas à proprement parler unique, mais nous faisons une exception en disant qu'on ne prend que les pgcd positifs.

LEMooJIGRooARiIPC

Lemme 3.158.
Soit une partie S de $\mathbb{N}$.

(1) Le pgcd de S est le plus grand élément de $\mathbb{N}$ divisant tous les éléments de S.

(2) Le ppcm de S est le plus petit élément de $\mathbb{N}$ que tous les éléments de S divisent.

Démonstration. En deux parties.

(1) **Pour le pgcd** Soit δ, le pgcd de S. Si d divise également tous les éléments de S, nous avons $d \mid \delta$ par définition du pgcd. Le lemme 3.156 dit qu'alors $d \leqslant \delta$.

(2) **Pour le ppcm** Soit le ppcm μ de S. Si m est également divisé par tous les éléments de S nous avons $\mu \mid m$ et donc $\mu \leqslant m$.

□

LEMooEVIZooPAkQZW

Lemme 3.159 ([1]).
Soient $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}$ tels que $ab = q^k$ et $\operatorname{pgcd}(a, b) = 1$. Alors il existe $\alpha, \beta \in \mathbb{Z}$ tels que $a = \alpha^k$ et $b = \beta^k$.

Démonstration. Nous décomposons a, b et q en facteurs premiers suivant le théorème 3.62 :

SUBEQooBJEQooDiWbYs

$$a = \prod_i p_i^{a_i} \tag{3.251a}$$
$$b = \prod_i p_i^{b_i} \tag{3.251b}$$
$$q = \prod_i p_i^{q_i}. \tag{3.251c}$$

D'un part, en utilisant la commutativité et l'associativité du produit,

$$ab = \prod_i p_i^{a_i+b_i}. \tag{3.252}$$

D'autre part, puisque $ab = q^k$, nous avons

$$ab = (\prod_i p_i^{q_i})^k = \prod_i p_i^{kq_i}. \tag{3.253}$$

En vertu de l'unicité de la décomposition en facteurs premiers, pour chaque i nous avons

$$a_i + b_i = kq_i. \tag{3.254}$$

Comme a et b sont premiers entre eux, si $a_i \neq 0$ alors $b_i = 0$ et inversement. Prenons un i tel que $a_i \neq 0$. Alors $b_i = 0$ et nous avons $a_i = kq_i$. Idem pour les b_i.

Donc tous les a_i et les b_i qui sont non nuls sont des multiples de k. Nous posons $a_i = ks_i$ et nous reportons dans (3.251a) :

$$a = \prod_i p_i^{ks_i} = (\prod_i p_i^{s_i})^k, \tag{3.255}$$

de telle sorte que a soit une puissance k^{e}. La même chose tient pour b. □

PROPooNQBOooHWqTvs

Proposition 3.160.
Soient $a, b \in \mathbb{Z} \setminus \{0\}$ décomposés en $a = \prod_{p\in\mathcal{P}} p^{a_p}$ et $b = \prod_{p\in\mathcal{P}} p^{b_p}$. En posant

$$m_p = \min\{a_p, b_p\} \tag{3.256a}$$
$$M_p = \max\{a_p, b_p\}, \tag{3.256b}$$

nous avons

$$\operatorname{pgcd}(a,b)=\prod_{p\in\mathcal{P}}p^{m_p} \tag{3.257a}$$

$$\operatorname{ppcm}(a,b)=\prod_{p\in\mathcal{P}}p^{M_p}. \tag{3.257b}$$

Pour rappel, la définition de pgcd et ppcm sont dans 1.113.

Démonstration. Nous commençons par le pgcd. Nous notons $\delta=\prod_{p\in\mathcal{P}}p^{m_p}$ et nous prouvons que δ est un pgcd de $\{a,b\}$. Il y a deux propriétés à vérifier.

(1) **δ divise a et b** Puisque $m_p=\min\{a_p,b_p\}$, nous avons $m_p\leqslant a_p$ et $m_p\leqslant b_p$. Le lemme 3.63 nous dit alors que $\delta\mid a$ et $\delta\mid b$.

(2) **Si s divise a et b** De même, si $s\mid a$ et $s\mid b$, nous avons $s_p\leqslant a_p$ et $s_p\leqslant b_p$, ce qui montre que $s_p\leqslant m_p$ et donc que $s\mid\delta$.

Pour le ppcm, nous posons $\mu=\prod_{p\in\mathcal{P}}p^{M_p}$, et nous prouvons que μ est un ppcm de $\{a,b\}$.

(1) **a et b divisent μ** Pour tout p, nous avons $M_p\geqslant a_p$. Le lemme 3.63 implique que $a\mid\mu$. Idem pour b, donc tous les éléments de $\{a,b\}$ divisent μ.

(2) **Si a et b divisent r** Supposons que a et b divisent un certain nombre r. Alors $a_p\leqslant r_p$ et $b_p\leqslant r_p$. Donc $r_p\geqslant\max\{a_p,b_p\}=M_p$. Nous en déduisons que $\mu\mid r$.

Puisque les pgcd et ppcm sont uniques (lemme 3.155 et remarque 3.157), nous avons prouvé que δ et μ sont les nombres recherchés. □

CORooQIMHooUzLUJY

Corolaire 3.161.
Soit un nombre premier p. Un élément $m\in\mathbb{Z}^*$ vérifie $\operatorname{pgcd}(m,p^n)\neq1$ si et seulement si $m=qp$ pour un certain q.

Démonstration. Nous considérons les décompositions en facteurs premiers $m=\prod_{s\in\mathcal{P}}s^{a_s}$ et $p^n=\prod_{s\in\mathcal{P}}s^{b_s}$. Par la partie unicité du théorème 3.62, nous savons que $b_s=0$ pour $s\neq p$ et $b_p=n$.

Nous prenons ensuite l'expression du pgcd donné par la proposition 3.160 :

$$\operatorname{pgcd}(m,p^n)=\prod_{s\in\mathcal{P}}s^{\min\{a_s,b_s\}}. \tag{3.258}$$

Le minimum est toujours zéro lorsque $s\neq p$, donc $\operatorname{pgcd}(m,p^n)=p^{\min\{a_s,n\}}$.

Nous avons donc $\operatorname{pgcd}(m,p^n)\neq1$ si et seulement si $a_p\neq0$. Mais $a_p\neq0$ si et seulement si m est un multiple de p. □

LemheKdsa

Lemme 3.162.
Un entier $n\geqslant1$ se décompose de façon unique en produit de la forme $n=qm^2$ où q est un entier sans facteurs carrés et m, un entier.

Démonstration. Pour $n=1$, c'est évident. Nous supposons $n\geqslant2$.

En ce qui concerne l'existence, nous décomposons n en facteurs premiers[66] et nous séparons les puissances paires des puissances impaires :

$$n=\prod_{i=1}^{r}p_i^{2\alpha_i}\prod_{j=1}^{s}q_j^{2\beta_j+1} \tag{3.259a}$$

$$=\underbrace{\left(\prod_{i=1}^{r}p_i^{2\alpha_i}\prod_{j=1}^{s}q^{2\beta_j}\right)}_{m^2}\underbrace{\prod_{j=1}^{s}q_j}_{q}. \tag{3.259b}$$

Nous passons à l'unicité. Supposons que $n=q_1m_1^2=q_2m_2^2$ avec q_1 et q_2 sans facteurs carrés (dans leur décomposition en facteurs premiers). Soit $d=\operatorname{pgcd}(m_1,m_2)$ et k_1, k_2 définis par $m_1=dk_1$, $m_2=dk_2$. Par construction, $\operatorname{pgcd}(k_1,k_2)=1$. Étant donné que

$$n=q_1d^2k_1^2=q_2d^2k_2^2, \tag{3.260}$$

EaWPOtto

[66] Théorème 3.62.

nous avons $q_1k_1^2 = q_2k_2^2$ et donc k_1^2 divise $q_2k_2^2$. Mais k_1 et k_2 n'ont pas de facteurs premiers en commun, donc k_1^2 divise q_2, ce qui n'est possible que si $k_1 = 1$ (parce que k_1^2 n'a que des facteurs premiers alors que q_2 n'en a pas). Dans ce cas, $d = m_1$ et m_1 divise m_2. Si $m_2 = lm_1$ alors l'équation (3.260) se réduit à $n = q_1m_1^2 = q_2l^2m_1^2$ et donc

$$q_1 = q_2l^2, \tag{3.261}$$

ce qui signifie $l = 1$ et donc $m_1 = m_2$. □

Les nombres premiers ne sont pas si rares que ça dans $\mathbb{N}$. Nous allons voir dans 17.134 que la somme des inverses des nombres premiers diverge. Pour comparaison, la somme des inverses des carrés converge par la proposition 17.141. Il y a donc, dans un certains sens, plus de nombres premiers que de carrés ; dans un autre sens, il y en a autant : une infinité dénombrable.

3.10.4 Ordre d'un élément dans un groupe fini

Voir plus d'informations dans la partie 7.2 sur les groupes monogènes.

LEMooRFKQooWTdYcr

Lemme 3.163 ([1]).
Si g est un élément d'ordre s, et si $g^r = e$, alors $s \mid r$.

THOooSUWKooICbzqM

Théorème 3.164 (Théorème de Cauchy[106, 107]).
Soit G, un groupe cyclique d'ordre n. Si d divise n, alors G possède un unique sous-groupe d'ordre d.
En particulier, G possède des éléments de tous les ordres divisant n.

Démonstration. En plusieurs parties.

(1) **Existence** L'hypothèse est que G est un groupe cyclique. Donc nous pouvons considérer une générateur g de G. Nous considérons $H_d = \text{gr}(g^{n/d})$, et nous prouvons que H_d est un sous-groupe d'ordre d.

D'abord nous avons $(g^{n/d})^d = g^n = e$. Donc $|H_d| \leqslant d$. Pour prouver que $|H_d| \geqslant d$, nous supposons par l'absurde qu'il existe $k < d$ tel que $(g^{n/d})^k = e$. Nous aurions alors $g^{nk/d} = e$ avec $nk/d < n$, ce qui contredirait que g est générateur d'un groupe d'ordre n.

(2) **Unicité** Soit H, un sous-groupe de G d'ordre d. Nous allons prouver que $H = \text{gr}(g^{n/d})$. Vu que H et H_d ont le même cardinal, il suffira de montrer que $H \subset H_d$ pour avoir $H = H_d$.

Vu que $\{e\}$ est l'unique sous-groupe d'ordre 1, nous supposons que $d > 1$. Soit $h \neq e$ dans H. Vu que g est générateur de G, il existe $k \in \mathbb{N}^*$ tel que $g^k = h$. Vu que H est d'ordre d, nous avons $h^d = e$ (corolaire 2.74). Donc

$$g^{kd} = e. \tag{3.262}$$

Le lemme 3.163 dit alors que $n \mid kd$. Soit $t \in \mathbb{N}^*$ tel que $nt = kd$; nous pouvons écrire $k = tn/d$ et récrire $g^k = h$ avec cette valeur de k :

$$h = g^{tn/d} = (g^{n/d})^t \in \text{gr}(g^{n/d}). \tag{3.263}$$

Vu que h a été pris arbitrairement dans H, nous en déduisons que $H \subset \text{gr}(g^{n/d})$.

□

Le lemme suivant indique que sous hypothèse de commutativité, l'ordre d'un élément est une notion multiplicative.

LemyETtdy

Lemme 3.165 ([108]).
Soit G un groupe et $a, b \in G$ tels que $ab = ba$ d'ordres respectivement r et s, deux nombres premiers entre eux. Alors l'élément ab est d'ordre rs.

Démonstration. Étant donné que $(ab)^{rs} = a^{rs}b^{rs} = 1$, l'ordre de ab divise rs. Et comme r et s sont premiers entre eux, l'ordre de ab s'écrit sous la forme r_1s_1 avec $r_1 \mid r$ et $s_1 \mid s$. Nous avons

$$a^{r_1s_1}b^{r_1s_1} = (ab)^{r_1s_1} = 1, \tag{3.264}$$

que nous élevons à la puissance r_2 où r_2 est défini en posant $r = r_1r_2$:

$$a^{rs_1}b^{rs_1} = 1. \tag{3.265}$$

Et comme $a^{rs_1} = 1$, nous concluons que $b^{rs_1} = 1$. Donc $s \mid rs_1$. Par le lemme de Gauss 3.58, nous avons en fait $s \mid s_1$. Puisqu'on a aussi $s_1 \mid s$, nous avons $s = s_1$.

Le même type d'argument donne $r = r_1$, et finalement l'ordre de ab est $r_1s_1 = rs$. □

LemSkIOOG

Lemme 3.166 ([62]).
Un sous-groupe d'indice 2 est un sous-groupe normal.

Démonstration. Si H est un tel sous-groupe d'un groupe G, alors G possède exactement deux classes à gauche par rapport à H (théorème de Lagrange 2.73) et se partitionne donc en deux parties : $G = H \cup xH$ avec $x \notin H$. De même pour les classes à droite : $G = H \cup Hx$. Puisque la classe à droite Hx n'est pas H, on a $xH = Hx$, et H est normal dans G par la proposition 3.136. □

PropubeiGX

Lemme 3.167 ([109]).
Soit H, un sous-groupe normal d'indice m de G. Alors pour tout $a \in G$ nous avons $a^m \in H$.

Démonstration. Par définition de l'indice, le groupe G/H est d'ordre m. Donc si $[a] \in G/H$, nous avons $[a]^m = [e]$, ce qui signifie $[a^m] = [e]$, ou encore $a^m \in H$. □

PROPooVWVIooQzuAlA

Proposition 3.168 ([109]).
Soit un groupe fini G et H, un sous-groupe normal d'ordre n et d'indice m avec m et n premiers entre eux. Alors H est l'unique sous-groupe de G à être d'ordre n.

Démonstration. Soit H' un sous-groupe d'ordre n. Si $h \in H'$ alors $h^n = 1$ et $h^m \in H$ par le lemme 3.167. Étant donné que m et n sont premiers entre eux, par le théorème de Bézout 3.46, il existe $a, b \in \mathbb{Z}$ tels que

$$am + bn = 1. \tag{3.266}$$

Et donc, $h = h^1 = (h^m)^a(h^n)^b$. En tenant compte du fait que $h^n = 1$ et $h^m \in H$, nous avons $h \in H$. Ce que nous venons de prouver est que $H' \subset H$ et donc que $H = H'$ parce que $|H'| = |H| = |G|/m$. □

3.169.
Notons que cette proposition ne dit pas qu'il existe un sous-groupe d'ordre n et d'indice m. Il dit juste que si il y en a un et si il est normal, alors il n'y en a pas d'autre.

LemqAUBYn

Lemme 3.170.
L'ensemble des ordres d'un groupe commutatif est stable par PPCM[67].

Autrement dit, si $x \in G$ est d'ordre r et si $y \in G$ est d'ordre s, alors il existe un élément d'ordre $\operatorname{ppcm}(r, s)$.

Démonstration. Soit $m = \operatorname{ppcm}(r, s)$. Afin d'écrire m sous une forme pratique, nous considérons les décompositions en facteurs premiers de r et s :

$$r = \prod_{i=1}^{k} p_i^{\alpha_i} \tag{3.267a}$$

$$s = \prod_{i=1}^{k} p_i^{\beta_i} \tag{3.267b}$$

où $\{p_i\}_{i=1,\ldots,k}$ est l'ensemble des nombres premiers arrivant dans les décompositions de r et de s. Si nous posons

$$r' = \prod_{\substack{i=1 \\ \alpha_i > \beta_i}}^{k} p_i^{\alpha_i} \tag{3.268a}$$

$$s' = \prod_{\substack{i=1 \\ \alpha_i \leqslant \beta_i}}^{k} p_i^{\beta_i}, \tag{3.268b}$$

alors $\operatorname{ppcm}(r, s) = r's'$ et r' et s' sont premiers entre eux. L'élément $x^{r/r'}$ est d'ordre r' et l'élément $y^{s/s'}$ est d'ordre s'. Maintenant nous utilisons le fait que G soit commutatif et le lemme 3.165 pour conclure que l'ordre de $x^{r/r'}y^{s/s'}$ est $r's' = m$. □

3.10.5 Écriture des fractions

THOooWYQVooRBaAAM

Théorème 3.171 ([110]).
Tout élément de $\mathbb{Q}^+$ s'écrit de façon unique comme quotient de deux entiers premiers entre eux.

[67] Définition 1.113.

Démonstration. En deux parties[68]

(1) **Unicité** Supposons avoir $\frac{a}{b} = \frac{c}{d}$ avec $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(c,d) = 1$. Nous avons

$$ad = bc \tag{3.269}$$

donc

(1a) a divise bc mais est premier avec b donc a divise c par le lemme de Gauss 3.58.

(1b) c divise ad mais est premier avec d donc c divise a par le lemme de Gauss 3.58.

En conclusion a divise c et c divise a, ergo[69] $a = c$. L'égalité $b = d$ est alors immédiate.

(2) **Existence** Soit le quotient $\frac{a}{b}$. Nous avons

$$\frac{a}{b} = \frac{a/\operatorname{pgcd}(a,b)}{b/\operatorname{pgcd}(a,b)}, \tag{3.270}$$

qui est encore un quotient d'entiers parce que $\operatorname{pgcd}(a,b)$ divise aussi bien a que b. Il faut montrer que les nombres $a/\operatorname{pgcd}(a,b)$ et $b/\operatorname{pgcd}(a,b)$ sont premiers entre eux. Pour cela nous supposons que k est un diviseur commun. En particulier, les nombres $a/k\operatorname{pgcd}(a,b)$ et $b/k\operatorname{pgcd}(a,b)$ sont des entiers, ce qui fait que $k\operatorname{pgcd}(a,b)$ est un diviseur commun de a et b. Étant donné que $\operatorname{pgcd}(a,b)$ est le plus grand tel diviseur, nous devons avoir $k\operatorname{pgcd}(a,b) = \operatorname{pgcd}(a,b)$ c'est-à-dire que $k = 1$. Donc les nombres $a/\operatorname{pgcd}(a,b)$ et $b/\operatorname{pgcd}(a,b)$ sont premiers entre eux.

□

PROPooWBFJooWisSZX

Proposition 3.172 ([1])**.**
Soient $l, l, d_1, d_2 \in \mathbb{N}$ tels que

$$\frac{k}{d_1} = \frac{l}{d_2} \tag{3.271}$$

avec $\operatorname{pgcd}(k, d_1) = 1$.
Alors

(1) $d_1 \leqslant d_2$

(2) $d_1 = \frac{d_2}{\operatorname{pgcd}(l,d_2)}$.

PROPooRZDDooLJabov

Proposition 3.173.
Les entiers p et q sont premiers entre eux[70] *si et seulement si p^2 et q^2 sont premiers entre eux.*

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que p^2 et q^2 ne sont pas premiers entre eux. Donc il existe δ divisant p^2 et q^2. Si δ' est un facteur premier de δ, alors δ' divise δ et donc aussi p^2 et q^2. Le lemme 3.64 implique que δ divise p et q. Donc p et q ne sont pas premiers entre eux.

(2) $\Leftarrow$ Si p^2 et q^2 sont premiers entre eux, par le théorème de Bézout 3.46 il existe $a, b \in \mathbb{Z}$ tels que

$$ap^2 + bq^2 = 1 \tag{3.272}$$

Dans ce cas, $(ap)p + (bq)q = 1$, ce qui montre (par encore Bézout, mais l'autre sens) que p et q sont premiers entre eux.

□

Une des conséquences de ces résultats sera le fait que $\sqrt{n}$ est irrationnelle dès que n n'est pas un carré parfait, théorème 4.26. L'irrationalité de $\sqrt{2}$ est la proposition 4.25.

[68] Définitions des pgcd et ppcm en 1.113.
[69] Lemme 3.60.
[70] Premiers entre eux, définition 3.52.

3.10.6 Équation diophantienne linéaire à deux inconnues

subsecZVKNooXNjPSf

Soient a, b et c des entiers naturels donnés. Nous considérons l'équation

EqTOVSooIbxIIq

$$ax + by = c \tag{3.273}$$

à résoudre[111] pour $(x, y) \in \mathbb{N}^2$.

Si a ou b est nul, c'est facile ; nous supposons donc que a et b sont tous deux non nuls. Nous commençons par simplifier l'équation en cherchant les diviseurs communs. Soit $d = \text{pgcd}(a, b)$ et notons $a = da'$, $b = db'$. Nous avons déjà l'équation

$$d(a'x + b'y) = c, \tag{3.274}$$

et donc si c n'est pas un multiple de d, il n'y a pas de solution[71]. Si par contre c est un multiple de d alors nous écrivons $c = c'd$ et l'équation devient

$$a'x + b'y = c' \tag{3.275}$$

C'est maintenant que nous utilisons le théorème de Bézout 3.46 : puisque a' et b' sont premiers entre eux, nous avons la relation $a'u + b'v = 1$ pour certains[72] nombres entiers u et v. Nous récrivons notre équation sous la forme $a'x + b'y = c'(a'u + b'v)$ et rassemblons les termes :

$$a'(x - c'u) = b'(c'v - y). \tag{3.276}$$

C'est-à-dire que si (x, y) est une solution, alors a' divise $b'(c'v - y)$. Mais comme a' et b' sont premiers entre eux, le nombre a' doit forcément[73] diviser $c'v - y$. Disons $c'v - y = ka'$. Alors $a'(x - c'u) = b'ka'$ et donc

$$x = b'k + c'u. \tag{3.277}$$

Nous trouvons alors une expression pour y en injectant ce résultat dans $a'x + b'y = c'$ et en utilisant le théorème de Bézout : $a'c'u = (1 - b'v)c'$. Au final nous avons prouvé que toutes les solutions sont de la forme

EqYCQVooZzHuRq

$$\begin{cases} x = b'k + c'u & \text{(3.278a)} \\ y = vc' - a'k & \text{(3.278b)} \end{cases}$$

avec $k \in \mathbb{Z}$. Si nous ne voulons réellement que les solutions dans $\mathbb{N}$ et non dans $\mathbb{Z}$, il faut seulement un peu restreindre les valeurs de k. Il en reste un nombre fini parce que l'équation pour x borne k vers le bas tandis que celle pour y borne k vers le haut.

Par ailleurs, il est très vite vérifié que tous les couples (x, y) de la forme (3.278) sont solutions.

Exemple 3.174.
Résoudre l'équation $2x + 6y = 52$.

Nous pouvons factoriser 2 dans le membre de gauche et simplifier alors toute l'équation par 2 :

$$x + 3y = 26. \tag{3.279}$$

Nous cherchons une relation de Bézout pour $u+3v = 1$. Ce n'est heureusement pas très compliqué : $u = -5$, $v = 2$. Nous pouvons alors écrire

$$x + 3y = 26 \times (-5 + 3 \times 2), \tag{3.280}$$

et donc $x + 5 \times 26 = -3(y - 26 \times 2)$, et en posant $k = y - 26 \times 2$ nous avons

$$x = -3k - 130. \tag{3.281}$$

En injectant nous trouvons l'équation $3y - 3k - 130 = 26$ et donc

$$y = 52 + k. \tag{3.282}$$

△

[71] Exemple : $8x + 2y = 9$. Le membre de gauche est certainement un nombre pair et il n'y a donc pas de solution.
[72] Nous avons décrit un algorithme pour les trouver en démontrant l'équation 3.242.
[73] C'est Gauss 3.58 qui le dit, et vous savez que lorsque Gauss dit, c'est *forcément* vrai.

3.10.7 Quotients

Nous écrivons $a = b \mod p$ essentiellement si il existe $k \in \mathbb{Z}$ tel que $b + kp = a$. Plus généralement nous notons $[a]_p = \{a + kp | k \in \mathbb{Z}\}$ et l'écriture « $a = n \mod p$ » peut tout autant signifier $a = [b]_p$ que $a \in [b]_p$. La différence entre les deux est subtile mais peut de temps en temps valoir son pesant d'or.

Proposition 3.175.
Soit $n \in \mathbb{N}$. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène. Si $n \neq 0$, il est cyclique d'ordre n.

Démonstration. Nous considérons la surjection canonique $\mu: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Si $a \in \mathbb{Z}$, alors $\mu(a) = a\mu(1)$. Par conséquent $\mathbb{Z}/n\mathbb{Z} = \text{gr}\big(\mu(1)\big)$ parce que tout groupe contenant $\mu(1)$ contient tous les multiples de $\mu(1)$, et par conséquent contient $\mu(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$.

Soit $x \in \mathbb{Z}/n\mathbb{Z}$ et considérons x_0, le plus petit naturel représentant x. Nous notons $x = [x_0]$. Le théorème de la division euclidienne 3.40 donne l'existence de q et r avec $0 \leqslant r < n$ et $q \geqslant 0$ tels que

$$x_0 = nq + r. \tag{3.283}$$

Nous avons $[x_0] = [r] = \mu(r)$ parce que $x_0 - r$ est un multiple de n. Nous avons donc $[x_0] \in \mu(\mathbb{N}_{n-1})$. Par conséquent

$$\mathbb{Z}/n\mathbb{Z} = \mu(\mathbb{Z}) = \mu(\mathbb{N}_{n-1}). \tag{3.284}$$

La restriction $\mu: \mathbb{N}_{n-1} \to \mathbb{Z}/n\mathbb{Z}$ est donc surjective. Montrons qu'elle est également injective. Si $\mu(x_0) = \mu(x_1)$, alors $x_1 = x_0 + kn$. Si nous supposons que $x_1 > x_0$, alors $k > 0$ et si $x_0 \in \mathbb{N}_{n-1}$, alors $x_1 > n - 1$.

L'ordre de $\mathbb{Z}/n\mathbb{Z}$ est donc le même que le cardinal de $\mathbb{N}_{n-1}$, c'est-à-dire n. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est donc fini, d'ordre n et monogène parce que $\mathbb{Z}/n\mathbb{Z} = \text{gr}(\mu(1))$. Il est donc cyclique. □

Lemme 3.176 ([112]).
Soit $q \in \mathbb{N}$ avec $q \geqslant 2$. Soient $n, d \in \mathbb{N}$ tels que $q^d - 1 \mid q^n - 1$. Alors $d \mid n$.

Démonstration. Par le théorème de division euclidienne 3.40, il existe $a, b \in \mathbb{Z}$ tels que $n = ad + b$ avec $0 \leqslant b < d$. En remarquant que $q^d \in [1]_{q^d-1}$ nous avons

$$q^n = (q^d)^a q^b \in [1]_{q^d-1} q^b = [q^b]_{q^d-1}. \tag{3.285}$$

Pour cela nous avons utilisé d'abord le fait que si $a \in [z]_k$, alors $a^n \in [z^n]_k$ et ensuite le fait que $[1]_k x = [x]_k$. D'autre part l'hypothèse $q^d - 1 \mid q^n - 1$ implique

$$q^n \in [1]_{q^d-1}. \tag{3.286}$$

Par conséquent le nombre q^n est à la fois dans $[q^b]_{q^d-1}$ et dans $[1]_{q^d-1}$. Cela implique que

$$[1]_{q^d-1} = [q^b]_{q^d-1}, \tag{3.287}$$

ou encore que $q^b \in [1]_{q^d-1}$ ou encore que $q^d - 1 \mid q^b - 1$.

Étant donné que $b < d$ et que $q \geqslant 2$, nous avons que $q^b - 1 < q^d - 1$; donc pour que $q^d - 1$ divise $q^b - 1$, il faut que $q^b - 1$ soit zéro, c'est-à-dire $b = 0$.

Mais dire $b = 0$ revient à dire que $d \mid n$, ce qu'il fallait démontrer. □

3.11 Coefficients multinomiaux

3.11.1 Théorème multinomial

DEFooCQPRooFeWeOS

Définition 3.177 (multiindices[113]).
*Un **multiindice** pour $\mathbb{R}^n$ est un élément de $\mathbb{N}^n$. Sa taille est définie par*

$$|\alpha| = \sum_i \alpha_i. \tag{3.288}$$

Nous disons que $\beta \leqslant \alpha$ lorsque $\beta_i \leqslant \alpha_i$ pour tout i.

Nous définissons sa factorielle par

$$\alpha! = \prod_{k=1}^{n} (\alpha_k!) = \alpha_1! \times \ldots \times \alpha_n!. \tag{3.289}$$

EQooMZAMooMJuLKD

En ce qui concerne les coefficients binomiaux, nous posons

$$\binom{\alpha}{\beta} = \frac{\alpha!}{(\alpha-\beta)!\beta!} = \prod_{i=1}^{n} \binom{\alpha_i}{\beta_i}. \tag{3.290}$$

EQooKBURooKFBxnt

Si $x \in \mathbb{R}^n$ et si $\alpha \in \mathbb{N}^n$, nous notons

$$x^\alpha = \prod_{i=1}^{n} x_i^{\alpha_i}. \tag{3.291}$$

THOooNHAUooQvuytn

Théorème 3.178 (Théorème multinomial[113])**.**
Soit $x \in \mathbb{R}^n$, et $\alpha \in \mathbb{N}^n$. Nous avons

$$(x_1 + \ldots + x_n)^k = \sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha|=k}} \frac{k!}{\alpha!} x^\alpha. \tag{3.292}$$

Démonstration. Le cas $n = 2$ est la formule binomiale 3.75 :

$$(x_1 + x_2)^k = \sum_{l=0}^{k} \binom{k}{l} x_1^l x_2^{k-l} \tag{3.293a}$$

$$= \sum_{l=0}^{k} \frac{k!}{l!(k-l)!} x_1^l x_2^{k-l} \tag{3.293b}$$

$$= \sum_{\alpha_1+\alpha_2=k} \frac{k!}{\alpha_1!\alpha_2!} x_1^{\alpha_1} x_2^{\alpha_2} \tag{3.293c}$$

$$= \sum_{\substack{\alpha \in \mathbb{N}^2 \\ |\alpha|=k}} \frac{k!}{\alpha!} x^\alpha. \tag{3.293d}$$

Et maintenant, nous faisons une récurrence sur n, en tenant k fixé. Nous supposons que la formule est démontrée pour tout $n \leqslant N$, et nous allons avec $N+1$. Soit $x = (x_1, \ldots, x_{N+1})$, et posons $y = (x_1, \ldots, x_N)$. Nous avons

$$(x_1 + \ldots + x_{N+1})^k = \big((x_1 + \ldots + x_N) + x_{N+1}\big)^k \tag{3.294a}$$

$$= \sum_{i+j=k} \frac{k!}{i!j!} (x_1 + \ldots + x_N)^i x_{N+1}^j \tag{3.294b}$$

$$= \sum_{i+j=k} \frac{k!}{i!j!} \sum_{\substack{\alpha \in \mathbb{N}^N \\ |\alpha|=i}} x_{N+1}^j \frac{i!}{\alpha!} y^\alpha \tag{3.294c}$$

$$= \sum_{j=0}^{k} \sum_{\substack{\alpha \in \mathbb{N}^N \\ |\alpha|=k-j}} x_{N+1} \frac{k!}{j!} \frac{1}{\alpha!} y^\alpha \tag{3.294d}$$

$$= \sum_{\substack{\beta \in \mathbb{N}^{N+1} \\ |\beta|=k}} \frac{k!}{\beta_{N+1}!\alpha!} x_{N+1}^{\beta_{N+1}} x_1^{\alpha_1} \ldots x_N^{\alpha_N} \qquad \text{cf. justif.} \tag{3.294e}$$

SUBEQooTQFGooHyUbCi

$$= \sum_{\substack{\beta \in \mathbb{N}^{N+1} \\ |\beta|=k}} x^\beta \frac{k!}{\beta!}. \tag{3.294f}$$

Justification pour (3.294e). Les deux sommes ensemble font une somme sur tous $\beta = (\alpha, j) \in \mathbb{N}^{N+1}$ avec $|\beta| = |\alpha| + j = (k-j) + j = k$. □

LEMooBSYRooDboTor

Lemme 3.179 ([1])**.**
Soit une application $f\colon \mathbb{N}^n \to \mathbb{R}$. Nous avons

$$\sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha|=2}} \frac{1}{\alpha!} f(\alpha) = \frac{1}{2} \sum_{k,l} f(e_k + e_l). \tag{3.295}$$

Démonstration. Nous avons

$$\{\alpha \in \mathbb{N}^n \text{ tel que } |\alpha| = 2\} = \{e_k + e_l \text{ tel que } k, l = 1, \dots, n\}, \tag{3.296}$$

mais nous ne pouvons pas sommer en faisant $\sum_{\substack{\alpha\in\mathbb{N}^2\\|\alpha|=2}} = \sum_{k,l}$ parce que à droite, les termes (k,l) et (l,k) sont identiques.

Au lieu de ça, remarquons que nous avons une bijection

$$\begin{aligned}\varphi\colon \{(k,l) \in \{1,\dots,n\}^2 \text{ tel que } k \leqslant n\} &\to \{e_k + e_l\}_{k,l=1,\dots,n}\\ (k,l) &\mapsto e_k + e_l.\end{aligned} \tag{3.297}$$

Prouvons que cette application est injective. Si $\varphi(k,l) = \varphi(s,t)$, alors $e_k + e_l = e_s + e_t$. Le produit scalaire avec e_k donne

$$1 + \delta_{kl} = \delta_{st} + \delta_{tk}. \tag{3.298}$$

(1) **Si $k < l$** Alors $1 = \delta_{sk} + \delta_{tk}$. Nous avons donc forcément $k = s$ ou $k = t$, mais pas les deux en même temps.

(1a) **Si $s = k$** Dans ce csa $t \neq k$, et nous avons $e_k + e_l = e_k + e_t$, donc $e_l = e_t$ et donc $l = t$. Nous avons donc $(k,l) = (s,t)$, ce qu'il fallait.

(1b) **Si $t = k$** Alors $e_l = e_s$ et donc $l = s$, ce qui donnerait $(k,l) = (l,k)$, ce qui est impossible parce que $k < l$.

(2) **Si $k = l$** Alors $2e_k = e_s + t_t$. Le produit scalaire avec e_k donne $2 = \delta_{sk} + \delta_{tk}$ et donc $s = t = k$.

Nous pouvons donc sommer de la façon suivante :

$$\sum_{\substack{\alpha\in\mathbb{N}^n\\|\alpha|=2}} \frac{1}{\alpha!} f(\alpha) = \sum_{k\leqslant l} \frac{1}{(e_k+e_l)!} f(e_k+e_l) \tag{3.299a}$$

$$= \sum_{k<l} f(e_k+e_l) + \sum_k \frac{1}{2} f(2e_k) \tag{3.299b}$$

$$= \frac{1}{2}\sum_{k\neq l} f(e_k+e_l) + \sum_k \frac{1}{2} f(2e_k) \qquad \text{cf. justif.} \tag{3.299c}$$

SUBEQooZERNooQeAAgb

$$= \frac{1}{2}\sum_{k,l} f(e_k+e_l). \tag{3.299d}$$

Justification pour (3.299c). Nous avons $f(e_l+e_l) = f(e_l+e_k)$. Donc $\sum_{k<l} f(e_k+e_l) = \sum_{k>l} f(e_k+e_l)$. □

3.12 Polynômes de plusieurs variables

DEFooZNHOooCruuwI

Définition 3.180.
*L'ensemble des **polynôme de** n **variables** sur l'anneau A est $A^{(\mathbb{N}^n)}$, c'est-à-dire l'ensemble des suites indexées par $\mathbb{N}^n$ et dont seulement une quantité finie de coefficients sont non nuls.*

Le produit sur $A[X_1,\dots,X_n]$ est défini par

$$(PQ)(k_1,\dots,k_n) = \sum_{\substack{(l_1,\dots,l_n),(m_1,\dots,m_n)\in\mathbb{N}^n\times\mathbb{N}^n\\ l_i+m_i=k_i}} P_{l_1,\dots,l_n} Q_{m_1,\dots,m_n}. \tag{3.300}$$

3.181.
Dans $A[X_1,\dots,X_n]$, la multiplication n'est pas la multiplication de fonctions $\mathbb{N}^n \to \mathbb{K}$, parce que le but est d'obtenir la multiplication usuelle au niveau des évaluations.

DEFooFDBAooHvfMue

Définition 3.182.
*Si P est un polynôme de n variables sur A, et si $(x_1,\dots,x_n) \in A^n$, **l'évaluation** de P sur $(x_1,\dots,x_n)$ est*

$$P(x_1,\dots,x_n) = \sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} P_{k_1,\dots,k_n} x_1^{k_1}\dots x_n^{k_n}. \tag{3.301}$$

Notez que la somme, bien que sur $\mathbb{N}^n$, est une somme finie.

3.183.
Comme dans le cas des polynômes d'une seule variable, les X_i dans la notation $A[X_1, \dots, X_n]$ sont à prendre à la légère. L'anneau des polynômes de n variables sur A aurait mieux fait d'être noté par exemple par $\mathcal{P}_n(A)$.

Le fait est que nous avons les polynômes élémentaires définis par

$$X_1(k_1, \dots, k_n) = \begin{cases} 1 & \text{si } (k_1, \dots, k_n) = (1, 0 \dots, 0) \\ 0 & \text{sinon.} \end{cases} \tag{3.302}$$

et que l'anneau des polynômes peut être vu comme A (les polynômes constants) étendus par les X_i.

Quoi qu'il en soit, les X_i dans la notation $A[X_1, \dots, X_n]$ sont des indices muets. L'anneau $A[X_1, \dots, X_n]$ est exactement le même que $A[T_1, \dots, T_n]$.

3.12.1 Divisibilité et classes d'association

DivisibiliteAnneauDeInXgrs

Définition 3.184.
*On dit de deux éléments $a, b \in A$ qu'ils sont **associés** si il existe un inversible $u \in A$ tel que $a = ub$.*

*La **classe d'association** d'un élément $a \in A$ est l'ensemble des éléments qui lui sont associés.*

LemRmVTRq

Lemme 3.185.
Si A est un anneau intègre et si $a, b \in A$ sont deux éléments vérifiant $a \mid b$ et $b \mid a$, alors ils sont associés, c'est-à-dire qu'il existe un inversible $u \in A$ tel que $a = ub$.

Démonstration. Les hypothèses à propos de la divisibilité nous indiquent que $a = xb$ et $b = ya$ pour certains $x, y \in A$. Alors,

$$b(1 - yx) = 0. \tag{3.303}$$

Étant donné que A est intègre, cela montre que $b = 0$ ou $1 - yx = 0$. Si $b = 0$ nous avons immédiatement $a = 0$ et le lemme est prouvé. Si au contraire $yx = 1$, c'est que y et x sont inversibles et inverses l'un de l'autre. □

Exemple 3.186.
Dans $\mathbb{Z}[i]$, les inversibles sont ± 1 et $\pm i$. Donc les éléments associés à z sont z, $-z$, iz et $-iz$.

Notons au passage que la notion de divisibilité dans $\mathbb{Z}[i]$ n'est pas immédiatement intuitive. En effet bien que 7 ne soit pas divisible par 2 (ni dans $\mathbb{Z}$ ni dans $\mathbb{Z}[i]$), le nombre $7 + 6i$ est divisible par $2 + i$ dans $\mathbb{Z}[i]$. En effet :

$$(2 + i)(4 + i) = 7 + 6i. \tag{3.304}$$

△

Exemple 3.187.
Si $\mathbb{K}$ est un corps, l'élément XY de $\mathbb{K}[X, Y]$ n'est pas premier parce que $XY \mid X^2Y^2$ alors que XY ne divise ni X^2 ni Y^2. △

LEMooLXPSooYjULCJ

Lemme 3.188 ([1])**.**
Si a et b sont associés, alors $(a) = (b)$.

Démonstration. Vu que a et b sont associés, il existe un inversible u tel que $a = ub$ et $b = va$ (en posant $v = u^{-1}$). Si $x \in (a)$, alors il existe $\alpha, \beta \in A$ tels que $x = \alpha a \beta = \alpha u b \beta \in AbA = (b)$. Donc $(a) \subset (b)$. L'inclusion dans l'autre sens se fait de la même manière. □

3.12.2 PGCD et PPCM

Pour le théorème de Bézout et autres opérations avec des modulo, voir le thème 3. Le pgcd et le ppcm sont définis en 1.113.

LEMooGWKMooLEepxz

Lemme 3.189.
Soient A un anneau intègre et $S \subset A$. Si δ est un PGCD de S, alors l'ensemble des PGCD de S est la classe d'association[74] *de δ.*

De la même façon si μ est un PPCM de S, alors l'ensemble des PPCM de S est la classe d'association de μ.

[74] Éléments associés, définition 3.184.

Démonstration. Soient δ un PGCD de S et u un inversible dans A. Si $x \in S$ nous avons $\delta \mid x$ et donc $x = a\delta$. Par conséquent $x = au^{-1}u\delta$ et donc $u\delta$ divise x. De la même manière, si d divise x pour tout $x \in S$, alors d divise δ et donc $\delta = ad$ et $u\delta = aud$, ce qui signifie que d divise $u\delta$.

Dans l'autre sens nous devons prouver que si δ' est un autre PGCD de S, alors il existe un inversible $u \in A$ tel que $\delta' = u\delta$. Comme δ' divise x pour tout $x \in S$, nous avons $\delta' \mid \delta$, et symétriquement nous trouvons $\delta \mid \delta'$. Par conséquent (lemme 3.185), il existe un inversible u tel que $\delta = u\delta'$.

Le même type de raisonnement tient pour le PPCM. □

Si δ est un PGCD de S, nous dirons *par abus de langage* que δ est *le* PGCD de S, gardant en tête qu'en réalité toute sa classe d'association est PGCD. Nous noterons aussi, toujours par abus que $\delta = \text{pgcd}(S)$.

Remarque 3.190.
La classe d'association d'un élément n'est pas toujours très grande. Les inversibles dans $\mathbb{Z}$ étant seulement ± 1, nous pouvons obtenir l'unicité du PGCD et du PPCM en imposant qu'ils soient positifs.

Pour les polynômes, nous obtenons l'unicité en demandant que le PGCD soit unitaire.

Dans les cas pratiques, il y a donc en réalité peu d'ambiguïté à parler du PGCD ou du PPCM d'un ensemble.

3.12.3 pgcd, ppcm dans un anneau principal

Juste pour ne pas l'oublier, un anneau principal est toujours commutatif.

PROPooPZXNooNpVZCm

Proposition 3.191 ([72, 1]).
Soit un anneau principal[75] *A. Soit une partie $S \subset A$ d'éléments non nuls. Alors :*

ITEMooPTAGooXNHQut

(1) S admet un pgcd,

ITEMooHCZAooNkFHqc

(2) S admet un ppcm,

ITEMooMJPXooDadqdP

(3) L'élément $\delta \in A$ est un pgcd de S si et seulement si il engendre

$$J = \bigcup_{\alpha \text{ fini dans } S} \sum_{s\in\alpha} sA. \tag{3.305}$$

Démonstration. En ce qui concerne l'existence, nous savons que tout idéal est principal et admet donc un générateur. Les parties I et J de la proposition 3.11 sont des idéaux principaux et admettent donc des générateurs qui sont dont respectivement ppcm et pgcd de S. Les parties (1) et (2) sont prouvées.

Il reste à prouver (3). Le sens réciproque est déjà dans 3.11. Nous supposons donc que $\delta \in \text{pgcd}(S)$ et nous prouvons que $(\delta) = J$.

Vu que J est un idéal, il admet un générateur d, qui est également un pgcd de S. Les éléments d et δ sont donc associés par le lemme 3.189. Donc $(d) = (\delta)$ par 3.188. Et au final, $(\delta) = (d) = J$. □

Pour rappel, la notation (a) représente l'idéal engendré par a, c'est-à-dire

$$(a) = \{ax \text{ tel que } x \in A\} = aA. \tag{3.306}$$

3.12.4 Anneaux intègres et corps

Le fait d'être intègre pour un anneau n'assure pas le fait d'être un corps. Nous avons cependant ce résultat pour les anneaux finis.

PropanfinintimpCorp

Proposition 3.192.
Un anneau fini intègre est un corps.

Démonstration. Soit A un tel anneau. Soit $a \neq 0$. Les applications

$$l_a : x \mapsto ax \tag{3.307a}$$
$$r_a : x \mapsto xa \tag{3.307b}$$

sont injectives. En tant que applications injectives entre ensembles finis, elles sont surjectives. Il existe donc b et c tels que $1 = ba = ac$. Nous trouvons que b et c sont égaux parce que [76]

$$b = b(ac) = (ba)c = c. \tag{3.308}$$

[75] Définition 3.37.

[76] Il faut être un peu souple avec les notations communément employées dans les ouvrages mathématiques, et que nous reprenons telles quelles. Dans l'équation qui suit, $b(ac)$ est le produit de b par l'élément ac, et non quelque chose comme le produit de b avec l'idéal (ac) par exemple.

Par conséquent b est un inverse de a. □

PropzhFgNJ

Proposition 3.193.
Soit $n \in \mathbb{N}^*$. Les conditions suivantes sont équivalentes :

(1) *n est premier.*

(2) *$\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.*

(3) *$\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Démonstration. L'équivalence entre les deux premiers points est le contenu du corolaire 3.123. Le fait que $\mathbb{Z}/n\mathbb{Z}$ soit un corps lorsque $\mathbb{Z}/n\mathbb{Z}$ est intègre est la proposition 3.192. Le fait que $\mathbb{Z}/n\mathbb{Z}$ soit intègre lorsque $\mathbb{Z}/n\mathbb{Z}$ est un corps est une propriété générale des corps : ce sont en particulier des anneaux intègres (lemme 3.23). □

3.13 Anneau factoriel

DEFooVCATooPJGWKq

Définition 3.194 (Anneau factoriel)**.**
*Un anneau commutatif A est **factoriel** si il vérifie les propriétés suivantes.*

(1) *L'anneau A est intègre*[77].

(2) *Si $a \in A$ est non nul et non inversible, alors il admet une décomposition en facteurs irréductibles : $a = p_1 \dots p_k$ où les p_i sont irréductibles*[78].

ITEMooKVDBooTASwVO

(3) *Si $a = q_1 \dots q_m$ est une autre décomposition de a en irréductibles, alors $m = k$ et il existe une permutation*[79] *$\sigma \in S_k$ telle que p_i et $q_{\sigma(i)}$ soient associés*[80].

Un anneau factoriel permet de caractériser le pgcd et le ppcm de nombres.

LEMooLVKMooSLuzao

Lemme 3.195 ([114])**.**
Soit un anneau factoriel A et un élément irréductible $p \in A$. Si $p|xy$, alors p divise x ou y ou les deux.

Démonstration. Comme nous sommes dans un anneau factoriel, nous pouvons écrire q, x et y comme produits d'irréductibles, et profiter de la plus ou moins unicité de ces décompositions (la propriété 3.194(3)). Nous notons $q = q_1 \dots q_k$, $x = x_1 \dots x_m$ et $y = y_1 \dots y_l$. L'égalité $pq = xy$ devient :

$$pq_1 \dots q_k = x_1 \dots x_m y_1 \dots y_l. \tag{3.309}$$

Il existe un des x_j ou y_j qui est associé à p. Fixons un i et disons que c'est x_i (si c'est un des y_j, adaptez) : il existe un inversible u tel que $x_i = pu$. Nous avons alors[81]

$$x = pux_1 \dots x_{i-1}x_{i+1} \dots x_m. \tag{3.310}$$

Donc p divise x et fin de l'histoire. □

PROPooOQSXooYidPQv

Proposition 3.196 ([114])**.**
Dans un anneau factoriel, tout élément irréductible est premier[82].

Démonstration. Soit un anneau factoriel A et un élément irréductible p dans A. Nous devons prouver qu'il est premier.

(1) **p est non nul** Si $p = 0$, nous avons $p = 0 \times 0$. Comme 0 n'est pas inversible (un anneau factoriel est par définition intègre), p serait un produit de deux non inversibles.

(2) **Non inversible** L'élément p est non inversible parce que c'est dans la définition d'un élément irréductible.

(3) **Si $p \mid xy$** Si p divise xy, alors il divise x ou y ; c'est le lemme 3.195.

[77] Anneau intègre, définition 3.22.
[78] Élément irréductible, définition 3.14.
[79] Définition 2.2.
[80] Définition 3.184.
[81] Le fait que A soit commutatif est utilisé partout.
[82] Élément premier, définition 3.13.

□

LEMooGKOSooRKtfDJ

Lemme 3.197 ([1]).
Si A est un anneau factoriel, et si p est irréductible dans A, alors :

(1) L'idéal pA est premier.

(2) L'anneau A/pA est intègre.

Démonstration. En deux parties.

(1) pA **est premier** D'abord pA est strictement inclus dans A parce que p n'étant pas inversible, l'élément 1 n'est pas dans pA.

Soient $a, b \in A$ tels que $ab \in pA$. Cela signifie qu'il existe $x \in A$ tel que $px = ab$, ou encore que p divise ab. Le lemme 3.195 dit alors que p divise a ou b. Supposons pour fixer les idées que $p \mid a$. Il existe y tel que $a = py \in pA$.

(2) **L'anneau A/pA est intègre** C'est la proposition 3.90.

□

PROPooOXQMooVEzlyG

Proposition 3.198.
Soit une famille $\{a_n\}$ d'éléments de A qui se décomposent en irréductibles comme

$$a_i = \prod_k p_k^{\alpha_{k,i}}. \tag{3.311}$$

Alors

$$\text{pgcd}\{a_n\} = \prod_k p_k^{\min_i\{\alpha_{k,i}\}}. \tag{3.312}$$

De plus le PGCD est :

(1) Un multiple de tous les diviseurs communs des a_i.

(2) Unique pour cette propriété à multiple près par un inversible[83].

De la même manière,

$$\text{ppcm}\{a_n\} = \prod_k p_k^{\max_i\{\alpha_{k,i}\}}. \tag{3.313}$$

Un anneau factoriel a une relation de préordre partiel donnée par $a < b$ si a divise b. En termes d'idéaux, cela donne l'ordre inverse de celui de l'inclusion[84] : $a < b$ si et seulement si $(b) \subset (a)$.

EXooCWJUooCDJqkr

Exemple 3.199.
L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel parce que 4 a au moins deux décompositions distinctes en irréductibles :

$$4 = 2 \cdot 2, \tag{3.314}$$

et

$$4 = (1 + i\sqrt{3})(1 - i\sqrt{3}). \tag{3.315}$$

△

Nous allons voir dans l'exemple 3.217 que $\mathbb{Z}[i\sqrt{2}]$ est factoriel parce qu'il sera euclidien.

3.13.1 Autour du théorème de Bézout

Rappel de notations : si A est un anneau et si $p \in A$, nous notons (p) l'idéal engendré[85] par p.

PROPooXQKMooWJlEFq

Proposition 3.200 (Bézout dans un anneau principal[1, 115]).
Soit un anneau principal A. Soient $a_1, \ldots, a_n \in A$ et $\delta \in \text{pgcd}(a_1, \ldots, a_n)$. Alors il existe $u_1, \ldots, u_n \in A$ tels que

$$a_1u_1 + \ldots + a_nu_n = \delta \tag{3.316}$$

[83] Soyez prudent avec cette affirmation : je n'en n'ai pas de démonstrations sous la main et ne suis pas certain que ce soit vrai.
[84] Voir proposition 3.145.
[85] Définition 3.6 et caractérisation 3.7.

Démonstration. Soit $\delta \in \text{pgcd}(a_1, \ldots, a_n)$. Nous utilisons la proposition 3.191 pour la partie $S = \{a_1, \ldots, a_n\}$. Dans notre cas, nous savons que δ engendre $J = a_1A + \ldots + a_nA$. En particulier $\delta \in a_1A + \ldots + a_nA$ et donc il existe $u_1, \ldots, u_n \in A$ tels que $\delta = u_1a_1 + \ldots + u_na_n$[86]. □

Le lemme de Gauss est une application immédiate du théorème de Bézout. Il y aura aussi un lemme de Gauss à propos de polynômes (lemme 8.51), et une généralisation directe au théorème de Gauss, théorème 8.50.

LemSdnZNX

Lemme 3.201 (Lemme de Gauss dans un anneau principal[116])**.**
Soit A un anneau principal et $a, b, c \in A$ tels que a divise bc. Si a est premier avec c, alors a divise b.

Démonstration. Comme a est premier avec c, nous avons $\text{pgcd}(a, c) = 1$ et Bézout (3.46) nous donne donc $s, t \in A$ tels que $sa + tc = 1$. En multipliant par b,

$$sab + tbc = b. \tag{3.317}$$

Mais les deux termes du membre de gauche sont multiples de a parce que a divise bc. Par conséquent b est somme de deux multiples de a et donc est multiple de a. □

LEMooQJGIooEtVnyj

Lemme 3.202 ([72])**.**
Soit un anneau principal A. Soient $a, b, c \in A$ tels que

(1) $\text{pgcd}(a, b) = 1$

(2) $\text{pgcd}(a, c) = 1$.

Alors $\text{pgcd}(a, bc) = 1$.

Démonstration. Le théorème de Bézout 3.200 donne des éléments $u, v, x, y \in A$ tels que $ua + vb = 1$ et $xa + yc = 1$. En multipliant ces équations l'une avec l'autre,

$$(ua + vb)(xa + yc) = 1. \tag{3.318}$$

En développant, nous trouvons

$$(uax + uc + vbx)a + (vy)bc = 1. \tag{3.319}$$

Donc le théorème de Bézout (dans l'autre sens) nous indique que $\text{pgcd}(a, bc) = 1$. □

PROPooYTMYooEYxuQc

Proposition 3.203 ([117, 3])**.**
Soient un anneau principal[87] *A ainsi que $a, b \in A$.*

(1) Nous avons $\delta \in \text{pgcd}(a, b)$ si et seulement si $(a) + (b) = (\delta)$.

(2) Nous avons $\mu \in \text{ppcm}(a, b)$ si et seulement si $(a) \cap (b) = (\mu)$.

Démonstration. En plusieurs parties. On commence par le pgcd.

(1) **Si $\sigma \in \text{pgcd}(a, b)$** Vu que $\delta \in \text{pgcd}(a, b)$, il existe $a_1, b_1 \in A$ tels que $a = \delta a_1$ et $b = \delta b_1$. Un élément général de $(a) + (b)$ s'écrit $ax + by$, c'est-à-dire

$$ax + by = \delta a_1 x + \delta b_1 y = \delta(a_1 x + b_1 y) \in (\delta). \tag{3.320}$$

Cela prouve que $(a) + (b) \subset (\delta)$.

Pour l'autre inclusion, nous faisons appel à 3.200 disant qu'il existe $u, v \in A$ tels que $au_1 + bu_2 = \delta$. Cela montre que $\delta \in (a) + (b)$ et donc que $(\delta) \subset (a) + (b)$.

(2) **Si $(a) + (b) = (\delta)$** Nous supposons que $(a) + (b) = (\delta)$. Nous devons montrer qu'alors $\delta \in \text{pgcd}(a, b)$. Vu que a et b sont dans $(a) + (b) = (\delta)$ il existe x, y tels que $a = \delta x$ et $b = \delta y$. Donc δ divise a et b.

Supposons que d divise également a et b. Nous avons $a = da_1$ et $b = db_1$. Tout élément de $(a) + (b)$ s'écrit $ra + sb$, c'est-à-dire, en utilisant le fait que A est commutatif :

$$ra + sb = rda_1 + rdb_1 = d(ra_1 + rb_1). \tag{3.321}$$

Donc d divise tout élément de $(a) + (b)$. En particulier $d \mid \delta$.

[86] Je rappelle que A est commutatif.
[87] Définition 3.37.

Et on continue avec le ppcm.

(1) **Si $(a)\cap(b)=(\mu)$** Vu que μ est dans (a), l'élément μ est multiple de a. Et idem pour b. Donc μ est un multiple commun de a et b.

Supposons que m soit également un multiple commun de a et b. Nous avons alors $m\in(a)\cap(b)=(\mu)$, c'est-à-dire que $m\mid\mu$. Donc on a bien $\mu\in\operatorname{ppcm}(a,b)$.

(2) **Si $\mu\in\operatorname{ppcm}(a,b)$** Nous prouvons que $(a)\cap(b)=(\mu)$. Soit $x\in(a)\cap(b)$. Nous avons $x=aa_1$ et $x=bb_1$; donc x est multiple de a et de b. Vu que μ est un ppcm, nous avons $\mu\mid x$ et donc $x\in(\mu)$, ce qui signifie $(a)\cap(b)\subset(\mu)$.

Dans l'autre sens, vu que μ divise a et b nous avons $\mu\in(a)\cap(b)$ et donc $(\mu)\subset(a)\cap(b)$.

□

3.13.2 Théorème chinois

ThofPXwiM

Théorème 3.204 (Théorème des restes chinois[118])**.**
Soit un anneau principal A ainsi que des éléments $a_1,\dots,a_r\in A\setminus\{0\}$ deux à deux premiers entre eux. Nous notons a le produit $a=a_1\dots a_r$.

ITEMooWBSWooGWjnNx

(1) Il existe une unique application

$$f\colon A/(a)\to A/(a_1)\times\dots\times A/(a_r) \tag{3.322}$$

telle que

$$f([x]_a)=\big([x]_{a_1},\dots,[x]_{a_r}\big) \tag{3.323}$$

pour tout $x\in A$.

ITEMooANYPooGPgEQc

(2) Cette application f est un isomorphisme d'anneaux.

ITEMooTUOKooHcSwTD

(3) Il existe $u_1,\dots,u_r\in A$ tels que

$$\sum_{i=1}^{r}u_i\frac{a}{a_i}=1. \tag{3.324}$$

Notez ici que a_i n'est pas spécialement inversible, mais a étant le produit de tous les a_i, ça va.

ITEMooGXOEooUdKmzU

(4) Si des $u_i\in A$ vérifient $\sum_{i=1}^{r}u_ia/a_i=1$ alors la réciproque

$$f^{-1}\colon A/(a_1)\times\dots\times A/(a_r)\to A/(a) \tag{3.325}$$

vérifie

$$f^{-1}\big([x_1]_{a_1},\dots,[x_r]_{a_r}\big)=\sum_{i=1}^{r}[x_iu_i\frac{a}{a_i}] \tag{3.326}$$

pour tout $x_1,\dots,x_r\in A$.

Démonstration. En plusieurs points.

(1) **Pour (1) et (2)** Vu que les a_i sont premiers entre eux, nous avons $a=a_1\dots a_r\in\operatorname{ppcm}(a_1,\dots,a_r)$ et donc $(a)=\bigcap_{i=1}^{r}(a_i)$ par 3.203. Pour l'existence, l'unicité et fait que ce soit un isomorphisme d'anneaux, le théorème 3.134 fait tout le boulot.

(2) **Pour (3)** Les a_i sont premiers entre eux. Montrons que les a/a_i aussi. Supposons pour cela que p divise tous les a/a_i. En particulier $p\mid a/a_1=a_2\dots a_r$. Vu que les $a_2,\dots,a_r$ sont premiers entre eux, le lemme de Gauss 3.201 dit qu'il existe un $k=2,\dots,r$ tel que $p\mid a_k$. Mais p divise aussi a/a_k. Donc il existe $l\neq k$ tel que $p\mid a_l$. L'élément p est un diviseur commun de a_k et a_l. Pas possible parce que les a_i sont premiers deux à deux.

Nous avons $1\in\operatorname{pgcd}(a_1,\dots,a_r)$ et donc Bézout 3.200 dit qu'il existe des u_i tels que

$$\sum_{i=1}^{n}u_i\frac{a}{a_i}=1. \tag{3.327}$$

EQooMBGBooKoGKwJ

(3) **Pour (4)** Lorsque nous caculons

$$f\big(\sum_{i=1}^{r}[x_iu_ia/a_i]\big), \tag{3.328}$$

nous avons un vecteur d'éléments de la forme $[\sum_{i=1}^{r}x_iu_i\frac{a}{a_i}]_{a_k}$. En vertu de (3.203), tous les termes avec $i\neq k$ sont nuls et donc

$$f\big(\sum_{i=1}^{r}[x_iu_ia/a_i]\big)=\big([x_1u_1\frac{a}{a_1}]_{a_1},\dots,[x_ru_r\frac{a}{a_r}]_{a_r}\big). \tag{3.329}$$

EQooZBYVooAoUnfM

Par ailleurs nous prenons la classe par rapport à (a_k) des deux côtés de (3.327). Comme précédemment tous les termes $i\neq k$ sont nuls et il reste

$$[u_ka/a_k]_{a_k}=[1]_{a_k}. \tag{3.330}$$

Nous avons donc

$$[x_ku_k\frac{a}{a_k}]=[x_k]_{a_k}\underbrace{[u_k\frac{a}{a_k}]_{a_k}}_{=[1]_{a_k}}=[x_k]_{a_k}. \tag{3.331}$$

En remettant dans (3.329) nous trouvons ce qu'il faut :

$$f\big(\sum_{i=1}^{r}[x_iu_ia/a_i]\big)=\big([x_1]_{a_1},\dots,[x_k]_{a_k}\big). \tag{3.332}$$

□

3.13.3 Idéal premier

PROPooZICGooNmblhl

Proposition 3.205 ([119, 1], thème 6)**.**
Soit un anneau principal A et un élément $p\neq 0$ dans A. Nous avons équivalence de :

ITEMooBTEAooWlFUTX

(1) (p) est un idéal premier,

ITEMooKQRMooBNPDMX

(2) p est un élément premier,

ITEMooZYYJooCWiBhL

(3) p est un élément irréductible,

ITEMooHPAIooYoQzqD

(4) (p) est un idéal maximum propre[88].

Démonstration. En plusieurs implications.

(1) **(1) implique (2)** En plusieurs points.

- La condition $p\neq 0$ est dans les hypothèses de la proposition.
- Si p était inversible, nous aurions $(p)=A$ et donc pas que (p) est un idéal premier.
- Soient $a,b\in A$ tels que $p\mid ab$. En particulier, $(ab)\in(p)$. Mais comme (p) est un idéal premier, cela implique soit $a\in(p)$ soit $b\in(p)$. Donc soit p divise a soit p divise b.

(2) **(2) implique (3)** Un anneau principal est intègre ; c'est dans la définition 3.37. Dans un anneau intègre, tout élément premier est irréductible, c'est la proposition 3.42.

(3) **(3) implique (4)** Soit un idéal I contenant (p). Puisque A est principal, I est engendré par un seul élément ; soit $I=(a)$. Vu que $p\in I$, l'élément a divise p. Mais comme p est un élément premier, $a\mid p$ implique $a=p$ ou $a=1$. Dans le premier cas, $I=(a)=(p)$, et dans le second cas, $I=(a)=(1)=A$. Donc (p) est bien un idéal maximum.

De plus l'idéal (p) est propre. En effet avoir $(p)=A$ dirait en particulier que $1\in(p)$, c'est-à-dire qu'il existe $x\in A$ tel que $xp=1$. Or p étant irréductible, il est non inversible.

(4) **(4) implique (1)** C'est la proposition 3.90(3).

□

Un exemple d'élément premier non irréductible est $[4]_6$ dans l'anneau non principal $\mathbb{Z}/6\mathbb{Z}$. Voir 3.215 et le lemme 3.216.

[88] Ce « propre » n'est pas dans l'énoncé sur Wikipédia. Je ne comprends pas pourquoi, et j'ai posé la question sur la page de discussion.
https://fr.wikipedia.org/wiki/Idéal_premier

3.13.4 Anneau noethérien

DEFooPWMHooCnrQuJ

Définition 3.206.
Un anneau est dit ***noethérien*** *si toute suite croissante d'idéaux est stationnaire (à partir d'un certain rang).*

Montrer que tout anneau principal est noethérien est le premier pas pour montrer que tout anneau principal est factoriel.

LEMooHQPVooTfkhRV

Lemme 3.207.
Tout anneau principal[89] *est noethérien.*

Démonstration. Soit (J_n) une suite croissante d'idéaux et J la réunion. L'ensemble J est encore un idéal parce que les J_i sont emboités. Étant donné que l'idéal est principal nous pouvons prendre $a \in J$ tel que $J = (a)$. Il existe N tel que $a \in J_N$. Alors pour tout $n \geqslant N$ nous avons

$$J \subset J_N \subset J_n \subset J. \tag{3.333}$$

La première inclusion est le fait que $J = (a)$ et $a \in J_N$. La seconde est la croissance des idéaux et la troisième est le fait que J est une union. Par conséquent pour tout $n \geqslant N$ nous avons $J_N = J_n = J$. La suite est par conséquent stationnaire. □

Exemple 3.208.
Il y a moyen d'avoir un anneau noetherien non principal. C'est le cas de $\mathbb{Z}/6\mathbb{Z}$ dont nous parlerons dans 3.216. △

THOooANCAooBChmwp

Théorème 3.209 ([120, 72])**.**
Tout anneau principal est factoriel.

Démonstration. Soit un anneau principal A. Nous devons prouver les trois points de la définition 3.194. D'abord A est intègre parce que ça fait partie de la définition 3.37 d'un anneau principal. Le gros morceau est l'existence et l'unicité d'une décomposition en irréductibles.

mini lemme

Nous prouvons que si a est ni nul ni inversible, il est divisible par un irréductible.

Soit $a \in A$ que nous supposons être ni nul ni inversible. L'idéal aA ne contient pas tout A parce que a n'est pas inversible ; par le théorème de Krull 3.87 il existe un idéal maximal M contenant aA. Tous les idéaux étant principaux dans A, l'idéal M est principal.

Par définition d'idéal principal, il existe $p \in A$ tel que $M = pA$. Résumé :

$$a \in aA \subsetneq M = pA. \tag{3.334}$$

Comme l'idéal pA est maximal, la proposition 3.25 dit que p est irréductible. Et donc $p \mid a$ avec p est irréductible.

Existence

Nous définissons des suites (a_n) et (p_n) par récurrence. D'abord $a_0 = a$, et en suite, si a_n est défini nous définissons a_{n+1} et p_{n+1} de la façon suivante.

(1) Si a_n est inversible, nous nous arrêtons et la suite est finie.

(2) Si a_n n'est pas inversible, nous définissons a_{n+1} et p_{n+1} par la relation donnée par le mini-lemme :

$$a_n = p_{n+1}a_{n+1} \tag{3.335}$$

avec p_{n+1} irréductible.

Pour tout n assez petit pour que la suite ne soit pas finie, nous avons

$$a = a_0 = p_1a_1 = p_1p_2a_2 = \ldots = p_1 \ldots p_na_n \tag{3.336}$$

où les p_i sont irréductibles.

Nous montrons à présent que la suite des (a_n) est finie. Considérons les idéaux $I_n = a_nA$, et montrons qu'ils sont croissants en montrant que a_{n+1} n'est pas dans I_n.

[89] Définition 3.37.

En effet supposons que $a_{n+1} \in I_n = a_n A$. Il existerait $k \in A$ tel que $a_n k = a_{n+1}$, c'est-à-dire $p_{n+1}a_{n+1}k = a_{n+1}$. Vu que l'anneau est intègre et que les a_i sont non nums, nous simplifions par a_{n+1} : $p_{n+1}k = 1$. Cela n'est pas possible parce que p_{n+1} n'est pas inversible. Bref, nous avons uns suite strictement croissante d'idéaux.

L'anneau A est principal et donc noetherien (lemme 3.207). Donc toute suite croissante d'idéaux est stationnaire. Oh mais ça c'est pas possible si la suite des (a_n) est infinie parce que nous venons de prouver qu'elle est toujours strictement croissante.

Bon. Ben c'est que la suite des (a_n) est finie. Il existe donc un N tel que a_N est inversible. Pour ce N nous avons

$$a = a_0 = p_1 a_1 = p_1 p_2 a_2 = \ldots = p_1 \ldots p_N a_N. \tag{3.337}$$

Il nous reste à prouver que $p_N a_N$ est irréductible.

D'abord $p_N a_N$ est non ivnersible parce que p_N n'est pas inversible et a_N est inversible. Ensuite supposons que $p_N a_N = st$ avec $s, t \in A$. Nous allons prouver qu'au moins s ou t est inversible. Nous avons

$$p_N = s(ta_N^{-1}). \tag{3.338}$$

Vu que p_N est irréductible, il n'est pas le produit de deux non-inversibles. Soit s est inversible (alors on a gagné), soit ta_N^{-1} est inversible, et alors t est inversible parce que a_N^{-1} est inversible.

Unicité

Soient des irréductibles $p_1, \ldots, p_k$, $q_1, \ldots, q_m$ tels que $a = p_1 \ldots p_k = q_1 \ldots q_m$. Nous utilisons le lemme 3.202 : si p_1 était premier avec tous chacun des q_j, il serait premier avec le produit, ce qui serait absurde parce que le produit est a et p_1 divise a. Bref, il y a un des q_j qui n'est pas premier avec p_1.

Nous considérons $\sigma_1 \in S_1$ tel que p_1 n'est pas premier avec $q_{\sigma_1(1)}$. Au passage, nous notons $q_k^{(1)} = q_{\sigma_1(k)}$. Soit un diviseur commun d non inversible entre p_1 et $q_1^{(1)}$. Nous avons des éléments u, v tels que

$$p_1 = du \quad q_1^{(1)} = dv. \tag{3.339}$$

Vu que p_1 et $q_1^{(1)}$ sont irréductibles, ils ne peuvent pas être produit de deux non inversibles. Donc u et v sont inversibles. Nous pouvons écrire $d = q_1^{(1)} v^{-1}$, et donc

$$p_1 = q_1^{(1)} u v^{-1}. \tag{3.340}$$

Nous récrivons $p_1 \ldots p_k = q_1 \ldots q_m$ avec ces valeurs :

$$dup_2 \ldots p_k = dvq_2^{(1)} \ldots q_m^{(1)}. \tag{3.341}$$

Nous simplifions par d et nous avons

$$(up_2)p_3 \ldots p_k = (vq_2^{(1)})q_3^{(1)} \ldots q_m^{(1)}. \tag{3.342}$$

Par récurrence nous construisons les σ_i et les $q_j^{(i)}$. □

PROPooPVFOooJvWRIh

Proposition 3.210.
Un corps est un anneau principal et un anneau factoriel.

Démonstration. Un anneau est principal quand :

- Commutatif
- intègre
- tous les idéaux sont principaux.

Un corps est toujours commutatif. Un corps est un anneau intègre par le lemme 3.23. Donc un corps, les seuls idéaux sont $\{0\}$ et $\mathbb{K}$. Le premier est principal parce que $0A = \{0\}$. Et le second est également principal parce que $\mathbb{K} = 1\mathbb{K}$.

Donc un corps est un anneau principal.

Le fait qu'un corps soit un anneau factoriel est maintenant le théorème 3.209. □

EXooYCTDooGXAjGC

Exemple 3.211 ($\mathbb{Z}[i\sqrt{5}]$ n'est ni factoriel ni principal)**.**
Puisque $(i\sqrt{5})^2 = -5$, les éléments de $\mathbb{Z}[i\sqrt{5}]$ sont les éléments de $\mathbb{C}$ de la forme $a + bi\sqrt{5}$ avec $a, b \in \mathbb{Z}$. Nous définissons la **norme** sur $\mathbb{Z}[i\sqrt{5}]$ par[90]

$$\begin{aligned} N\colon \mathbb{Z}[i\sqrt{5}] &\to \mathbb{N} \\ z &\mapsto z\bar{z}. \end{aligned} \tag{3.343}$$

Le fait que ce soit à valeurs dans $\mathbb{N}$ est un simple calcul :

$$N(x + iy\sqrt{5}) = (x + iy\sqrt{5})(x - iy\sqrt{5}) = x^2 + 5y^2. \tag{3.344}$$

De plus N est multiplicative : $N(z_1z_2) = N(z_1)N(z_2)$.

Nous pouvons maintenant déterminer les inversibles de $\mathbb{Z}[i\sqrt{5}]$. Si α est inversible, alors il existe β tel que $\alpha\beta = 1$. Au niveau de la norme,

$$N(\alpha)N(\beta) = 1, \tag{3.345}$$

ce qui implique que $N(\alpha) = 1$. Or l'équation $x^2 + 5y^2 = 1$ dans $\mathbb{N}$ donne $y = 0$, $x = \pm 1$.

Au final, les inversibles de $\mathbb{Z}[i\sqrt{5}]$ sont ± 1.

L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est alors pas factoriel (définition 3.194) parce que

$$2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}). \tag{3.346}$$

Cela donne deux décompositions du nombre 6 en produit d'éléments non associés[91] (2 n'est associé qu'à 2 et -2) parce que les inversibles sont 1 et -1.

Le fait que $\mathbb{Z}[i\sqrt{5}]$ ne soit pas factoriel implique qu'il ne soit pas principal, théorème 3.209. △

3.14 Anneau $\mathbb{Z}/6\mathbb{Z}$

SECooSWGKooEeOZTO

Nous allons donner quelques propriétés de cet anneau, et en particulier voir que dans cet anneau non intègre, la notion d'élément irréductible n'est pas très intéressante.

Voici pour commencer un calcul de la table de multiplication de $A = \mathbb{Z}/6\mathbb{Z}$. Pour les multiples de (par exemple) $[4]_6$ nous écrivons

$$1 \times [4]_6 = [4_6] \tag{3.347}$$

et ensuite

$$2 \times [4]_6 = [8]_6 = [2]_6, \tag{3.348}$$

puis

$$3 \times [4]_6 = [2 + 4]_6 = [6]_6 = [0]_6, \tag{3.349}$$

et caetera. Le résultat est :

$\times$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	0	0	0	0	0	0
$[1]_6$	0	1	2	3	4	5
$[2]_6$	0	2	4	0	2	4
$[3]_6$	0	3	0	3	0	3
$[4]_6$	0	4	2	0	4	2
$[5]_6$	0	5	4	3	2	1

(3.350)

Pour ne pas alourdir, nous n'avons pas écrit $[x]_6$ partout au lieu de x.

3.212 (Inversibles)**.**
Les éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$ sont ceux qui ont un $[1]_6$ dans leur table de multiplication. Ce sont donc

$$U(\mathbb{Z}/6\mathbb{Z}) = \{[1]_6, [5]_6\}. \tag{3.351}$$

3.213 (Diviseurs de zéro)**.**
Les diviseurs de zéro sont ceux qui ont un $[0]_6$ dans leur table de multiplication, c'est-à-dire

$$\{[2]_6, [3]_6, [4]_6\}. \tag{3.352}$$

[90] C'est le carré de la norme usuelle, mais c'est l'usage dans le milieu.
[91] Définition 3.184.

3.214 (Irréductibles)**.**
Les irréductibles sont ceux qui ne sont ni inversibles ni produit de deux éléments non inversibles. Les non inversibles sont :

$$\{[0]_6, [2]_6, [3]_6, [4]_6\}. \tag{3.353}$$

Ils sont candidats à être irréductibles. Les produits de ces éléments (on oublie les crochets) sont :

$$2 \times 2 = 4 \tag{3.354a}$$
$$2 \times 3 = 0 \tag{3.354b}$$
$$2 \times 4 = 2 \tag{3.354c}$$
$$3 \times 3 = 3 \tag{3.354d}$$
$$3 \times 4 = 0 \tag{3.354e}$$
$$4 \times 4 = 4. \tag{3.354f}$$

Donc $[0]_6$, $[2]_6$, $[3]_6$ et $[4]_6$ ne sont plus candidats à être irréductible. Bref, il ne reste aucun candidats.

L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'a aucun élément irréductible.

NORMooAXOKooAQMXoB

3.215 (Éléments premiers)**.**
Les éléments non nuls et non inversibles sont 2, 3 et 4.

(1) **Pour 2** L'élément $[2]_6$ divise 2, 4 et 0.

- Les (a, b) tels que $ab = 2$ sont : $(1, 2)$, $(2, 4)$ et $(5, 4)$. L'élément 2 divise donc toujours a ou b.
- Les (a, b) tels que $ab = 4$ sont : $(1, 4)$, $(2, 5)$ et $(4, 4)$. L'élément 2 divise donc toujours a ou b.
- Les (a, b) tels que $ab = 0$ sont : $(0, x)$, $(3, 2)$ et $(4, 3)$. L'élément 2 divise donc toujours a ou b. En particulier, $[2]_6$ divise $[0]_6$; c'est important.

Donc $[2]_6$ est un élément premier.

(2) **Pour 3** L'élément $[3]_6$ divise 3 et 0.

- Les (a, b) tels que $ab = 3$ sont : $(1, 3)$ et $(3, 5)$. L'élément 3 divise donc toujours a ou b.
- Les (a, b) tels que $ab = 0$ sont : $(0, x)$, $(3, 2)$ et $(4, 3)$. L'élément 3 divise donc toujours a ou b.

Donc $[3]_6$ est un élément premier. L'élément $[4]_6$ divise 4, 2 et 0.

- Les (a, b) tels que $ab = 4$ sont : $(1, 4)$, $(2, 5)$ et $(4, 4)$. L'élément 4 divise donc toujours a ou b.
- Les (a, b) tels que $ab = 2$ sont : $(1, 2)$, $(2, 4)$ et $(5, 4)$. L'élément 4 divise donc toujours a ou b.
- Les (a, b) tels que $ab = 0$ sont : $(0, x)$, $(3, 2)$ et $(4, 3)$. L'élément 4 divise donc toujours a ou b.

Donc $[4]_6$ est un élément premier.

Au final, les éléments premiers dans $\mathbb{Z}/6\mathbb{Z}$ sont

$$\{[2]_6, [3]_6, [4]_6\}. \tag{3.355}$$

Vous noterez que $\mathbb{Z}/6\mathbb{Z}$ a des éléments premiers non irréductibles. Cela est un contre-exemple à la proposition 3.205 dans le cas d'un anneau non-intègre.

LEMooZSELooGOFEIz

Lemme 3.216 ([1])**.**
L'anneau $\mathbb{Z}/6\mathbb{Z}$ est noetherien, mais ni intègre ni principal[92]*.*

Démonstration. Comme c'est un anneau fini, toute suite croissante de quoi que ce soit devient stationnaire ; donc $\mathbb{Z}/6\mathbb{Z}$ est noetherien.

Puisque $\mathbb{Z}/6\mathbb{Z}$ a des diviseurs de zéro, il n'est pas intègre. Et s'il n'est pas intègre, il n'est pas factoriel non plus. □

ExeDufyZI

Exemple 3.217.
Prouvons que $\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien. Pour cela nous démontrons que

$$\begin{aligned} N\colon \mathbb{Z}[i\sqrt{2}] &\to \mathbb{N} \\ a + bi\sqrt{2} &\mapsto a^2 + 2b^2 \end{aligned} \tag{3.356}$$

EqOZUIooZGmHWl

[92] Toutes les définitions dans le thème 6.

est un stathme euclidien.

Soient $z = a + bi\sqrt{2}$, $t = a' + b'i\sqrt{2}$. Nous cherchons q et r tels que la division euclidienne s'écrive $z = qt + r$. Soient $\alpha, \beta \in \mathbb{Q}$ tels que

$$\frac{z}{t} = \alpha + \beta i\sqrt{2}. \tag{3.357}$$

Nous désignons par $\alpha + \epsilon_1$ et $\beta + \epsilon_2$ les entiers les plus proches de α et β. Nous avons $|\epsilon_1|, |\epsilon_2| \leqslant \frac{1}{2}$. Nous posons alors naturellement

$$q = (\alpha + \epsilon_1) + (\beta + \epsilon_2)i\sqrt{2} \tag{3.358}$$

et nous calculons $r = z - qt$:

$$2b'\epsilon_2 - a'\epsilon_1 + i\sqrt{2}\big(\epsilon_1 b' - a'\epsilon_2\big). \tag{3.359}$$

Nous trouvons

$$N(r) = a'^2\epsilon_1^2 + 4b'^2\epsilon_2^2 + 2a'^2\epsilon_1^2 + 2b'^2\epsilon_2^2 \leqslant \frac{3}{4}a'^2 + \frac{3}{2}b'^2. \tag{3.360}$$

D'autre part $N(t) = a'^2 + 2b'^2$, et nous avons donc bien $N(r) < N(t)$.

En ce qui concerne la seconde propriété du stathme, un petit calcul montre que

$$N(zt) = (a^2 + 2b^2)(a'^2 + 2b'^2), \tag{3.361}$$

et tant que $t \neq 0$ nous avons bien $N(zt) > N(z)$. △

Notons en particulier que $\mathbb{Z}[i\sqrt{2}]$ est factoriel et principal.

ExluqIkE

Exemple 3.218 (Décomposition en facteurs irréductibles dans $\mathbb{Z}[i\sqrt{2}]$)**.**
Les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$ sont ± 1, donc deux éléments a et b sont associés (définition 3.184) si et seulement si $a = \pm b$.

De plus si p est irréductible[93], alors $-p$ est irréductible. Les éléments irréductibles de $\mathbb{Z}[i\sqrt{2}]$ arrivent donc par pairs d'éléments associés. Soit $\{p_i\}$ une sélection de un élément irréductible parmi chaque paire. Tout élément x de $\mathbb{Z}[i\sqrt{2}]$ peut alors être écrit $x = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n}$. Cette écriture va être pratique pour comparer des décompositions en facteurs irréductibles d'éléments. △

Le lemme suivant fait en pratique partie de l'exemple 3.221, mais nous l'isolons pour plus de clarté[94].

LemTScCIv

Lemme 3.219.
Si a et b sont deux éléments premiers entre eux de $\mathbb{Z}[i\sqrt{2}]$, et si il existe $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $ab = y^3$, alors a et b sont des cubes (dans $\mathbb{Z}[i\sqrt{2}]$).

Démonstration. D'après l'exemple 3.218 nous pouvons écrire

$$y = \pm p_1^{\sigma_1} \dots p_n^{\sigma_n} \tag{3.362a}$$
$$a = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n} \tag{3.362b}$$
$$b = \pm p_1^{\beta_1} \dots p_n^{\beta_n} \tag{3.362c}$$

où les p_i sont les irréductibles de $\mathbb{Z}[i\sqrt{2}]$ « modulo ± 1 » au sens où la liste des irréductibles est $\{p_i\} \cup \{-p_i\}$ (union disjointe). Étant donné que a et b sont premiers entre eux, α_i et β_i ne peuvent pas être non nuls en même temps alors que leur somme doit faire $3\sigma_i$. Nous avons donc pour chaque i soit $\alpha_i = 3\sigma_i$ soit $\beta_i = 3\sigma_i$ (et bien entendu si $\sigma_i = 0$ alors $\alpha_i = \beta_i = 0$).

Étant donné que ± 1 sont également deux cubes, a et b sont bien des cubes.

Notons que nous avons utilisé de façon capitale le fait que $\mathbb{Z}[i\sqrt{2}]$ était factoriel. □

3.14.1 Équations diophantiennes

ExZPVFooPpdKJc

Exemple 3.220.
L'équation diophantienne

$$x^2 = 3y^2 + 8 \tag{3.363}$$

n'a pas de solution. En effet si nous prenons l'équation modulo 3 nous obtenons

$$[x^2]_3 = [3y^2 + 8]_3 = [8]_3 = [2]_3. \tag{3.364}$$

Or dans $\mathbb{Z}/3\mathbb{Z}$, aucun carré n'est égal à deux : $0^2 = 0 \neq 2$, $1^2 = 1 \neq 2$ et $2^2 = 4 = 1 \neq 2$. △

[93] Définition 3.14

[94] Merci à Marvoir pour m'avoir souligné le manque.

ExmuQisZU

Exemple 3.221.
Résolvons l'équation diophantienne

$$x^2 + 2 = y^3. \tag{3.365}$$

Une première remarque est que x doit être impair. En effet si $x = 2k$, nous devons avoir y^3 pair. Mais un cube pair est divisible par 8. Donc $y^3 = 8l$ pour un certain l. L'équation devient $4k^2 + 2 = 8l$, c'est-à-dire $2k^2 + 1 = 4l$. Le membre de gauche est impair tandis que celui de droite est pair. Impossible.

Nous pouvons écrire l'équation sous la forme $x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$. Et nous considérons $\mathbb{Z}[i\sqrt{2}]$ muni de son stathme N donné par (3.356).

L'élément $i\sqrt{2}$ est irréductible parce que $N(i\sqrt{2}) = 2$, et si nous avions $i\sqrt{2} = pq$, alors nous aurions $N(p)N(q) = 2$, ce qui n'est possible que si $N(p)$ ou $N(q)$ vaut 1.

Nous prouvons maintenant que les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux. Supposons que d soit un diviseur commun ; alors il divise aussi la somme et la différence. Donc d divise à la fois $2x$ et $2i\sqrt{2}$.

Étant donné que $i\sqrt{2}$ est irréductible et que $2i\sqrt{2} = (-i\sqrt{2})^3$, les diviseurs de $2i\sqrt{2}$ sont les puissances de $(-i\sqrt{2})$. Alors nous devrions avoir $d = (i\sqrt{2})^\beta$ et donc

$$x = (i\sqrt{2})^\beta q \tag{3.366}$$

pour un certain $q \in \mathbb{Z}[i\sqrt{2}]$. Dans ce cas nous avons $N(x) = 2^\beta N(q)$, mais nous avons déjà précisé que x ne pouvait pas être pair, donc $\beta = 0$ et nous avons $d = 1$.

Comme les nombres $x \pm i\sqrt{2}$ sont premiers entre eux et que leur produit doit être un cube, ils doivent être séparément des cubes (lemme 3.219). Nous devons donc résoudre séparément $x \pm i\sqrt{2} = y^3$.

Cherchons les x et y entiers tels que $x + i\sqrt{2} = y^3$. Si nous posons $z = a + bi\sqrt{2}$, il suffit de calculer z^3 :

```
----------------------------------------------------------------------
| Sage Version 4.8, Release Date: 2012-01-20                         |
| Type notebook() for the GUI, and license() for information.        |
----------------------------------------------------------------------
sage: var('a,b')
(a, b)
sage: z=a+I*sqrt(2)*b
sage: (z**3).expand()
3*I*sqrt(2)*a^2*b - 2*I*sqrt(2)*b^3 + a^3 - 6*a*b^2
```

En identifiant cela à $x + i\sqrt{2}$ nous trouvons le système

$$\begin{cases} x = a^3 - 6ab^2 & \text{(3.367a)} \\ 1 = 3a^2b - 2b^3 & \text{(3.367b)} \end{cases}$$

où, nous le rappelons, x, a et b sont des entiers. La seconde équation montre que b doit être inversible : $b(3a^2 - 2b^2) = 1$. Il y a donc les possibilités $b = \pm 1$. Pour $b = 1$ l'équation devient $3a^2 - 2 = 1$, c'est-à-dire $a = \pm 1$. Pour $b = -1$ l'équation devient $3a^2 - 2 = -1$, impossible. En conclusion les possibilités sont

$$(x, z) = (-5, 1 + i\sqrt{2}) \tag{3.368a}$$
$$(x, z) = (5, -1 + i\sqrt{2}) \tag{3.368b}$$
$$\tag{3.368c}$$

Le travail avec $x - i\sqrt{2}$ donne les mêmes résultats.

Les deux solutions de l'équation $x^2 + 2 = y^3$ sont alors $(5, 3)$ et $(-5, 3)$. △

3.14.2 Triplets pythagoriciens et équation de Fermat pour $n = 4$

Définition 3.222.
*Les solutions entières (positives) de l'équation $x^2 + y^2 = z^2$ sont appelés **triplets pythagoriciens**.*

Ils donnent toutes les possibilités de triangles rectangles dont les côtés ont des longueurs entières.

PROPooUWNPooDwsOtJ

Proposition 3.223 ([1]).
*Les éléments (x, y, z) d'un triplet pythagoricien sont premiers dans leur ensemble[95] si et seulement si ils sont premiers deux à deux. Dans ce cas nous disons que c'est une triplet **primitif***

[95] Définition 3.54.

Démonstration. Dans un sens si x, y, z sont premiers deux à deux, ils sont premiers dans leur ensemble.

Dans l'autre sens, si x, y, z sont premiers dans leur ensemble, nous montrons qu'ils sont premiers deux à deux. Supposons que x, y ne soient pas premiers entre eux. Soit p un facteur premier commun : $x = pk$, $y = pl$. Alors

$$p^2(k^2 + l^2) = z^2. \tag{3.369}$$

Donc p^2 divise z^2 et donc p divise z.

Exactement le même raisonnement tient si x, z ou y, z ont un facteur commun. □

LemTripletsPythagoriciensPrimitifs

Lemme 3.224.
Dans un triplet pythagoricien primitif (x, y, z), on a toujours z impair et :

- *soit x impair et y pair ;*
- *soit x pair et y impair.*

Démonstration. Remarquons que le fait d'imposer que le triplet soit primitif, interdit aux nombres x et y d'être pairs en même temps. En effet, si c'était le cas, alors x^2 et y^2 seraient aussi pairs, donc leur somme z^2 aussi, d'ou z serait pair et les trois nombres ne seraient pas premiers entre eux.

Nous montrons à présent que les nombres x et y ne sont pas tous les deux impairs. Par l'absurde, si $x = 2a + 1$, nous avons $x^2 = 4a^2 + 4a + 1 \in [1]_4$; de la même manière, $y^2 \in [1]_4$. On en déduit alors que $z^2 = x^2 + y^2 \in [2]_4$. Le nombre z^2 est donc pair, donc z est pair : disons $z = 2c$. Alors, $z^2 = 4c^2 \in [0]_4$. Comme les classes modulo 4 sont disjointes, nous aboutissons à une contradiction. □

PropXHMLooRnJKRi

Proposition 3.225 (Triplets pythagoriciens[121, 122])**.**
Un triplet $(x, y, z) \in (\mathbb{N}^*)^3$ est solution de $x^2 + y^2 = z^2$ si et seulement si il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ premiers entre eux tels que subeqLVHFooVgWsFx

$$\begin{cases} x = d(u^2 - v^2) & \text{(3.370a)} \\ y = 2duv & \text{(3.370b)} \\ z = d(u^2 + v^2) & \text{(3.370c)} \end{cases}$$

ou SUBEQSooRQKBooCBsqYA

$$\begin{cases} x = 2duv & \text{(3.371a)} \\ y = d(u^2 - v^2) & \text{(3.371b)} \\ z = d(u^2 + v^2) & \text{(3.371c)} \end{cases}$$

La différence entre les deux est seulement d'inverser les rôles de x et y.

Démonstration. Montrons d'abord que les formules proposées sont bien des solutions ; nous vérifions (3.370) :

$$x^2 + y^2 = d^2(u^2 - v^2)^2 + 4d^2u^2v^2 = d^2(u^2 + v^2)^2, \tag{3.372}$$

qui correspond bien au z^2 proposé. Une vérification du même style fonctionne pour (3.371).

Réciproquement, supposons que (x, y, z) soit un triplet pythagoricien primitif. Sans perte de généralité[96], grâce au lemme 3.224, nous pouvons supposer que y est pair tandis que y et z seront impairs. Notons $y = 2k$, alors

$$y^2 = 4k^2 = (z - x)(z + x) = z^2 - x^2.$$

Plusieurs choses à dire sur cela.

- D'abord, $z - x$ et $z + x$ sont tous les deux pairs. On pose $z - x = 2a$ et $z + x = 2b$.
- Ensuite, on a $4k^2 = 4ab$, donc $k^2 = ab$.
- Enfin, a et b sont premiers entre eux. En effet, si d est un diviseur commun de a et de b, alors d divise $a + b = z$ et $a - b = x$. Sous cette même hypothèse, d^2 est aussi un diviseur de $ab = k^2$, donc aussi de y^2, et donc, d divise y. Or, comme le triplet pythagoricien $(x; y; z)$ est primitif, ce diviseur commun n'est autre que 1.

Supposons que p soit un diviseur premier de k. Alors p^2 est un diviseur de $k^2 = ab$. Comme a et b sont premiers entre eux, p^2 est soit un diviseur de a, soit un diviseur de b. En faisant cela pour tous les diviseurs premiers de k, on constate que a et b sont deux carrés d'entiers. On prend alors u et v tels que

$$u^2 = b \qquad \text{et} \qquad v^2 = a. \tag{3.373}$$

[96] En échangeant les rôles de x et y ici, nous obtenons à la fin la seconde forme des solutions.

Vérifions alors les égalités demandées :

$$u^2+v^2=b+a=\frac{1}{2}(z+x)+\frac{1}{2}(z-x)=z \tag{3.374}$$
$$u^2-v^2=b-a=\frac{1}{2}(z+x)-\frac{1}{2}(z-x)=x \tag{3.375}$$
$$2uv=2\sqrt{a}\sqrt{b}=2\sqrt{k^2}=2k=y. \tag{3.376}$$

□

Remarque 3.226.
Les solutions dans lesquelles x, y ou z sont nuls sont faciles à classer. La solution $(1,0,1)$ n'est pas dans les formes proposées. En effet elle ne peut pas être de la première forme : avoir $y=0$ demanderait qu'un nombre parmi d, u et v soit nul, ce qui est interdit. La solution $(1,0,1)$ ne peut pas non plus être de la seconde forme parce que x y est pair.

propFKKKooFYQcxE

Proposition 3.227 ([121]).
Les équations $x^4+y^4=z^2$ et $x^2+y^4=z^4$ n'ont pas de solution dans $(\mathbb{N}^*)^3$.

Démonstration. Si la première équation n'a pas de solution, alors la seconde n'en a pas non plus parce que z^4 est un carré. Nous nous concentrons donc sur l'équation $x^4+y^4=z^2$ et nous supposons qu'il existe au moins une solution dans $(\mathbb{N}^*)^3$. Nous en choisissons une (x,y,z) avec z minimum (les z dans différentes solutions étant dans $\mathbb{N}$, il en existe forcément un minimum[97]). Du coup, les trois nombres x, y et z sont premiers dans leur ensemble parce qu'une division par leur pgcd donnerait une nouvelle solution qui contredirait la minimalité de z.

Nous posons $x^4=\bar{x}^2$ et $y^4=\bar{y}^2$. Ils vérifient l'équation $\bar{x}^2+\bar{y}^2=z^2$ et par la proposition 3.225, il existe $u,v\in\mathbb{N}^*$ premiers entre eux tels que, sans perte de généralité[98], on ait

$$\begin{cases}\bar{x}=2uv & \text{(3.377a)}\\ \bar{y}=u^2-v^2 & \text{(3.377b)}\\ z=u^2+v^2. & \text{(3.377c)}\end{cases}$$

eqnFKKKooFYQcxE1 eqnFKKKooFYQcxE2

Si u est pair, alors v est impair (et inversement) parce que $\text{pgcd}(u,v)=1$ Si u est pair, alors $u=2a$ et $v=2b+1$, ce qui donne $\bar{y}=4a^2-4b^2-4b-1\in[-1]_4$. Or nous avons déjà vu qu'un carré est dans $[0]_4$ ou dans $[1]_4$. Il faut donc que u soit impair. Le lemme 3.224 implique alors que v soit pair.

De l'équation 3.377b, nous en déduisons que $v^2+\bar{y}=u^2$; de plus u^2, v^2 et $\bar{y}$ sont premiers dans leur ensemble : en effet, u et v sont premiers entre eux, et si l'un parmi u^2 et v^2 a un facteur commun avec $\bar{y}$, alors l'autre doit l'avoir aussi (dans une égalité $a+b=c$, si deux des nombres ont un diviseur commun, le troisième l'a aussi). Comme $\bar{y}=y^2$, le triplet (v,y,u) est un triplet pythagoricien primitif. Nous appliquons de nouveau la proposition 3.225, en se souvenant que v est pair : il existe donc deux nombres r et s premiers entre eux tels que

eqnFKKKooFYQcxE3

$$\begin{cases}v=2rs & \text{(3.378a)}\\ y=r^2-s^2 & \text{(3.378b)}\\ u=r^2+s^2. & \text{(3.378c)}\end{cases}$$

Avec cela, $\bar{x}=2uv=4rs(r^2+s^2)$. Remarquons que les trois nombres r, s et r^2+s^2 sont premiers entre eux dans leur ensemble ; or, comme $\bar{x}$ est un carré ces nombres doivent séparément être des carrés :

$$\begin{cases}r=\alpha^2 & \text{(3.379a)}\\ s=\beta^2 & \text{(3.379b)}\\ r^2+s^2=\gamma^2. & \text{(3.379c)}\end{cases}$$

En mettant les deux premiers dans la troisième équation, nous avons $\alpha^4+\beta^4=\gamma^2$. Donc $(\alpha^2,\beta^2,\gamma)$ est une solution. Nous allons montrer que $\gamma<z$, ce qui terminera la preuve, puisque z était supposé minimal. Nous avons :

$$\begin{aligned}z&=u^2+v^2 && \text{par 3.377c}\\ &=r^2+s^2+4r^2s^2 && \text{par 3.378}\\ &=\gamma^2+4r^2s^2\\ &>\gamma^2,\end{aligned}$$

[97] Voir quelque chose comme le lemme 2.50.
[98] En inversant les rôles de x et y au besoin.

et a fortiori $\gamma < z$. □

3.15 Polynômes

3.15.1 Polynômes d'une variable

Et voilà la définition que tout le monde attendait ; la définition des anneaux de polynômes. Pour ne pas taper trop fort du premier coup, nous commençons par les polynômes d'une seule variable[99].

L'ensemble des polynômes sur A sera simplement $A^{(\mathbb{N})}$ (notation 3.101). Puisque $\mathbb{N}$ est un ensemble bien particulier possédant plein de structure, nous allons pouvoir installer sur $A^{(\mathbb{N})}$ une structure non seulement de A-module (ça c'est déjà fait), mais en plus d'anneau, ainsi qu'une évaluation.

DEFooFYZRooMikwEL

Définition 3.228.
*L'ensemble des **polynômes** en une indéterminée sur l'anneau A est l'anneau*

$$\mathcal{P}(A) = A^{(\mathbb{N})} \tag{3.380}$$

défini en 3.101.

3.229.
En ce qui concerne la notation $A[X]$, voir 3.15.2. Pour $\mathbb{K}(X)$ lorsque $\mathbb{K}$ est un corps, voir 8.84.

DefDegrePoly

Proposition-Définition 3.230 ([123]).
Soit P non nul dans $\mathcal{P}(A)$. Nous notons a_n la valeur[100] de P en $n \in \mathbb{N}$: $P = (a_n)_{n\in\mathbb{N}}$.

(1) L'ensemble $\{n \in \mathbb{N}$ tel que $a_n \neq 0\}$ est fini dans $\mathbb{N}$.

(2) Cet ensemble possède un minimum et un maximum.

*Le **degré** de P est*

$$\deg(P) = \max\{n \in \mathbb{N} \text{ tel que } a_n \neq 0\}, \tag{3.381}$$

*et la **valuation** de P est*

$$\mathrm{val}(P) = \min\{n \text{ tel que } a_n \neq 0\}. \tag{3.382}$$

Nous notons

$$\mathcal{P}_n(A) = \{P \in \mathcal{P}(A) \text{ tel que } \deg(P) \leqslant n\}, \tag{3.383}$$

EQooAULWooDggqWT

Dans le cas du polynôme nul, l'ensemble $\{n \in \mathbb{N}$ tel que $a_n \neq 0\}$ est vide, et les définitions ne s'appliquent pas. Nous convenons que

$$\mathrm{val}(0) = +\infty \tag{3.384a}$$
$$\deg(0) = -\infty. \tag{3.384b}$$

Démonstration. Le fait que P soit non nul implique que $A = \{n \in \mathbb{N}$ tel que $a_n \neq 0\}$ est non vide. De plus cet ensemble est fini parce que $P \in A^{(\mathbb{N})}$. Toute partie finie non vide de $\mathbb{N}$ étant majorée et minorée (lemme 2.33(1)), le lemme 2.32 définit correctement le minimum et le maximum de A. □

Vu que $A^{(\mathbb{N})}$ est engendré par les e_i, tout polynôme sur A s'écrit $P = \sum_{i=1}^{n} a_i e_i$.

DEFooNXKUooLrGeuh

Définition 3.231.
Nous ajoutons deux structures à $A^{(\mathbb{N})}$.

L'évaluation *Si $\alpha \in A$ et si $P \in A^{(\mathbb{N})}$, nous définissons $P(\alpha)$ par*

$$P(\alpha) = (\sum_{i=0}^{n} a_i e_i)(\alpha) = \sum_{i=0}^{n} a_i \alpha^i, \tag{3.385}$$

EQooDJISooTEkMQw

étant entendu que $\alpha^0 = 1$ dans A.

Cette définition s'étend immédiatement au cas où B est un anneau qui étend A. Dans ce cas nous pouvons définir $P(b)$ pour tout $P \in A^{(\mathbb{N})}$ et $b \in B$ avec la même formule (3.385).

[99] Pour les polynômes à plusieurs variables, voir la définition 3.180.
[100] Ici il y a une énorme subtilité de terminologie. Formellement, P est une application $\mathbb{N} \to A$. Cela n'a rien à voir avec le fait que P puisse être évalué sur A avec des formules du type $P(x) = \sum_n a_n x^n$. D'ailleurs nous n'avons pas encore vu cette évaluation.

Le produit *C'est ici que la structure particulière de $\mathbb{N}$ est utilisée. Nous définissons le produit $A^{\mathbb{N}} \times A^{(\mathbb{N})} \to A^{(\mathbb{N})}$ de la façon suivante. Si $(P_k)_{k\in\mathbb{N}}$ est la suite (presque partout nulle) d'éléments de A qui définit P et si $(Q_k)_{k\in\mathbb{N}}$ est celle de Q, nous notons*

$$(PQ)_n = \sum_{k=0}^{n} P_k Q_{n-k}, \tag{3.386}$$

EQooTNCSooKklish

et donc $PQ = \sum_i (PQ)_i e_i$. Plus explicitement,

$$(\sum_{i=0}^{n} a_i e_i)(\sum_{j=0}^{m} b_j e_j) = \sum_{k=0}^{\infty} \Big(\sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j \Big) e_k. \tag{3.387}$$

EQooCIBUooAgpxiL

Notons qu'à droite, la somme sur k est une somme finie.

PROPooGDQCooHziCPH

Proposition 3.232.
Soit un anneau A. À propos de structure sur $A^{(\mathbb{N})}$.

(1) Avec le produit, l'ensemble $A^{(\mathbb{N})}$ devient un anneau.

(2) L'application

$$\begin{aligned} g\colon A^{(\mathbb{N})} &\to A \\ P &\mapsto P(\alpha) \end{aligned} \tag{3.388}$$

est un morphisme d'anneaux[101]*. En particulier, $(PQ)(\alpha) = P(\alpha)Q(\alpha)$.*

Démonstration. En plusieurs points

(1) **Anneau** L'identité pour le produit dans $A^{(\mathbb{N})}$ est le polynôme donné par $a_0 = 1$ et $a_i = 0$ pour $i \neq 0$. Cela se vérifie en utilisant directement la définition (3.387). La distributivité aussi[102].

(2) **Le morphisme** Nous notons P_k les éléments de la suite définissant P et Q_k ceux de Q. Alors nous avons

$$(P+Q)(\alpha) = \sum_k (P_k + Q_k)\alpha^k = \sum_k P_k\alpha^k + \sum_k Q_k\alpha^k = P(\alpha) + Q(\alpha). \tag{3.389}$$

Vous aurez noté que la première égalité était la définition (3.144b). De même,

$$P(\alpha)Q(\alpha) = \big(\sum_n P_n\alpha^n\big)\big(\sum_k Q_k\alpha^k\big) = \sum_k Q_k\big(\sum_n P_n\alpha^n\big)\alpha^k = \sum_k\sum_n Q_k P_n \alpha^{n+k} \tag{3.390a}$$

$$= \sum_m \big(\sum_{l=0}^{m} P_l Q_{m-l}\big)\alpha^m = \sum_m (PQ)_m\alpha^m = (PQ)(\alpha). \tag{3.390b}$$

□

LEMooWVUXooQlaepO

Lemme 3.233.
Si A est un anneau commutatif, alors $A^{(\mathbb{N})}$ est commutatif.

Démonstration. Soient $P, Q \in A^{(\mathbb{N})}$; pour rappel, le produit est donné par la définition 3.386. L'application

$$\begin{aligned} \varphi\colon \{0,\dots,n\} &\to \{0,\dots,n\} \\ k &\mapsto n-k \end{aligned} \tag{3.391}$$

[101] Définition 1.106.
[102] Je n'ai pas fait les calculs, écrivez-moi pour me dire si ça va facilement.

est une bijection. Voici maintenant le calcul :

$$(PQ)_n = \sum_{k=0}^{n} P_k Q_{n-k} \tag{3.392a}$$
$$= \sum_{k=0}^{n} P_{\varphi(k)} Q_{n-\varphi(k)} \tag{3.392b}$$
$$= \sum_{k=0}^{n} P_{n-k} Q_k \tag{3.392c}$$
$$= \sum_{k=0}^{n} Q_k P_{n-k} \tag{3.392d}$$
$$= (QP)_n. \tag{3.392e}$$

Justifications

- Pour (3.392b). Lemme 2.129 et le fait que φ soit une bijection.
- Pour (3.392d). Commutativité de A.

□

3.15.2 La notation $A[X]$

Si A est un anneau, nous avons déjà défini les polynômes en une indéterminée sur A comme étant le module $A^{(\mathbb{N})}$ qui est devenu un anneau par la proposition 3.232.

Le polynôme donné par la suite $(a_n)_{n\in\mathbb{N}}$ est souvent notée

$$\sum_k a_k X^k. \tag{3.393}$$

Par exemple avec $a = (4, 2, 8)$ nous avons $a = 8X^2 + 2X + 4$. Nous utiliserons souvent cette notation, qui est très pratique parce qu'elle s'adapte bien aux règles de multiplication et d'addition, en particulier la distributivité.

Il y a (au moins) deux façons de comprendre ce que signifie réellement « X » dans cette notation.

3.15.2.1 Première façon (qui botte en touche)

La première est de dire qu'il n'a pas de significations, et que X^2 est un simple abus de notations pour écrire $(0, 0, 1, 0, \cdots)$. Avec cette façon de voir, nous notons l'anneau des polynômes sur A par « $A[X]$ » où le X n'a pas d'autres raisons d'être que d'avertir le lecteur que nous réservons la lettre « X » pour utiliser la notation pratique des polynômes.

3.15.2.2 Seconde façon (la bonne)

3.234.

La seconde façon de voir le « X » est de nous rappeler que $A^{(\mathbb{N})}$ a une base en tant que module : les e_k dont nous avons parlé plus haut. Nous posons $X = e_1$, et nous prenons la convention $X^0 = 1$. Alors nous avons $e_k = X^k$ et nous notons $A[X]$ l'anneau $A^{(\mathbb{N})}$ exprimé avec X.

Dans les deux cas, il n'est pas vraiment légitime d'écrire des égalités comme « $P(X) = X^2 + 2X - 3$ », et encore moins de dire « Le polynôme P, *évalué* en X vaut $X^2 + 2X - 3$ » : il est plus correct d'écrire « $P = X^2 + 2X - 3$ ».

Le lemme suivant montre que ces notations tombent vraiment à point. La véritable difficulté de l'énoncé est de comprendre qu'il n'est pas trivial.

Nous avons vu dans la définition 3.231 que si B est un anneau qui étend A, et si $P \in A[X]$, alors nous avons une définition de $P(b)$ pour tout $b \in B$. Nous appliquons cela à $B = A[X]$, qui est un anneau qui étend A. Autrement dit, si P et Q sont des polynômes, ça a un sens d'écrire $P(Q)$ et le résultat sera un élément de $A[X]$.

Dans le cas particulier $Q = X$, nous avons une chouette formule.

LEMooGKWQooVOyeDX

Lemme 3.235.
Nous avons

$$P(X) = P \tag{3.394}$$

pour tout $P \in A[X]$.

Démonstration. Si $P = (a_k)_{k\in\mathbb{N}}$ alors par définition $P(\alpha) = \sum_k a_k\alpha^k$ dès que α est dans un anneau B qui étend A. Nous considérons le cas particulier $B = A[X]$ et $\alpha = X$, c'est-à-dire $Q = (0, 1, 0, \ldots)$, l'élément $P(X)$ de $A[X]$ vaut

EQooABULooFCEasf

$$\sum_k a_k X^k, \tag{3.395}$$

qui est exactement P lui-même. □

Mais il faut bien comprendre que si P est le polynôme $(-3, 2, 1, 0, \ldots)$, noté X^2+2X-3, écrire $P(X) = X^2 + 2X - 3$ est une pirouette de notations que rien ne justifie par rapport à simplement écrire $P = X^2 + 2X - 3$.

3.15.3 Action du groupe symétrique

DefActionGroupe

Définition 3.236 (Action de groupe Thème 9)**.**
Une ***action de groupe*** G *sur un ensemble* E *est une application* $\phi\colon G \times E \to E$ *telle que*

$$\begin{aligned} \phi(e, x) &= x, \qquad \forall x \in E; \\ \phi(gh, x) &= \phi\big(g, \phi(h, x)\big) \qquad \forall g, h \in G, \forall x \in E. \end{aligned}$$

On dit dans ce cas que G ***agit*** *sur* E.

Nous allons souvent noter l'élément $\phi(g, x)$ *pourra être noté de plein de façons :*

$$\phi(g, x) = \phi_g(x) = \phi_x(g) = g \cdot x. \tag{3.396}$$

La définition d'un groupe agissant continument sera la définition 15.3.

Par souci de notations, nous notons $\mathcal{P}_n(A)$ l'anneau des polynômes de n variables sur A. La propriété universelle de $\mathcal{P}_n(A) = A^{(\mathbb{N}^n)}$ du théorème 3.103 nous donne une application

$$g\colon \text{Fun}\big(\mathbb{N}^n, \mathcal{P}_n(A)\big) \to \text{Hom}_A\big(\mathcal{P}_n(A), \mathcal{P}_n(A)\big) \tag{3.397}$$

Avec cela nous pouvons énoncer et démontrer le lemme qui donne l'action de S_n[103] sur $\mathcal{P}_n(A)$.

LEMooIRVQooHvoNBq

Lemme 3.237 ([124])**.**
Pour $\sigma \in S_n$ *nous définissons*

$$\begin{aligned} \phi_\sigma\colon \mathbb{N}^n &\to \mathcal{P}_n(A) \\ m &\mapsto e_{\sigma(m)}. \end{aligned} \tag{3.398}$$

Alors l'application

$$\begin{aligned} \rho\colon S_n &\to \text{Hom}_A\big(\mathcal{P}_n(A), \mathcal{P}_n(A)\big) \\ \sigma &\mapsto g(\phi\sigma) \end{aligned} \tag{3.399}$$

est une action[104].

Démonstration. Nous commençons par donner une expression à notre ρ. Un élément de $\mathcal{P}_n(A)$ est de la forme $\sum_{m\in\mathbb{N}^n} a_m e_m$, et nous avons[105]

$$\rho(\sigma)\Big(\sum_{m\in\mathbb{N}^n} a_m e_m\Big) = \sum_m a_m \phi_\sigma(m) = \sum_m a_m e_{\sigma(m)}. \tag{3.400}$$

Nous avons tout de suite $\rho(\text{Id}) = \text{Id}$.

En ce qui concerne la composition, nous avons d'une part

$$\rho(\sigma_1\sigma_2)\Big(\sum_m a_m e_m\Big) = g(\phi_{\sigma_1\sigma_2})\Big(\sum_m a_m e_m\Big) = \sum_m a_m e_{\sigma_1\sigma_2(m)}, \tag{3.401}$$

[103] Définition du groupe symétrique S_n en 2.2.
[104] Définition 3.236.
[105] La somme est définie par 2.129, et ça va être important. Ah oui, en réalité partout, les sommes sont finies parce que les a_m $(m \in \mathbb{N}^n)$ sont presque tous nuls. Il faudrait écrire sur la somme sur $\{m \in \mathbb{N}^2 \text{ tel que } a_m \neq 0\}$, mais vous vous imaginez la complication dans la notation.

et d'autre part,

$$\rho(\sigma_1)\rho(\sigma_2)\big(\sum_m a_m e_m\big) = \rho(\sigma_1)\big(\sum_m a_m e_{\sigma_2(m)}\big) \tag{3.402a}$$
$$= \rho(\sigma_1)\big(\sum_m a_{\sigma_2^{-1}(m)} e_m\big) \tag{3.402b}$$
SUBEQooTSCYooCUWiRx
$$= \sum_m a_{\sigma_2^{-1}(m)} e_{\sigma_1(m)} \tag{3.402c}$$
$$= \sum_m a_m e_{\sigma_1\sigma_2(m)} \tag{3.402d}$$
SUBEQooQPGPooVxqJdT

La proposition 2.131 est utilisée pour (3.402b) et pour (3.402d). □

PROPooUIZOooCqQzJh

Proposition 3.238 ([1]).
Soient un anneau A ainsi que des éléments a_i et b_i. Si $\prod_{i=1}^n a_i$ est non nul, alors

$$\deg \prod_{i=1}^n (a_i X + b_i) = n. \tag{3.403}$$

De plus le coefficient de X^n est $\prod_{i=1}^n a_i$.

3.15.4 Corps des fractions

DEFooGJYXooOiJQvP

Proposition 3.239 ([125]).
Soit un anneau commutatif et intègre[106] A. Nous posons $E = A \times A \setminus \{0\}$, et nous définissons les deux opérations suivantes sur E :

ITEMooWBWHooYsXFkO

(1) $(a,b) + (c,d) = (ad + cb, bd)$;

ITEMooGOOIooCHqLRl

(2) $(a,b)(c,d) = (ac, bd)$.

Nous notons a/b la classe de (a,b). Alors

ITEMooRXFAooUqQfIV

(1) La relation $(a,b) \sim (c,d)$ si et seulement si $ad = bc$ est une relation d'équivalence[107].

ITEMooSFZEooUqFGIB

(2) La somme passe au quotient : si $(x,y) \sim (a,b)$ et $(z,t) \sim (c,d)$, alors

$$(x,y) + (z,t) \sim (a,b) + (c,d). \tag{3.404}$$

ITEMooIZDTooEoALGh

(3) Le produit passe au quotient : si $(x,y) \sim (a,b)$ et $(z,t) \sim (c,d)$, alors

$$(x,y)(z,t) \sim (a,b)(c,d). \tag{3.405}$$

ITEMooOTZJooMkarjT

(4) Le quotient

$$\mathrm{Frac}(A) = \big(A \times A \setminus \{0\}\big)/\sim \tag{3.406}$$

muni des sommes et produit passées au quotient est un corps dont

ITEMooLFSEooAIrbFK

(4a) La classe de $(0,1)$ est neutre pour la somme.

ITEMooYUNEooAKZJEh

(4b) La classe de $(1,1)$ est neutre pour la multiplication.

ITEMooOGPCooAZGWoF

(4c) L'opposé de a/b est $(-a)/b$.

ITEMooECDBooJdJEza

(4d) Si $a \neq 0$, alors l'inverse de a/b est b/a.

ITEMooZOTMooMaIblt

(5) Soit un couple $(\mathbb{K}, \epsilon)$ où $\mathbb{K}$ est un corps commutatif et $\epsilon\colon A \to \mathbb{K}$ est un morphisme injectif d'anneaux tels que pour tout $\lambda \in \mathbb{K}$, il existe $(a,b) \in A \times A^*$ tels que

$$\lambda = \epsilon(a)\big(\epsilon(b)\big)^{-1} \tag{3.407}$$

Alors il y a un isomorphisme de corps entre $\mathbb{K}$ et $\mathrm{Frac}(A)$.

*Un corps $\mathbb{K}$ ayant les propriétés de (5) est est un **corps des fractions** de A. Lorsque nous parlons du corps des fractions de A sans précisions[108], nous parlons de $\mathrm{Frac}(A)$.*

[106] Définition 3.22.
[107] Définition 1.55.
[108] Par exemple lorsque nous dirons que $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$.

Démonstration. En plein de parties.

(1) **Pour (1) : relation d'équivalence** Il faut vérifier les conditions de la définition 1.55. Vu que $ab = ba$ nous avons $(a,b) \sim (a,b)$. Pour la symétrie c'est la même chose. Pour la transitivité, si $(a,b) \sim (c,d)$ et $(c,d) \sim (x,y)$ alors $ad = bc$ et $cy = dx$.

Si $c = 0$ alors comme $d \neq 0$ et $ad = bc$, nous avons $a = 0$ (par 3.22(2)) et comme $cy = dx$, nous avons $x = 0$. Donc $ay = 0 = bx$.

Si $c \neq 0$, alors nous multiplions les deux égalités entre elles : $adcy = bcdx$. Nous pouvons simplifier par d et c en vertu de la définition 3.22(3) d'un anneau intègre. Il reste $ay = bx$, c'est-à-dire $(a,b) \sim (x,y)$.

(2) **Pour (2)** L'hypothèse est que $xb = ya$ et $zd = tc$. Nous avons

$$(a,b) + (c,d) = (ad + cb, bd) \tag{3.408a}$$
$$(x,y) + (z,t) = (xt + yz, yt). \tag{3.408b}$$

Pour voir qu'ils sont équivalents, nous vérifions que $(ad+cb)(yt) = bd(xt+yz)$. Il suffit de développer et de substituer xb par ya et zd par tc là où vous les trouvez.

(3) **Pour (3)** L'hypothèse est que $xb = ya$ et $zd = tc$. Nous avons

$$(x,y)(z,t) = (xz, yt) \tag{3.409a}$$
$$(a,b)(c,d) = (ax, bd). \tag{3.409b}$$

Encore une fois, on vérifie que $xzbd = ytac$.

(4) **Pour (4)** Il y a quelques vérifications à faire pour l'associativité et la distributivité[109].
Nous nous concentrons sur les sous-points.

(4a) **Pour (4a)** Simple vérification : $(a,b) + (0,1) = (a+0, b) = (a,b)$.

(4b) **Pour (4b)** Nous devons prouver que si $(x,y) \in 1/1$, alors $(a,b)(x,y) \sim (1,1)$. L'hypothèse est que $(x,y) \sim (1,1)$, c'est-à-dire $x = y$. À partir de là il suffit de calculer $(a,b)(x,y))$ et de voir que $ayb = bxa$.

(4c) **Pour (4c)** Nous avons $(a,b) + (-a,b) = (0,b^2) \sim (0,1)$. Donc

$$\overline{(a,b)} + \overline{(-a,b)} = \overline{(a,b) + (-a,b)} = \overline{0,1}. \tag{3.410}$$

(4d) **Pour (4d)** Nous avons simplement le calcul

$$(a,b)(b,a) = (ab, ab) \sim (1,1). \tag{3.411}$$

(5) **Morphisme de corps** Nous considérons l'application

$$\begin{aligned} f\colon A \times A^* &\to \mathbb{K} \\ (a,b) &\mapsto \epsilon(a)\epsilon(a)^{-1}, \end{aligned} \tag{3.412}$$

et nous prouvons que $f(a,b) = f(x,y)$ si et seulement si $(a,b) \sim (x,y)$.

(5a) $\Rightarrow$ Si $f(a,b) = f(x,y)$, alors nous avons

$$\epsilon(a)\epsilon(b)^{-1} = \epsilon(x)\epsilon(y)^{-1} \tag{3.413a}$$
$$\epsilon(a)\epsilon(y) = \epsilon(x)\epsilon(b) \tag{3.413b}$$
$$\epsilon(ay) = \epsilon(xb) \tag{3.413c}$$
$$ay = xb \qquad \epsilon \text{ est injectif} \tag{3.413d}$$
$$(a,b) \sim (x,y) \tag{3.413e}$$

(5b) $\Leftarrow$ Même calcul, à l'envers, en partant de $ay = bx$.

Nous pouvons donc définir

$$\begin{aligned} \varphi\colon \text{Frac}(A) &\to \mathbb{K} \\ \overline{(a,b)} &\mapsto f(a,b) = \epsilon(a)\epsilon(b)^{-1}. \end{aligned} \tag{3.414}$$

[109] Je vous invite à les faire parce que je n'ai pas vérifié.

(5a) **φ est injectif** Si $\varphi\big(\overline{(a,b)}\big) = \varphi\big(\overline{(x,y)}\big)$, alors $f(a,b) = f(x,y)$, c'est-à-dire $(a,b) \sim (x,y)$ par ce qui a été fait juste au-dessis.

(5b) **φ est un morphisme** D'abord

$$\varphi\big(\overline{(a,b)(c,d)}\big) = \varphi\big(\overline{(ad,bc)}\big) = f(ad,bc) = \epsilon(ad)\epsilon(bc)^{-1}. \tag{3.415}$$

Et en même temps,

$$\varphi\big(\overline{(a,b)}\big)\varphi\big(\overline{(c,d)}\big) = f(a,b)f(c,d) = \epsilon(a)\epsilon(b)^{-1}\epsilon(c)\epsilon(d)^{-1}. \tag{3.416}$$

Le fait que ce soit égal provient de

$$\epsilon(bc)^{-1} = [\epsilon(b)\epsilon(c)]^{-1} = \epsilon(b)^{-1}\epsilon(c)^{-1}. \tag{3.417}$$

□

DEFooXHKGooCcJbTR

Définition 3.240 ([1]).
Lorsque A est un anneau de polynômes[110]*, alors les éléments de* $\mathrm{Frac}(A)$ *sont des* ***fractions rationnelles****.*

PROPooUULNooKbwuEw

Proposition 3.241.
Soit un anneau commutatif A. Nous considérons l'application

$$\begin{aligned} i\colon A &\to \mathrm{Frac}(A) \\ a &\mapsto a/1. \end{aligned} \tag{3.418}$$

(1) Elle est injective.

(2) Elle est un morphisme d'anneaux[111]*.*

Démonstration. En plusieurs parties.

(1) **Injective** Supposons que $f(a) = f(b)$, c'est-à-dire que $a/1 = b/1$. En vertu de la relation d'équivalence donnée en 3.239, nous avons $a1 = b1$, c'est-à-dire $a = b$.

(2) **Morphisme d'anneaux** D'abord nous avons

$$i(a) + i(b) = (a/1) + (b+1) \tag{3.419a}$$
$$= (a1 + 1b)/1 \tag{3.419b}$$
$$= i(a+b). \tag{3.419c}$$

Ensuite,

$$i(a)i(b) = (a/1)(b/1) = ab/1 = i(ab). \tag{3.420}$$

Et enfin $i(1) = 1/1$ est bien l'unité de $\mathrm{Frac}(A)$ par 3.239(4b).

□

NORMooFBKEooBQuATg

3.242.
Si $a \in A$, nous nous permettrons de noter également a l'élément $a/1$ de $\mathrm{Frac}(A)$. Ce sera toujours clair dans le contexte.

NORMooVYEMooUiUfnE

3.243.
En vertu de la proposition 3.241, à partir de maintenant, nous allons identifier la partie $i(\mathbb{Z})$ à $\mathbb{Z}$. Nous nous autorisons donc à dire que $4 \in \mathbb{Q}$ ou que $-7 \in \mathbb{Q}$, et même que $0 \in \mathbb{Q}$.

PROPooTXGUooRvViwT

Proposition 3.244 (Règle de simplification de fraction[1])**.**
Soit un anneau commutatif A. Si $a, x, y \in A$ avec $a, y \neq 0$, nous avons

(1)

$$ax/a = x/1. \tag{3.421}$$

Si vous avez suivi 3.242, cela signifie que $ax/a = x$ dans $\mathrm{Frac}(A)$*.*

(2)

$$ax/ay = x/y \tag{3.422}$$

[110] Définition 3.228.
[111] Définition 1.106.

dans Frac(A).

LEMooBJRCooIZnaid

Lemme 3.245.
Soient un anneau A ainsi que $a, b, x, y \in A$. Si $b, y \neq 0$, nous avons $ay = bx$ dans A si et seulement si nous avons $ab^{-1} = xy^{-1}$ dans Frac(A)[112].

Démonstration. Deux parties.

(1) $\Rightarrow$ Nous supposons avoir $ay = bx$ dans A. En passant aux classes, cela donne l'égalité $ay/1 = bx/1$ dans Frac(A). Nous multiplions les deux membres par $(b/1)^{-1}(y/1)^{-1}$. En utilisant les différents points de la définition 3.239, et en particulier (4d), nous avons$(b/1)^{-1}(y/1)^{-1} = 1/by$. Nous avons donc

$$(ay/1)(1/by) = (bx/1)(1/by). \tag{3.423}$$

En utilisant les relations de simplification de la proposition 3.244, nous avons $ay/by = a/b$ à gauche et $bx/by = x/y$ à droite. Bref, nous avons

$$a/b = x/y. \tag{3.424}$$

Le membre de gauche peut être récrit $a/b = (a/1)(b/1)^{-1}$, ce qui peut s'écrire ab^{-1}.

$\Leftarrow$ L'hypothèse s'écrit, sans abus de notations sous la forme

$$(a/1)(b/1)^{-1} = (x/1)(y/1)^{-1}. \tag{3.425}$$

En multipliant les deux côtés par $(b/1)(y/1)$ nous trouvons

$$ay/1 = xb/1. \tag{3.426}$$

Nous pouvons écrire cela explicitement avec la relation d'équivalence qui définit Frac(A) (définition 3.239) :

$$(ay, 1) \sim (xb, 1), \tag{3.427}$$

c'est-à-dire $ay1 = 1xb$, ce que nous voulions. □

La proposition suivante montre encore que le corps des fractions est le plus petit corps que l'on puisse imaginer à partir d'un anneau.

PROPooIJBEooDjsoHr

Proposition 3.246 ([18, 1])**.**
Soit un anneau commutatif A. Tout corps commutatif contenant un sous-anneau isomorphe[113] *à A contient un sous-corps isomorphe à* Frac(A).

Démonstration. Soit un corps $\mathbb{K}$ contenant un sous-anneau A' isomorphe à A. Nous notons $\sigma : A' \to A$ un isomorphisme d'anneaux entre A' et A.

(1) **Une partie bien choisie**
Nous considérons la partie suivante de $\mathbb{K}$:

$$S = \{ab^{-1} \text{ tel que } a, b \in A'\}. \tag{3.428}$$

(2) **S est un corps** Deux éléments arbitraires de S sont ab^{-1} et xy^{-1}. Nous devons prouver plusieurs choses.

(2a) **Neutres** En prenant $a = b = 1$ nous avons $ab^{-1} = 1 \in S$. En prenant $a = 0$ et $b = 1$ nous avons $ab^{-1} = 0 \in S$.

(2b) **Somme** Il faut remarquer que $ab^{-1} + xy^{-1} = (ay + xb)(by)^{-1}$. En effet,

$$\begin{aligned}(ay + xb)(by)^{-1} &= (ay + xb)y^{-1}b^{-1} && \text{(3.429a)}\\ &= ayy^{-1}b^{-1} + xby^{-1}b^{-1} && \text{(3.429b)}\\ &= ab^{-1} + xy^{-1} && \text{(3.429c)}\end{aligned}$$

SUBEQooRGPSooXaBGvx
SUBEQooOHJGooWrfPow

Justifications :

[112] Rappel de 3.243 : si $a \in A$, nous nommons $a \in$ Frac(A) l'élément $a/1$, c'est-à-dire la classe de $(a, 1)$
[113] Morphisme d'anneaux, définition 1.106.

- Pour (3.429b). Distributivité.
- Pour (3.429c). Commutativité dans A.

(2c) **Produit** Il s'agit du même genre de calculs en utilisant les mêmes propriétés. Nous avons

$$(ab^{-1})(xy^{-1}) = (ax)(by)^{-1}. \tag{3.430}$$

(3) **Ce qui va être notre isomorphisme**

Ensuite nous montrons que l'application

$$\begin{aligned}\varphi\colon S &\to \text{Frac}(A)\\ ab^{-1} &\mapsto \sigma(a)/\sigma(b)\end{aligned} \tag{3.431}$$

est bien définie et est un isomorphisme de corps.

(4) **Bien définie**

Si $ab^{-1} = xy^{-1}$ alors $ay = xb$. Puisque σ est un isomorphisme nous avons aussi $\sigma(a)\sigma(y) = \sigma(x)\sigma(b)$ et donc $\sigma(a)/\sigma(b) = \sigma(x)/\sigma(y)$ par définition des classes de Frac(A).

(5) **Morphisme** Deux éléments arbitraires de S sont ab^{-1} et xy^{-1}. Calculons un peu :

SUBEQooRONTooKVTRdZ
$$\varphi\big((ab^{-1})(xy^{-1})\big) = \varphi(axy^{-1}b^{-1}) \tag{3.432a}$$
SUBEQooNOTAooZVJvmC
$$= \varphi\big((ax)(by)^{-1}\big) \tag{3.432b}$$
$$= \sigma(ax)/\sigma(by) \tag{3.432c}$$
SUBEQooVQUOooVvViEU
$$= \big(\sigma(a)/\sigma(b)\big)\big(\sigma(x)/\sigma(y)\big) \tag{3.432d}$$
$$= \varphi(ab^{-1})\varphi(xy^{-1}). \tag{3.432e}$$

Justifications :

- Pour (3.432a). Commutativité dans A.
- Pour (3.432b). Associativité dans A.
- Pour (3.432d). Définition 3.239(2) de la multiplication de fractions.

(6) **Surjectif**

Tout élément de Frac(A) est de la forme a'/b' avec $a', b' \in A$, et donc de la forme $\sigma(a)/\sigma(b)$ avec $a, b \in A'$. Un tel élément est l'image par φ de $ab^{-1} \in S$.

(7) **Injectif**

Si $\varphi(ab^{-1}) = \varphi(xy^{-1})$ alors $\sigma(a)/\sigma(b) = \sigma(x)/\sigma(y)$, et par définition des classes nous avons $\sigma(a)\sigma(y) = \sigma(b)\sigma(x)$. De là nous avons $\sigma(ay) = \sigma(bx)$ et donc $ay = bx$ (parce que σ est un isomorphisme). Nous en déduisons que $ab^{-1} = xy^{-1}$.

□

3.247.
Soit un anneau A et son anneau des polynômes $\mathcal{P}(A)$. Si $\alpha \in A$, nous avons la définition 3.231 qui donne l'évaluation $P(\alpha)$.

Si par contre P et Q sont des polynômes sur A, nous n'avons pas encore défini ce que serait l'évaluation de la fraction rationnelle P/Q en α. Nous comblons à présent ce manque.

DEFooLBIWooCPCaSY
Définition 3.248 (Évaluation d'une fraction rationnelle)**.**
Soit un corps $\mathbb{K}$ *contenant l'anneau* A*. Si* $R = P/Q \in \text{Frac}(A)$ *et si* $\alpha \in \mathbb{K}$ *nous définissons*[114]

$$R(\alpha) = (P/Q)(\alpha) = P(\alpha)Q^{-1}(\alpha). \tag{3.433}$$

Dans cette formule, les polynômes, l'inverse et le produit sont calculés dans $\mathbb{K}$ *et non dans* A*.*

[114] Les fractions rationnelles, définition 3.239.

3.15.5 Corps totalement ordonné

Rappel. Vu qu'un corps est un anneau, nous avons déjà défini la notion d'être totalement ordonné en 1.115 valeur absolue sur un corps en 1.121.

DefKCGBooLRNdJf

Définition 3.249.
Ordre et choses reliées dans un corps.

ItemVXOZooTYpcYN

(1) *La suite (x_n) dans le corps totalement ordonné $\mathbb{K}$ est **de Cauchy** si pour tout $\epsilon > 0$ dans $\mathbb{K}$, il existe $N \in \mathbb{N}$ tel que si $p, q \geqslant N$ alors $|x_p - x_q| \leqslant \epsilon$.*

ITEMooDERQooLmJwFR

(2) *La suite (x_n) dans le corps totalement ordonné $\mathbb{K}$ est **convergente** si il existe $q \in \mathbb{K}$ tel que pour tout $\epsilon > 0$ dans $\mathbb{K}$, il existe N tel que si $k \geqslant N$ alors $|x_k - q| \leqslant \epsilon$.*

ITEMooKZZYooDaidGU

(3) *Un corps totalement ordonné est **complet** si toute suite de Cauchy y est convergente.*

ITEMooMWASooEzhVyh

(4) *Si $a, \epsilon \in \mathbb{K}$ avec $\epsilon > 0$ alors nous définissons la **boule ouverte** de centre a et de rayon ϵ par*

$$B(a, \epsilon) = \{x \in \mathbb{K} \text{ tel que } |a - x| < \epsilon\}, \tag{3.434}$$

*et la **boule fermée** par*

$$\overline{B(a, \epsilon)} = \{x \in \mathbb{K} \text{ tel que } |a - x| \leqslant \epsilon\}. \tag{3.435}$$

Lemme 3.250.
Une suite (x_k) converge vers q si et seulement si pour tout $\epsilon > 0$, il existe $N > 0$ tel que $x_k \in B(q, \epsilon)$ pour tout $k \geqslant N$.

Démonstration. Il s'agit de mettre côte à côte les points (2) et (4) de la définition 3.249. □

3.251.
Ces boules prendront une nouvelle force avec le super-théorème 9.158.

PROPooJZIMooHOimlv

Proposition 3.252 ([1])**.**
Soit une suite de Cauchy (x_n) dans $\mathbb{Q}$. Nous supposons que (x_n) admette une sous-suite convergente vers $q \in \mathbb{Q}$. Alors $x_n \to q$.

Démonstration. Soit $\epsilon > 0$. Nous considérons $N > 0$ tel que si $n, k \geqslant N$ alors $|x_k - q| < \epsilon/2$. Soit $k > N$ tel que $|x_k - q| < \epsilon/2$. Cela existe ; il suffit de prendre k assez loin dans la sous-suite qui converge vers q. Pour tout $n \geqslant k$ nous avons alors

$$|x_n - q| \leqslant |x_n - x_k| + |x_k - q| = \epsilon/2 + \epsilon/2 = \epsilon. \tag{3.436}$$

□

Parmi ces définitions, celles de suite convergente, de Cauchy et de corps complet seront utilisées dans le cas de $\mathbb{Q}$ (et de $\mathbb{R}$ pour la complétude). Elles seront prouvées être équivalentes aux définitions topologiques dans le cas particulier de $\mathbb{R}$ et $\mathbb{Q}$ lorsque la topologie métrique sera définie. Dans cet état d'esprit nous n'allons pas démontrer tout de suite que $\mathbb{R}$ est un corps complet. Nous allons directement démontrer que c'est un espace topologique complet.

LEMooQXDCooPEABBm

Lemme 3.253 (À propos de boules)**.**
Soient un corps totalement ordonné $\mathbb{K}$ et des éléments $x, y \in \mathbb{K}$. Soit aussi $\epsilon > 0$ dans $\mathbb{K}$. Nous avons :

ITEMooXJGVooSebiip

(1) *$y \in B(x, \epsilon)$ si et seulement si $x - \epsilon < y < x + \epsilon$.*

ITEMooRUBBooRayiMs

(2) *Si $y \in \overline{B(x, \epsilon)}$ alors $y \in B(x, \epsilon')$ pour tout $\epsilon' > \epsilon$.*

Démonstration. Pour rappel,

$$|x - y| = \begin{cases} x - y & \text{si } x - y \geqslant 0 \\ y - x & \text{si } x - y \leqslant 0. \end{cases} \tag{3.437}$$

Nous pouvons maintenant démontrer nos assertions.

(1) **Pour (1)** En deux parties.

(1a) $\Rightarrow$ Nous supposons que $|x-y|<\epsilon$.
Si $x-y\geqslant 0$ alors l'hypothèse signifie $x-y<\epsilon$, ce qui donne $y>x-\epsilon$. Mais l'inégalité $x-y\geqslant 0$ donne également $x\geqslant y$ et donc $x+\epsilon\geqslant y+\epsilon>y$. Notez le jeu de l'inégalité non stricte qui se change en inégalité stricte.
Si $x-y\leqslant 0$ nous pouvons faire le même raisonnement.

(1b) $\Leftarrow$ Des inégalités $x-\epsilon<y$ et $y<x+\epsilon$ nous tirons $x-y<\epsilon$ et $y-x<\epsilon$. Donc quel que soit le signe de $x-y$ nous avons toujours $|x-y|<\epsilon$.

(2) **Pour (2)** C'est immédiat parce que

$$|x-y|\leqslant\epsilon<\epsilon'. \tag{3.438}$$

□

LEMooVZNCooRJatKK

Lemme 3.254 ([126]).
Tout anneau totalement ordonné est de caractéristique nulle.

Démonstration. Si $x\in A$ vérifie $x>0$, alors la définition 1.115(1) nous permet d'écrire

$$x+1_A>1_A>0. \tag{3.439}$$

Nous avons tenu compte de 1.117(4). Il n'existe en particulier aucun p tel que $p1_A=0$. Sinon nous aurions $(p-1)1_A+1_A=0$. □

3.16 Polynômes à coefficients dans un anneau commutatif

LEMooXTMAooMdHjPN

Lemme 3.255.
Nous considérons un polynôme $P\in A[X]$, et le quotient $A[X]/(P)$. Pour tout polynôme $Q\in A[X]$ nous avons les égalités

$$Q(\bar{X})=\overline{Q(X)}=\bar{Q}. \tag{3.440}$$

Démonstration. Si $Q=\sum_k a_kX^k$, alors par la linéarité de la prise de classes,

$$\bar{Q}=\sum_k a_k\overline{X^k}. \tag{3.441}$$

EQooXQRMooIPGFVM

Nous insistons sur le fait que cette égalité n'est rien d'autre que l'itération de la définition de la somme dans l'espace quotient : $\bar{x}+\bar{y}=\overline{x+y}$ ainsi que du produit $k\bar{x}=\overline{kx}$ (définition 3.12). Toujours par définition du produit appliqué à l'élément $\bar{X}$ nous avons $(\bar{X})^2=\overline{X^2}$; par récurrence $\overline{X^k}=\bar{X}^k$, et

$$\bar{Q}=\sum_k a_k\bar{X}^k=Q(\bar{X}). \tag{3.442}$$

Le fait que $\bar{Q}=\overline{Q(X)}$ n'est rien d'autre que le fait que dans $A[X]$ nous avons $Q=Q(X)$, comme expliqué dans le lemme 3.235. □

3.16.1 Monômes

3.256.
Les éléments de la forme λX^k avec $\lambda\in A$ et $k\in\mathbb{N}$ sont des **monômes**.

Nous allons aussi considérer

$$A_n[X]=\{P\in A[X]\text{ tel que }\deg(P)\leqslant n\}. \tag{3.443}$$

Cet ensemble est un sous-module libre.

3.16.2 Évaluation

Soit $P\in A[X]$. À priori, P n'est qu'une suite dans A indexée par $\mathbb{N}$.

Nous avons déjà défini son évaluation sur un élément $\alpha\in A$ dans la définition 3.231 :

$$P(\alpha)=\sum_k a_k\alpha^k. \tag{3.444}$$

Cette somme est toujours finie.

NORMooQFTJooLBcPxl

3.257.
L'ensemble $A[X]$ est une algèbre et donc un espace vectoriel. Il possède un unique élément nul qui est celui dont tous les coefficients sont nuls ; cela est immédiat par la construction en tant que suites presque nulles.

Il n'y a à priori pas équivalence entre le fait d'être un polynôme nul et le fait de s'évaluer à zéro sur tous les éléments de A. Cela sera discuté dans le théorème 8.110 et l'exemple 21.36.

DEFooRFBFooKCXQsv

Définition 3.258.
Soient un anneau A et un anneau B qui contient A (comme sous-anneau). Pour $\alpha \in B$ nous définissons $A[\alpha]_B$ comme étant l'intersection de tous les sous-anneaux de B contenant A.

Comme dit plus haut, nous nous permettons d'écrire $A[\alpha]$ sans préciser B lorsque ce dernier sera clair dans le contexte.

PROPooPMNSooOkHOxJ

Proposition 3.259.
Soient un anneau A et un anneau B qui contient A (comme sous-anneau). Pour tout $\alpha \in B$ nous avons

$$A[\alpha] = \{P(\alpha) \text{ tel que } P \in A[X]\} \tag{3.445}$$

où encore une fois, $P(\alpha)$ est calculé dans B ; le contexte est clair là-dessus.

Démonstration. Si A' est un sous-anneau de B contenant A et α, alors A' contient tous les $P(\alpha)$ avec $P \in A[X]$. Nous avons donc

$$\{P(\alpha) \text{ tel que } P \in A[X]\} \subset A[\alpha]. \tag{3.446}$$

Par ailleurs, $\{P(\alpha)$ tel que $P \in A[X]\}$ est un sous-anneau de B contenant A et α. Donc $A[\alpha]$ y est inclus. □

3.16.3 Polynômes sur un anneau intègre

ThoBUEDrJ

Théorème 3.260.
L'anneau A est intègre si et seulement si $A[X]$ est intègre.

Démonstration. Soient P et Q des éléments non nuls de $A[X]$. Puisque l'anneau A est intègre, nous avons

$$\deg(PQ) = \deg(P) + \deg(Q) \tag{3.447}$$

et le produit ne peut pas être nul. L'anneau $A[X]$ est donc intègre.

Si $A[X]$ est intègre, A est intègre parce qu'il peut être considéré comme sous-anneau de $A[X]$. □

3.261.
Si A n'est pas intègre, soient $\alpha, \beta \in A$ non nuls tels que $\alpha\beta = 0$. Le produit des polynômes $X \mapsto \alpha X$ et $X \mapsto \beta$ est $(\alpha X) \cdot (\beta) = 0$; le degré du produit n'est pas la somme des degrés.

Les personnes qui ont tout compris jusqu'ici remarqueront que la notation « $X \mapsto P(X)$ » n'est pas correcte parce que du point de vue que nous adoptons ici, un polynôme n'est pas une application.

Corolaire 3.262.
Si A est intègre, les inversibles de $A[X]$ sont les éléments inversibles de A.

Démonstration. Pour que Q soit inversible, il faut un P tel que $PQ = 1$. Mais l'anneau A étant intègre, les degrés s'additionnent. Par conséquent ils doivent être de degré zéro et il faut que $P, Q \in A$. Donc Q est un inversible de A. □

3.16.4 Division euclidienne

Le théorème suivant établit la **division euclidienne** dans $A[X]$ du polynôme P par un polynôme D.

ThodivEuclPsFexf

Théorème 3.263.
Soit $D \neq 0$ dans $A[X]$ de coefficient dominant inversible dans A. Pour tout $P \in A[X]$, il existe $Q, R \in A[X]$ tels que

$$P = QD + R \tag{3.448}$$

avec $\deg(R) < \deg(D)$.

Les polynômes Q et R sont déterminés de façon univoque par cette condition.

DefMPZooMmMymG

Définition 3.264.
*Le polynôme Q est le **quotient** et R est le **reste** de la division euclidienne de P par D. Si le reste de la division de P par D est nul on dit que D **divise** P et on note $D \mid P$. Autrement dit D divise P si il existe Q tel que $P = QD$.*[115]

3.265.
Le théorème 3.263 nous incite à utiliser le degré comme stathme euclidien sur $A[X]$ dès que A est un anneau intègre. Or cela ne fonctionne pas en général, parce que très peu de polynômes ont à priori un coefficient dominant inversible.

LEMooIDSKooQfkeKp

Lemme 3.266 (Thème 18)**.**
Si $\mathbb{K}$ est un corps[116]*, alors l'anneau $\mathbb{K}[X]$ est euclidien et principal.*

Démonstration. Puisque $\mathbb{K}$ est un corps, tous les éléments sont inversibles et le degré donne un stathme par le théorème 3.263. L'anneau $\mathbb{K}[X]$ est donc euclidien et par conséquent principal (proposition 3.38). □

Dans le théorème 8.43 nous donnerons une preuve directe du fait que $\mathbb{K}[X]$ est principal en montrant que tous ses idéaux sont principaux. Nous y démontrerons donc un peu moins pour un peu plus cher, mais avec le plaisir de ne pas devoir passer par un stathme.

DefDSFooZVbNAX

Définition 3.267 ([127])**.**
*Soit un anneau A. Deux polynômes P et Q dans $A[X]$ sont dits **étrangers** entre eux si 1 est un pgcd*[117] *de P et Q. Un ensemble de polynômes $(P_i)_{i\in I}$ est étranger **dans leur ensemble** si 1 est un* pgcd *des P_i.*

*Les polynômes P et Q sont **premiers entre eux** si les seuls diviseurs communs de P et Q sont les inversibles.*

Les notions de polynômes étrangers entre eux ou de polynômes premiers entre eux ne sont pas identiques, comme le montre l'exemple suivant.

Exemple 3.268 ([1])**.**
Soient dans $\mathbb{Z}[X]$ les polynômes $P(X) = 2X + 2$ et $Q(X) = 2X^2 + 2$. Le nombre 2 est diviseur commun et n'est pas un diviseur de 1. Donc 1 n'est pas un pgcd de P et Q. Ils ne sont pas étrangers.

Mais ils sont premiers entre eux parce qu'ils n'ont pas d'autres diviseurs communs que les inversibles (1 et -1). △

3.16.5 Polynôme primitif

DefContenuPolynome

Définition 3.269.
*Un **contenu** du polynôme $P = \sum_i a_i X^i \in \mathbb{K}[X]$ est un pgcd de ses coefficients : $c(P) = \text{pgcd}\left(\{a_i\}\right)$.*

NORooQITDooKsTMKm

3.270.
Quand il y a unicité du pgcd d'un ensemble, on peut parler du contenu au singulier.

Le contenu d'un polynôme sera surtout utilisé juste pour savoir si il est inversible ou non. Dans un anneau intègre, ça demande un peu d'abus de langage, mais comme le lemme 3.26 dit que si un pcgd est inversible, ils le sont tous, au moins discuter de l'inversibilité du contenu dans un anneau intègre a un sens et est bien défini.

DEFooDVOOooKaPZQC

Définition 3.271 (Polynôme primitif[128])**.**
Il existe deux notions de polynômes primitifs. Vu qu'il existe des anneaux unitaires qui sont des corps finis[118]*, il faut faire attention au contexte.*

ITEMooCNHAooVfIYEW

*(1) Si A est un anneau unitaire, P est un **polynôme primitif** $c(P)$ est inversible*[119]*.*

(2) Si $\mathbb{K}$ est un corps fini, un polynôme dans $\mathbb{K}[X]$ est primitif si il est le polynôme minimal d'un générateur du groupe commutatif du corps.

[115] Ceci se rapproche tout naturellement des notions générales de divisibilité dans un anneau intègre, vues en sous-section 3.12.1.
[116] Définition 1.213.
[117] Définition 1.113.
[118] Je pense à $\mathbb{Z}/n\mathbb{Z}$, mais faites attention, j'ai pas vérifié. Écrivez-moi pour me dire si c'est un bon exemple.
[119] Pas mal d'auteurs disent que $c(P)$ soit être égal à 1. Mais en général ces auteurs se rétractent bien vite en disant que $c(P)$ n'est défini qu'à inversible près. Voir aussi 3.270.

3.272.
Pour rappel, il y a plusieurs façons de périphraser le fait que les coefficients soient premiers entre eux. Nous pouvons dire …

(1) Le pgcd de ses coefficients est 1 parce que c'est la définition 3.52 pour avoir des nombres premiers entre eux.

(2) Le contenu de ses coefficients est 1. Parce que le contenu est précisément le pgcd, définition 3.269.

La notion de polynôme primitif au sens du pgcd est particulière aux polynômes à coefficients dans un anneau comme le montre le lemme suivant.

Lemme 3.273.
Si $\mathbb{K}$ est un corps, tout polynôme unitaire dans $\mathbb{K}[X]$ non nul est primitif au sens du pgcd.

Démonstration. Un polynôme unitaire a un 1 parmi ses coefficients, donc le pgcd est forcément 1. □

Lemme 3.274 ([129]).
Soit un anneau factoriel[120] *A. Soient des polynômes primitifs P_1 et P_2 dans $A[X]$. Soient $a_1, a_2 \in A^*$ tels que*

$$a_1P_1 = a_2P_2. \tag{3.449}$$

Alors

(1) Les éléments a_1 et a_2 sont associés dans A.

(2) Les polynômes P_1 et P_2 sont associés dans $A[X]$.

Démonstration. Vu que les P_i sont primitifs, nous avons $c(a_iP_i) = u_ia_i$ où u_i est un inversible ($u_i = c(P_i)$). Les éléments u_1a_1 et u_2a_2 sont donc deux pgcd du même ensemble : les coefficients de a_1P_1 (qui sont les mêmes que ceux de a_2P_2). Le lemme 3.189 entre en jeu pour dire que u_1a_1 et u_2a_2 sont associés : il existe un inversible v tel que $u_1a_1 = vu_2a_2$. Au final, $a_1 = u_1^{-1}vu_2a_2$ et nous voyons que a_1 et a_2 sont associés.

Nous écrivons l'égalité $a_1P1 = a_2P_2$ avec la valeur trouvée de a_1 : $u_1^{-1}vu_2a_2P_1 = a_2P_2$. On voudrait simplifier par a_2 (surtout que A est commutatif), mais comme a_2 n'est pas spécialement inversible, il faut le justifier. L'anneau A est intègre ; donc l'anneau $A[X]$ l'est aussi (théorème 3.260). Et comme $A[X]$ est intègre, on peut faire la simplification.

Au final nous avons $u_1^{-1}vu_2P_1 = P_2$, et comme $u_1^{-1}vuy$ est inversible, P_1 et P_2 sont associés. □

LEMooHJECooTeELgN

Lemme 3.275 (de Gauss[129]).
Soit un anneau factoriel A. Soient $P, Q \in A[X]$.

ITEMooISPDooXdRywE

(1) Les polynômes P et Q sont primitifs si et seulement si le polynôme PQ est primitif.

ITEMooLWEEooLcDlfp

(2) Il existe un inversible $u \in A$ tel que $c(PQ) = uc(P)c(Q)$.

Démonstration. En plusieurs parties.

(1) **(1)⇒** Nous supposons que P et Q sont primitifs. Et, par l'absurde, nous supposons que PQ n'est pas primitif. Donc $c(PQ)$ n'est pas inversible dans A. Vu que A est factoriel, tout élément non inversible est un produit d'irréductibles ; c'est le cas de $c(PQ)$. Soit p un irréductible entrant dans la décomposition de $c(pQ)$.

Le lemme 3.197 dit que l'anneau $B = A/pA$ est intègre[121].

Considérons la surjection canonique $\pi\colon A \to B$ que nous prolongeons en un morphisme d'anneaux

$$\begin{aligned}\phi\colon A[X] &\to B[X]\\ \sum_i a_iX^i &\mapsto \sum_i \pi(a_i)X^i.\end{aligned} \tag{3.450}$$

Notons que p ne divise pas tous les coefficients de P. En effet, sinon $c(P)$ serait un multiple de p (proposition 3.198) et ne pourrait pas être inversible. Donc $\phi(P) \neq 0$ dans $B[X]$. De même nous savons que $\phi(Q) \neq 0$.

[120] Définition 3.194. Je rappelle qu'un anneau factoriel est toujours commutatif.

[121] Ici, ma source [129] précise que p est premier. C'est vrai par la proposition 3.196, mais ça me semble inutile. Écrivez-moi pour me dire si le fait que p soit premier est important.

L'anneau B est intègre parce que A est intègre (proposition 3.260). Donc $\phi(P)\phi(A)\neq 0$, et comme ϕ est un morphisme, $\phi(PQ)\neq 0$, ce qui signifie que p ne divise pas tous les coefficients de PQ, ce qui est contraire à l'hypothèse de l'absurde.

Nous en déduisons que $c(PQ)$ n'est pas inversible, et donc que PQ est primitif.

(2) **(1)⇐**

Nous supposons que PQ est primitif, et nous montrons que P et Q le sont. En factorisant un pgcd des coefficients de P nous pouvons écrire $P=c(P)P_1$ avec P_1 primitif (lemme 3.28). Par la partie précédente nous savons que P_1Q_1 est primitif. Nous avons donc l'égalité

$$PQ=c(P)c(Q)P_1Q_1 \tag{3.451}$$

où à la fois PQ et P_1P_2 sont primitifs. Vu que PQ est primitif, $c(P)c(Q)P_1Q_1$ est primitif, de telle sorte que[122]

$$c\Big(c(P)c(Q)P_1Q_1\Big)=c(P)c(Q)c(P_1Q_1) \tag{3.452}$$

est inversible. Vu que $c(P_1Q_1)$ est également inversible, nous en déduisons que $c(P)c(Q)$ est inversible. Si $u\in A$ vérifie $c(P)c(Q)u=1$, alors $c(Q)u$ est un inverse de $c(P)$. De même $uc(P)$ est un inverse de $c(Q)$. Bref, ils sont inversibles et les polynômes P et Q sont primitifs.

(3) **Pour (2)**

Soient $P,Q\in A[X]$. Nous considérons les polynômes primitifs P_1, Q_1 et R_1 définis par $P=c(P)P_1$, $Q=c(Q)Q_1$ et $PQ=c(PQ)R_1$. Nous avons

$$c(P)c(Q)P_1Q_1=PQ=c(PQ)R_1. \tag{3.453}$$

En prenant le contenu des deux côtés nous avons

$$c\Big(c(P)c(Q)P_1Q_1\Big)=c\Big(c(PQ)R_1\Big), \tag{3.454}$$

et en tenant compte du lemme 3.27, cela devient

$$c(P)c(Q)c(P_1Q_1)=c(PQ)c(R_1) \tag{3.455}$$

où les éléments $c(P_1Q_1)$ et $c(R_1)$ sont inversibles. En posant $u=c(P_1Q_1)^{-1}c(R_1)$, nous avons bien

$$c(P)c(Q)=uc(PQ). \tag{3.456}$$

□

3.276.
Dans toute la démonstration, il y a une ambiguïté entre $c(P)$ qui serait le pgcd des coefficients de P, c'est-à-dire un ensemble et $c(P)$ qui serait un représentant de cet ensemble.

Grâce au lemme 3.29, nous savons que si δ est un pgcd et si u est inversible, alors $u\delta$ est un pgcd. Donc à partir de l'équation

$$c(P)c(Q)=uc(PQ), \tag{3.457}$$

en fait nous savons qu'il existe des représentants de $c(P)$, $c(Q)$ et $c(PQ)$ tels que

$$c(P)c(Q)=c(PQ). \tag{3.458}$$

3.16.6 Racines des polynômes

Définition 3.277 (Ordre d'un polynôme)**.**
Soit P un polynôme irréductible[123] *de degré n sur $\mathbb{F}_p[X]$. L'**ordre** de P est*

$$\min\{k \text{ tel que } P\mid X^k-1\}. \tag{3.459}$$

Définition 3.278.
*Soient A un anneau et $P\in A[X]$. On appelle **racine** un élément $\alpha\in A$ tel que $P(\alpha)=0$; c'est-à-dire que, en remplaçant toutes les occurrences de X par α dans l'expression de P, on obtient 0.*

[122] Utilisation du lemme 3.27.
[123] Définition 3.14.

PropHSQooASRbeA

Proposition 3.279.
Soient A un anneau et P un polynôme non nul dans $A[X]$. Si $\alpha \in A$ est une racine de P alors $X-\alpha$ divise P, et réciproquement.

Démonstration. Nous notons le polynôme $\mu = X - \alpha$ par analogie avec le polynôme minimal dont il sera question dans la très semblable proposition 8.101. Le sens réciproque est clair : si μ divise P, alors α est racine de P.

Pour le sens direct, remarquons que si α est racine de P, alors P est de degré au moins égal à 1, et nous pouvons donc effectuer la division euclidienne[124] de P par μ : il existe des polynômes Q et R tels que

PropHSQooASRbeA1
$$P = Q\mu + R \tag{3.460}$$

avec $\deg(R) < \deg(\mu)$. Donc R est une constante, élément de A : appelons-le a. En évaluant (3.460) en α, il vient

$$0 = P(\alpha) = Q(\alpha)\mu(\alpha) + a, \tag{3.461}$$

et nous en déduisons que $a = 0$, ce qui montre que $P = Q\mu$ et que μ divise P. □

DEFooTGZYooCYiKQa

Définition 3.280 (Racine simple et multiple d'un polynôme)**.**
*Soit A un anneau ainsi qu'un polynôme $P \in A[X]$ et $\alpha \in A$ racine de P. La **multiplicité** de α par rapport à P est l'entier h tel que P est divisible par $(X-\alpha)^h$ mais pas divisible par $(X-\alpha)^{h+1}$. Nous noterons $\theta_\alpha(P)$ la multiplicité de α par rapport à P.*

*Si la multiplicité d'une racine est égale à 1, nous disons que c'est une **racine simple**. Sinon, c'est une **racine multiple**.*

3.281.
Pour une définition générale d'une racine simple de l'équation $f(x) = 0$, voir la définition 36.50. La proposition 3.279 nous indique que toute racine est de multiplicité au moins égale à 1.

LEMooZUUVooQgsdXs

Lemme 3.282.
Soient un anneau A ainsi que $x, r \in A$. Nous avons

$$x^n - r^n = (x-r)\sum_{k=0}^{n-1} x^k r^{n-k-1}. \tag{3.462}$$

Démonstration. Nous effectuons la distribution, et nous calculons un peu :

$$(x-r)\sum_{k=0}^{n-1} x^k r^{n-k} = \sum_{k=0}^{n-1} x^{k+1} r^{n-k-1} - \sum_{k=0}^{n-1} x^k r^{n-k} \tag{3.463a}$$
$$= \sum_{k=1}^{n} x^k r^{n-k} - \sum_{k=0}^{n-1} x^k r^{n-k} \tag{3.463b}$$
$$= -r^n + \sum_{k=1}^{n-1}(x^k r^{n-k} - x^k r^{n-k}) + x^n \tag{3.463c}$$
$$= x^n - r^n. \tag{3.463d}$$

□

PROPooQCZSooVokxXQ

Proposition 3.283 ([130])**.**
Soient un anneau A, un polynôme $P \in A[X]$ de degré n, ainsi qu'une racine $\alpha \in A$ de P. Alors il existe un polynôme $Q \in A[X]$ de degré $n-1$ tel que $P = (X-\alpha)Q$.

Démonstration. D'après le lemme 3.282, pour chaque k, nous avons $x^k - r^k = (x-r)S_k(x)$ où S_k est un polynôme de degré $k-1$ (ou moins).

[124] Théorème 3.263.

Soit un polynôme P tel que $P(\alpha)=0$. Nous pouvons écrire

$$\begin{aligned}P(x)&=P(x)-P(\alpha) &(3.464a)\\ &=\sum_{k=0}^{n}a_kx^k-\sum_{k=0}^{n}a_k\alpha^k &(3.464b)\\ &=\sum_{k=1}^{n}a_k(x^k-\alpha^k) &(3.464c)\\ &=\sum_{k=1}^{n}a_k(x-\alpha)S_k(x) &(3.464d)\\ &=(x-\alpha)\sum_{k=1}^{n}a_lS_k(x) &(3.464e)\\ &=(x-\alpha)Q(x) &(3.464f)\end{aligned}$$

où Q est le polynômde de degré $n-1$ donné par $Q=\sum_{k=1}^{n}a_kS_k$. □

PropahQQpA

Proposition 3.284.
L'élément $\alpha\in A$ est une racine de multiplicité[125] *h du polynôme P si et seulement si il existe $Q\in A[X]$ tel que $P=(X-\alpha)^hQ$ avec $Q(\alpha)\neq 0$.*

Démonstration. Par définition de la multiplicité de α, le polynôme P est divisible par $(X-\alpha)^h$ mais pas par $(X-\alpha)^{h+1}$. Il existe donc un polynôme Q tel que

$$P=(X-\alpha)^hQ. \tag{3.465}$$

Si $Q(\alpha)$ était nul, la proposition 3.283 nous dirait que $Q=(X-\alpha)S$ pour un cetain polynôme S. Cela ferait $P=(X-\alpha)^{h+1}S$, ce qui est contraire à l'hypothèse sur la multiplicité. □

LemIeLhpc

Lemme 3.285.
Soient P et Q des polynômes non nuls de $A[X]$ et $\alpha\in A$. Alors

(1) $\theta_\alpha(P+Q)\leqslant\min\{\theta_\alpha(P),\theta_\alpha(Q)\}$, et l'égalité a lieu si $\theta_\alpha(P)\neq\theta_\alpha(Q)$;

ItemIeLhpciv

(2) $\theta_\alpha(PQ)\geqslant\theta_{\alpha(P)}+\theta_\alpha(Q)$, et l'égalité a lieu si A est intègre.

Dans le théorème suivant, la partie importante en pratique est le point (2) parce qu'il dit que, lorsque nous cherchons les racines d'un polynôme, nous pouvons nous arrêter lorsque nous en avons trouvé autant que le degré, multiplicité comprise.

ThoSVZooMpNANi

Théorème 3.286.
Soit A un anneau intègre et $P\in A[X]\setminus\{0\}$, un polynôme de degré n.

(1) Si $\alpha_1,\dots,\alpha_p\in A$ sont des racines deux à deux distinctes de multiplicités $k_1,\dots,k_p$, alors il existe $Q\in A[X]$, de degré $n-\sum_{i=1}^{p}k_i$, tel que

$$P=Q\prod_{i=1}^{p}(X-\alpha_i)^{k_i} \tag{3.466}$$

et $Q(\alpha_i)\neq 0$ pour tout i.

ITEMooWGOBooGApPOo

(2) La somme des multiplicités des racines de P est au plus $\deg(P)$.

Démonstration. Si $p=1$, soit α une racine de multiplicité k de P. La définition de la multiplicité d'une racine nous dit que P est divisible par $(X-\alpha)^k$ mais pas par $(X-\alpha)^{k+1}$. Donc il existe $Q\in A[X]$ tel que $P=Q(X-\alpha)^k$. Il reste à voir que $Q(\alpha)\neq 0$. Cela est une conséquence de la proposition 3.279 : si $Q(\alpha)$ était nul, on pourrait lui factoriser $(X-\alpha)$ et donc avoir $(X-\alpha)^{k+1}$ qui se factorise dans P, ce qui n'est pas possible.

Nous supposons que $p\geqslant 2$ et nous effectuons une récurrence sur p. Nous considérons donc les $p-1$ premières racines $\alpha_1,\dots,\alpha_{p-1}$ et un polynôme $R\in A[X]$ tel que $R(\alpha_i)\neq 0$ pour $i=1,\dots,p-1$ et

$$P=\underbrace{(X-\alpha_1)^{k_1}\dots(X-\alpha_{p-1})^{k_{p-1}}}_{S}R. \tag{3.467}$$

[125] Multiplicité d'une racine, définition 3.280.

Par hypothèse $P(\alpha_p) = S(\alpha_p)R(\alpha_p) = 0$. L'anneau A étant intègre, $S(\alpha_p) \neq 0$ parce que $\alpha_i \neq \alpha_p$ pour $i \neq p$. Par conséquent, $R(\alpha_p) = 0$.

Nous devons encore vérifier que la multiplicité α_p est k_p par rapport à R. Pour cela nous utilisons le point (2) du lemme 3.285 afin de dire que le degré de α_p pour $P = SR$ est k_p. Par conséquent

$$R = (X - \alpha_p)^{k_p} T \tag{3.468}$$

avec $T(\alpha_p) \neq 0$ et enfin

$$P = \prod_{i=1}^{p} (X - \alpha_i) T. \tag{3.469}$$

De plus $T(\alpha_i) \neq 0$, sinon $R(\alpha_i)$ serait nul. □

CORooUGJGooBofWLr

Corolaire 3.287.
Un polynôme de degré n sur un anneau intègre possède au maximum n racines distinctes.

Démonstration. Le théorème 3.286(2) dit que la somme des multiplicités des racines de P est au maximum n. Mais la proposition 3.279 dit que toutes les racines ont une multiplicité au moins égale à un. Donc il ne peut pas y en avoir plus de n. □

Proposition 3.288 ([131, 132]).
Soit un anneau intègre et $n > 0$. Les racines n^e de l'unité forment un groupe cyclique dont l'ordre divise n.

LEMooHDJIooPTpUCJ

Lemme 3.289.
Soit le polynôme $P = X^2 - 1$ sur l'anneau intègre[126] *A. Si $1 \neq -1$*[127]*, alors les racines de P sont ± 1.*

Démonstration. Le fait que ± 1 sont racines est le lemme 1.103(2)(5). Puisque par hypothèse $1 \neq -1$, le corolaire 3.287 termine la preuve. □

CORooZCSOooHQVAOV

Corolaire 3.290 (Conséquence du lemme de Gauss[133]).
Soient A un anneau factoriel et $\mathrm{Frac}(A)$ son corps des fractions. Un polynôme non constant $P \in A[X]$ est irréductible (sur A) si et seulement si il est irréductible et primitif au sens du pgcd[128] *sur $\mathrm{Frac}(A)[X]$.*

Exemple 3.291.
Il ne faudrait pas croire qu'être irréductible dans un anneau A implique d'être irréductible dans le corps des fractions. En effet soit $A = \mathbb{Z}[\sqrt{5}]$ et $P = X^2 - X - 1$. Nous savons que sa factorisation est

$$P = \left(X - \frac{1+\sqrt{5}}{2}\right)\left(X - \frac{1-\sqrt{5}}{2}\right). \tag{3.470}$$

Si vous ne le saviez pas, faites juste le calcul pour vous en assurer.

Ce polynôme est irréductible sur $\mathbb{Z}[\sqrt{5}]$ mais pas irréductible sur $\mathrm{Frac}\left(\mathbb{Z}[\sqrt{5}]\right)$. △

3.16.7 Quelques identités

LemISPooHIKJBU

Lemme 3.292 ([1, 134]).
Quelques identités de polynômes.

ItemLTBooAcyMtN

(1) Si n est impair, alors $1 + X$ divise $1 + X^n$.

ItemLTBooAcyMtNii

(2) Pour tout n nous avons $X^n - 1 = (X - 1)(1 + X + \cdots + X^{n-1})$.

ITEMooILIVooHtmWLm

(3) $X^n - a^n = (X - a)\sum_{i=0}^{n-1} a^i X^{n-1-i}$.

Démonstration. Plusieurs points.

(1) **Pour (1)** Nous allons utiliser le lemme 3.142 avec $a = 1$, $b = -X$ et $r = n - 1$. Notez que n étant impair, $r = n - 1$ est encore positif. En ce qui concerne le membre de gauche de (3.222), nous remarquons que $(-X)^n = (-1)^n X^n = -X^n$. Nous avons donc :

$$1 + X^n = (a - b)\sum_{k=0}^{n-1} a^{n-1-kb^k} = (1 + X)(\cdots). \tag{3.471}$$

Cela prouve que $1 + X$ divise $1 + X^n$.

[126] Définition 3.22.
[127] À mon avis cette hypothèse n'est pas nécessaire. Et d'ailleurs j'ai un peu du mal à voir des exemples exotiques d'anneaux intègres dans lesquels $1 = -1$. Il y aurait $[0, 1]$ modulo 2, certaines de ses parties, comme $\mathbb{Z}/2\mathbb{Z}$. Et quoi d'autre ?
[128] Définition 3.271.

(2) **Pour (2)** Posons $P = X + \ldots + X^{n-1}$. Nous avons $XP = P - X + X^n$ et donc

$$(X-1)(1+P) = X + XP - 1 - P = X + (P - X + X^n) - 1 - P = X^n - 1. \tag{3.472}$$

(3) **Pour (3)** Déjà fait dans (3.222).

□

3.16.8 Générateurs pour le groupe multiplicatif

PROPooKSCRooPyInSv

Proposition 3.293 ([135]).
Si p est un nombre premier, tout sous-groupe de $\big((\mathbb{Z}/p\mathbb{Z})^*, \cdot\big)$ est cyclique[129].

Démonstration. Soit un sous-groupe H d'ordre $|H| = n$ de $(\mathbb{Z}/p\mathbb{Z})^*$. Nous prouvons par récurrence sur n que H est cyclique.

(1) $n = 1$ Si H est un sous-groupe d'ordre 1, alors $H = \{[1]_p\}$ et c'est cyclique, pas de problèmes.

(2) **Récurrence** Nous supposons que tous les sous-groupes de $\big((\mathbb{Z}/p\mathbb{Z})^*$ d'ordre plus petit que n sont cycliques, et nous prouvons que H est également cyclique.

Nous allons faire deux cas suivant que n est la puissance d'un nombre premier ou non.

(2a) **Si $n = q^k$** Nous supposons que $n = q^k$ pour un certain nombre premier q. Nous supposons aussi, par l'absurde que H n'est pas cyclique. Les éléments de H ont un ordre qui divise q^k (corolaire 2.74), mais pas d'ordre q^k. Donc pour tout x dans H nous avons $x^{q^{k-1}} = 1$. En particulier le polynôme $P = X^{X^{q-1}} - 1$ a au moins q^k racines dans $\mathbb{Z}/p\mathbb{Z}$: les éléments de H.
Hélas le degré de P étant q^{k-1}, il ne peut pas avoir plus de q^{k-1} racines distinctes par 3.286. Contradiction. Donc H est cylcique.

(2b) **Cas général**
Nous supposons que $|H|$ n'est pas la puissance d'un nombre premier.

(2b.i) **Un morphisme** Le corolaire 3.65 nous indique que $n = ab$ pour deux nombres a, b tels que $\text{pgcd}(a, b) = 1$. Nous considérons l'application

$$\begin{aligned} f\colon H &\to H \\ x &\mapsto x^a. \end{aligned} \tag{3.473}$$

Étant donné que H est abélien, f est un morphisme de groupes. Tout élément $x \in H$ vérifie $f(x)^b = x^{ab} = 1$. Donc

$$\text{Image}(f) \subset \{y \in H \text{ tel que } y^b = 1\}. \tag{3.474}$$

(2b.ii) **Ordre du noyau et de l'image** Par le coup des racines distinctes de polynôme $X^b - 1$, nous avons $|\text{Image}(f)| \leqslant b$. De même nous avons

$$\ker(f) = \{x \in H \text{ tel que } x^a = 1\}, \tag{3.475}$$

et donc $|\ker(f)| \leqslant a$.
Le premier théorème d'isomorphisme 2.20 nous indique que

$$\frac{H}{\ker(f)} \simeq \text{Image}(f), \tag{3.476}$$

et comme tout est abélien, tous les sous groupes sont normaux[130], et nous avons, par le théorème de Lagrange 2.73 que

$$ab = |H| = \underbrace{|\ker(f)|}_{\leqslant a}\underbrace{|\text{Image}(f)|}_{\leqslant b} \leqslant ab. \tag{3.477}$$

Le premier membre est égal au dernier. Donc toutes les inégalités sont des égalités. Nous avons donc $|\ker(f)| = a$ et $|\text{Image}(f)| = b$.

(2b.iii) **Hypothèse de récurrence** C'est le moment d'utiliser l'hypothèse de récurrence : les groupes $\ker(f)$ et $\text{Image}(f)$ sont cycliques. Soient des générateurs h et h'. Quel est l'ordre de hh' ? Le lemme 3.165 nous indique que hh' est d'ordre $ab = n$. Donc hh' est générateur de H qui est donc cyclique.

□

[129] Définition 2.149.
[130] « distingué » et « normal » sont synonymes.

Chapitre 4

Les rationnels et les réels

4.1 Les rationnels

Note : pour l'existence et l'unicité de l'écriture $q = k/d$, il faut voir le théorème 3.171.

Une construction très explicite est faite dans [39]. Ici nous allons prendre plus court :

DEFooBPJNooRqrblS

Définition 4.1.
*Le corps des fractions de $\mathbb{Z}$ (définition 3.239) est noté $\mathbb{Q}$ et ses éléments sont les **rationnels**.*

La proposition suivante provient de 3.241.

PROPooKUIYooCxMHTX

Proposition 4.2 ([1]).
L'application

$$\begin{aligned} i\colon \mathbb{Z} &\to \mathbb{Q} \\ a &\mapsto a/1 \end{aligned} \tag{4.1}$$

est un morphisme injectif.

4.1.1 Relation d'ordre

PROPooEBCHooYEQkIO

Proposition 4.3 ([1]).
Soient $a, b \in \mathbb{Z}$ tels que $ab \geqslant 0$[1]. Alors si $(x, y) \sim (a, b)$, nous avons $xy \geqslant 0$.

Démonstration. L'hypothèse $(x, y) \sim (a, b)$ dit que $ab = ya$. L'astuce est de calculer $(xy)(bb)$ en nous servant de $xb = ya$:

$$(xy)b^2 = yayb = aby^2. \tag{4.2}$$

Vu que $ab \geqslant 0$ et $y^2 \geqslant 0$, le membre de droite est positif (proposition 1.205). Nous avons donc aussi $xyb^2 \geqslant 0$. La proposition 1.205(7) dit encore que dans ce cas $xy \geqslant 0$. □

PROPooEOZWooLxRPXa

Proposition 4.4 ([1]).
La partie

$$\mathbb{Q}^+ = \{a/b \text{ tel que } ab > 0\} \subset \mathbb{Q} \tag{4.3}$$

est bien définie et est une positivité[2]

Démonstration. Le fait que ce soit bien défini est la proposition 4.3.

(1) Supposons pour le plaisir de la contradiction que $a/b \in \mathbb{Q}^+$ et $-(a/b) \in \mathbb{Q}^+$. En utilisant la propriété 3.239(4c) nous avons $ab > 0$ et $(-a)b > 0$. En utilisant 1.193(1) nous avons

$$\begin{cases} (ab) > 0 & \text{(4.4a)} \\ -(ab) > 0. & \text{(4.4b)} \end{cases}$$

En utilisant 1.205(2) nous trouvons $ab(-ab) > 0$. En utilisant encore une des nombreuses propriétés déjà citées, nous trouvons $-a^2b^2 > 0$, c'est-à-dire

$$a^2b^2 < 0, \tag{4.5}$$

ce qui est faux parce que $a^2b^2 \geqslant 0$.

[1] Définition 1.200 pour l'ordre dans $\mathbb{Z}$.
[2] Définition 1.107.

(2) Supposons que $a/b \in \mathbb{Q}^+$ et $x/y \in \mathbb{Q}^+$ (b et y sont non nuls). Cette hypothèse signifie que $ab > 0$ et $xy > 0$. Nous devons prouver que $(a/b) + (x/y) \in \mathbb{Q}^+$. Nous avons

$$\frac{a}{b} + \frac{x}{y} = \frac{ay + bx}{by}. \tag{4.6}$$

Nous avons un petit calcul à faire :

$$by(ay + bx) = aby^2 + b^2xy. \tag{4.7}$$

EQooLGUJooYAUXPJ

Par hypothèse, $ab > 0$. Nous savons aussi que $y^2 \geqslant 0$. Mais dans notre cas nous avons $y^2 \neq 0$. Donc $aby^2 > 0$. Même raisonnement pour b^2xy. Bref ce que nous avons dans (4.7) est strictement positif.

□

DEFooZEXXooUtOhqB

Proposition-Définition 4.5 (Ordre sur $\mathbb{Q}$[39])**.**
Nous considérons l'ensemble

$$\mathbb{Q}^+ = \{a/b \text{ tel que } ab > 0\} \subset \mathbb{Q}. \tag{4.8}$$

ITEMooUSILooIfkVsR

(1) $\mathbb{Q}^+$ *est une positivité sur* $\mathbb{Q}$.

ITEMooSDSVooEOTRLY

(2) Pour $\alpha, \beta \in \mathbb{Q}$ *nous disons* $\alpha \leqslant \beta$ *si et seulement si*

$$\beta - \alpha \in \mathbb{Q}^+ \cup \{0\}. \tag{4.9}$$

Cela définit un ordre total[3].

Démonstration. Plusieurs points.

(1) **Pour (1)** C'est la proposition 4.4.

(2) **Pour (2)** C'est la proposition 1.108.

□

PROPooNSICooAQczDh

Proposition 4.6 ([1])**.**
Soient $q_1, q_2, r_1, r_2 \in \mathbb{Q}$ *tels que*

$$\begin{cases} q_1 \geqslant r_1 & \text{(4.10a)} \\ q_2 \geqslant r_2. & \text{(4.10b)} \end{cases}$$

Alors $q_1 + q_2 \geqslant r_1 + r_2$.

PROPooCILQooOuyrfI

Proposition 4.7 ([1])**.**
Soit $q \in \mathbb{Q}$.

(1) Nous avons $q^2 \geqslant 0$.

(2) Nous avons $q^2 = 0$ *si et seulement si* $q = 0$.

PROPooXNBVooIvBmkW

Proposition 4.8 ([1])**.**
L'application

$$\begin{aligned} i\colon \mathbb{Z} &\to \mathbb{Q} \\ a &\mapsto a/1 \end{aligned} \tag{4.11}$$

est un morphisme injectif qui respecte l'ordre.

Démonstration. Le fait que ce soit un morphisme injectif est la proposition 4.2.

Le respect de l'ordre doit encore être fait[4]. □

4.9.

Le lemme suivant 4.12 dit que tout rationnel est majoré par un naturel. Vu que les naturels et les rationnels ne sont pas du tout les mêmes ensembles (les entiers sont des classes de naturels et les rationnels des classes d'entiers), l'énoncé n'a à priori pas de sens.

La réalité est que nous identifions $\mathbb{N}$ à une partie de $\mathbb{Q}$ via les propositions 1.195 et 4.8. L'énoncé exact serait que si $q \in \mathbb{Q}$, il existe $n \in \mathbb{N}$ tel que $i\big(\iota(n)\big) > q$.

[3] Définition 1.26.

[4] Rédigez une preuve, faites un scan de votre feuille et envoyez-moi.

PROPooTEREooZgblWu

Proposition 4.10 ([1]).
Si $q > 0$ dans $\mathbb{Q}$, alors il existe $a, b \in \mathbb{N}$ tels que $q = a/b$.

Démonstration. Posons $q = a/b$ avec $a, b \in \mathbb{Z}$. Si $a, b > 0$, c'est bon. Si $a = 0$ alors $q = 0 = 0/1$ c'est bon aussi. Supposons que ce ne soit pas le cas. L'hypothèse $q > 0$ dit que $q = a/b$ avec $ab > 0$. La proposition 1.205(8) dit qu'il n'y a que deux possibilités : soit $a, b > 0$, soit $a, b < 0$.

Supposons que $a, b < 0$. En vertu des classes d'équivalence, nous avons $a = a/b = (-a)/(-b)$. Vu que nous avons $-a > 0$ et $-b > 0$, c'est bon. □

PROPooPSGBooLuMXoI

Proposition 4.11 ([1]).
Soit $a > 0$ et $b > 1$. Alors $a > a/b$.

Démonstration. Pour prouver que $a > a/b$, nous devons calculer

$$a - \frac{a}{b} = \frac{a}{1} - \frac{a}{b} = \frac{ab - a}{b}. \tag{4.12}$$

Nous devons donc évaluer la quantité $b(ab-a)$. Vu que $b > 1$, le lemme 1.203 dit que $ab > a$. Donc $ab-a > 0$. Le produit $b(ab - a)$ est donc le produit de deux entiers strictement positifs. En vertu de la proposition 1.205(2) nous avons donc $b(ab - a) > 0$, et donc $a > a/b$. □

LEMooEBTIooGMoHsj

Lemme 4.12.
Tout rationnel est strictement majoré par un naturel.

Démonstration. Si $q < 0$, alors $n = 0$ fait l'affaire. Si $q = 0$, alors $n = 1$ fonctionne. Supposons donc que $q = a/b > 0$ avec $ab > 0$ ainsi que $a, b \in \mathbb{N}$[5]. Si $b = 1$, alors $n = a + 1$ fonctionne.

Si $b > 1$, alors la proposition 4.11 dit que $a > a/b$, et donc $n = a$ fonctionne. □

PROPooBTCCooVVvaeL

Proposition 4.13.
Si $q < 1$ dans $\mathbb{Q}$, alors $ql < l$ pour tout $l \in \mathbb{Q}^+$.

Démonstration. Si $q < 0$ c'est facile. Supposons que $0 < q < 1$. Vu que $q - 1 < 0$ et $l > 0$, nous avons

$$ql - l = (q - 1)l < 0. \tag{4.13}$$

Mais dire $ql - l < 0$ signifie $ql < l$. □

LEMooMUYAooDLgDcf

Lemme 4.14.
Si $q \in \mathbb{Q}$, alors il existe $k \in \mathbb{N}$ tel que $kq \in \mathbb{Z}$.

PROPooMXGPooDUkOuv

Proposition 4.15.
Le corps $\mathbb{Q}$ est archimédien[6].

Démonstration. Soit $x, y \in \mathbb{Q}$ avec $x > 0$. Si $y \leqslant 0$, nous avons directement $x \geqslant y$. Sinon, il existe $m \in \mathbb{N}$ tel que $mx \in \mathbb{N}$ (lemme 4.14). Vu que $\mathbb{N}$ est archimédien (proposition 1.174), il existe $n \in \mathbb{N}$ tel que $nmx > y$. □

4.1.2 Caractéristique

LEMooYCPUooNxEPhB

Lemme 4.16.
Le corps $\mathbb{Q}$ est de caractéristique[7] *nulle.*

Démonstration. Il s'agit de comprendre le noyau de l'application définie dans la définition 3.114. Pour $n \in \mathbb{Z}$ nous avons $\mu(n) = n \in \mathbb{Q}$. La seule façon d'avoir $\mu(n) = 0$ est d'avoir $n = 0$. Donc $\ker(\mu) = \{0\}$ et $\mathbb{Q}$ est de caractéristique nulle. □

4.1.3 Infini dénombrable

PROPooDHIAooZysvNs

Proposition 4.17.
L'ensemble des rationnels est infini dénombrable[8].

[5] Existe pas la proposition 4.10.
[6] Définition 1.162.
[7] Définition 3.114.
[8] Ouais, je sais, dans les définitions prises ici, un ensemble dénombrable est toujours infini. Mais l'excès de précision ne tue pas, loin s'en faut.

Démonstration. L'ensemble $\mathbb{Z}$ est infini (lemme 1.211) et la proposition 3.241 donne une injection $f\colon \mathbb{Z} \to \mathbb{Q}$. Donc $f(\mathbb{Z})$ est infini.

L'ensemble $\mathbb{Q}$ contient une partie infinie. Il est donc infini par le lemme 1.76.

L'application

$$\begin{aligned} g\colon \mathbb{Z}^2 &\to \mathbb{Q} \\ a,b &\mapsto a/b \end{aligned} \tag{4.14}$$

est surjective alors que $\mathbb{Z}^2$ est dénombrable. Le lemme 2.43 dit alors que $\mathbb{Q}$ est fini ou dénombrable. Vu que nous avons déjà prouvé que $\mathbb{Q}$ était infini, nous déduisons que $\mathbb{Q}$ est infini dénombrable. □

4.2 Suite de Cauchy dans un corps totalement ordonné

LEMooLTBIooSZnvsQ

Lemme 4.18 ([99, 1])**.**
Tout corps commutatif de caractéristique nulle contient un sous-corps isomorphe à $\mathbb{Q}$.

Démonstration. Soit un corps $\mathbb{K}$ de caractéristique nulle. Nous savons du lemme 3.114 que

$$\begin{aligned} \mu\colon \mathbb{Z} &\to \mathbb{K} \\ n &\mapsto n1_{\mathbb{K}} \end{aligned} \tag{4.15}$$

est un morphisme d'anneaux vérifiant $\ker(\mu) = \{0\}$. Nous posons $Z = \mu(\mathbb{Z})$. L'application $\mu\colon \mathbb{Z} \to Z$ est un isomorphisme d'anneaux. Prouvons cela :

(1) **Morphisme** L'application μ est un morphisme par le lemme 3.114.

(2) **Surjectif** Par définition les éléments de Z sont dans l'image de $\mathbb{Z}$.

(3) **Injectif** Si $x, y \in \mathbb{Z}$ vérifient $\mu(x) = \mu(y)$, alors $\mu(x-y) = 0$ parce que μ est un morphisme. Mais $\mathbb{K}$ est de caractéristique nulle, c'est-à-dire $\ker(\mu) = \{0\}$. Donc $x - y = 0$.

Le corps $\mathbb{K}$ contient donc un sous-anneau isomorphe à $\mathbb{Z}$. Puisque $\mathbb{Z}$ et $\mathbb{K}$ sont commutatifs, la proposition 3.246 s'applique et $\mathbb{K}$ contient un sous-corps isomorphe à $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. □

La proposition suivante donne des précisions à propos du lemme 4.18.

PROPooKNROooFdgIeQ

Proposition 4.19 ([1])**.**
Soit un corps totalement ordonné $\mathbb{K}$. Nous considérons l'application

$$\begin{aligned} \mu\colon \mathbb{Z} &\to \mathbb{K} \\ n &\mapsto n \cdot 1_{\mathbb{K}} \end{aligned} \tag{4.16}$$

et ensuite

$$\begin{aligned} \sigma\colon \mathbb{Q} &\to \mathbb{K} \\ a/b &\mapsto \mu(a)\mu(b)^{-1}. \end{aligned} \tag{4.17}$$

Alors

(1) L'application σ est bien définie.

(2) L'application σ est un morphisme de corps.

(3) Si $q \leqslant q'$ dans $\mathbb{Q}$, alors $\sigma(q) \leqslant \sigma(q')$.

Démonstration. En plusieurs morceaux.

(1) **σ est bien définie** Montrons que σ est bien définie. Pour cela nous considérons $a, b, x, y \in \mathbb{Z}$ tels que $a/b = x/y$ dans $\mathbb{Q}$. Par définition des classes (définition 3.239 du corps des fractions), nous avons $ay = bx$ dans $\mathbb{Q}$. Vu que μ est un morphisme nous avons alors

$$\mu(a)\mu(y) = \mu(b)\mu(x) \tag{4.18}$$

et donc $\mu(a)\mu(b)^{-1} = \mu(x)\mu(y)^{-1}$, c'est-à-dire $\sigma(a/b) = \sigma(x/y)$. L'application σ est donc bien définie.

(2) **Morphisme pour la somme**

L'application μ est un morphisme d'anneaux, comme déjà dit depuis le lemme 3.114. Notons aussi que, parce que $\mathbb{K}$ est commutatif,

$$\mu(qy)^{-1} = \mu(q)^{-1}\mu(y)^{-1}. \tag{4.19}$$

En utilisant la définition 3.239(1) de la somme nous avons

$$\begin{aligned}
\sigma(p/q + x/y) &= \sigma\big((py + qx)/qy\big) && (4.20a)\\
&= \big[\mu(py) + \mu(qx)\big]\mu(qy)^{-1} && (4.20b)\\
&= \mu(py)\mu(qy)^{-1} + \mu(qx)\mu(qy)^{-1} && (4.20c)\\
&= \mu(p)\mu(q)^{-1} + \mu(x)\mu(y)^{-1} && (4.20d)\\
&= \sigma(p/q) + \sigma(x/y). && (4.20e)
\end{aligned}$$

(3) **Morphisme pour le produit** Même genre de calculs que pour la somme.

(4) **Croissante**

Nous savons aussi par le lemme 1.117(4) que $1 \geqslant 0$. Puisque μ est un morphisme d'anneaux,

$$\mu(n+1) = \mu(n) + \mu(1) = \mu(n) + 1 \tag{4.21}$$

La définition 3.249(1) dit alors que $\mu(n) \geqslant 0$ pour tout $n \in \mathbb{N}$. Nous avons pour la même raison que si $m \geqslant n$ dans $\mathbb{N}$, alors $\mu(m) \geqslant \mu(n)$ dans $\mathbb{K}$.

Soient maintenant $p, q \in \mathbb{N}$, et prouvons que $\sigma(p/q) \geqslant 0$. D'abord

$$\sigma(p/q) = \mu(p)\mu(q)^{-1} \tag{4.22}$$

où $\mu(p) \geqslant 0$ et $\mu(q) \geqslant 0$. Ensuite le lemme 1.117(5) nous indique que $\mu(q)^{-1} \geqslant 0$. Enfin la condition 3.249(2) nous permet de conclure que $\sigma(p/q) \geqslant 0$.

Finalement, si $q_1 \geqslant q_2$ dans $\mathbb{Q}$, alors $q_1 - q_2 \geqslant 0$, et nous avons

$$\sigma(q_1) = \sigma(q_2 + q_1 - q_2) = \sigma(q_2) + \sigma(q_1 - q_2) \geqslant \sigma(q_2) \tag{4.23}$$

par la condition 3.249(1).

□

NORMooJRRZooTwTVYG

4.20.
Si $\mathbb{K}$ est un corps totalement ordonné, la proposition 4.19 nous donne un morphisme de corps $\sigma\colon \mathbb{Q} \to \mathbb{K}$ qui respecte l'ordre. Pour $q \in \mathbb{Q}$ et $k \in \mathbb{K}$ nous notons

$$qk = \sigma(q)k. \tag{4.24}$$

EQooERFIooMpZVEs

Nous pourrons donc écrire $\frac{k}{2}$ pour $\sigma(1/2)k$.

Le lemme suivant explique que la notation (4.24) n'est pas complètement idiote.

LEMooWIONooGTKfcJ

Lemme 4.21.
Soit un corps commutatif totalement ordonné $\mathbb{K}$. Soit $k \in \mathbb{K}$. Nous avons

$$k + k = 2k. \tag{4.25}$$

Démonstration. Vu que $\sigma\colon \mathbb{Q} \to \mathbb{K}$ est un morphisme, il vérifie $\sigma(1) = 1$, donc

$$\begin{aligned}
k + k &= \sigma(1)k + \sigma(1)k && (4.26a)\\
&= \big(\sigma(1) + \sigma(1)\big)k && (4.26b)\\
&= \sigma(2)k && (4.26c)\\
&= 2k. && (4.26d)
\end{aligned}$$

□

PROPooTFVOooFoSHPg

Proposition 4.22.
Toute suite convergente dans un corps totalement ordonné est de Cauchy[9].

Démonstration. Soit un corps totalement ordonné $\mathbb{K}$ et une suite $x_n \xrightarrow{\mathbb{K}} x$. Soit $\epsilon > 0$. Il est important de se rendre compte que $\epsilon \in \mathbb{K}$ et que l'inégalité est au sens de l'ordre dans $\mathbb{K}$; en particulier ce n'est pas $\epsilon \in \mathbb{R}$ ni $\epsilon \in \mathbb{Q}$. D'ailleurs nous n'avons pas encore défini $\mathbb{R}$.

Vu que (x_n) converge vers x, il existe $N \in \mathbb{N}$ tel que pour tout $k > N$,

$$|x_k - x| < \epsilon. \tag{4.27}$$

Soient $p, q > N$. Alors en utilisant la majoration du lemme 1.122(4),

EQooMQYGooLpgFQO
$$|x_p - x_q| = \big|(x_p - x) + (x - x_q)\big| \leqslant |x_p - x| + |x - x_q| \leqslant 2\epsilon. \tag{4.28}$$

En analyse en général, on s'arrête là et on dit que (x_n) est de Cauchy parce qu'il n'y a pas vraiment de différence entre réaliser une majoration avec ϵ ou avec 2ϵ. Détaillons toutefois comment ça se passe dans le cas où ϵ est un élément d'un corps totalement ordonné.

Le 2ϵ arrivant à la fin de (4.28) est en réalité $\epsilon + \epsilon = \sigma(2)\epsilon$ en vertu de ce qui est raconté en 4.20 et en vertu du lemme 4.21.

Considérons $\epsilon' = \sigma(1/2)\epsilon$, que nous pouvons noter $\epsilon' = \epsilon/2$. Vu que $\epsilon' > 0$, il existe un N' tel que pour tout $p, q > N'$ nous ayons

$$|x_p - x_q| \leqslant 2\epsilon' = \sigma(2)\sigma(1/2)\epsilon = \sigma(1)\epsilon = \epsilon. \tag{4.29}$$

Ce dernier ϵ étant bien celui fixé au début de la preuve, nous en déduisons que (x_n) est de Cauchy. □

4.2.1 Suites de Cauchy dans les rationnels

PropFFDJooAapQlP

Proposition 4.23 ([39]).
Principales propriétés des suites de Cauchy[10] *dans* $\mathbb{Q}$.

ItemRKCIooJguHdji
(1) *Toute suite convergente est de Cauchy*[11].

ItemRKCIooJguHdjii
(2) *Toute suite de Cauchy est bornée.*

ItemRKCIooJguHdjiii
(3) *Si* $x_n \to 0$ *et si* (y_n) *est bornée, alors* $x_n y_n \to 0$

(4) *Si* (x_n) *et* (y_n) *sont de Cauchy alors* $(x_n + y_n)$, $(x_n - y_n)$ *et* $(x_n y_n)$ *sont également de Cauchy.*

ITEMooIAFSooAIUpAN
ItemRKCIooJguHdjvi
(5) *Si il existe* $a, b \in \mathbb{Q}$ *tels que* $x_n \to a$ *et* $y_n \to b$ *alors* $x_n + y_n \to a + b$, $x_n - y_n \to a - b$ *et* $x_n y_n \to ab$.

(6) *Soit* (x_n) *une suite de Cauchy qui ne converge pas vers zéro. Alors il existe* n_0 *tel que la suite* $\left(\frac{1}{x_n}\right)_{n \geqslant n_0}$ *soit de Cauchy.*

Démonstration. Point par point.

(1) C'est la proposition 4.22.

(2) Soit (x_n) une suite de Cauchy dans $\mathbb{Q}$. Avec $\epsilon = 1$ dans la définition, si $q > N$, nous avons

$$|x_q - x_N| \leqslant 1. \tag{4.30}$$

Et donc pour tout q plus grand que N, $x_N - 1 \leqslant x_q \leqslant x_N + 1$, ou encore, pour tout n :

$$|x_n| \leqslant \max\{|x_1|, |x_2|, \dots, |x_N|, |x_N + 1|\}. \tag{4.31}$$

La suite est donc bornée.

(3) Soit $\epsilon > 0$. Les hypothèses disent qu'il existe un N tel que $|x_n| \leqslant \epsilon$ dès que $n \geqslant N$. Et il existe aussi $M \geqslant 0$ tel que $|y_n| \leqslant M$ pour tout n. Du coup, lorsque $n \geqslant N$ nous avons $|x_n y_n| \leqslant M\epsilon$.

[9] Définition 3.249(1).
[10] Définition 3.249(1).
[11] Et non la réciproque, qui sera justement la grande innovation des nombres réels.

(4) En ce qui concerne la somme,

$$|x_p + y_p - x_q - y_q| \leqslant |x_p - x_q| + |y_p - y_q|. \tag{4.32}$$

EqDCNBooAzrrBi

Soit N_1 tel que si $p, q \geqslant N_1$ alors $|x_p - x_q| \leqslant \epsilon$ et N_2 de même pour la suite (y_n). En prenant $N = \max\{N_1, N_2\}$, la somme (4.32) est plus petite que 2ϵ dès que $p, q \geqslant N$.

Passons à la démonstration du fait que le produit de deux suites de Cauchy est de Cauchy. Les suites (x_n) et (y_n) sont bornées et quitte à prendre le maximum, nous disons qu'elles sont toutes les deux bornées par le nombre M : pour tout n nous avons $|x_n| \leqslant M$ et $|y_n| \leqslant M$. Nous avons :

$$|x_p y_p - x_q y_q| \leqslant |x_p y_p - x_q y_p| + |x_q y_p - x_q y_q| \leqslant |y_p||x_p - x_q| + |x_q||y_p - y_q|. \tag{4.33}$$

Puisque (x_n) et (y_n) sont de Cauchy, si p et q sont assez grands, les deux différences sont majorées par ϵ et nous avons

$$|x_p y_p - x_q y_q| \leqslant M\epsilon + M\epsilon = 2M\epsilon, \tag{4.34}$$

ce qui prouve que $(x_n y_n)$ est de Cauchy.

(5) En ce qui concerne la somme, nous pouvons tout de suite calculer

$$|x_n + y_n - (a + b)| \leqslant |x_n - a| + |y_n - b|. \tag{4.35}$$

Il existe une valeur de n à partir de laquelle le premier terme est plus petit que ϵ et une à partir de laquelle le second terme est plus petit que ϵ. En prenant le maximum des deux, la somme est plus petite que 2ϵ.

En ce qui concerne le produit,

$$|x_n y_n - ab| \leqslant |x_n y_n - a y_n| + |a y_n - ab| \leqslant |y_n||x_n - a| + |a||y_n - b|. \tag{4.36}$$

Les suites $|x_n - a|$ et $|y_n - b|$ convergent vers zéro ; la suite (y_n) est bornée parce que convergente (combinaison des points (1) et (2)) et a (la suite constante) est également bornée. Donc par le point (3), nous avons

$$y_n|x_n - a| + a|y_n - b| \to 0. \tag{4.37}$$

Au passage nous avons également utilisé la propriété de la somme que nous venons de démontrer.

(6) Soit (x_n) une suite de Cauchy dans $\mathbb{Q}$ ne convergeant pas vers zéro : il existe $\alpha > 0$ tel que pour tout $N \in \mathbb{N}$, il existe $n \geqslant N$ tel que $|x_n| > \alpha$. Mais notre suite est de Cauchy, donc il existe $n_0 \in \mathbb{N}$ tel que si $p, q \geqslant n_0$ alors

$$|x_p - x_q| \leqslant \frac{\alpha}{2}. \tag{4.38}$$

En fixant $N = n_0$, on obtient un naturel $n \geqslant n_0$ tel que $|x_n| \geqslant \alpha$. De plus, comme la suite est de Cauchy, si $p > n$ nous avons aussi $|x_n - x_p| \leqslant \frac{\alpha}{2}$. Cela implique $|x_p| \geqslant \frac{\alpha}{2}$ et en particulier $x_p \neq 0$.

Nous venons de prouver que la suite ne s'annule plus à partir de l'indice n, et même que $|x_k| \geqslant \alpha/2$ pour tout $k \geqslant n$. La suite $(1/x_k)_{k \geqslant n}$ est donc bien définie.

Soit $\epsilon > 0$. Soit n_0 tel que $|x_p - x_q| < \epsilon$ pour tout $p, q > n_0$. Soit K plus grand que n_0 et que n. En prenant $p, q \geqslant K$, nous avons $|x_p| > \frac{\alpha}{2}$ et $|x_q| > \frac{\alpha}{2}$. Nous en déduisons que

$$\left|\frac{1}{x_p} - \frac{1}{x_q}\right| \leqslant \frac{|x_q - x_p|}{|x_p x_q|} \leqslant \frac{4}{\alpha^2}|x_q - x_p| \leqslant \frac{4}{\alpha^2}\epsilon. \tag{4.39}$$

Donc $\left(\frac{1}{x_n}\right)$ est de Cauchy.

□

4.3 Insuffisance des rationnels

Nous allons voir qu'il n'existe pas de nombres rationnels x tels que $x^2 = 2$, mais que pourtant il existe une infinité de suites de rationnels (x_n) tels que $x_n^2 \to 2$.

LemJPIUooWFHaFM

Lemme 4.24.
Un entier x est pair si et seulement si l'entier x^2 est pair.

Démonstration. Si x est un nombre pair, alors il existe un entier a tel que $x = 2a$ alors $x^2 = 4a^2$ est pair.

Inversement, si x est impair alors il existe un entier a tel que $x = 2a + 1$ et alors $x^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$ est impair. □

Le théorème 4.26 nous dira que tous les $\sqrt{n}$ sont irrationnels dès que n n'est pas un carré parfait. Voici déjà le résultat pour $n = 2$. Le fait que $\sqrt{2}$ existe dans $\mathbb{R}$ sera la proposition 4.99.

PropooRJMSooPrdeJb

Proposition 4.25 (Irrationalité de $\sqrt{2}$)**.**
Il n'existe pas de fractions d'entiers dont le carré soit égal à 2.

Démonstration. Nous supposons que la fraction d'entiers a/b est telle que $a^2/b^2 = 2$, et nous allons construire une suite d'entiers strictement décroissante et strictement positive, ce qui est impossible.

Grâce au lemme 4.24 nous avons successivement les affirmations suivantes :

- $\frac{a^2}{b^2} = 2$ avec $a \neq 0$ et $b \neq 0$.
- $a^2 = 2b^2$, donc a^2 est pair.
- a est alors pair et a^2 est divisible par 4. Soit $a^2 = 4k$.
- $4k/b^2 = 2$, donc $4k = 2b^2$, donc $b^2 = 2k$ et b^2 est pair.
- Nous déduisons que b est pair.

La fraction $\frac{a/2}{b/2}$ est alors une nouvelle fraction d'entiers dont le carré vaut 2. En procédant de la même façon, en remplaçant a par $a/2$ et b par $b/2$, on obtient que la fraction d'entiers $\frac{a/4}{b/4}$ a la même propriété.

En particulier, tous les nombres de la forme $a/2^n$ sont des entiers. Ils forment une suite strictement décroissante d'entiers strictement positifs. Impossible, me diriez-vous ? Et vous auriez bien raison : toute partie non vide de $\mathbb{N}$ admet un plus petit élément[12] Il n'y a donc pas de fractions d'entiers dont le carré vaut 2. □

En fait le théorème suivant va nous montrer que le nombre $\sqrt{n}$ est soit entier, soit irrationnel. Cela dit, nous ne savons pas encore qu'il existe un élément dans $\mathbb{R}$ dont le carré vaut n. Ce sera pour le corolaire 11.97. Donc l'écriture $\sqrt{n}$ est abusive pour le moment.

THOooYXJIooWcbnbm

Théorème 4.26.
Soit un naturel n. Il existe un rationnel x tel que $x^2 = n$ si et seulement si n est un carré parfait.

Démonstration. Supposons que $\sqrt{n}$ soit rationnel. Le théorème 3.171 nous donne $p, q \in \mathbb{N}$ premiers entre eux tels que $\sqrt{n} = p/q$. La proposition 3.173 nous enseigne de plus que p^2 et q^2 sont premiers entre eux. Nous avons

$$p^2 = nq^2. \tag{4.40}$$

Le nombre q est alors un diviseur commun de q^2 et de p. Donc $q = 1$ et $n = p^2$ est un carré parfait. □

4.3.1 Série géométrique

<++>

LEMooOTVUooImvusn

Lemme 4.27 (Série géométrique)**.**
Si $q \neq 1$ dans $\mathbb{Q}$ et $p \in \mathbb{N}$ nous avons

$$\sum_{k=0}^{p} q^k = \frac{1 - q^{p+1}}{1 - q}. \tag{4.41}$$

Démonstration. En posant $S_p = 1 + q + q^2 + \cdots + q^p$, nous avons $S_p - qS_p = 1 - q^{p+1}$ et donc

$$S_p = \sum_{k=0}^{p} q^k = \frac{1 - q^{p+1}}{1 - q}. \tag{4.42}$$

□

[12] Proposition 1.180.

PROPooLBRCooBtJqwt

Proposition 4.28.
La suite donnée par

$$x_n = 1 + \frac{1}{1!} + \cdots + \frac{1}{n!} \tag{4.43}$$

est de Cauchy et ne converge pas dans $\mathbb{Q}$.

Démonstration. Si $p > q > 0$ nous avons

$$\begin{aligned}
x_p - x_q &= \sum_{k=q+1}^{p} \frac{1}{k!} && (4.44a)\\
&\leqslant \sum_{k=q+1}^{p} \frac{1}{(q+1)!} \frac{1}{(q+1)^{k-q-1}} && (4.44b)\\
&\leqslant \frac{1}{(q+1)!} \lim_{p\to\infty} \sum_{k=0}^{p} \frac{1}{(q+1)^k} && (4.44c)\\
&\leqslant \frac{1}{(q+1)!} \frac{1}{1-\frac{1}{q+1}} && (4.44d)\\
&\leqslant \frac{1}{(q+1)!} \frac{q+1}{q} && (4.44e)\\
&\leqslant \frac{1}{q!q}. && (4.44f)
\end{aligned}$$

Justifications :

- Pour (4.44b), il s'agit de remplacer dans $k!$ tous les facteurs plus grands que $(q+1)$ par $q+1$. Cela rend le dénominateur plus petit.
- Pour (4.44c), il y a une inégalité parce que la suite $p \mapsto \sum_{k=0}^{p} 1/(q+1)^k$ est une suite strictement croissante.
- Pour (4.44d), le lemme 4.27 donne la valeur de la somme finie. En ce qui concerne la limite, nous avons demandé $p > q > 0$ et donc $q + 1 > 1$. Dans ce cas la limite fonctionne.

Cette inégalité une fois établie nous permet de prouver les assertions. La suite (x_n) est de Cauchy car, pour tout $\epsilon \in \mathbb{Q}$ s'écrivant $\epsilon = \frac{a}{b}$ avec $a, b \in \mathbb{N}$, en prenant $p, q > b$, nous avons

$$x_p - x_q \leqslant \frac{1}{b!b} < \frac{1}{b} < \frac{a}{b} = \epsilon. \tag{4.45}$$

Montrons par l'absurde que cette suite ne converge pas dans $\mathbb{Q}$. Pour cela, nous supposons que $\lim_{n\to\infty} x_n = \frac{a}{b} \in \mathbb{Q}$. Pour tout $p > q$ nous avons établi

$$0 < x_p - x_q < \frac{1}{qq!}. \tag{4.46}$$

Prenons la limite $p \to \infty$; par stricte croissance de la suite, les inégalités restent strictes :

$$0 < \frac{a}{b} - x_q < \frac{1}{qq!}. \tag{4.47}$$

Si $n > b$ alors nous pouvons écrire

$$\frac{a}{b} - x_n = \frac{\alpha}{n!} \tag{4.48}$$

avec $\alpha \in \mathbb{Z}$ parce que le dénominateur commun entre $\frac{a}{b}$ et x_n est dans $n!$. En prenant donc $q > n$ dans (4.47) nous pouvons écrire

$$0 < \frac{\alpha}{q!} < \frac{1}{qq!}, \tag{4.49}$$

c'est-à-dire $0 < \alpha < \frac{1}{q}$, ce qui est impossible pour $\alpha \in \mathbb{Z}$. □

LEMooDTXYooKwmlZh

Lemme 4.29.
Soit $A > 0$ dans $\mathbb{Q}$. Il existe un rationnel $q > 0$ tel que $q^2 < A$.

Démonstration. Vu que $\mathbb{Q}$ est archimédien (proposition 4.15), il existe $n \in \mathbb{N}$ tel que $1 < nA$. Pour ce n, nous avons

$$\left(\frac{1}{n}\right)^2 < \frac{1}{n} < A. \tag{4.50}$$

□

La proposition suivante donne une suite de rationnels qui convergerait dans $\mathbb{R}$ vers $\sqrt{A}$ (non encore défini à ce stade). Il est expliqué dans [136] que la suite peut être vue comme une forme de méthode de Newton 36.54 ; voir l'exemple 36.57. Si vous aimez les dessins et les approches géométriques, il y a une explication sur Wikipédia[137].

PROPooSTQXooHIIGVf

Proposition 4.30 ([136]).
Soient $A > 0$ dans $\mathbb{Q}$ et $x_0 \in \mathbb{Q}$. La suite (x_k) définie par

$$x_{k+1} = \frac{1}{2}\left(x_k + \frac{A}{x_k}\right) \tag{4.51}$$

EQooOUIVooUqWbXc

a les propriétés suivantes :

(1) *La suite $y_k = x_k^2$ converge dans $\mathbb{Q}$ vers A.*

(2) *La suite (x_k) est de Cauchy dans $\mathbb{Q}$.*

(3) *La suite (x_k) ne converge pas dans $\mathbb{Q}$ dans le cas de $A = 2$.*

Démonstration. En plusieurs points.

(1) **La suite s_k** En posant $y_k = x_k^2$ nous calculons que

$$y_{k+1} - A = \frac{(y_k - A)^2}{4y_k}. \tag{4.52}$$

Autrement dit, la suite $s_k = y_k - A$ vérifie

$$s_{k+1} = \frac{s_k^2}{4(A + s_k)}. \tag{4.53}$$

Quelle que soit la valeur de $s_0 = x_0^2 - A$, nous avons

$$s_1 = \frac{s_0^2}{4(A + s_0)} = \frac{(x_0^2 - A)^2}{4(A + x_0^2 - A)} = \frac{(x_0^2 - A)^2}{4x_0^2} > 0. \tag{4.54}$$

Donc à partir de s_1, tous les éléments sont positifs. Vu que $A > 0$ nous avons aussi

$$s_{k+1} < \frac{s_k^2}{4s_k} = \frac{s_k}{4} \tag{4.55}$$

et donc $s_k < s_0/4^k$. Donc $s_k \to 0$.

(2) **La suite (y_k)** Nous venons de prouver que si $y_k = A + s_k$, alors $s_k \to 0$. Autrement dit, la suite y_k converge vers A dans $\mathbb{Q}$.

La suite (y_k) est donc de Cauchy par la proposition 4.23(1).

(3) **La suite (x_k) est de Cauchy** Soit $\epsilon > 0$ dans $\mathbb{Q}$. Puisque (y_k) est de Cauchy, il existe $n_0 \in \mathbb{N}$ tel que

$$|x_r^2 - x_s^2| < \epsilon \tag{4.56}$$

pour tout $r, s \geqslant n_0$.

Soit par ailleurs $q \neq 0$ dans $\mathbb{Q}$ tel que $q^2 < A$, assuré par le lemme 4.29. Quitte à augmenter la valeur de n_0, nous supposons que $x_r, x_s > q$, et en particulier que $x_r + x_s \neq 0$. Cela permet d'écrire d'abord

$$x_r^2 - x_s^2 = (x_r + x_s)(x_r - x_s) \tag{4.57}$$

et ensuite de prendre la valeur absolue et de diviser par $|x_r + x_s|$:

$$|x_r - x_s| = \frac{|x_r^2 - x_s^2|}{|x_r + x_s|} < \frac{\epsilon}{2q}. \tag{4.58}$$

Donc (x_k) est une suite de Cauchy.

(4) **Pas de convergence pour $A = 2$** Supposons que $x_k \to a \in \mathbb{Q}$. Dans ce cas nous aurions $x_k^2 \to a^2 = A = 2$ (proposition 4.23(5)). Mais nous savons par la proposition 4.25 que $a^2 = 2$ est impossible dans $\mathbb{Q}$.

□

Notons que cette proposition ne présume en rien de l'existence ou de la non-existence dans $\mathbb{Q}$ d'un élément qui pourrait décemment être nommé $\sqrt{A}$. Il se fait que le théorème 4.26 dira que $\sqrt{n}$ est soit entier, soit irrationnel.

4.31.
Un petit programme en Python pour explorer la suite de la proposition 4.30.

```
#!/usr/bin/python3

def rec(A,x):
    return ((x**2+A)/x)/2

A = 3        # Compute square root of 3
x = 1000     # Initial guess: 1000

for i in range(1,100):
    print(i, x, x**2, x**2-A)
    x = rec(A, x)
```

tex/frido/codeSnip_4.py

4.4 Les réels

Une construction des réels via les coupures de Dedekind est donnée dans [138].

NormooHRDZooRGGtCd

4.32.
La construction des réels va nécessiter un petit « bootstrap » au niveau de la topologie. En effet la notion de suite de Cauchy est une notion topologique (définition 9.332) alors que la topologie métrique (celle entre autres de $\mathbb{Q}$) ne sera définie que par le théorème 9.158. Nous avons donc dû définir en la définition 3.249 *ex nihilo* les notions de

- suite de Cauchy
- suite convergente
- complétude

Nous allons ensuite construire $\mathbb{R}$ comme ensemble de classes d'équivalence de suites de Cauchy dans $\mathbb{Q}$. Ce ne sera que plus tard, après avoir défini la notion d'espace métrique que nous allons voir que sur $\mathbb{R}$, ces trois notions coïncident avec celles topologiques[13]. Et par conséquent que $\mathbb{R}$ sera un espace métrique complet[14].

Dans cette optique, il est intéressant de lire ce que dit Wikipédia à propos des suites de Cauchy dans l'article consacré à la construction des nombres réels[139].

4.4.1 L'ensemble

DEFooGXOPooFReesm

Définition 4.33.
Soit $\mathcal{E}$ l'ensemble des suites de Cauchy[15] dans $\mathbb{Q}$. Soit aussi l'ensemble $\mathcal{E}_0$ constituée des suites qui convergent vers zéro[16].

PROPooCYPMooRwMUnI

Proposition 4.34 ([1]).
En posant

$$x + y = (x_n + y_n) \tag{4.59}$$

[13] Proposition 9.342.
[14] Théorème 4.78 pour la complétude en tant que corps et théorème 4.22 pour la complétude en tant que espace métrique.
[15] Définition 3.249(1)
[16] Nous rappelons qu'à ce niveau nous n'avons pas encore prouvé que toutes les suites de Cauchy convergent.

et

$$xy = (x_n y_n), \tag{4.60}$$

l'ensemble $\mathcal{E}$ devient un anneau[17] *commutatif dont le neutre de l'addition est la suite constante $x_n = 0$ et le neutre pour la multiplication est la suite constante $x_n = 1$.*

PROPooNUQVooAAkicK

Proposition 4.35.
La partie $\mathcal{E}_0$ est un idéal[18] *de l'anneau $\mathcal{E}$.*

Démonstration. Nous savons par la proposition 4.23(1) que les suites convergentes sont de Cauchy ; par conséquent $\mathcal{E}_0 \subset \mathcal{E}$.

L'ensemble structuré $(\mathcal{E}_0, +)$ est un sous-groupe de $\mathcal{E}$ par les propriétés de la proposition 4.23 (il s'agit du fait que la somme de deux suites convergeant vers zéro est une suite convergente vers zéro).

En ce qui concerne la propriété fondamentale des idéaux, si $x \in \mathcal{E}_0$ et $y \in \mathcal{E}$ nous devons prouver que $xy \in \mathcal{E}_0$. Puisque $(\mathcal{E}_0, \cdot\ )$ est commutatif, cela suffira pour être un idéal bilatère. Vu que y est une suite de Cauchy, elle est bornée ; et étant donné que $x \to 0$ nous avons alors $xy \to 0$ (par la proposition 4.23(3)). □

DefooFKYKooOngSCB

Théorème-Définition 4.36 (L'anneau des réels[39])**.**
Sur l'ensemble quotient $\mathcal{E}/\mathcal{E}_0$, les opérations

(1) $\bar{u} + \bar{v} = \overline{u + v}$

(2) $\bar{u} \cdot \bar{v} = \overline{uv}$

sont bien définies et donnent à $\mathcal{E}/\mathcal{E}_0$ une structure de corps commutatif appelé ***corps des réels*** *et noté $\mathbb{R}$*

Démonstration. Nous divisons la preuve en plusieurs parties.

(1) **Les opérations sont bien définies** La partie $\mathcal{E}_0$ est un idéal par la proposition 4.35. Le quotient est donc bien défini et est un anneau par la proposition 3.12(2).

(2) **Caractérisation des classes** Soit $q \in \mathbb{Q}$ et une suite x convergente vers q. Cette suite est de Cauchy comme toute suite convergente. Montrons que

$$\bar{x} = \{\text{suites qui convergent vers } q\}. \tag{4.61}$$

Si $y \in \bar{x}$ alors $y = x + h$ avec $h \in \mathcal{E}_0$, et comme $h_n \to 0$, on a $y_n \to q$. Réciproquement, si $y_n \to q$ alors pour chaque n nous avons

$$y_n = x_n + (y_n - x_n), \tag{4.62}$$

mais $y_n - x_n \to 0$. Donc la suite $y - x \in \mathcal{E}_0$ ce qui signifie que $y \in \bar{x}$.

(3) **Neutre et unité** Il est vite vérifié que $\bar{0}$, la classe de la suite constante égale à zéro est neutre pour l'addition. De même, $\bar{1}$, est un neutre pour la multiplication.

(4) **Corps** Nous devons prouver que tout élément non nul est inversible. C'est-à-dire que si $x \in \mathcal{E}$ ne converge pas vers zéro[19] alors il existe $y \in \mathcal{E}$ tel que $xy \in \bar{1}$.

Nous savons par la proposition 4.23(6) que x étant une suite de Cauchy dans $\mathbb{Q}$, il existe $n_0 \in \mathbb{N}$ tel que $\left(\frac{1}{x_n}\right)_{n \geqslant n_0}$ est une suite de Cauchy. Nous posons alors

$$y_n = \begin{cases} 0 & \text{si } n \leqslant n_0 \\ \frac{1}{x_n} & \text{si } n > n_0. \end{cases} \tag{4.63}$$

Nous avons alors

$$(xy)_n = \begin{cases} 0 & \text{si } n \leqslant n_0 \\ 1 & \text{si } n > n_0 \end{cases} \tag{4.64}$$

et donc $xy \in \bar{1}$.

□

[17] Définition 1.100.
[18] Définition 3.3.
[19] $x \in \mathcal{E}$ peut soit ne pas converger du tout, soit converger vers autre chose que zéro.

NORMooWBYNooBQaPPk

4.37 (Quelques notations entre $\mathbb{Q}$ et $\mathbb{R}$).
Si $k \mapsto x_k$ est une suite, nous notons (x_k) avec des parenthèses la suite elle-même. Le k dans (x_k) est un indice muet, et dans les cas où il peut y avoir une ambiguïté, nous pouvons noter $(x_k)_{k\in\mathbb{N}}$. Cette dernière notation est plus lourde, mais plus exacte.

Le mieux est d'écrire simplement x la suite, mais alors il faut être prudent et ne pas noter x la limite. Nous éviterons donc d'écrire $x_k \to x$.

Si (x_k) est une suite de Cauchy dans $\mathbb{Q}$, nous notons $\bar{x}$ l'élément de $\mathbb{R}$ qui lui correspond. En fait $\bar{x} = (x_k)$: $\bar{x}$ est la suite-elle même, mais pour nous souvenir de l'origine nous allons adopter cette notation.

D'autre part nous définissons

$$\begin{aligned}\varphi\colon \mathbb{Q} &\to \mathbb{R}\\ q &\mapsto \overline{[k \mapsto q]},\end{aligned} \tag{4.65}$$

c'est-à-dire que $\varphi(q)$ est la classe de la suite constante $x_k = q$.

PropooEPFCooMtDOfP

Proposition 4.38.
Soit l'application

$$\begin{aligned}\varphi\colon \mathbb{Q} &\to \mathbb{R}\\ q &\mapsto \bar{q}.\end{aligned} \tag{4.66}$$

où par $\bar{q}$ nous entendons la classe de la suite constante égale à q (qui est de Cauchy).

(1) C'est un homomorphisme[20] *de corps injectif.*

(2) Image(φ) *est un sous-corps de* $\mathbb{R}$

(3) $\varphi\colon \mathbb{Q} \to$ Image(φ) *est un isomorphisme de corps.*

Démonstration. Le fait que ce soit un homomorphisme est simplement

- $\varphi(q + q') = \overline{q + q'} = \bar{q} + \overline{q'}$
- $\varphi(qq') = \overline{qq'} = \bar{q}\overline{q'}$.

En ce qui concerne l'injectivité, si q est tel que $\varphi(q) = \bar{0} = \mathcal{E}_0$, c'est que

$$\varphi(q) = \{\text{suites de Cauchy qui convergent vers zéro}\} \tag{4.67}$$

Mais nous savons aussi que[21]

$$\varphi(q) = \bar{q} = \{\text{suites de Cauchy qui convergent vers } q\} \tag{4.68}$$

Nous en déduisons que $q = 0$. □

NORMooJIRRooDuqmru

4.39.
Lorsque dans la suite nous parlerons d'un élément de $\mathbb{Q}$ comme étant un réel, nous aurons en tête l'image de cet élément par φ.

LEMooYLQBooFistHs

Lemme 4.40.
Soient $q, l \in \mathbb{Q}$ tels que $\bar{q} = \bar{l}$. Alors $q = l$ dans $\mathbb{Q}$.

Démonstration. La suite constante $x_n = q$ est un représentant de $\bar{q}$, et la suite constante $y_n = l$ est représentant de $\bar{l}$. Dire que $\bar{l} = \bar{q}$ signifie qu'il existe une suite $z \in \mathcal{E}_0$ tel que

$$x = y + z. \tag{4.69}$$

Pour tout n nous avons donc $x_n = y_n + z_n$, ou encore

$$z_n = q - l \tag{4.70}$$

pour tout n. Puisque z est une suite constante, elle ne peut appartenir à $\mathcal{E}_0$ que si elle est la suite constante nulle, c'est-à-dire si $q = l$. □

[20] Voir -1.1.
[21] Voir dans la démonstration du théorème 4.36.

4.4.2 Relation d'ordre

Définition 4.41.
Nous définissons les parties $\mathcal{E}^+$ et $\mathcal{E}^-$ de $\mathcal{E}$ par

(1) $x \in \mathcal{E}^+$ si et seulement si pour tout $\epsilon > 0$ (ϵ est dans $\mathbb{Q}$), il existe N_ϵ tel que $n > N_\epsilon$ implique $x_n > -\epsilon$.

(2) $x \in \mathcal{E}^-$ si et seulement si pour tout $\epsilon > 0$, il existe N_ϵ tel que $n > N_\epsilon$ implique $x_n < \epsilon$.

Nous notons aussi $\mathcal{E}^{++} = \mathcal{E}^+ \setminus \mathcal{E}_0$.

LEMooJOYQooCDlhHW

Lemme 4.42 (À propos du zéro)**.**
Les parties $\mathcal{E}^+$ et $\mathcal{E}^-$ partitionnent $\mathcal{E}$ de la façon suivante :

ITEMooKRBYooZGhhch

(1) $\mathcal{E}^+ \cap \mathcal{E}^- = \mathcal{E}_0$

ITEMooRCIZooHUIymE

(2) Le neutre pour l'addition dans $\mathbb{R}$ est $\bar{\mathcal{E}}_0$ c'est-à-dire la classe de la suite constante nulle.

ITEMooZRVXooANHspZ

(3) $\mathcal{E}^+ \cup \mathcal{E}^- = \mathcal{E}$

Démonstration. En deux parties.

(1) **Pour (1)** On prouve d'abord que $\mathcal{E}^+ \cap \mathcal{E}^- \subset \mathcal{E}_0$, l'inclusion inverse est évidente. Soit $\epsilon > 0$ et $x \in \mathcal{E}^+ \cap \mathcal{E}^-$. Il existe un $N \in \mathbb{N}$ tel que $x_n > -\epsilon$ et $x_n < \epsilon$ pour tout $n \geqslant N$. Par conséquent, $|x_n| \leqslant \epsilon$ pour tout $n \geqslant N$ et la suite x converge vers zéro, c'est-à-dire $x \in \mathcal{E}_0$.

(2) **Pour (2)** Soit $a \in \mathbb{R}$. Nous montrons que si $x_n = 0$ pour tout n, alors $a + \bar{x} = a$. Nous notons y un représentant de a. Par définition, $a + \bar{x} = \overline{y + x}$. Et donc

$$a + \bar{x} = \overline{y + x} = \bar{y} = a. \tag{4.71}$$

(3) **Pour (3)** Soit $x \in \mathcal{E} \setminus \mathcal{E}^-$, et prouvons que $x \in \mathcal{E}^+$. La condition $x \notin \mathcal{E}^-$ donne qu'il existe un $\alpha > 0$ (dans $\mathbb{Q}$) tel que pour tout n, il existe $p > n$ avec $x_p > \alpha$. Mais x est une suite de Cauchy, donc nous avons un n_0 tel que si $n, p \geqslant n_0$ alors $|x_n - x_p| \leqslant \frac{\alpha}{2}$. En particulier, si $n \geqslant n_0$, et si $p > n$ est tel que $x_p > \alpha$, on obtient

$$x_n > \frac{\alpha}{2} > 0 \tag{4.72}$$

Par conséquent $x \in \mathcal{E}^+$ parce que $x \in \mathcal{E}$ et les x_n sont tous positifs à partir d'un certain rang.

□

LEMooXNWSooHbNcAV

Lemme 4.43 ([1])**.**
Si $x \in \mathcal{E}^{++}$, alors il existe N tel que $x_n > 0$ pour tout $n > N$.

Démonstration. La suite x ne tend pas vers zéro. Donc il existe $\delta > 0$ tel que pour tout $N > 0$ il existe $n > N$ vérifiant $x_n > \delta$.

Mais la suite x est également de Cauchy. Écrivons cette condition pour $\delta/2$. Il existe $N_2 > 0$ tel que $p, q > N_2$ implique $|x_p - x_q| < \delta/2$.

Nous fixons $n > N_2$ tel que $x_n > \delta$. Alors pour tout $p > N_2$ nous avons aussi

$$|x_p - x_n| < \frac{\delta}{2}. \tag{4.73}$$

Cela implique que $x_p > \delta/2 > 0$ pour tout $p > N_2$. □

La proposition suivante est une version plus précise du lemme 4.43. Elle peut également être démontrée en utilisant la proposition 3.252.

PROPooZRCCooFGdtIl

Proposition 4.44 ([18])**.**
Soit une suite de Cauchy (x_n) dans $\mathbb{Q}$. Nous supposons que

(1) $x \in \mathcal{E}^+$

(2) x ne converge pas vers 0.

Note : ces hypothèses signifient que $x \in \mathcal{E}^{++}$.

Alors il existe $r \in \mathbb{Q}^+ \setminus \{0\}$ et $N \in \mathbb{N}$ tel que

$$x_n \geqslant r \tag{4.74}$$

pour tout $n \geqslant N$.

Démonstration. Fixons $\epsilon \in \mathbb{Q}^+ \setminus \{0\}$, et procédons par l'absurde. Du coup nous savons trois choses sur la suite (x_n).

ITEMooTNZDooHKZdBe

(1) Hypothèse absurde : pour tout $q \in \mathbb{Q}^+ \setminus \{0\}$ et pour tout $N \in \mathbb{N}$, il existe $p \geqslant N$ vérifiant $x_p < q$.

(2) Vu que $x \in \mathcal{E}^{++} \subset \mathcal{E}^+$, il existe $P_1 \in \mathbb{N}$ tel que $x_n > -\epsilon$ pour tout $n \geqslant P_1$.

(3) La suite x est de Cauchy. Donc il existe $P_2 \in \mathbb{N}$ tel que si $m, n \geqslant P_2$, nous avons $|x_m - x_n| < \epsilon/2$.

Nous considérons $P \geqslant \max\{P_1, P_2\}$ et nous prenons $q = \epsilon/2$, $N = P$ dans la propriété (1). Il existe donc $p > P$ tel que $x_p < \epsilon/2$.

Prenons aussi $n > p$ et écrivons les deux autres propriétés :

(1) $x_n > -\epsilon$ parce que $n > p > P > P_1$.

(2) $|x_n - x_p| < \epsilon/2$ parce que $n, p > P > P_2$.

Du coup nous avons

$$x_n < x_p + \frac{\epsilon}{2} < \epsilon, \tag{4.75}$$

et donc $-\epsilon < x_n < \epsilon$.

Au final, nous avons prouvé que pour tout $\epsilon \in \mathbb{Q}^+ \setminus \{0\}$, il existe P tel que $n > P$ implique $|x_n| < \epsilon$. Cela signifie que

$$x_n \xrightarrow{\mathbb{Q}} 0, \tag{4.76}$$

c'est-à-dire $x \in \mathcal{E}_0$, ce qui est contraire à l'hypothèse. □

LEMooRKSXooFsIohe

Lemme 4.45 ([39]).
Quelques propriétés du partitionnement.

ITEMooRQVKooCnwWOY

(1) $x \in \mathcal{E}^-$ *si et seulement si* $(-x) \in \mathcal{E}^+$

ITEMooJUPOooOBubqA

(2) $x \in \mathcal{E}^+$ *et* $y \in \mathcal{E}^+$ *implique* $x + y \in \mathcal{E}^+$

ITEMooDQLJooPViuVC

(3) $x \in \mathcal{E}^+$ *et* $y \in \mathcal{E}^+$ *implique* $xy \in \mathcal{E}^+$

(4) Si $x, y \in \mathcal{E}$ *sont tels que* $x - y \in \mathcal{E}_0$ *alors soit* $x, y \in \mathcal{E}^+$ *soit* $x, y \in \mathcal{E}^-$.

Démonstration. Point par point.

(1) Définition de $\mathcal{E}^+$ et $\mathcal{E}^-$.

(2) Pour $n \geqslant N_{\epsilon/2}$ nous avons $x_n > -\epsilon/2$ et $y_n > -\epsilon/2$. Donc $x_n + y_n > -\epsilon$.

(3) Si x ou y est dans $\mathcal{E}_0$ alors $xy \in \mathcal{E}_0$ et c'est bon. Si par contre $x, y \in \mathcal{E}^{++}$ alors le lemme 4.43 nous indique que pour n suffisamment grand, $x_n > 0$ et $y_n > 0$. Et dans ce cas, $(xy)_n > 0$, c'est-à-dire $xy \in \mathcal{E}^+$.

(4) Supposons que $x - y \in \mathcal{E}_0$ avec $x \in \mathcal{E}^+$ et prouvons qu'alors $y \in \mathcal{E}^+$. Soit donc $\epsilon > 0$; il existe n_1 tel que $x_n > -\frac{\epsilon}{2}$ dès que $n \geqslant n_1$. Mais $x - y \in \mathcal{E}_0$, donc il existe n_2 tel que $|x_n - y_n| < \frac{\epsilon}{2}$ dès que $n \geqslant n_2$. En prenant n plus grand que n_1 et n_2, nous avons en même temps

$$\begin{cases} x_n > -\frac{\epsilon}{2} & \text{(4.77a)} \\ |x_n - y_n| < \frac{\epsilon}{2}. & \text{(4.77b)} \end{cases}$$

Cela implique que $y_n > -\epsilon$ et donc que $y \in \mathcal{E}^+$.

Nous pouvons de même prouver que si $x \in \mathcal{E}^-$ alors $y \in \mathcal{E}^-$.

□

DefooLMQIooTgzZXd

Définition 4.46 (Positivité dans $\mathbb{R}$).
Vocabulaire et notations. Rappel que $\mathcal{E}$ *et* $\mathcal{E}_0$ *sont définis dans 4.33.*

(1) Nous notons $\mathbb{R} = \mathcal{E}/\mathcal{E}_0$.

(2) Nous notons $\mathbb{R}^+ = \bar{\mathcal{E}}^+ = \mathcal{E}^+/\mathcal{E}_0$.

(3) Nous notons $\mathbb{R}^- = \bar{\mathcal{E}}^-$.

(4) *Un élément de $\mathbb{R}$ est **positif** si il est la classe d'une suite de Cauchy appartenant à $\mathcal{E}^+$.*

(5) *Un élément de $\mathbb{R}$ est **négatif** si il est la classe d'une suite de Cauchy appartenant à $\mathcal{E}^-$.*

(6) *Lorsque nous parlons de nombres réels, le symbole « 0 » signifie $\mathcal{E}_0$ ou plus précisément la classe d'un élément de $\mathcal{E}_0$ modulo $\mathcal{E}_0$.*

REMooOCXLooKQrDoq

4.47.
Avec les conventions de la définition 4.46, et en anticipant sur nos connaissances à propos des réels,

(1) zéro est positif et négatif.

(2) L'intersection entre $\mathbb{R}^+$ et $\mathbb{R}^-$ est le singleton $\{0\}$.

(3) L'ensemble des nombres *strictement* positifs est noté $(\mathbb{R}^+)^*$ ou $\mathbb{R}^+ \setminus \{0\}$.

(4) Le mot « positif » signifie « positif ou nul » ; le mot « négatif » signifie « négatif ou nul ». Ce sont des conventions qui sont également celles de Wikipédia[140].

DEFooBXHJooOEYPRI

Définition 4.48 (Ordre sur $\mathbb{R}$)**.**
Si $x, y \in \mathbb{R}$ nous notons $x \leqslant y$ si et seulement si $y - x \in \overline{\mathcal{E}^+}$.

PROPooYMJVooNAsXae

Proposition 4.49.
Le couple $(\mathbb{R}, \leqslant)$ est un corps totalement ordonné[22]

Démonstration. Il s'agit de vérifier, dans l'ordre, les définitions 1.23, 1.26 et 1.115. Pour la suite nous considérons $x, y, z \in \mathbb{R}$ et des suites de Cauchy a, b, c représentant x, y, z, c'est-à-dire telles que $x = \bar{a}$, $y = \bar{b}$ et $z = \bar{c}$.

(1) **Réflexivité** Pour savoir si $x \geqslant x$, nous devons nous demander si $x - x \in \overline{\mathcal{E}^+}$. Nous avons $x - x = \bar{a} - \bar{a} = \bar{0} = 0$.

(2) **antisymétrie** Nous supposons que $x \geqslant y$ et $y \geqslant x$. Du côté des suites de Cauchy, cela signifie que $\overline{a - b \in \mathcal{E}^+}$ et $b - a \in \mathcal{E}^+$. Le lemme 4.45(1) nous indique alors que $a - b = -(b - a) \in \mathcal{E}^-$. Donc

$$a - b \in \mathcal{E}^+ \cap \mathcal{E}^- = \{\bar{0}\}. \tag{4.78}$$

Donc le réel $x - y$ est la classe de la suite constante 0. Le lemme 4.42(2) dit alors que $x - y = 0$ ou encore que $x = y$.

(3) **transitivité** Nous supposons que $x \leqslant y$ et $y \leqslant z$. L'hypothèse $x \leqslant y$ signifie $y - x \in \bar{\mathcal{E}}^+$ ou encore que $b - a \in \mathcal{E}^+$. Même chose pour $y \leqslant z$ qui signifie que $c - b \in \mathcal{E}^+$. Nous avons alors

$$\begin{aligned} c - a &= c - b + b - a && \text{(4.79a)}\\ &= (c - b) + (b - a) && \text{(4.79b)}\\ &\in \mathcal{E}^+ + \mathcal{E}^+ && \text{(4.79c)}\\ &\subset \mathcal{E}^+ && \text{(4.79d)} \end{aligned}$$

où nous avons utilisé le lemme 4.45(2). Puisque $c - a \in \mathcal{E}^+$, nous avons $z - x = \overline{c - a} \geqslant 0$.

(4) **Ordre total** Nous devons prouver que pour $x, y \in \mathbb{R}$ nous avons toujours $x \leqslant y$ ou $y \leqslant x$. Supposons que nous n'ayons pas $x \leqslant y$, c'est-à-dire $\overline{b - a} \notin \mathcal{E}^+$. Vu le lemme 4.42(3) nous avons $\overline{b - a} \in \mathcal{E}^-$, ce qui donne, par le lemme 4.45(1) que $\overline{a - b} \in \mathcal{E}^+$, c'est-à-dire $y \leqslant x$.

(5) **Corps ordonné** Enfin nous devons vérifier les deux conditions de la définition 1.115.

Pour la première condition, nous supposons $x \leqslant y$, c'est-à-dire $b - a \in \mathcal{E}^+$. Nous avons donc

$$(b + c) - (a + c) = b + x - a - c = b - a \in \mathcal{E}^+, \tag{4.80}$$

donc $\overline{a + c} \leqslant \overline{b + c}$, c'est-à-dire $x + z \leqslant y + z$.

Pour la seconde condition, c'est le lemme 4.45(3).

□

[22] Corps totalement ordonné, définition 3.249.

Définition 4.50.
Puisque $\mathbb{R}$ est un corps totalement ordonné (proposition 4.49), si $x \in \mathbb{R}$, nous définissons $|x|$ conformément à 1.121.

LEMooTJAXooKEqPCG

Lemme 4.51.
L'application

$$\begin{aligned} \varphi\colon \mathbb{Q} &\to \mathbb{R} \\ q &\mapsto \bar{q} \end{aligned} \tag{4.81}$$

dont nous avons déjà parlé dans la proposition 4.38 est strictement croissante.

Démonstration. Nous supposons $q < l$ dans $\mathbb{Q}$. Nous devons montrer que $\bar{q} \leqslant \bar{l}$ dans $\mathbb{R}$, c'est-à-dire que $\bar{q} \leqslant \bar{l}$ et $\bar{q} \neq \bar{l}$.

Considérons la suite constante $x_n = l - q \in \mathbb{Q}$. Pour tout $\epsilon > 0$ dans $\mathbb{Q}$ nous avons

$$x_n = l - q > 0 > -\epsilon, \tag{4.82}$$

et donc $x_n \in \mathcal{E}^+$. Donc $\overline{l-q} \geqslant 0$. Cela signifie $\bar{q} \leqslant \bar{l}$.

D'autre part le lemme 4.40 dit que $\bar{q} = \bar{l}$ uniquement si $q = l$, ce qui est exclu parce que $q < l$. Donc $\bar{q} \neq \bar{l}$. □

LEMooNHMTooEdtBnQ

Lemme 4.52.
Si $a, b \in \mathbb{R}^+$ satisfont $a + b = 0$, alors $a = b = 0$.

Démonstration. Par hypothèse nous avons $a \in \mathcal{E}^+\mathcal{E}_0$ et $b \in \mathcal{E}^+/\mathcal{E}_0$. Nous considérons $x, y \in \mathcal{E}^+$ tels que $a = \bar{x}$ et $b = \bar{y}$. Par 4.36 nous avons $a + b = \overline{x+y}$. L'hypothèse $a + b = 0$ signifie donc que

$$x + y \in \mathcal{E}_0. \tag{4.83}$$

EQooYMZTooZYuAaK

Supposons que x n'est pas dans $\mathcal{E}_0$. Alors x ne converge[23] pas vers 0. Par la proposition 4.44, il existe $r > 0$ dans $\mathbb{Q}$ et $N_1 > 0$ dans $\mathbb{N}$ tels que $x_n > r$ pour tout $n > N_1$.

Vu que $y \in \mathcal{E}^+$, il existe $N_2 > 0$ dans $\mathbb{N}$ tel que $y_n > -r/2$ pour tout $n > N_2$.

Donc pour $n > \max\{N_1, N_2\}$ nous avons[24] :

$$x_n + y_n \geqslant r - \frac{r}{2} = \frac{r}{2} > 0. \tag{4.84}$$

Donc la suite $x + y$ ne peut pas converger vers zéro et nous n'avons pas $x + y \in \mathcal{E}_0$. Contradiction avec (4.83). Nous en déduisons que $a = 0$.

Nous déduisons que $b = 0$ alors immédiatement parce que $a + b = 0$ avec $a = 0$ donne $b = 0$. □

Voici une version dans $\mathbb{R}$ du lemme 1.203.

LEMooKAXFooIPyzJC

Lemme 4.53.
Soit $a > 0$ dans $\mathbb{R}$ et $b > 1$ dans $\mathbb{R}$. Alors

(1) Si $\lambda > 1$ dans $\mathbb{R}$ nous avons

$$\lambda a > a. \tag{4.85}$$

ITEMooDIVAooDjQXRL

(2) Si $0 < \lambda < 1$ dans $\mathbb{R}$ nous avons

$$\lambda a < a. \tag{4.86}$$

Remarque 4.54.
Comme déjà mentionné plus haut, à chaque fois que nous parlerons d'un élément de $\mathbb{Q}$ comme étant un élément de $\mathbb{R}$, nous considérons la classe de la suite constante.

PROPooWYPNooCcBERG

Proposition 4.55 ([1]).
Soient $a \leqslant b$ dans $\mathbb{R}$.

ITEMooDCOXooAKcSKk

(1) Si $\lambda > 0$ alors $\lambda a \leqslant \lambda b$.

(2) Si $\lambda < 0$ alors $\lambda a \geqslant \lambda b$.

LemooYNOVooOwoRwD

Lemme 4.56.
Si $x, y, z \in \mathbb{R}$ avec $x > 0$ sont tels que $z > y/x$ alors $zx > y$.

[23] Je rappelle que x et y sont des suites de Cauchy dans $\mathbb{Q}$.
[24] Notez l'utilisation de la proposition 4.6.

Démonstration. Nous savons que

$$z - \frac{y}{x} \in \mathcal{E}^+ \setminus \{0\} = \mathcal{E}^{++}. \tag{4.87}$$

Puisque $x \in \mathcal{E}^{++}$, multiplier par x fait rester dans $\mathcal{E}^{++}$:

$$zx - x\frac{y}{x} \in \mathcal{E}^{++}. \tag{4.88}$$

Un représentant de $x\frac{y}{x}$ est la suite $n \mapsto x_n \frac{y_n}{x_n} = y_n$. Donc $x\frac{y}{x} = y$. Cela signifie que $zx - y \in \mathcal{E}^{++}$ et donc que $zx > y$. □

LemooMWOUooVWgaEi

Lemme 4.57.
Pour tout $a \in \mathbb{R}$, il existe $p \in \mathbb{N}$ tel que $p > a$.

Démonstration. Nous allons donner deux preuves différentes de ce lemme.

(1) **Première façon**

L'élément a de $\mathbb{R}$ admet un représentant (a_n) qui est une suite de Cauchy dans $\mathbb{Q}$. C'est donc une suite bornée, c'est-à-dire qu'il existe $m, q \in \mathbb{N}$ tels que $|a_n| \leqslant m/q$ pour tout n (proposition 4.23(2)). Soit M un naturel strictement plus grand que m/q[25].

La suite de Cauchy $(M - a_n)_{n\in\mathbb{N}}$ est constituée de rationnels positifs et est donc dans $\mathcal{E}^+$. La classe de $M - a$ est donc un réel positif[26]. Par définition de la relation d'ordre, $M \geqslant a$.

(2) **Seconde façon**

La suite (a_n) est majorée par $\frac{m}{q}$, donc on a dans $\mathbb{Q}$ et pour tout n :

$$a_n \leqslant \frac{m}{q} = M \leqslant qM. \tag{4.89}$$

L'application $\varphi\colon \mathbb{Q} \to \mathbb{R}$ est croissante, donc

$$\varphi\big((a_n)\big) \leqslant \varphi(qM). \tag{4.90}$$

□

En corolaire, nous avons

LEMooMWOUooVWgbFi

Lemme 4.58.
Pour tout $x \in \mathbb{R}$, il existe $q \in \mathbb{Z}$ tel que $q < x$.

Démonstration. Utilisation du lemme précédent avec $a = -x$: on prend $q = -p$. □

ThoooKJTTooCaxEny

Théorème 4.59 ([39])**.**
Le corps $\mathbb{R}$ est archimédien[27]*.*

Démonstration. La proposition 4.49 dit que $\mathbb{R}$ est totalement ordonné. Soient $x, y \in \mathbb{R}$ avec $x > 0$; posons $a = \frac{y}{x}$. Le lemme 4.57 nous donne un $p \in \mathbb{N}$ tel que $p > a$. Nous concluons alors avec le lemme 4.56 :

$$px > ax = \frac{y}{x}x = y. \tag{4.91}$$

□

Le lemme suivant n'est pas loin de dire que $\mathbb{Q}$ est dense dans $\mathbb{R}$, à part que nous n'avons pas encore donné de topologie sur $\mathbb{R}$.

LemooHLHTooTyCZYL

Lemme 4.60.
À propos de rationnels entre des réels.

ITEMooGVTMooQsoTCi

(1) Si $x, y \in \mathbb{R}$ sont tels que $x < y$, alors il existe $s \in \mathbb{Q}$ tel que $x < s < y$.

ITEMooCVDSooAjimCL

(2) Si $\epsilon > 0$ dans $\mathbb{R}$, il existe $n \in \mathbb{N}$ tel que $\frac{1}{n} < \epsilon$.

ITEMooASUXooImjqzK

(3) Si $a \in \mathbb{R}$ vérifie $|a| < \epsilon$ pour tout $\epsilon > 0$, alors $a = 0$.

[25] Lemme 4.12.
[26] Et nous allons d'ailleurs arrêter de toujours préciser « la classe de » lorsque ce n'est pas nécessaire.
[27] Définition 1.162.

Démonstration. Nous avons par hypothèse que $y-x>0$ et donc le fait que $\mathbb{R}$ soit archimédien (théorème 4.59) nous donne $q\in\mathbb{N}$ tel que $q(y-x)>1$. Soit

$$E=\{n\in\mathbb{Z}\text{ tel que }\frac{n}{q}\leqslant x\}. \tag{4.92}$$

Cet ensemble n'est pas vide à cause du lemme 4.58 ; de plus, comme $|x|q\leqslant n_0$ pour un certain n_0 (à cause du lemme 4.57), l'ensemble E est majoré par n_0. Donc E possède un plus grand élément[28] p qui vérifie

$$\frac{p}{q}\leqslant x<\frac{p+1}{q}. \tag{4.93}$$

De plus $(p+1)/q<y$ parce que

$$\frac{p+1}{q}=\frac{p}{q}+\frac{1}{q}\leqslant x+\frac{1}{q}<x+y-x=y \tag{4.94}$$

où nous avons utilisé l'inégalité stricte $y-x>\frac{1}{q}$.

Nous avons donc

$$x<\frac{p+1}{q}<y, \tag{4.95}$$

et le nombre $(p+1)/q$ convient comme s. Le point (1) est prouvé.

Pour le point (2), par le point (1) nous considérons $s\in\mathbb{Q}$ tel que $0<s<\epsilon$. Si $s=p/q$ avec $p,q\in\mathbb{N}$ nous avons

$$0<\frac{1}{q}\leqslant\frac{p}{q}<\epsilon. \tag{4.96}$$

Pour (3), supposons $a\neq 0$. Alors $|a|>0$. Par le point (1), il existe $s\in\mathbb{R}$ tel que $0<m<|a|$, ce qui est contraire à l'hypothèse. □

REMooXOIOooHjwMvA

Remarque 4.61.
Le lemme 4.60 a également pour conséquence que des ensembles comme $[-1,1]$ ne sont pas bien ordonnés (définition 1.26). En effet la partie $]0,1[$ ne possède pas de minimum parce que si $x\in]0,1[$ alors $0<x$ et il existe $s\in\mathbb{Q}$ (a fortiori $s\in\mathbb{R}$) tel que $0<s<x$, c'est-à-dire que x n'est pas un minimum de $]0,1[$.

Tant que nous y sommes dans les encadrements de réels…

4.62.
Soit $q_0\in\mathbb{Q}$ tel que $0\leqslant q_0<1$. On définit alors $d_1\in\{0,1\}$ comme valant 1 si $2q_0\geqslant 1$ et 0 sinon. Puis on pose $q_1=2q_0-d_1$.

Poursuivant de la sorte, on crée une suite $(d_n)_{n\geqslant 1}$: c'est le **développement dyadique** de q_0.

PROPooSZZBooUmsPeM

Proposition 4.63 ([1])**.**
Si $q\neq q'$, alors leurs développement dyadiques sont différents.

LEMooRSLIooVrZMxM

Lemme 4.64 ([1])**.**
Soit q, q' deux rationnels tels que $0\leqslant q<q'<1$. Il existe deux entiers naturels a et N tels que $q<\frac{a}{2^N}<q'$.

Démonstration. On crée les développements dyadiques de q et q', que l'on note respectivement $(d_n)_{n\geqslant 1}$ et $(d'_n)_{n\geqslant 1}$. Notons

$$E=\{n\in\mathbb{N}\text{ tel que }d_n\neq d'_n\}. \tag{4.97}$$

Comme $q\neq q'$, les développements dyadiques sont différents[29], l'ensemble E est non-vide, et il admet un plus petit élément N. Or, $q<q'$, et donc nécessairement $d_N<d'_N$. On construit alors $a=\sum_{i=1}^{N}d_i2^i$. □

CorDensiteDyadiques

Corolaire 4.65.
Deux choses.

(1) *Pour tous réels x, y tels que $0\leqslant x<y\leqslant 1$, il existe un nombre de la forme $d=a/2^n$, avec $n\in\mathbb{N}$ et $a\in\mathbb{N}$, $a\leqslant 2^n$, tel que $x<d<y$.*

(2) *La partie*

$$D=\{\frac{a}{2^b}\text{ tel que }a\in\mathbb{Z},b\in\mathbb{N}\} \tag{4.98}$$

est dense dans $\mathbb{R}$.

[28] Lemme 1.206.
[29] Proposition 4.63.

Ce D est nommé l'ensemble des ***fractions dyadiques***.

Démonstration. Soit $\epsilon > 0$. Le lemme 4.60(1) nous permet de considérer un rationnel q tel que $x < q < y$. Une utilisation combinée de 4.60(2) et de 3.32 permet de choisir n tel que $\frac{1}{2^n} < \epsilon$. Nous posons

$$a = \min\{s \in \mathbb{N} \text{ tel que } \frac{s}{2^n} > q\}. \tag{4.99}$$

Nous avons $a/2^n < q + \epsilon$, sinon prendre $a - 1$ aurait convenu. Nous avons donc

$$x < q \leqslant \frac{a}{2^n} < a + \epsilon < y. \tag{4.100}$$

En ce qui concerne la densité, soient $r \in \mathbb{R}$ et $\epsilon > 0$. Nous considérons $n \in \mathbb{N}$ tel que $1/2^n < \epsilon$. Ensuite nous posons

$$a = \min\{a \in \mathbb{N} \text{ tel que } \frac{a}{2^n} \geqslant r\}. \tag{4.101}$$

Nous avons alors $\frac{a}{2^n} - r < \epsilon$. Cela prouve que $B(r, \epsilon) \cap D \neq \varnothing$. □

LEMooEGYLooCGrDrl

Lemme 4.66 ([1])**.**
Soient des réels a, b, x, y tels que

$$a \leqslant x \leqslant b \tag{4.102}$$

et

$$a \leqslant y \leqslant b, \tag{4.103}$$

alors $|x - y| \leqslant |b - a|$.

LEMooNLGSooSGdvAo

Lemme 4.67.
Si $a \in \mathbb{R}$.

(1) $a^2 \geqslant 0$

(2) $a^2 = 0$ *si et seulement si* $a = 0$.

Démonstration. Il a trois possibilités : $a < 0$, $a = 0$ et $a > 0$. Nous les faisons une par une.

(1) **Si $a = 0$** Alors en posant $a = \bar{x}$ nous avons $x_n \xrightarrow{\mathbb{Q}} 0$. La définition 4.36 dit que $a^2 = \bar{x}\bar{x} = \overline{xx}$. Mais $(xx)_n \to 0$. Donc $a^2 = \overline{xx} = \bar{0} = 0$. Nous avons donc prouvé que $a^2 = 0$.

(2) **Si $a > 0$** Nous avons encore $a^2 = \overline{xx}$. La proposition 4.44 dit qu'il existe $r \in \mathbb{Q}$ tel que $x_n > r$ pour tout n assez grand. Nous avons, pour ces n que $(xx)_n > r^2 > 0$ (utilisation de 4.7), et donc $xx \in \mathcal{E}^+ \setminus \mathcal{E}_0$. Donc $a^2 = \overline{xx} > 0$.

(3) **Si $a < 0$** Même raisonnement, mais avec $x_n < r$ pour n assez grand. Ensuite nous avons quand même $(xx)_n > r^2$.

□

PROPooRJOWooGbieCA

Proposition 4.68 ([1])**.**
Si $x, y \geqslant 0$ dans $\mathbb{R}$, alors

$$|x - y| = \max\big(|x| - |y|, |y| - |x|\big). \tag{4.104}$$

LEMooFQMVooDNaTDT

Lemme 4.69.
Soient $a, b, x \in \mathbb{R}$ tels que $a + x = b + x$. Alors $a = b$.

PROPooVIDJooSzXPLP

Proposition 4.70.
Si $a > b$ dans $\mathbb{R}$, alors

$$\frac{1}{a} < \frac{1}{b}. \tag{4.105}$$

4.4.3 $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$

NORMooXRGFooPCujZI

4.71.
Pour rappel, $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$, et $\mathbb{R}$ est l'ensemble des classes de suites de Cauchy dans $\mathbb{Q}$. Comme expliqué dans 4.39, à partir du moment où $\mathbb{R}$ est défini, nous notons « $\mathbb{Q}$ » ce qui en réalité $\varphi(\mathbb{Q})$ où φ est l'application qui à $q \in \mathbb{Q}$ fait correspondre la classe d'équivalence des suites de Cauchy dans $\mathbb{Q}$ convergeant dans $\mathbb{Q}$ vers q. Voir la proposition 4.38.

4.72.
Pour se convaincre que $\mathbb{R} \setminus \mathbb{Q}$ n'est pas vide, on peut remarquer que la proposition 4.25 dit qu'il n'existe pas d'éléments $q \in \mathbb{Q}$ tel que $q^2 = 2$. Or la proposition 4.99 dit qu'un tel élément existe dans $\mathbb{R}$.

Voila. Vous êtes convaincu ? Maintenant nous allons en faire une preuve un peu plus formelle,qui ne mélange pas $\mathbb{Q}$ et $\varphi(\mathbb{Q})$.

LEMooAYBFooHEUPZG

Lemme 4.73 ([1]).
Plusieurs choses plus ou moins reliées.

ITEMooTHFAooVPPHCc

(1) *La partie $\mathbb{R} \setminus \mathbb{Q}$ n'est pas vide.*

ITEMooVXUOooOVByJv

(2) *Si $x \in \mathbb{R} \setminus \mathbb{Q}$, et si $q \in \mathbb{Q} \setminus \{0\}$ alors $qx \in \mathbb{R} \setminus \mathbb{Q}$.*

ITEMooHXTAooGBWeLL

(3) *Si $x \in \mathbb{R} \setminus \mathbb{Q}$ et si $q \in \mathbb{Q}$, alors $x + q \in \mathbb{R} \setminus \mathbb{Q}$.*

ITEMooFOQRooRoftNW

(4) *Soit $\epsilon > 0$ dans $\mathbb{R}$. Il existe $x \in \mathbb{R} \setminus \mathbb{Q}$ tel que $0 < x < \epsilon$.*

Démonstration. En plusieurs points.

(1) **Pour (1)** Les propositions 4.28 et 4.30 (au choix) donnent des suites de Cauchy $(x_n)_{n\in\mathbb{N}}$ dans $\mathbb{Q}$ qui ne convergent pas dans $\mathbb{Q}$. Il n'existe donc pas de $q \in \mathbb{Q}$ tel que $(x_n)_{n\in\mathbb{N}} \in \bar{q} = \varphi(q)$. Par contre la classe de $(x_n)_{n\in\mathbb{N}}$ est bien dans $\mathbb{R}$.

(2) **Pour (3)** Si $x + q = p \in \mathbb{Q}$, alors $x = p - q \in \mathbb{Q}$.

(3) **Pour (2)** Supposons que $qx = p \in \mathbb{Q}$. Vu que $q \neq 0$, nous avons $x = pq^{-1} \in \mathbb{Q}$ parce que $\mathbb{Q}$ est un corps (c'est même sa définition 4.1).

(4) **Pour (4)** Soit $\epsilon > 0$. Soit $r \in \mathbb{R} \setminus \mathbb{Q}$ (existence par (1)). Nous considérons :

(4a) $\epsilon' \in \mathbb{Q}$ avec $\epsilon \in \mathbb{Q}$ (par exemple $1/n$ donné par le lemme 4.60(2)).

(4b) $q \in \mathbb{Q}$ avec $q > r$. Par exemple $r < q < r + 1$ sonné par le lemme 4.60(1).

(4c) $p = \epsilon' q^{-1} \in \mathbb{Q}$.

Avec tout ça, la proposition 4.55(1) nous donne $pr < pq$. Au final :

$$pr < pq = \epsilon' < \epsilon. \tag{4.106}$$

Vu que $p \in \mathbb{Q}$ et $r \in \mathbb{R} \setminus \mathbb{Q}$, la proposition 4.55(2) assure que $pr \in \mathbb{R} \setminus \mathbb{Q}$.

□

4.4.4 Complétude

Le théorème 19.163 donne une complétion de tout espace métrique en un espace complet. Il serait tentant de l'utiliser ici pour définir $\mathbb{R}$ à partir de $\mathbb{Q}$. Cette méthode ne fonctionne cependant pas parce que la démonstration de 19.163 utilise le fait que $\mathbb{R}$ est complet.

LEMooXCVRooOSZYWv

Lemme 4.74.
Nous avons

$$|\varphi(q)| = \varphi(|q|) \tag{4.107}$$

pour tout $q \in \mathbb{Q}$.

Démonstration. Soit $q \in \mathbb{Q}$. Si $q \geqslant 0$ alors nous avons d'une part $|q| = q$ dans $\mathbb{Q}$, et d'autre part $\varphi(q) \geqslant 0$ dans $\mathbb{R}$. Donc au final

$$|\varphi(q)| = \varphi(q) = \varphi(|q|). \tag{4.108}$$

Supposons au contraire que $q < 0$. Alors $|q| = -q$ dans $\mathbb{Q}$, mais aussi $\varphi(q) \leqslant 0$. Donc

$$|\varphi(q)| = -\varphi(q) = \varphi(-q) = \varphi(|q|). \tag{4.109}$$

□

LemooRTGFooYVstwS

Lemme 4.75 ([39, 1]).
Toute suite de Cauchy dans $\mathbb{Q}$ converge dans $\mathbb{R}$ vers le réel qu'elle représente.

Plus précisément, en suivant les notations de 4.37, si (x_k) est une suite de Cauchy dans $\mathbb{Q}$, alors

(1) $\varphi(x_k)$ *est une suite de Cauchy dans* $\mathbb{R}$.

(2) $\varphi(x_k) \xrightarrow{\mathbb{R}} \bar{x}$.

Ici $\bar{x}$ *est la classe de la suite* x. *C'est donc un élément de* $\mathbb{R}$.

Démonstration. Soit (x_n) une suite de Cauchy de $\mathbb{Q}$, c'est-à-dire que $x_k \in \mathbb{Q}$ pour tout k et qu'elle est de Cauchy. Elle représente un réel $\bar{x} \in \mathbb{R}$, et nous voulons prouver que pour la topologie de $\mathbb{R}$ nous avons $\lim_{n\to\infty} \varphi(x_n) = \bar{x}$.

(1) $\varphi(x_k)$ **est de Cauchy**

Soit $\epsilon > 0$ dans $\mathbb{R}$. Nous considérons $\epsilon' \in \mathbb{Q}$ tel que $0 < \epsilon' < \epsilon$. Plus précisément tel que

$$0 < \varphi(\epsilon') < \epsilon. \tag{4.110}$$

Soit $N > 0$ tel que $|x_p - x_q| < \epsilon'$ pour tout $p, q \geqslant N$. Cela existe parce que (x_k) est dans Cauchy dans $\mathbb{Q}$. Nous avons alors

$$\begin{aligned} |\varphi(x_p) - \varphi(x_q)| &= |\varphi(x_p - x_q)| && \text{(4.111a)}\\ &= \varphi\big(|x_p - x_q|\big) && \text{(4.111b)}\\ &\leqslant \varphi(\epsilon') && \text{(4.111c)}\\ &\leqslant \epsilon. && \text{(4.111d)} \end{aligned}$$

Justifications :

- Pour (4.111b). C'est le lemme 4.74.
- Pour (4.111c). L'application φ est croissante, lemme 4.51.

Donc la suite $\varphi(x_k)$ est de Cauchy.

(2) $\varphi(x_k) \xrightarrow{\mathbb{R}} \bar{x}$ Nous devons prouver que pour tout $\epsilon \in \mathbb{R}$, il existe N tel que $n > N$ implique $\varphi(x_n) \in B\big(\bar{x}, \epsilon\big)$. Nous allons faire ça en deux parties. D'abord $\epsilon \in \mathbb{Q}$ et ensuite $\epsilon \in \mathbb{R}$.

(2a) **Avec** $\epsilon \in \mathbb{Q}$ Soit $\epsilon \in \mathbb{Q}$. Puisque x est une suite de Cauchy dans $\mathbb{Q}$, il existe N tel que si $p, n > N$ nous avons

$$x_p - \epsilon < x_n < x_p + \epsilon. \tag{4.112}$$

Ces inégalités sont dans $\mathbb{Q}$. Nous fixons p et nous commençons par écrire plus en détail la première inéquation :

$$x_p - \epsilon - x_n < 0. \tag{4.113}$$

Autrement dit, pour tout n nous avons

$$(\overline{x_p - \epsilon})_n < x_n. \tag{4.114}$$

Pour rappel, la suite $\overline{x_p - \epsilon}$ est la suite constante dans $\mathbb{Q}$. La suite

$$n \mapsto x_n - (\overline{x_p - \epsilon})_n \tag{4.115}$$

est dans $\mathcal{E}^+$. Donc, en vertu de la définition 4.48 nous avons

$$\bar{x} - \overline{x_p - \epsilon} \geqslant 0. \tag{4.116}$$

Nous pouvons aussi bien écrire

$$\bar{x} \geqslant \varphi(x_p) - \varphi(\epsilon). \tag{4.117}$$

En prenant l'autre inégalité de (4.112) nous trouvons de la même manière que

$$\bar{x} \leqslant \varphi(x_p) + \varphi(\epsilon). \tag{4.118}$$

Ces deux inégalités ensemble montrent que

$$\varphi(x_p) \in B\big(\bar{x}, \varphi(\epsilon)\big). \tag{4.119}$$

(2b) **Avec $\epsilon \in \mathbb{R}$** Nous considérons $\epsilon \in \mathbb{R}$ et $\epsilon' \in \mathbb{Q}$ tel que $\varphi(\epsilon') < \epsilon$. Par le point précédent, il existe N tel que $p > N$ implique

$$\varphi(x_p) \in B\big(\bar{x}, \varphi(\epsilon')\big). \tag{4.120}$$

Étant donné que $\varphi(\epsilon') < \epsilon$ nous avons

$$\varphi(x_p) \in B\big(\bar{x}, \varphi(\epsilon')\big) \subset B\big(\bar{x}, \epsilon\big). \tag{4.121}$$

□

PROPooZSQYooWRKNGY

Proposition 4.76.
Soit une suite convergente $x_k \xrightarrow{\mathbb{Q}} q$. Alors

$$\varphi(x_k) \xrightarrow{\mathbb{R}} \varphi(q) \tag{4.122}$$

où φ est la fonction qui à un rationnel fait correspondre la classe de la suite constante correspondante[30].

Démonstration. Le fait d'avoir une convergence $x_k \to q$ dans $\mathbb{Q}$ implique que la suite (x_k) est de Cauchy, par la proposition 4.23(1).

Le lemme 4.75 nous indique que $\varphi(x_k)$ est une suite dans $\mathbb{R}$ qui converge vers $\bar{q}$, la classe de la suite (x_k).

À prouver : $\varphi(x) = \bar{q}$. Autrement dit, nous devons prouver que la classe de la suite constante $a_k = q$ et la classe de la suite x sont les mêmes.

La suite $(x_k - q)$ est de Cauchy dans $\mathbb{Q}$ et converge vers zéro par hypothèse. Donc les suites x et (q) sont dans la même classe. □

PROPooFGBOooHiZqbs

Proposition 4.77 ([1])**.**
Deux choses à propos de suites de rationnels convergeant vers un réel.

ITEMooMAVYooKFtqlx

(1) Soit un réel x. Il existe une suite de rationnels strictement croissante qui converge vers x.

ITEMooVOVYooFUbccG

(2) Si de plus $x > 0$, alors la suite (toujours strictement croissante) peut être choisie parmi les rationnels strictement positifs.

Démonstration. Le lemme 4.60 nous sera d'une grande aide. Soit $x \in \mathbb{R}$. Il existe $q_0 \in \mathbb{Q}$ tel que $x - 1 < q_0 < x$. Ensuite nous construisons la suite par récurrence : q_k est choisi tel que $q_{k-1} < q_k < x$. Cela règle le point (1).

Pour (2). Il suffit de faire la même chose, en partant de $0 < q_0 < x$. □

Notez la grande similitude entre ce théorème et le théorème 9.360. Ils ne sont pas équivalents, ne parlent pas exactement du même objet « $\mathbb{R}$ », ni des mêmes notions de suites de Cauchy et de complétude.

THOooUFVJooYJlieh

Théorème 4.78 (Complétude de $\mathbb{R}$, critère de Cauchy[39])**.**
Nous avons :

(1) Le corps $\mathbb{R}$ est un corps complet (définition 3.249(3))

(2) Une suite dans $\mathbb{R}$ est convergente (définition 3.249(2)) si et seulement si elle est de Cauchy (définition 3.249(1)).

Démonstration. Soit (x_n) une suite de Cauchy dans $\mathbb{R}$. Pour chaque n, il existe par le lemme 4.60 un $y_n \in \mathbb{Q}$ tel que

$$x_n - \frac{1}{n} < y_n < x_n + \frac{1}{n}. \tag{4.123}$$

(1) **(y_n) est une suite de Cauchy dans $\mathbb{Q}$** Nous prouvons que (y_n) est une suite de Cauchy dans $\mathbb{Q}$ (définition 3.249(1)). Vu que (x_n) est de Cauchy pour le corps $\mathbb{R}$, si $\epsilon > 0$ dans $\mathbb{R}$ est donné, il existe n_ϵ tel que si $p, q \geqslant n_\epsilon$, alors $|x_p - x_q| < \epsilon$.

Nous avons :

$$|y_p - y_q| \leqslant |y_p - x_p| + |x_p - x_q| + |x_q - y_q| < \frac{1}{p} + \epsilon + \frac{1}{q}. \tag{4.124}$$

En choisissant $N_\epsilon > \max\{n_\epsilon, \frac{1}{\epsilon}\}$ (ce qui est possible par le lemme 4.57), et en prenant $p, q > N_\epsilon$, nous avons

$$|y_p - y_q| \leqslant 3\epsilon, \tag{4.125}$$

ce qui prouve que (y_p) est une suite de Cauchy dans $\mathbb{Q}$, pour la notion de suite de Cauchy dans $\mathbb{Q}$.

[30] Voir les notations en 4.37.

(2) **Le réel représenté**

Puisque (y_p) est de Cauchy dans $\mathbb{Q}$, elle représente un réel que nous notons $\bar{y}$.

(3) **Convergence de (x_n)**

Nous prouvons que $x_n \xrightarrow{\mathbb{R}} \bar{y}$.

Nous savons qu'une suite de Cauchy de rationnels converge dans $\mathbb{R}$ vers le réel qu'elle représente, c'est-à-dire : $y_n \xrightarrow{\mathbb{R}} \bar{y}$ où chaque $y_n \in \mathbb{Q}$ est vu comme la suite constante (cela est le lemme 4.75). Autrement dit, pour $\epsilon > 0$, il existe un $N_\epsilon \in \mathbb{N}$ tel que si $p > N_\epsilon$ alors $|\bar{y} - y_p| < \epsilon$. Pour un tel p nous avons

$$|\bar{y} - x_p| \leqslant |\bar{y} - y_p| + |y_p - x_p| \leqslant \epsilon + \frac{1}{p}. \tag{4.126}$$

Donc dès que p est plus grand que $\max\{N_\epsilon, \frac{1}{\epsilon}\}$, nous avons $|\bar{y} - x_p| < 2\epsilon$, ce qui signifie que la suite (x_n) converge vers $\bar{y}$ dans $\mathbb{R}$.

Ceci achève de prouver que $\mathbb{R}$ est un corps complet.

En ce qui concerne l'équivalence entre les suites convergentes et de Cauchy, nous venons de prouver que toute suite de Cauchy dans $\mathbb{R}$ est convergente. La réciproque est la proposition 4.22.

□

Nous avons terminé avec la construction des réels. Les propriétés topologiques arrivent en la section 11.3. En particulier le théorème 9.360 pour la complétude de $\mathbb{R}$ en tant qu'espace métrique.

LEMooSWBTooSkmheK

Lemme 4.79 ([1]).
Soit $\epsilon > 0$. Si $a, x \in \mathbb{R}$ vérifient $|x - a| < \epsilon$ alors $x < a + \epsilon$ et $x > a - \epsilon$.

4.4.5 Intervalles

Nous avons déjà défini la notion d'intervalle pour un espace totalement ordonné en 1.31.

LEMooCZLZooTtkXgR

Lemme 4.80 ([1]).
Si I et J sont des intervalles, alors $I \setminus J$ est une union de 0, 1 ou 2 intervalles.

PROPooJEXCooHwHAKq

Proposition 4.81 ([1]).
Soient un intervalle I et des intervalles $\{I_k\}_{k=1,\dots,n}$ tels que $I = \bigcup_{k=1}^{n} I_k$. Alors il existe des intervalles $\{J_i\}_{i=1,\dots,m}$ tels que

(1) $I = \bigcup_{i=1}^{m} J_i$,

(2) les J_i sont disjoints,

(3) pour tout $i = 1, \dots, m$, il existe un $k = 1, \dots, n$ tel que $J_i \subset I_k$.

Démonstration. Nous posons

$$\begin{cases} A_1 = I_1 & \text{(4.127a)} \\ A_k = I_k \setminus \bigcup_{l=1}^{k-1} A_l. & \text{(4.127b)} \end{cases}$$

Les A_k sont par construction disjoints. Avec une récurrence utilisant le lemme 4.80, on démontre que si A_k est une union finie disjointe d'intervalles, alors A_{k+1} aussi.

Finalement $I = \bigcup_{k=1}^{n} A_k$ est donc une union finie d'intervalles disjoints. □

4.4.6 Maximum, supremum et compagnie

Ce n'est un secret pour personne que $\mathbb{R}$ est un ensemble totalement ordonné[31] : il y a des éléments plus grands que d'autres, et mieux : à chaque fois que je prends deux éléments différents dans $\mathbb{R}$, il y en a un des deux qui est plus grand que l'autre. Il n'y a pas d'*ex æquo* dans $\mathbb{R}$.

La définition du maximum d'une partie est la définition 1.32.

[31] Proposition 4.49.

Proposition 4.82.
Soient $x_1, \dots, x_k \in \mathbb{R}$. Alors nous avons

$$\frac{1}{\min(x_i)} = \max\left(\frac{1}{x_i}\right). \tag{4.128}$$

Démonstration. En effet notons $y = \min(x_i)$. Nous avons alors $1/x_i \leqslant 1/y$ pour tout i. □

Définition 4.83.
Soit A, une partie de $\mathbb{R}$.

*(1) Un nombre M est un **majorant** de A si M est plus grand que tous les éléments de A : pour tout $x \in A$, $M \geqslant x$.*

*(2) Un nombre m est un **minorant** de A si m est plus petit que tous les éléments de A : pour tout $x \in A$, $m \leqslant x$.*

Nous parlons de majorant ou de minorants stricts *lorsque les inégalités sont strictes.*

Nous insistons sur le fait que l'inégalité n'est pas stricte. Ainsi, 1 est un majorant de $[0, 1]$. Dès qu'un ensemble a un majorant, il en a plein. Si s majore l'ensemble A, alors $s+1$, $s+4$, et $s+\frac{3}{7}$ majorent également A.

Exemple 4.84.
Une petite galerie d'exemples de majorants.

- L'intervalle fermé $[4, 8]$ admet entre autres 8 et 130 comme majorants,
- l'intervalle ouvert $]4, 8[$ admet également 8 et 130 comme majorants,
- 7 n'est pas un majorant de $[1, 5] \cup]8, 32]$,
- 10/10 majore les notes qu'on peut obtenir à un devoir.
- l'intervalle $[4, \infty[$ n'a pas de majorant.

△

DefSupeA

Proposition-Définition 4.85 (Least-upper-bound property[141])**.**
Soit A une partie majorée de $\mathbb{R}$. Il existe un unique élément $M \in \mathbb{R}$ tel que

(1) $M \geqslant x$ pour tout $x \in A$,

(2) pour tout ε, le nombre $M - \varepsilon$ n'est pas un majorant de A, c'est-à-dire qu'il existe un élément $x \in A$ tel que $x > M - \varepsilon$.

*Cet élément est nommé **supremum** de A et est noté* $\sup(A)$*. De la même façon, **l'infimum** de A, noté* $\inf A$ *est l'unique réel $m \in \mathbb{R}$ vérifiant*

(1) $m \leqslant a$ pour tout $a \in A$,

(2) pour tout $\epsilon > 0$, le nombre $m + \epsilon$ n'est pas un minorant : il existe $a \in A$ tel que $a \leqslant m + \epsilon$.

Par convention, si la partie n'est pas bornée vers le haut, nous dirons que son supremum n'existe pas, ou bien qu'il est égal à $+\infty$, suivant les contextes. Pour votre culture générale, sachez toutefois que $\infty \notin \mathbb{R}$.

Démonstration. Nous faisons la preuve pour l'infimum.

(1) **Unicité**

En ce qui concerne l'unicité, soient m_1 et m_2, deux infimums de A. Supposons $m_1 > m_2$. Alors il existe $\epsilon > 0$ tel que $m_2 < m_2 + \epsilon < m_1$ (c'est le lemme 4.60). Cela prouve que $m_2 + \epsilon$ est un minorant de A et donc que m_2 n'est pas un infimum.

(2) **Existence**

Soit A, une partie de $\mathbb{R}$. Nous allons trouver son infimum en suivant une méthode de dichotomie. Pour cela nous allons construire trois suites en même temps de la façon suivante. D'abord nous choisissons un point x_0 de A et un point x_1 qui minore A (qui existe par hypothèse) :

$$\begin{aligned} &x_0 \text{ est un élément de } A,\\ &x_1 \text{ est un minorant de } A,\\ &a_0 = x_0\\ &b_0 = x_1\\ &b_1 = x_1. \end{aligned} \tag{4.129}$$

Ensuite, nous faisons la récurrence suivante :

$$\begin{aligned} x_{n+1} &= \frac{a_n + b_n}{2},\\ a_{n+1} &= \begin{cases} a_n & \text{si } x_{n+1} \text{ minore } A\\ x_{n+1} & \text{sinon,} \end{cases}\\ b_{n+1} &= \begin{cases} x_{n+1} & \text{si } x_{n+1} \text{ minore } A\\ b_n & \text{sinon.} \end{cases} \end{aligned} \tag{4.130}$$

Nous allons montrer que (a_n) et (b_n) sont des suites convergentes de même limite et que cette limite est l'infimum de A.

Soit $n \in \mathbb{N}$; il y a deux possibilités. Soit $a_n = a_{n-1}$ et $b_n = x_n$, soit $a_n = x_n$ et $b_n = b_{n-1}$. Supposons que nous soyons dans le premier cas (le second se traite de façon similaire). Alors nous avons

$$\begin{aligned} |a_n - b_n| &= |a_{n-1} - x_n|\\ &= \left|a_{n-1} - \frac{a_{n-1} + b_{n-1}}{2}\right|\\ &= \frac{1}{2}|a_{n-1} - b_{n-1}|, \end{aligned} \tag{4.131}$$

ce qui prouve que $|a_n - b_n| \to 0$. Nous montrons maintenant que la suite (a_n) est de Cauchy. En effet nous avons

$$|a_n - a_{n-1}| = \begin{cases} 0\\ \left|\frac{a_n - b_n}{2}\right| \end{cases} \leqslant \frac{1}{2n}. \tag{4.132}$$

Il en est de même pour la suite (b_n). Ce sont deux suites de Cauchy (donc convergentes par la proposition 4.22) qui convergent vers la même limite. Soit ℓ cette limite.

Le nombre ℓ minore A. En effet si $a \in A$ est plus petit que ℓ, les éléments b_n tels que $|b_n - \ell| < |a - \ell|$ ne peuvent pas minorer A. D'autre part, pour tout ϵ, le nombre $\ell + \epsilon$ ne peut pas minorer A. En effet, ℓ est la limite de la suite décroissante (a_n), donc il existe a_n entre ℓ et $\ell + \epsilon$. Mais a_n ne minore pas A, donc $\ell + \epsilon$ ne minore pas non plus A.

Nous avons prouvé que toute partie minorée de $\mathbb{R}$ possède un infimum.

La preuve que toute partie majorée possède un supremum se fait de la même façon. □

LEMooSSVKooDPhSkq

Lemme 4.86.
Soit une partie A de $\mathbb{R}$. Si M est un majorant de A, alors $M \geqslant \sup(A)$.

Démonstration. Si $M < \sup(A)$, alors en posant $\epsilon = \sup(A) - M$, le nombre $\sup(A) - \epsilon$ est encore un majorant de A, ce qui est impossible par définition d'un supremum. □

PROPooGOPOooYyZSuU

Proposition 4.87 ([1])**.**
Soit $A \subset \mathbb{R}$. Alors

ITEMooAQNRooXFnsrA

(1) Si $\lambda \geqslant 0$, nous avons $\inf(\lambda A) = \lambda \inf(A)$.

ITEMooPCDXooRJraYV

(2) Si $\lambda \geqslant 0$, nous avons $\sup(\lambda A) = \lambda \sup(A)$.

ITEMooHPBEooGaKRDf

(3) Si $\lambda \leqslant 0$, nous avons $\inf(\lambda A) = \lambda \sup(A)$.

(4.133)

Démonstration. En plusieurs parties. Vérification des conditions de la définition 4.85.

(1) **Pour (1)** Nous posons $m = \inf(A)$, et nous prouvons que $\lambda m = \inf(\lambda A)$. Si $a \in A$, alors $m \leqslant a$ et donc $\lambda m \leqslant \lambda a$ par la proposition 4.55. Donc λm minore λA.

Vu que $m = \inf(A)$, si $\epsilon > 0$, il existe $a \in A$ tel que $m + \epsilon/\lambda \geqslant a$. Donc, en multipliant par λ, $\lambda m + \epsilon \geqslant \lambda a$. Et donc $\lambda m + \epsilon$ ne minore pas λA.

(2) **Pour (2)** Même raisonnement que pour (1)[32].

(3) **Pour (3) avec $\lambda = -1$** Nous posons $s = \sup(A)$, et nous pouvons que $-s = \inf(-A)$. Soit $a \in A$. Nous avons $s \geqslant a$, et donc $-s \leqslant -a$, de telle sorte que $-s$ minore $-A$.

Soit $\epsilon > 0$. Nous voulons un $a \in A$ tel que $-s + \epsilon \geqslant a$. Vu que $s = \sup(A)$, il existe $a \in A$ tel que $a > s - \epsilon$, et donc, en multipliant par -1 : $-a < -s + \epsilon$.

(4) **Pour (3), cas général** Nous posons $\lambda = -\lambda'$ avec $\lambda' > 0$. Nous avons alors

$$\begin{aligned}
\inf(\lambda A) &= \inf\big(-(\lambda' A)\big) && && (4.134a)\\
&= -\sup(\lambda' A) && \text{cas } \lambda = -1 && (4.134b)\\
&= -\lambda' \sup(A) && \text{par (2)} && (4.134c)\\
&= \lambda \sup(A). && && (4.134d)
\end{aligned}$$

□

LEMooTRJZooSTuHWs

Lemme 4.88.
Soit une partie bornée A dans $\mathbb{R}$. Si (x_n) est une suite dans A convergente vers $\sup(A)$, alors il existe une sous-suite croissante qui converge également vers $\sup(A)$.

Démonstration. Nous posons $s = \sup(A)$, et nous construisons en parallèle une suite (y_n) et une application $\varphi\colon \mathbb{N} \to \mathbb{N}$ par récurrence. D'abord nous posons

$$\begin{cases} y_1 = \min\{x_k \text{ tel que } x_k \in B(s,1)\} & (4.135a)\\ \varphi(1) = \min\{k \text{ tel que } x_k = y_1\}. & (4.135b) \end{cases}$$

et ensuite la récurrence :

$$\begin{cases} y_{n+1} = \min\{x_k \text{ tel que } k > \varphi(n), x_k \in B(s, 1/(n+1))\} & (4.136a)\\ \varphi(n+1) = \min\{k > \varphi(n) \text{ tel que } x_k = y_{n+1}\}. & (4.136b) \end{cases}$$

Voyons que ces définitions fonctionnent. D'abord y_{n+1} est bien défini quelle que soit la valeur $\varphi(n)$ parce qu'à partir d'un certain rang, tous les x_k sont dans $B(s, 1/(n+1))$. De plus (y_n) est bien une suite croissante parce que le minimum est pris sur des ensembles de plus en plus petits. Et enfin $y_n \to s$ parce que $y_n \in B(s, 1/n)$. □

4.4.6.1 Intervalles

LEMooRMUCooMKiTGr

Lemme 4.89 ([1]).
Soit une partie A de $\mathbb{R}$.

ITEMooIQECooFjJFKz

(1) Nous supposons que A admette un supremum qui n'est pas dans A. Si x est un élément de A strictement plus petit que $\sup(A)$, alors il existe $y \in A$ tel que $x < y < \sup(A)$.

(2) Nous supposons que A admette un infimum qui n'est pas dans A. Si x est un élément de A strictement plus grand que $\inf(A)$, alors il existe $y \in A$ tel que $\inf(A) < y < x$.

Démonstration. Soit $\epsilon > 0$. Par définition 4.85 d'un supremum, le nombre $\sup(A) - \epsilon$ n'est pas un majorant de A. Autrement dit, il existe $y \in A$ tel que $y > \sup(A) - \epsilon$. Vu que $\sup(A)$ est plus grand que tous les éléments de A et qu'il n'est pas lui-même dans A, nous avons aussi $\sup(A) > y$. En mettant bout à bout :

$$x < \sup(A) - \epsilon < y < \sup(A). \tag{4.137}$$

□

[32] J'ai pas vraiment vérifié. Écrivez-moi si ça pose problème.

PROPooHPMWooQJXCAS

Proposition 4.90 ([1]).
Tous les intervalles[33] *de* $\mathbb{R}$ *sont d'une des formes suivantes :*

(1) $]a,b[= \{x \in \mathbb{R} \text{ tel que } a < x < b\}$

(2) $[a,b[= \{x \in \mathbb{R} \text{ tel que } a \leqslant x < b\}$

(3) $]a,b] = \{x \in \mathbb{R} \text{ tel que } a < x \leqslant b\}$

(4) $[a,b] = \{x \in \mathbb{R} \text{ tel que } a \leqslant x \leqslant b\}$

(5) $]-\infty,a] = \{x \in \mathbb{R} \text{ tel que } x \leqslant a\}$

(6) $]-\infty,a[= \{x \in \mathbb{R} \text{ tel que } x < a\}$

(7) $]a,\infty[= \{x \in \mathbb{R} \text{ tel que } x > a\}$

(8) $[a,\infty[= \{x \in \mathbb{R} \text{ tel que } x \geqslant a\}$.

(9) $]-\infty,\infty[= \mathbb{R}$.

Démonstration. Il y a beaucoup de cas, et nous ne les feront pas tous[34].

(1) **Si I est borné vers le haut et vers le bas** Il y a 4 possibilités suivant que $\inf(I)$ et $\sup(I)$ soient ou non dans I.

(2) **Si $\inf(I) \in I$ et $\sup(I) \in I$** Nous prouvons que $I = [\inf(I), \sup(I)]$.

(2a) **Dans un sens** Si $x \in I$ nous avons $\inf(I) \leqslant x \leqslant \sup(I)$ parce que $\inf(I)$ est un minorant de toute élément de I alors que $\sup(I)$ est un majorant de tout élément de I. Donc $x \in [\inf(I), \sup(I)]$.

(2b) **Dans l'autre sens** Soit $\inf(I) \leqslant x \leqslant \sup(I)$. Vu que I est un intervalle et que $\sup(I)$ et $\inf(I)$ sont deux éléments de I, nous avons $x \in I$.

(3) **$\inf(I) \in I$ et $\sup(I) \notin I$** Nous allons démontrer que $I = [\inf(I), \sup(I)[$.

(3a) **Dans un sens** Soit $x \in I$. Nous savons (par définition de l'infimum et du supremum) que $\inf(I) \leqslant x \leqslant \sup(x)$. Mais nous sommes dans un cas où $\sup(I) \neq x$ parce que $\sup(I)$ n'est pas dans I. Donc

$$\inf(I) \leqslant x < \sup(I), \tag{4.138}$$

ce qui montre que $I \subset [\inf(I), \sup(I)[$.

(3b) **Dans l'autre sens** Soit $x \in [\inf(I), \sup(I)[$. Nous utilisons le lemme 4.89(1) : il existe $y \in I$ tel que $\inf(I) \leqslant x < y < \sup(I)$. Vu que $\inf(I) \in I$, que $y \in I$ et que I est un intervalle, nous avons aussi $x \in I$ et donc $I \subset [\inf(I), \sup(I)[$.

(4) **$\inf(I) \notin I$ et $\sup(I) \in I$** C'est le même raisonnement, mais en utilisant l'autre partie du lemme.

(5) **$\inf(I) \notin I$ et $\sup(I) \notin I$** Nous prouvons que $I =]\inf(I), \sup(I)[$.

(5a) **Dans un sens** Nous avons

$$I \subset \{x \in \mathbb{R} \text{ tel que } \inf(I) \leqslant x \leqslant \sup(I)\}. \tag{4.139}$$

Mais comme $\inf(I)$ et $\sup(I)$ ne sont pas dans I, nous pouvons les enlever dans le membre de droite :

$$I \subset \{x \in \mathbb{R} \text{ tel que } \inf(I) < x < \sup(I)\} =]\inf(I), \sup(I)[. \tag{4.140}$$

(5b) **Dans l'autre sens** Si $x \in I$, nous avons $\inf(I) < x < \sup(I)$. En utilisant les deux parties du lemme, nous avons y_1 et y_2 dans I tels que

$$\inf(I) < y_1 < x < y_2 < \sup(I). \tag{4.141}$$

Vu que I est un intervalle, nous en déduisons que $x \in I$.

[33] Définition 1.31.
[34] Si vous avez un doute, écrivez-moi.

(6) $\inf(I) = -\infty$, $\sup(I) \in I$ Nous prouvons que $I =]-\infty, \sup(I)]$.

(6a) **Dans un sens** L'inclusion $I \subset \{x \in \mathbb{R} \text{ tel que } x \leqslant \sup(I)\}$ est automatique : $\sup(I)$ majore tous les éléments de I.

(6b) **Dans l'autre sens** Soit $x \leqslant \sup(I)$. Vu que I n'a pas d'infimum, il existe $y \in I$ tel que $y < x < \sup(I)$. Comme I est un intervalle nous déduisons que $x \in I$.

Je vous laisse voir les autres cas. □

4.4.6.2 Quelques exemples

En matière de notations, le maximum de l'ensemble A est noté $\max A$, le supremum est noté $\sup A$. Le minimum et l'infimum sont notés $\min A$ et $\inf A$.

Exemple 4.91.
Exemples de différence entre majorant, supremum et maximum.

- Le nombre 10 est un supremum, majorant et maximum de l'intervalle fermé $[0, 10]$,
- Le nombre 10 est un majorant et un supremum, mais pas un maximum de l'intervalle ouvert $]0, 10[$,
- Le nombre 136 est un majorant, mais ni un maximum ni un supremum de l'intervalle $[0, 10]$.

△

En utilisant les notations concises, ces différents cas s'écrivent ainsi :

$$10 = \max[0, 10] = \sup[0, 10] \quad 10 = \sup[0, 10[\tag{4.142}$$

Exemple 4.92.
Si on dit qu'un pont s'effondre à partir d'une charge de 10 tonnes, alors 10 tonnes est un *supremum* des charges que le pont peut supporter : si on met $9,999999$ tonnes dessus, il tient encore le coup, mais si on ajoute un gramme, alors il s'effondre (on sort de l'ensemble des charges acceptables). △

Exemple 4.93.
Si on dit qu'un pont résiste jusqu'à 10 tonnes, alors 10 tonnes est un *maximum* de la charge acceptable. Sur ce pont-ci, on peut ajouter le dernier gramme. Mais à partir de là, le moindre truc qu'on ajoute, il s'effondre. △

LEMooWCUXooFqTwDK

Lemme 4.94.
À propos de bornes d'un intervalle dans $\mathbb{R}$.

(1) La borne inférieure[35] *d'un intervalle est son infimum,*

(2) la borne supérieure est le supremum.

(3) Si de plus l'intervalle est fermé, l'infimum est un minimum et le supremum est un maximum.

Démonstration. Soit I un des intervalles $[a, b]$, $[a, b[$, $]a, b]$, $]a, b[$. Nous allons montrer que dans tous ces cas, a est l'infimum de I.

Nous allons prouver que dans tous ces cas, $a = \int(I)$ en vérifiant les deux conditions de la définition 4.85. D'abord par définition d'un intervalle, pour tout $t \in I$ nous avons $t \geqslant a$. Première condition vérifiée. Ensuite, nous prenons $\epsilon > 0$. Si $a + \epsilon \geqslant b$, alors n'importe quel élément de I est plus petit que $a + \epsilon$. Si $a + \epsilon < b$, alors nous avons

$$a < a + \epsilon < b. \tag{4.143}$$

Dans ce cas, le lemme 4.60 donne un réel t tel que $a < t < a + \epsilon < b$. Donc $t \in I$ et $a + \epsilon$ n'est pas un minorant de I. □

Exemple 4.95.
Quelques exemples dans les intervalles.

(1) $A = [1, 2]$. Tous les nombres plus petits ou égaux à 1 sont minorants, 1 est infimum et minimum. Le nombre 2 est un majorant, le maximum et le supremum.

[35] Ici par « borne inférieure » nous entendons le a dans les intervalles du type $]a, b]$, $[a, b]$, etc.

(2) $B =]3, \pi[$. Le nombre π est le supremum et est un majorant, mais n'est pas le maximum (parce que $\pi \notin B$). L'ensemble B n'a pas de maximum. Bien entendu, -1000 est un minorant.

Dans les deux cas, le nombre 53 est un majorant. △

Il existe évidemment de nombreux exemples plus vicieux.

Exemple 4.96.
Prenons $E = \{\frac{1}{n} \text{ tel que } n \in \mathbb{N}_0\}$, dont les premiers points sont indiqués sur la figure 4.1. Cet ensemble est constitué des nombres 1, $\frac{1}{2}$, $\frac{1}{3}$, … Le plus grand d'entre eux est 1 parce que tous les nombres de la forme $\frac{1}{n}$ avec $n \geqslant 1$ sont plus petits ou égaux à 1. Le nombre 1 est donc maximum de E.

L'ensemble E n'a par contre pas de minimum parce que tout élément de E s'écrit $\frac{1}{n}$ pour un certain n et est plus grand que $\frac{1}{n+1}$ qui est également dans E.

Prouvons que zéro est l'infimum de E. D'abord, tous les éléments de E sont strictement positifs, donc zéro est certainement un minorant de E. Ensuite, nous savons que pour tout $\varepsilon > 0$, il existe un n tel que $\frac{1}{n}$ est plus petit que ε. L'ensemble E possède donc un élément plus petit que $0 + \varepsilon$, et zéro est bien l'infimum. △

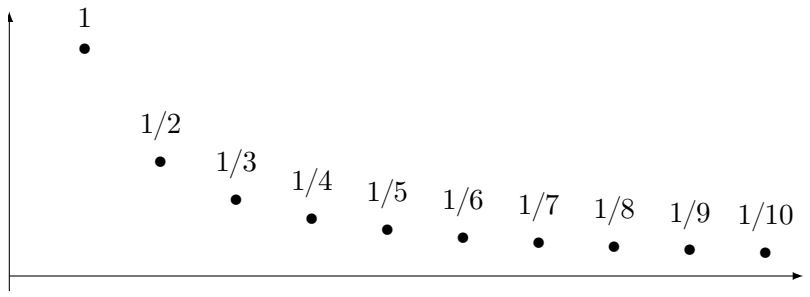


FIGURE 4.1 : Les premiers points du type $x_n = 1/n$.

LabelFigSuiteUnSurn

L'exemple suivant est une source classique d'erreurs en ce qui concerne l'infimum.

Exemple 4.97.
Les premiers points de l'ensemble $F = \{\frac{(-1)^n}{n} \text{ tel que } n \in \mathbb{N}_0\}$ sont représentés à la figure 4.2. Bien que (comme nous le verrons plus tard) la limite de la suite $x_n = (-1)^n/n$ soit zéro, il n'est pas correct de dire que zéro est l'infimum de l'ensemble F. Le dessin, au contraire, montre bien que -1 est le minium (aucun point est plus bas que -1), tandis que le maximum est $1/2$.

Nous reviendrons avec cet exemple dans la suite. Pour l'instant, ayez bien en tête que zéro n'est rien de spécial pour l'ensemble F en ce qui concerne les notions de maximum, minimum et compagnie. △

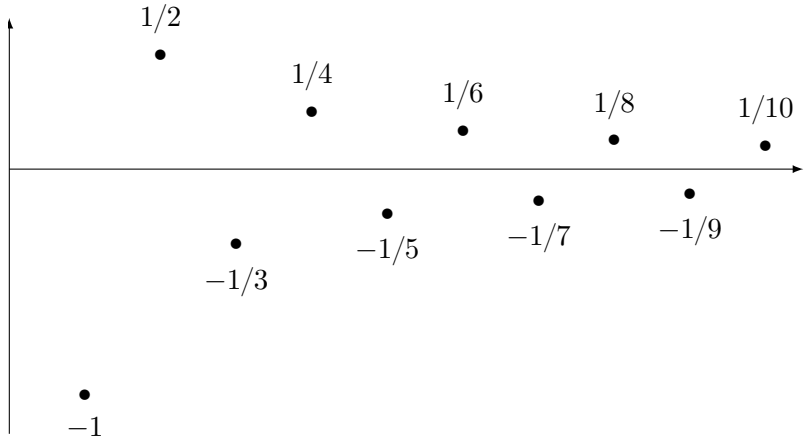


FIGURE 4.2 : Les quelques premiers points du type $(-1)^n/n$.

LabelFigSuiteInverseAlterne

PROPooQULXooVzUtAi

Proposition 4.98 ([1])**.**
Soient un ensemble E.

ITEMooBOMOooTDUpgb

(1) *Soit une partie $A \subset E$. Soient deux applications $f, g\colon E \to \mathbb{R}^+$. Nous avons*

$$\sup_{x\in A}\big(f(x)+g(x)\big) \leqslant \sup_{x\in A} f(x) + \sup_{x\in A} g(x). \tag{4.144}$$

ITEMooMWCRooSqwXgN

(2) *Si $A \subset \mathbb{R}^+$ et si $\lambda \geqslant 0$ alors*

$$\sup(\lambda A) = \lambda \sup(A). \tag{4.145}$$

4.4.7 Racines

SUBSECooMBCNooEqjjTY

Dans cette section, nous définissons $\sqrt{x}$ pour $x \in \mathbb{Q}^+$. Vous notez que c'est fait de façon assez algébrique[36], ou en tout cas, en restant proche des définitions. Des définitions plus technologiques utilisant la continuité de $x \mapsto x^n$ et qui prouvent que l'application est bijective sur un domaine choisi avec prudence existent (voir la définition 14.420). Il est même expliqué dans [136] que la méthode décrite ici permet de définir $\sqrt[n]{x}$ pour tout n entier, et pas seulement pour $n = 2$.

PROPooUHKFooVKmpte

Proposition 4.99.
Soit $q \in \mathbb{Q}^+$. Il existe un unique $r \in \mathbb{R}$ tel que $r^2 = q$.

Plus précisément, en termes des notations de 4.37, pour tout $q \in \mathbb{Q}^+$, il existe un unique $r \in \mathbb{R}^+$ tel que $r^2 = \varphi(q)$.

Démonstration. En deux parties : d'abord l'existence et ensuite l'unicité.

(1) **Existence** Si $q = 0$, c'est $r = 0$. Nous supposons $q > 0$. La suite (x_k) de la proposition 4.30 a la propriété d'être de Cauchy dans $\mathbb{Q}$. Donc il existe un réel r qui est la classe de cette suite. Nous posons donc

$$r = \bar{x}. \tag{4.146}$$

En ce qui concerne r^2, nous avons, par définition du produit dans $\mathbb{R}$,

$$r^2 = \bar{x}^2 = \overline{(x_k^2)}, \tag{4.147}$$

EQooPHLFooAZhchM

c'est la classe de la suite de Cauchy donnée par les x_k^2. Posons $y_k = x_k^2$; la relation (4.147) s'écrit

$$r^2 = \bar{y}. \tag{4.148}$$

La proposition 4.30 nous dit également que y est une suite de Cauchy et que

$$y_k \xrightarrow{\mathbb{Q}} q \tag{4.149}$$

La proposition 4.76 donne alors $\bar{y} = \bar{q}$, et finalement

$$r^2 = \bar{q} = \varphi(q). \tag{4.150}$$

Ici tout n'est pas encore terminé avec l'existence parce qu'il faut nous assurer que $r \geqslant 0$. Ce n'est pas très compliqué : si $r < 0$, alors nous pouvons faire le choix $-r$ qui convient tout aussi bien : $(-r)^2 = r^2$.

(2) **Unicité** Supposons $r_1, r_2 \in \mathbb{R}$ tels que $r_1^2 = r_2^2$. La proposition 4.49 dit que $\mathbb{R}$ est totalement ordonné ; disons pour fixer les idées que $r_1 \leqslant r_2$. Cela signifie, par définition de l'ordre sur $\mathbb{R}$, que $r_2 - r_1 \geqslant 0$. En posant $s = r_2 - r_1$ nous avons $r_2 = r_1 + s$. Passons au carré ; la distribution dans le calcul suivant provient du fait que $\mathbb{R}$ est un corps :

$$r_2^2 = (r_1 + s)^2 = r_1^2 + 2r_1 s + s^2. \tag{4.151}$$

Vu que $r_1^2 = q = r_2^2$, nous avons $2r_1 s + s^2 = 0$ ou encore

$$s(2r_1 + s) = 0. \tag{4.152}$$

Puisque $\mathbb{R}$ est un corps, c'est un anneau intègre[37] et la règle du produit nul s'applique : soit $s = 0$, soit $2r_2 + s = 0$. Puisque $r_2 > 0$ et que $s \geqslant 0$, nous avons $2r_2 + s > 0$ et donc $s = 0$.

Nous en déduisons que $r_1 = r_2$.

□

[36] Discutable parce que des limites sont utilisées.
[37] Lemme 3.23.

4.4.8 Partie entière, partie fractionnaire

LEMooLEXTooGAQxGB

Lemme-Définition 4.100 ([142]).
Pour tout réel x, il existe un unique entier n vérifiant

$$n \leqslant x < n+1. \tag{4.153}$$

Dans ce cas nous avons $x-n \in [0,1[$.

*Le nombre n ainsi défini est la **partie entière** de x, et il sera noté $\text{int}(x)$. Le nombre $x-\text{int}(x)$ est la **partie fractionnaire** de x que nous notons $\text{frac}(x)$.*

Démonstration. En plusieurs parties.

(1) **Existence** Soit $x \in \mathbb{R}$. Nous posons $A = \{n \in \mathbb{N} \text{ tel que } n \leqslant x\}$. Le lemme 4.57 dit qu'il existe $p \in \mathbb{N}$ tel que $p > x$. Donc $A \subset \{0,\dots,p\}$ et A est fini.

Le lemme 2.31 dit alors que A possède un maximum. En posant $n = \max(A)$ nous avons $n \leqslant x$ mais aussi $x < n+1$ parce que si $x \leqslant n+1$ nous aurions $n+1 \in A$, et n ne serait pas le maximum.

(2) **Unicité** Supposons que m et n aient les propriétés d'être une partie entière de x. Nous avons

$$\begin{cases} n \leqslant x & \text{EQooBVZLooQGJgTm} \quad (4.154a)\\ x < n+1 & \text{EQooLXPSooEkiSee} \quad (4.154b)\\ m \leqslant x & \text{EQooJQTDooSUowlT} \quad (4.154c)\\ x < m+1 & \text{EQooPFJWooPoeyoT} \quad (4.154d) \end{cases}$$

Supposons pour fixer les ides que $m \geqslant n$. Nous avons

$$\begin{aligned} m-n &\leqslant x-n && \text{par (4.154c)} && (4.155a)\\ &< n+1-n && \text{par (4.154b)} && (4.155b)\\ &= 1 && && (4.155c) \end{aligned}$$

Donc $m-n$ est un entier positif strictement inférieur à 1. Donc $m-n=0$.

(3) **L'encadrement** En partant de $n \leqslant x < n+1$ et en soustrayant n à tous les membres, nous trouvons $0 \leqslant x-n < 1$, qui signifie $x-n \in [0,1[$.

□

4.101.
Il est toutefois à noter que la partie fractionnaire de x n'est pas garantie d'être une fraction : elle pourrait être irrationnelle. Cette dénomination est donc un peu trompeuse.

LEMooMMSAooFiRkQd

Lemme 4.102.
Si $\lambda \in \mathbb{R}$ n'est pas un entier, alors $\text{int}(\lambda)+2 > \lambda$.

Démonstration. Par le définition 4.100, nous avons

$$\text{int}(\lambda) \leqslant \lambda \leqslant \text{int}(\lambda)+1 < \text{int}(\lambda)+2. \tag{4.156}$$

□

4.4.9 Le tore

4.103.
Cette section sur le tore est juste un avant-gout pour insister sur les classes d'équivalences. Ce que vous voulez réellement savoir est dans 12.0.4. Notez que la fonction τ qui sera définie là-bas n'est pas exactement la même que celle sur laquelle nous travaillons ici.

Bref, je crois que vous pouvez sauter cette partie sur le tore.

DEFooRWLLooHkdFDN

Définition 4.104 ([1]).
Nous considérons la relation d'équivalence $x \sim y$ si $x-y \in \mathbb{Z}$ sur $\mathbb{R}$. Et la relation $(x,y) \sim (x',y')$ si $x-x' \in \mathbb{Z}$ et $y-y' \in \mathbb{Z}$ sur $\mathbb{R}^2$.

DEFooTSSTooOFPxzu

Définition 4.105 ([1]).
*Le **tore** de $\mathbb{R}^2$ est l'ensemble $\mathbb{R}^2/\sim$. Nous le notons T.*

Nous considérons l'application

$$\begin{aligned}\tau\colon \mathbb{R} &\to]-\frac{1}{2},\frac{1}{2}] \\ x &\mapsto \begin{cases}\text{frac}(x) & \text{si } \text{frac}(x)\leqslant 1/2\\ \text{frac}(x)-1 & \text{si } \text{frac}(x)<1/2\end{cases}\end{aligned} \tag{4.157}$$

où $\text{frac}\colon \mathbb{R}\to[0,1[$ est la partie fractionnaire définie par le lemme 4.100. Nous posons aussi

$$\begin{aligned}\tau\colon \mathbb{R}^2 &\to]\frac{1}{2},\frac{1}{2}]\times]-\frac{1}{2},\frac{1}{2}] \\ (x,y) &\mapsto \big(\tau(x),\tau(y)\big).\end{aligned} \tag{4.158}$$

Notez que si $y=x+k$ avec $k\in\mathbb{Z}$, nous avons $\tau(y)=\tau(x)$, donc nous pouvons poser

$$\begin{aligned}\tau\colon \mathbb{R}/\sim &\to]-\frac{1}{2},\frac{1}{2}] \\ [x] &\mapsto \tau(x).\end{aligned} \tag{4.159}$$

Et enfin nous posons

$$\begin{aligned}\tau\colon T &\to]-\frac{1}{2},\frac{1}{2}]\times]-\frac{1}{2},\frac{1}{2}] \\ [(x,y)] &\mapsto \big(\tau(x),\tau(y)\big).\end{aligned} \tag{4.160}$$

EQooCRZHooMNPBDo

Tout cela pour rapporter le tore au carré de côté 1 centré en $(0,0)$.

PROPooNRNGooJahxQv

Proposition 4.106 ([1]).
Soit $x\in\mathbb{R}$. Parmi les éléments de $A_x=\{x+k \text{ tel que } k\in\mathbb{Z}\}$, l'élément le plus proche de 0 est $\tau(x)$.

Démonstration. Nous avons $\tau(x)\in\,]-1/2,1/2]$. Nommons y l'élément de A_x le plus proche de zéro. Si $1/2\in A_x$, alors c'est lui le plus proche : $y=1/2$. Dans ce cas nous avons $|\tau(x)|\leqslant 1/2=y$.

Si $1/2$ n'est pas dans A_x, alors l'hypothèse $|y|\leqslant|\tau(x)|$ donne $|y|<1/2$. Nous avons alors

$$|\tau(x)-y|\leqslant|\tau(x)|+|y|<1, \tag{4.161}$$

ce qui est impossible parce que $\tau(x)-y\in\mathbb{Z}$. □

LEMooQAQPooGGumSe

Lemme 4.107 ([1]).
Pour tout $\alpha,\beta,\gamma\in T$ nous avons

$$d(\alpha+\gamma,\beta+\gamma)=d(\alpha,\beta). \tag{4.162}$$

Démonstration. Soient $x\in\alpha$, $y\in\beta$ et $z\in\gamma$. Nous avons $\alpha+\gamma=[a+z]$ et $\beta+\gamma=[b+z]$, de telle sorte que

$$\begin{aligned}d(\alpha+\gamma,\beta+\gamma)&=\inf_{\substack{a\in\alpha+\gamma\\ b\in\beta+\gamma}}f(a,b) && \text{(4.163a)}\\ &=\inf_{\substack{k\in\mathbb{Z}^2\\ l\in\mathbb{Z}^2}}d(a+z+k,b+z+l) && \text{(4.163b)}\\ &=\inf_{\substack{k\in\mathbb{Z}^2\\ l\in\mathbb{Z}^2}}d(a+k,b+l) && \text{(4.163c)}\\ &=d(\alpha,\beta). && \text{(4.163d)}\end{aligned}$$

□

LEMooQNDHooFXYjtj

Lemme 4.108 ([1]).
Soit $\beta\in T$. Nous avons

$$d(0,\beta)=d\big(0,\tau(\beta)\big) \tag{4.164}$$

où à gauche nous avons la « distance »[38] sur T et à droite nous avons la distance usuelle sur $\mathbb{R}^2$.

[38] Qui n'en est pas une d'ailleurs.

Démonstration. Nous choisissons $b \in \beta$ et nous avons

$$\begin{aligned} d(0,\beta) &= \min_{\substack{k\in\mathbb{Z}^2\\ l\in\mathbb{Z}^2}} d(k,b+l) && (4.165a)\\ &= \min_{\substack{k\in\mathbb{Z}^2\\ l\in\mathbb{Z}^2}} f(0,b-k+l) && (4.165b)\\ &= \min_{k\in\mathbb{Z}^2} f(0,b+k) && (4.165c)\\ &= d\big(0,\tau(b)\big) \qquad \text{prop. 4.106} && (4.165d)\\ &= d\big(0,\tau(\beta)\big). && (4.165e) \end{aligned}$$

□

4.5 Les complexes

La notion de module d'un nombre complexe $|z|$ sera donnée beaucoup plus tard, dans le lemme 11.101. La raison est que le module demande la racine carrée.

Définition 4.109 (Nombres complexes[143])**.**
L'ensemble des ***nombres complexes*** $\mathbb{C}$ *est l'ensemble* $\mathbb{R}^2$ *muni des opérations suivantes :*

(1)

$$\begin{aligned} \times_{\mathbb{C}} : \mathbb{C}\times\mathbb{C} &\to \mathbb{C}\\ \big((x,y),(x',y')\big) &\mapsto (xx'-yy',xy'+yx') \end{aligned} \tag{4.166}$$

EQooIJWOooZBiKEW

(2)

$$\begin{aligned} +_{\mathbb{C}} : \mathbb{C}\times\mathbb{C} &\to \mathbb{C}\\ \big((x,y),(x',y')\big) &\mapsto (x+x',y+y') \end{aligned} \tag{4.167}$$

(3)

$$\begin{aligned} \cdot : \mathbb{R}\times\mathbb{C} &\to \mathbb{C}\\ \big(\lambda,(x,y)\big) &\mapsto (\lambda x,\lambda y). \end{aligned} \tag{4.168}$$

Lemme 4.110.
Le triplet $(\mathbb{C},+_{\mathbb{C}},\times_{\mathbb{C}})$ *est un anneau*[39] *commutatif dont le neutre pour l'addition est* $(0,0)$ *et le neutre pour la multiplication est* $(1,0)$*.*

Démonstration. Ce ne sont que des calculs. Juste pour vous montrer, voici la première partie pour l'associativité :

$$\begin{aligned} \big((a,b)(x,y)\big)(s,t) &= (ax-by,ay+bx)(s,t) && (4.169a)\\ &= (axs-bys-ayt-bxt,axt-byt+ays+bxs). && (4.169b) \end{aligned}$$

Nous avons utilisé la distributivité sur $\mathbb{R}$, provenant du fait que $\mathbb{R}$ est un corps par le théorème 4.36. □

LEMooXTDDooFAjWRm

Lemme 4.111.
L'anneau $\mathbb{C}$ *est un corps.*

Démonstration. Il suffit de trouver un inverse pour chaque élément non nul. Soit un élément non nul $(a,b) \in \mathbb{C}$. En combinant les lemmes 4.52 et 4.67 nous savons que $a^2+b^2 > 0$. En particulier, cet élément est inversible dans $\mathbb{R}$, et nous pouvons considérer l'élément suivant de $\mathbb{C}$:

$$z = \Big(\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}\Big). \tag{4.170}$$

Prouver que $z(a,b) = (1,0)$ est maintenant juste un calcul. □

Lemme 4.112.
L'application

$$\begin{aligned} \varphi\colon \mathbb{R} &\to \mathbb{C}\\ x &\mapsto (x,0) \end{aligned} \tag{4.171}$$

[39] Définition 1.100.

est un morphisme d'anneaux[40].

Démonstration. Simples calculs. Par exemple

$$\varphi(xx') = (xx', 0) = (x, 0)(x', 0) = \varphi(x)\varphi(x'). \tag{4.172}$$

□

4.113.
Admirez ...

- Un nombre complexe est un couple de réels.
- Un réel est une classe d'équivalence de suites de Cauchy de rationnels.
- Une suite de Cauchy de rationnels est une application $\mathbb{N} \to \mathbb{Q}$ vérifiant certaines propriétés.
- Un rationnel est une classe d'équivalences d'éléments de $\mathbb{Z}$.
- Un élément de $\mathbb{Z}$ est une classe d'équivalence de couples de naturels.
- Un naturel sera ... là c'est plus compliqué. Une construction vraiment rigoureuse des naturels risque d'être en dehors du cadre du Frido.

Bref, les objets que nous manipulons sont d'une effroyable complexité.

4.114.
À partir de maintenant, lorsque nous parlons de $\mathbb{R}$, nous parlons en réalité de $\varphi(\mathbb{R}) \subset \mathbb{C}$.

Lemme 4.115.
Nous avons $(0,1)^2 = (-1, 0)$. *Nous notons* $i = (0, 1)$.

Démonstration. Calcul direct à partir de la définition 4.166. □

L'étude de la série géométrique est reportée à (beaucoup) plus tard, à la proposition 12.186. Dans l'immédiat il nous est possible de calculer la somme partielle.

LEMooAFSCooWEVlvp

Lemme 4.116 (Somme partielle de la série géométrique)**.**
Soit $q \in \mathbb{C}$. *Nous avons*

$$\sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}. \tag{4.173}$$

Démonstration. Posons $S_N = 1 + q + \ldots + q^N$. Nous avons évidemment $S_N - qS_N = 1 - q^{N+1}$ et donc

$$S_N = \sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}. \tag{4.174}$$

EqASYTiCK

□

4.5.1 Conjugaison complexe

DEFooQDDVooRYDsAJ

Définition 4.117.
Si $z = a + bi$ *est un nombre complexe (avec* $a, b \in \mathbb{R}$*), son* ***complexe conjugué*** *est le nombre* $a - bi$.
Le conjugué complexe de $z \in \mathbb{C}$ *sera le plus souvent noté* $\bar{z}$.

PROPooKBOIooRJPXAH

Proposition 4.118 ([1])**.**
Si $x, y \in \mathbb{C}$, *alors nous avons* $\bar{x}\bar{y} = \overline{xy}$.

Démonstration. Il suffit de poser $x = a + bi$ et $y = c + di$. Un peu de calcul donne

$$\bar{x}\bar{y} = (a - bi)(c - di) = (ac - bd) - (ad + bc)i. \tag{4.175}$$

De même $xy = (ac - bd) + (ad + bc)i$, et donc bien

$$\overline{xy} = (ac - bd) - (ad + bc)i. \tag{4.176}$$

□

[40] Définition 1.106.

4.5.2 Norme, topologie, etc.

Rien ici. La norme sur $\mathbb{C}$ demande la racine carrée qui sera vue plus tard.
Quelques liens :

(1) La norme sur $\mathbb{C}^n$ est dans la proposition 12.38.

(2) La proposition 12.2 pour $|x+y| \leqslant |x| + |y|$.

(3) Si vous cherchez des propriétés de la valeur absolue, c'est la proposition 1.122.

Chapitre 5

Théorie des groupes (suite)

5.1 Suite de composition

DefJWZSooNcntfK

Définition 5.1 (Suite de composition)**.**
Soit un groupe G.

(1) *Une **suite de composition** dans G est une suite finie de sous-groupes $(G_i)_{i=0,\dots,n}$ telle que*

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \dots \subseteq G_1 \subseteq G_0 = G \tag{5.1}$$

et telle que G_{i+1} est normal[1] *dans G_i.*

(2) *Les groupes G_i/G_{i+1} sont les **quotients** de la suite de composition.*

(3) *Une suite de **Jordan-Hölder** est une suite de composition dont tous les quotients sont simples.*

L'objet de nos prochaines pérégrinations mathématiques est de montrer que tout groupe fini admet une suite de Jordan-Hölder (théorème 5.8).

LemsKpXCG

Lemme 5.2 (du papillon ou de Zassenhaus[144])**.**
Soient G un groupe et des sous-groupes A et B. Soient A' normal dans A et B' normal dans B. Alors

(1) *$A'(A\cap B')$ est normal dans $A'(A\cap B)$*

(2) *$(A'\cap B)B'$ est normal dans $(A\cap B)B'$*

(3) *Nous avons les isomorphismes de groupes*

$$\frac{A'(A\cap B)}{A'(A\cap B')} \simeq \frac{(A\cap B)B'}{(A'\cap B)B'} \simeq \frac{B'(A\cap B)}{B'(A'\cap B)}. \tag{5.2}$$

Démonstration. Nous n'allons pas démontrer chacun des points ; pour plus de détails, nous dirons simplement que « la preuve est très similaire dans les autres cas ».

Commençons par montrer que $A'(A\cap B')$ est un groupe. Si $a,b\in A'$ et $x,y\in A\cap B'$,

$$axby = xx^{-1}axbx^{-1}xy \tag{5.3}$$

En utilisant la normalité, $x^{-1}ax\in A'$, donc $xx^{-1}axbx^{-1}\in A'$ et donc le tout est dans $A'(A\cap B')$. L'ensemble $A'(A\cap B')$ est également stable pour l'inverse parce que

$$x^{-1}a^{-1} = \underbrace{x^{-1}a^{-1}x}_{\in A'}x^{-1}. \tag{5.4}$$

Nous montrons maintenant que $A'(A\cap B')$ est normal dans $A'(A\cap B)$. Soient $a,b\in A'$, $x\in A\cap B'$ et

[1] Nous rappelons au cas où, que « normal » signifie « distingué », définition 2.13.

$f \in A \cap B$. Alors

$$(bf)^{-1}(ax)(bf) = (bf)^{-1}(a \underbrace{xbx^{-1}}_{=c\in A'} xf) \tag{5.5a}$$
$$= f^{-1}b^{-1}acxf \tag{5.5b}$$
$$= f^{-1}b^{-1}acf \underbrace{f^{-1}xf}_{=y\in A\cap B'} \tag{5.5c}$$
$$= \underbrace{f^{-1}b^{-1}acf}_{\in A'} y \tag{5.5d}$$
$$\in A'(A \cap B'). \tag{5.5e}$$

Pour prouver l'isomorphisme

$$\frac{A'(A \cap B)}{A'(A \cap B')} \simeq \frac{(A \cap B)B'}{(A' \cap B)B'}, \tag{5.6}$$

nous allons utiliser le deuxième théorème d'isomorphisme (2.22) que nous appliquons à $H = A \cap B$ et $N = A'(A \cap B')$. La vérification que H normalise N est usuelle. Nous commençons par écrire

$$\frac{A'(A \cap B')(A \cap B)}{A'(A \cap B')} \simeq \frac{A \cap B}{A \cap B \cap A'(A \cap B')}. \tag{5.7}$$ EqkplNsF

Pour simplifier un peu cette expression nous prouvons d'abord que

$$(A \cap B) \cap A'(A \cap B') = (A' \cap B)(A \cap B'). \tag{5.8}$$ EqkhsyNh

L'inclusion $\supset$ est facile. Pour l'autre sens, étant donné que $A'(A \cap B') \subset A$ nous avons

$$A \cap B \cap A'(A \cap B) = B \cap A'(A \cap B). \tag{5.9}$$ EQooEEVIooHCbasF

Un élément de $B \cap A'(A \cap B)$ est un élément de B qui s'écrit sous la forme $s = ax$ avec $a \in A'$ et $x \in A \cap B$. Nous avons alors $a = sx^{-1}$ avec $s \in B$ et $x^{-1} \in A \cap B$. Par conséquent $a \in B$ et donc $a \in A' \cap B$. Donc un élément de $B \cap A'(A \cap B)$ s'écrit sous la forme ax avec $a \in A' \cap B$ et $x \in A \cap B$. Autrement dit

$$B \cap A'(A \cap B) \subset (A' \cap B)(A \cap B) \tag{5.10}$$

et nous avons

$$(A \cap B) \cap A'(A \cap B) = B \cap A'(A \cap B) \subset (A' \cap B)(A \cap B'), \tag{5.11}$$

et donc l'égalité (5.8). Toujours dans l'idée de simplifier (5.7) nous remarquons que $A \cap B'$ est un sous-ensemble de $A \cap B$, donc $A'(A \cap B')(A \cap B) = A'(A \cap B)$. Il reste donc

$$\frac{A'(A \cap B)}{A'(A \cap B')} = \frac{A \cap B}{(A' \cap B)(A \cap B')}. \tag{5.12}$$

Étant donné que les hypothèses sur A et B sont symétriques, le membre de droite peut aussi s'écrire en inversant A et B. Nous en sommes à

$$\frac{B'(A \cap B)}{B'(A' \cap B)} = \frac{A'(A \cap B)}{A'(A \cap B')}. \tag{5.13}$$

Nous devons encore justifier $B'(A \cap B) = (A \cap B)B'$ et $B'(A' \cap B) = (A' \cap B)B'$. Vérifions la première égalité, et laissons la seconde au lecteur. Si $b \in B'$ et $x \in A \cap B$, alors

$$bx = x \underbrace{x^{-1}bx}_{\in B'} \in (A \cap B)B'. \tag{5.14}$$

□ PROPooUIXNooJdKuAs

Proposition 5.3.
Si G est un groupe fini et si (G_i) est une suite de composition pour G, alors l'ordre de G est le produit des ordres de ses quotients.

Démonstration. Étant donné que G_{i+1} est toujours normal dans G_i, le théorème de Lagrange 2.73 s'applique et, à chaque pas de la suite de composition, nous avons :

$$\left|\frac{G_i}{G_{i+1}}\right| = \frac{|G_i|}{|G_{i+1}|}. \tag{5.15}$$

Il suffit maintenant d'écrire $|G|$ de façon télescopique :

$$|G| = \prod_{0\leqslant i\leqslant n-1} \frac{|G_i|}{|G_{i+1}|} \tag{5.16}$$

□

DEFooSZZSooCrgDyo

Définition 5.4.
*Nous disons que les deux suites de composition $(G_i)_{0\leqslant i\leqslant r}$ et $(H_j)_{0\leqslant j\leqslant s}$ sont **équivalentes** si $r = s$ et si il existe une permutation $\sigma \in S_{r-1}$ telle que*

$$\frac{G_i}{G_{i+1}} \simeq \frac{H_{\sigma(i)}}{H_{\sigma(i)+1}}. \tag{5.17}$$

Proposition 5.5 (Schreider)**.**
Deux suites de composition d'un même groupe admettent des raffinements équivalents.

Démonstration. Soient les suites de composition

$$\{e\} = G_m \subseteq \ldots \subseteq G_1 \subseteq G_0 = G \tag{5.18a}$$
$$\{e\} = H_n \subseteq \ldots \subseteq H_1 \subseteq H_0 = G \tag{5.18b}$$

Nous raffinons la suite (G_i) en ajoutant, entre G_{i+1} et G_i, les sous-groupes

$$G_{i+1} = G_{i+1}(G_i \cap H_n) \subset G_{i+1}(G_i \cap H_{n-1}) \subseteq \ldots \subseteq G_{i+1}(G_i \cap H_0) = G_i, \tag{5.19}$$

et de même pour (H_j). Le groupe $G_{i+1}(G_i \cap H_k)$ est normal dans $G_{i+1}(G_i \cap H_{k-1})$ parce que G_{i+1} étant normal dans G_i, et H_k dans H_{k-1}, le lemme 5.2 s'applique. Nous avons donc bien défini un raffinement.

Nous devons maintenant prouver que les deux raffinements ainsi construits sont des suites de composition équivalentes. D'abord elles ont la même longueur mn parce que chacun des m éléments de la suite (G_i) a été remplacé par n éléments et inversement, chacun des n éléments de la suite (H_j) a été remplacé par m éléments.

Par ailleurs, les quotients du raffinement de (G_i) sont de la forme

$$\frac{G_{i+1}(G_i \cap H_k)}{G_{i+1}(G_i \cap H_{k+1})} \simeq \frac{H_{k+1}(H_k \cap G_i)}{H_{k+1}(H_k \cap G_{i+1})} \tag{5.20}$$

EqPAYTCR

en vertu du lemme du papillon (5.2). Le membre de droite de (5.20) est un des quotients du raffinement de (H_j). □

LemBSicRJ

Lemme 5.6 (Schreider strictement décroissant)**.**
Soient Σ_1 et Σ_2, deux suites de composition strictement décroissantes du groupe G. Alors elles admettent des raffinements équivalents strictement décroissants.

Démonstration. Par hypothèse, Σ_1 et Σ_2 n'ont pas de répétitions. Soient Σ_1'' et Σ_2'', des raffinements équivalents donnés par le lemme de Schreider. Étant donné que ce sont des suites de composition équivalentes, elles ont le même nombre de quotients réduits à $\{e\}$, c'est-à-dire le même nombre de répétitions.

Les suites Σ_1' et Σ_2' obtenues en retirant les répétitions de Σ_1'' et Σ_2'' sont des raffinements équivalents de Σ_1 et Σ_2 et strictement décroissants. □

PROPooEQKFooHPeLCR

Proposition 5.7 ([145])**.**
Soit une groupe G et une suite de composition Σ de G. Nous avons équivalence entre :

ITEMooFEQHooAIUgCq

(1) Σ est strictement décroissante et n'admet pas de raffinement strictement décroissante autre que elle-même.

ITEMooMRMFooASVQGy

(2) Chaque groupe de la suite est normal maximum dans le suivant (G_{i+1} est normal dans G_i).

ITEMooPPKHooJBpDGj

(3) Les quotients de la suite sont des groupes simples.

Démonstration. En plusieurs parties.

(1) **(1) ⇒ (2)** Nous considérons la suite de composition strictement décroissante

$$\{e\} = G_n \subsetneq G_{n-1} \subsetneq \dots \subsetneq G_1 \subsetneq G_0 = G. \tag{5.21}$$

Nous supposons que G_{i+1} n'est pas normal maximum dans G_i. C'est-à-dire qu'il existe un sous-groupe N tel que

$$G_{i+1} \subsetneq N \subsetneq G_i \tag{5.22}$$

tel que N est normal dans G_i. Notez que G_{i+1} est normal dans G_i et est donc à fortiori normal dans N. Bref, en ajoutant N nous avons un raffinement strictement décroissant de Σ.

(2) **(2) ⇒ (1)** Nous faisons non-(1) implique non-(2). Dit que Σ a un raffinement strictement décroissant signifie qu'il existe un sous-groupe N tel que

$$G_{i+1} \subsetneq N \subsetneq G_i \tag{5.23}$$

où G_{i+1} est normal dans N et N est normal dans G_i. Donc G_{i+1} n'est pas normal maximum dans G_i.

(3) **(2) ⇔ (3)** C'est la proposition 2.77.

□

ThoLgxWIC

Théorème 5.8 (Jordan-Hölder[145]).
À propos de suites de Jordan-Hölder dans un groupe fini.

ITEMooRSDDooNHkFYO

(1) Tout groupe fini admet une suite de Jordan-Hölder.

ITEMooGBOCooBAgnyt

(2) Toutes les suites de Jordan-Hölder dans un groupe fini sont équivalentes.

Démonstration. En deux parties.

(1) **Pour (1)** Soit D, l'ensemble des suites de composition strictement décroissantes de G. Nous montrons d'abord que D est non vide. Si $|G| = 1$, c'est-à-dire $G = \{e\}$, nous avons la suite vide. Sinon nous avons la suite $G, \{ej\}$. Donc D est non vide.

Nous savons par la proposition 5.3 que si $(G_i)_{i=0,\dots,n}$ est une suite de composition, alors

$$\prod_{i=1}^{n} |G_i/G_{i+1}| = |G|. \tag{5.24}$$

Si de plus (G_i) est strictement décroissante, nous avons le lemme 2.15 qui dit que $|G_i/G_{i+1}| \geqslant 2$.

Donc si $s \in D$ est de longueur n, nous avons $\text{Card}(G) \geqslant 2^n > n$. Donc les longueurs des éléments de D sont bornées par $\text{Card}(G)$. Soit $s_M \in D$ de longueur maximale. Elle n'a pas de raffinement strictement décroissant. La proposition 5.7 dit qu'alors tous les quotients sont simples.

(2) **Pour (2)** Par définition, une suite de Jordan-Hölder n'a pas de raffinement strictement décroissant (à part elle-même) parce que G_{i+1} est normal maximum dans G_i. Si Σ_1 et Σ_2 sont des suites de Jordan-Hölder nous pouvons considérer les raffinements équivalents strictement décroissants Σ_1' et Σ_2' du lemme de Schreider 5.6. Nous avons $\Sigma_1' \sim \Sigma_2'$, mais par ce que nous venons de dire à propos de la maximalité, $\Sigma_1' = \Sigma_1$ et $\Sigma_2' = \Sigma_2$. D'où le résultat.

□

5.2 Groupes résolubles

DefOSYNooTROIKs

Définition 5.9 (Groupe résoluble[146, 147]).
*Le groupe G est **résoluble** si il existe une suite finie de sous-groupes G_i*

$$\{e\} = G_0 \subset G_1 \subset \dots \subset G_{n-1} \subset G_n = G \tag{5.25}$$

avec G_i normal dans G_{i+1} et G_{i+1}/G_i abélien.

Il s'agit d'un groupe qui admet une suite de composition[2] dont les quotients sont abéliens.

[2] Voir définition 5.1.

LemOARMooYhYmbH

Lemme 5.10 ([148]).
Soit G un groupe et H un sous-groupe normal. Le groupe G/H est abélien si et seulement si[3] $D(G) \subset H$.

Démonstration. Les propositions suivantes sont équivalentes :

- Le groupe G/H est abélien
- pour tout $x, y \in G$, $[x][y] = [y][x]$
- $[x][y][x^{-1}][y^{-1}] = [e]$
- $[xyx^{-1}y^{-1}] = [e]$
- $[x, y] \in H$, voir la définition 2.153.
- $D(G) \subset H$.

□

PropRWYZooTarnmm

Proposition 5.11 ([148]).
Un groupe est résoluble si et seulement si sa suite dérivée termine sur $\{e\}$.

Démonstration. Grâce au lemme 2.155 et à la proposition 2.156, si la suite dérivée termine sur $\{e\}$ alors la suite dérivée est une suite qui répond aux conditions de la définition 5.9 de groupe résoluble.

Il faut donc encore montrer le sens direct. Nous supposons que G est un groupe résoluble et nous étudions sa suite dérivée. Nous avons une suite

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G \tag{5.26}$$

avec G_i normal dans G_{i+1} et G_{i+1}/G_i abélien. Nous allons prouver par récurrence que $D^i(G) \subset G_{n-i}$.

Pour $i = 0$ nous avons bien $G \subset G_n$.

Notre hypothèse de récurrence est :

$$D^i(G) \subset G_{n-i}. \tag{5.27}$$

EqEAQEooEaclEo

Vu que G_{n-i}/G_{n-i-1} est abélien, le lemme 5.10 dit que

$$D(G_{n-i}) \subset G_{n-i-1}. \tag{5.28}$$

EqEDJXooLOLQcr

En dérivant (5.27) et en tenant compte de (5.28),

$$D^{i+1}(G) \subset D(G_{n-i}) \subset G_{n-i-1}. \tag{5.29}$$

Nous avons donc bien $D^i(G) \subset G_{n-i}$ pour tout i. En particulier pour $i = n$, nous trouvons $D^n(G) \subset G_0 = \{e\}$. □

PropBNEZooJMDFIB

Proposition 5.12.
Soient des groupes G et H. Nous supposons que G est résoluble[4] *et nous considérons un morphisme $\psi : G \to H$. Alors $\psi(G)$ est résoluble.*

Démonstration. Puisque G est résoluble, il existe une suite de sous-groupes G_i tels que

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G \tag{5.30}$$

avec G_i normal dans G_{i+1} et G_{i+1}/G_i abélien. Nous posons $\psi(G)_i = \psi(G_i)$ et nous avons $\psi(G)_0 = \psi\big(\{e\}\big) = \{e\}$ ainsi que $\psi(G)_0 = \psi(G)$; donc

$$\{e\} = \psi(G)_0 \subset \psi(G)_1 \subset \ldots \subset \psi(G)_{n-1} \subset \psi(G)_n = \psi(G). \tag{5.31}$$

La proposition 3.141 nous indique que $\psi(G)_i$ est normal dans $\psi(G)_{i+1}$, et que $\psi(G)_{i+1}/\psi(G)_i$ est abélien. □

[3] Ici $D(G)$ est le groupe dérivé de G, voir 2.154.
[4] Définition 5.9.

5.3 Action de groupes

Le concept d'action d'un groupe est donné par la définition 3.236

Lemme 5.13.
Pour tout $g \in G$,

(1) L'application $\phi_g : E \to E$ est injective,

(2) Pour l'inverse : $(\phi_g)^{-1} = \phi_{g^{-1}}$.

Démonstration. Si $x, y \in E$ sont tels que $\phi_g(x) = \phi_g(y)$ alors en appliquant $\phi_{g^{-1}}$ aux deux membres nous trouvons

$$(\phi_{g^{-1}}\phi_g)(x) = (\phi_{g^{-1}}\phi_g)(y), \tag{5.32}$$

ce qui donne $x = y$ parce que $\phi_{g^{-1}}\phi_g = \phi_{g^{-1}g} = \phi_e = \mathrm{Id}$.

Les trois dernières égalités écrites disent que $\phi_{g^{-1}}$ est l'inverse[5] de ϕ_g. □

Pour alléger les notations, on convient d'écrire $g \cdot x$, voire plus simplement gx au lieu de $\phi_g(x)$. Le deuxième axiome d'action de groupe dit que la notation ghx ne souffre d'aucune ambiguïté.

DEFooMZXFooXbwGjj

Définition 5.14 (Orbite)**.**
*Si G agit sur un ensemble E, nous notons $G \cdot x$ l'**orbite** de $x \in E$ sous l'action de G :*

$$\mathrm{Orb}(x) = G \cdot x = \{gx \text{ tel que } g \in G\}.$$

DEFooMDYGooLrOERP

Définition 5.15 (Stabilisateur)**.**
*Si G est un groupe agissant sur l'ensemble E, et si $x \in E$, nous notons G_x ou $\mathrm{Stab}(x)$ le **stabilisateur** de x :*

$$\mathrm{Stab}(x) = G_x = \{g \in G \text{ tel que } g \cdot x = x\}. \tag{5.33}$$

Définition 5.16 (Fixateur)**.**
*Si G est un groupe agissant sur l'ensemble E, et si $g \in G$, nous notons enfin $\mathrm{Fix}(g)$ le **fixateur** de g :*

$$\mathrm{Fix}(g) = \{x \in E \text{ tel que } g \cdot x = x\}. \tag{5.34}$$

DefuyYJRh

Définition 5.17.
*L'action de G sur E est **fidèle** si l'élément neutre est le seul élément de G à fixer tous les points de E, c'est-à-dire si*

$$(gx = x \quad \forall x \in E) \Rightarrow g = e. \tag{5.35}$$

Un exemple d'action fidèle tout à fait non trivial sera donné avec l'action du groupe modulaire sur le plan de Poincaré dans le théorème 25.96.

Le groupe G agit toujours sur lui même à gauche et à droite. L'action à gauche est $g \cdot h = gh$; celle à droite est $g \cdot h = hg^{-1}$.

DEFooCORTooEeOLPT

Définition 5.18.
*L'action **adjointe** définie par $g \cdot h = ghg^{-1}$ est une manière pour un groupe d'agir sur lui-même par automorphismes. Cela est souvent noté $\mathbf{Ad}(g)h = ghg^{-1}$.*

En effet pour tout $g \in G$, l'application $\mathbf{Ad}(g) : G \to G$ est un automorphisme de G.

Si H est un sous-groupe de G, nous notons G/H le quotient de G par la relation $g \sim gh$ pour tout $h \in H$. Lorsque la distinction est importante, nous noterons $(G/H)_g$ pour les classes à gauche et $(G/H)_d$ pour les classes à droite.

Nous avons une relation d'équivalence à gauche et une à droite. D'abord

$$x \sim_g y \Leftrightarrow xh = y \tag{5.36}$$

pour un certain $h \in H$. Ensuite

$$x \sim_d y \Leftrightarrow hx = y \tag{5.37}$$

pour un certain $h \in H$.

Le lemme suivant est une généralisation du théorème de Lagrange 2.73.

[5] Si vous décidez de dire ça à un jury dans un concours, soyez prêts à préciser les domaines.

LEMooUEFUooGQnEAY

Lemme 5.19.
L'ensemble $(G/H)_g$ est fini si et seulement si l'ensemble $(G/H)_d$ est fini. Si il en est ainsi, alors $(G/H)_g$ et $(G/H)_d$ ont même cardinal, qui vaut l'indice de H dans G.

Démonstration. L'application

$$\begin{aligned} f\colon (G/H)_g &\to (G/H)_d \\ [x]_g &\mapsto [x^{-1}]_d \end{aligned} \tag{5.38}$$

est une bijection bien définie. En effet si $x \sim_g y$, nous avons $h \in H$ tel que $y^{-1}h = x^{-1}$, c'est-à-dire que $x^{-1} \sim_d y^{-1}$ et f est bien définie. Le fait que f soit surjective est évident. Pour l'injectivité, soient $x, y \in G$ tels que

$$f([x]_g) = f([y]_g). \tag{5.39}$$

Alors $x^{-1} \sim_d y^{-1}$, ce qui implique l'existence de $h \in H$ tel que $hx^{-1} = y^{-1}$, ou encore que $xh^{-1} = y$, ce qui signifie que $x \sim_g y$.

Pour l'énoncé à propos de l'indice, nous procédons en plusieurs étapes simples.

(1) Les classes (les éléments de $(G/H)_g$) forment une partition de G.

(2) Toutes les classes ont le même nombre d'éléments par la bijection

$$\begin{aligned} f\colon [x]_g &\to [y]_g \\ xh &\mapsto yh. \end{aligned} \tag{5.40}$$

(3) Le nombre d'éléments dans une classe est égal à $|H|$ par la bijection

$$\begin{aligned} g\colon [x]_g &\to H \\ xh &\mapsto h. \end{aligned} \tag{5.41}$$

Par conséquent

$$|G| = |H| \cdot \text{ nombre de classes} = |H| \cdot \text{ Card}\big((G/H)_g\big), \tag{5.42}$$

et nous avons bien

$$\text{Card}\big((G/H)_g\big) = \frac{|G|}{|H|} = |G : H|. \tag{5.43}$$

Notez l'utilisation du lemme 3.245. □

Propszymlr

Proposition 5.20 (Orbite-stabilisateur[62])**.**
Soient G un groupe agissant sur un ensemble E et $x \in E$.

(1) Les ensembles $G \cdot x$ et G/G_x sont équipotents.

ITEMooCWUGooCOFHYk

(2) L'orbite de x est finie si et seulement si $\text{Stab}(x)$ est d'indice fini dans G. Dans ce cas nous avons

$$\text{Card}(G \cdot x) = |G : \text{Stab}(x)|, \tag{5.44}$$

EqnLCHCE

et

$$|G| = |\text{Stab}(x)||\mathcal{O}_x|. \tag{5.45}$$

EqCcwSXT

La formule (5.44) est nommée ***formule des classes****[149].*

Démonstration. En deux points.

(1) Soit l'application

$$\begin{aligned} \psi\colon G \cdot x &\to G/G_x \\ a \cdot x &\mapsto [a]. \end{aligned} \tag{5.46}$$

Cette application est bien définie parce que si $a \cdot x = b \cdot x$, alors il existe $h \in G_x$ tel que $b = ah$, et par conséquent $[a] = [b]$. Cette application est une bijection et par conséquent $G \cdot x$ est équipotent à G/G_x.

(2) Soit $y \in \mathcal{O}_x$ et $A_y = \{g \in G \text{ tel que } g \cdot x = y\}$. Nous avons

$$A_y = s \operatorname{Stab}(x). \tag{5.47}$$

En effet, si $a \in A_y$, alors $a \cdot x = y$ et $s^{-1}a \cdot x = s^{-1} \cdot y = x$. Par conséquent $s^{-1}a \in \operatorname{Stab}(x)$. Dans l'autre sens, supposons $a \in s\operatorname{Stab}(x)$. Soit $g \in \operatorname{Stab}(x)$ tel que $a = sg$. Alors nous avons $a \cdot x = sg \cdot x = s \cdot x = y$. Donc $a \in A_y$.

Nous venons de prouver que la partie A_y est une classe à gauche de $\operatorname{Stab}(x)$, par conséquent $|A_y| = |\operatorname{Stab}(x)|$ pour tout $y \in \mathcal{O}_x$. Les A_y pour différents y sont disjoints et nous avons de plus

$$\bigcup_{y \in \mathcal{O}_x} A_y = G. \tag{5.48}$$

Les ensembles A_y divisent donc G en $|\mathcal{O}_x|$ paquets de $|\operatorname{Stab}(x)|$ éléments. D'où la formule (5.45).

□

CORooRRVHooTyCjZZ

Corolaire 5.21.
Soit C_g la classe de conjugaison d'un élément g du groupe fini G. Alors

$$\operatorname{Card}(C_g) = |G : Z_G(g)| \tag{5.49}$$

où $Z_G(g)$ est le centralisateur de g dans G[6] de G.

Démonstration. C'est une application de la proposition 5.20 (formule (5.44)) dans le cas de l'action adjointe de G sur lui-même.

En effet, si nous considérons l'action adjointe, l'orbite est la classe de conjugaison : $C_g = G \cdot g$. Et le stabilisateur de g pour l'action adjointe n'est autre que le centralisateur de g :

$$\begin{aligned}
\operatorname{Fix}(g) &= \{h \in G \text{ tel que } h \cdot g = g\} && \text{(5.50a)}\\
&= \{h \in G \text{ tel que } hgh^{-1} = g\} && \text{(5.50b)}\\
&= \{h \in G \text{ tel que } gh = hg\} && \text{(5.50c)}\\
&= Z_G(g). && \text{(5.50d)}
\end{aligned}$$

Donc la formule $\operatorname{Card}(G \cdot g) = |G : G_g|$ devient, dans le cas de l'action adjointe de G sur lui-même : $\operatorname{Card}(C_g) = |G : Z_G(g)|$. □

LEMooVGOJooSBpIag

Lemme 5.22.
Soit G un groupe agissant sur l'ensemble E. On définit $x \sim x'$ si et seulement si il existe $g \in G$ tel que $g \cdot x = x'$. Alors

(1) la relation $\sim$ est une relation d'équivalence.

(2) la classe $[x]$ est l'orbite $\mathcal{O}_x$ de x sous G.

CorARFVMP

Corolaire 5.23 (Équation des orbites)**.**
Soient G un groupe agissant sur l'ensemble E et $\mathcal{O}_1, \dots, \mathcal{O}_k$ la liste des orbites (distinctes). Alors

(1) $E = \bigcup_i \mathcal{O}_i$, l'union est disjointe,

(2) $\operatorname{Card}(E) = \sum_i \operatorname{Card}(\mathcal{O}_i)$.

DefcSuYxz

Définition 5.24.
*Soit G un groupe agissant sur l'ensemble E. Un **domaine fondamental** ou une **transversale** est une partie de E contenant un et un seul élément de chaque orbite.*

Autrement dit, les images des éléments d'un domaine fondamental F forment une partition de l'ensemble :

$$E = \bigsqcup_{g \in G} g(F) \tag{5.51}$$

où $g(F) = \phi_g(F) = \{\phi_g(x) \text{ tel que } x \in F\}$. L'union est disjointe, c'est-à-dire que si $g \neq g'$, alors $g(F) \cap g'(F) = \varnothing$.

[6] Définition 2.10.

PropUyLPdp
Proposition 5.25 (Équation des classes[150]).
Soit G, un groupe fini opérant sur un ensemble E. Si E'' est un ensemble contenant exactement un élément de chaque orbite dans $E \setminus \mathrm{Fix}_G(E)$, alors

$$|G| = |\mathrm{Fix}_G(E)| + \sum_{x\in E''} \frac{|G|}{|\mathrm{Fix}_G(x)|}. \tag{5.52}$$

Si de plus G est un p-groupe, alors

$$|E| = |\mathrm{Fix}_G(E)| \mod p. \tag{5.53}$$

Démonstration. Par le corolaire 5.23, nous avons $|G| = \sum_{x\in E'} |\mathcal{O}_x|$ où E' est une transversale. En séparant la somme entre les orbites à un élément et les autres,

$$|G| = \mathrm{Card}(\mathrm{Fix}_G(E)) + \sum_{x\in E''} \frac{|G|}{|\mathrm{Fix}_G(x)|} \tag{5.54}$$

où nous avons utilisé le fait que $|G| = |\mathrm{Fix}_G(x)||\mathcal{O}_x|$.

Si G est un p-groupe alors si $x \in E''$, $\mathrm{Fix}_G(x)$ est un sous-groupe propre de G et donc $|\mathrm{Fix}_G(x)|$ est un diviseur propre de $|G|$. Du coup la fraction $|G|/|\mathrm{Fix}_G(x)|$ est une puissance non nulle de p et l'équation (5.52) devient immédiatement (5.53). □

Corolaire 5.26 (Équation des classes).
Soient G un groupe, et C_1,..., C_l la liste de ses classes de conjugaison contenant plus d'un élément. Alors

$$\mathrm{Card}(G) = \mathrm{Card}\big(Z(G)\big) + \sum_i |G : Z_{g_i}| = \mathrm{Card}\big(Z(G)\big) + \sum_i \frac{\mathrm{Card}(G)}{\mathrm{Card}\big(\mathrm{Fix}(g_i)\big)} \tag{5.55}$$

si $g_i \in C_i$.

Démonstration. Étant donné que les classes de conjugaison sont disjointes, le cardinal de G est bien la somme des cardinaux de ses classes. Les classes ne contenant qu'un seul élément sont celles des éléments de $Z(G)$. En ce qui concerne les autres orbites, $\mathrm{Card}(C_{g_i}) = |G : Z_{g_i}|$ par le théorème orbite-stabilisateur (proposition 5.20). □

THOooEFDMooDfosOw
Théorème 5.27 (Formule de Burnside).
Si G est un groupe fini agissant sur l'ensemble fini E et si Ω est l'ensemble des orbites, alors

$$\mathrm{Card}(\Omega) = \frac{1}{|G|} \sum_{g\in G} \mathrm{Card}\big(\mathrm{Fix}(g)\big). \tag{5.56}$$

Démonstration. Nous considérons l'ensemble

$$A = \{(g, x) \in G \times E \text{ tel que } gx = x\}, \tag{5.57}$$

et nous en calculons le cardinal de deux façons. D'abord

$$\begin{aligned}
\mathrm{Card}(A) &= \sum_{x\in E} \mathrm{Card}\{g \in G \text{ tel que } gx = x\} && \text{(5.58a)}\\
&= \sum_{x\in E} \mathrm{Card}(\mathrm{Fix}(x)) && \text{(5.58b)}\\
&= \sum_{\omega\in\Omega} \sum_{x\in\omega} \mathrm{Card}(\mathrm{Fix}(x)) && \text{(5.58c)}\\
&= \sum_{\omega\in\Omega} \frac{|G|}{\mathrm{Card}(\omega)} && \text{(5.58d)}\\
&= |G|. && \text{(5.58e)}
\end{aligned}$$

Pour obtenir (5.58d) nous avons utilisé l'équation des classes (5.45). L'autre façon de calculer $\mathrm{Card}(A)$ est de regrouper ainsi :

$$\mathrm{Card}(A) = \sum_{g\in G} \mathrm{Card}\{x \in E \text{ tel que } gx = x\} = \sum_{g\in G} \mathrm{Card}(\mathrm{Fix}(g)). \tag{5.59}$$

En égalisant les deux expressions de $\text{Card}(A)$ nous trouvons

$$|G|\,\text{Card}(\Omega) = \sum_{g\in G}\text{Card}(\text{Fix}(g)). \tag{5.60}$$

□

PROPooMYKKooLetZWi

Proposition 5.28 ([151]).
Soient G un groupe, et H, un sous-groupe du centre de G.

(1) H est normal dans G.

(2) Si G/H est monogène, alors G est abélien.

Démonstration. En deux parties.

(1) **Normal** Si $g\in G$ et si $h\in H$, alors $ghg^{-1}=gg^{-1}h=h\in H$.

(2) **Abélien** Soit $g_0\in G$ tel que $[g_0]$ engendre G/H. Soient $g\in G$ et $s\in[g]$. Il existe $h\in H$ tel que $s=gh^{-1}$, et donc tel que $g=sh$. Il existe aussi $n\in\mathbb{N}$ tel que $[s]=[g_0^n]$, et donc un $h_2\in H$ tel que $s=g_0^nh_2$.

Nous avons prouvé que pour tout $g\in G$, il existe $n\in\mathbb{N}$ et $h\in H$ tel que $g=g_0^nh$.

Soient $g_1,g_2\in G$. Nous avons $n,m\in\mathbb{N}$ et $h_1,h_2\in H$ tels que $g_1=g_0^nh_1$ et $g_2=g_0^mh_2$. Nous avons alors

$$\begin{aligned}
g_1g_2a &= g_0^nh_1g_0^mh_2 && && (5.61a)\\
&= g_0^ng_0^mh_1h_2 && \text{pcq.}h_1\in H\subset Z(G) && (5.61b)\\
&= g_0^mg_0^nh_1h_2 && && (5.61c)\\
&= g_0^mh_2g_0^nh_1 && && (5.61d)\\
&= g_2g_1, && && (5.61e)
\end{aligned}$$

et donc G est bien abélien.

□

PROPooWPQTooECUPLK

Proposition 5.29 ([152]).
L'indice du centre d'un groupe n'est jamais un nombre premier.

LEMooZJGVooRYrujB

Lemme 5.30 ([153]).
Soient un groupe cyclique G et un sous groupe H.

ITEMooUNOEooZoElYL

(1) Il existe $r,n\in\mathbb{N}$ tels que $r\mid n$ et $H\simeq r\mathbb{Z}/n\mathbb{Z}$.

ITEMooMUSSooBmNXEd

(2) $\text{Card}(H)=n/r$

ITEMooVPEKooKdPibk

(3) H est cyclique.

En particulier, tout sous-groupe d'un groupe cyclique est cyclique.

Démonstration. En plusieurs parties.

(1) **Pour (1)** Soit un générateur a de G. L'application

$$\begin{aligned}
f\colon\mathbb{Z}&\to G\\
k&\mapsto a^k
\end{aligned} \tag{5.62}$$

est un morphisme de groupe surjectif.

La partie $f^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$. La proposition 3.45(2) dit qu'il existe $r\in\mathbb{N}$ tel que $f^{-1}(H)=r\mathbb{Z}$. De même $\ker(f)$ est un sous-groupe de $\mathbb{Z}$, de telle sorte qu'il existe $n\in\mathbb{N}$ tel que $\ker(f)=n\mathbb{Z}$.

Nous avons

$$n\mathbb{Z}=\ker(f)=f^{-1}(e)\subset f^{-1}(H)=r\mathbb{Z}. \tag{5.63}$$

Étant donné que $n\mathbb{Z}\subset r\mathbb{Z}$, il existe $d\in\mathbb{N}$ tel que $n=dr$.

Nous considérons maintenant

$$\begin{aligned} g\colon r\mathbb{Z} &\to H \\ k &\mapsto a^k, \end{aligned} \tag{5.64}$$

qui est encore un morphisme de groupes. En utilisant le premier théorème d'isomorphismes 2.20(3), nous avons

$$\frac{r\mathbb{Z}}{\ker(g)} \simeq \text{Image}(g). \tag{5.65}$$

Mais $\ker(g) = n\mathbb{Z}$ et $\text{Image}(g) = H$. Donc nous avons bien $H \simeq r\mathbb{Z}/n\mathbb{Z}$.

(2) **Pour (2)** En ce qui concerne le cardinal, vu que nous avons un isompshisme,

$$\text{Card}(H) = \text{Card}(r\mathbb{Z}/n\mathbb{Z}) = n/r \tag{5.66}$$

par le lemme 2.152(3).

(3) **Pour (3)** Le fait que H soit cyclique est le lemme 2.152(2).

□

THOooRGSTooIWyhqt

Théorème 5.31 (Sous-groupe d'un groupe cyclique[153])**.**
Soit G un groupe cyclique[7] *d'ordre n. Pour chaque $d \in \mathbb{N}$ nous posons*

$$H_d = \{x \in G \text{ tel que } x^d = e\}. \tag{5.67}$$

(1) Ces H_d sont des sous-groupes de G.

(2) $\text{Card}(H_d) = d$.

ITEMooMJCXooCIWSmK

(3) L'ensemble des sous-groupes de G est $\{H_d \text{ tel que } d \mid n\}$.

ITEMooIEGUooPQWEep

(4) Si g est un générateur de G, alors H_d peut être décrit des façons suivantes :

$$H_d = \{x \in G \text{ tel que } x^d = e\} = \text{gr}(g^{n/d}). \tag{5.68}$$

Démonstration. Point par point.

(1) **H_d est un sous-groupe** ITEMooYAMOooVtbCrS Si $g, h \in H_d$, alors $(gh)^d = g^d h^d = ee = e$. De plus $(g^{-1})^d = (g^d)^{-1} = e^{-1} = e$.

(2) **Tout sous-groupe est un H_d avec $d \mid n$** ITEMooXEXFooIrFOTi Soit un sous-groupe H de G. Nous notons $\text{Card}(H) = d$. Le lemme 5.30(3) nous indique que H est cyclique. Soit un générateur $a \in H$; son ordre est le cardinal de H : $\text{ord}(a) = \text{Card}(H) = d$.

Tout élément de H vérifie $x^{\text{ord}(a)} = (a^k)^{\text{ord}(a)} = (a^{\text{ord}(a)})^k = e$. Donc $H \subset H_d$. En particulier $\text{Card}(H) \leqslant \text{Card}(H_d)$.

Tout sous-groupe de G est cyclique. En particulier H_d est cyclique, et nous pouvons considérer un générateur : il existe $a \in H_d$ tel que $\text{ord}(a) = \text{Card}(H_d)$. Étant donné que $a \in H_d$, il vérifie $a^d = e$, et donc

$$\text{ord}(a) \mid d. \tag{5.69}$$

Vu que $\text{ord}(a) = \text{Card}(H_d)$ et que $d = \text{Card}(H)$, nous avons $\text{Card}(H_d) \mid \text{Card}(H)$ et en particulier $\text{Card}(H_d) \leqslant \text{Card}(H)$. Donc $\text{Card}(H) = \text{Card}(H_d)$ et au final $H = H_d$.

Nous avons prouvé au passage que $\text{Card}(H_d) = d$. Vu que le cardinal d'un sous-groupe divise le cardinal du groupe[8], nous avons $d \mid n$.

(3) $\text{Card}(H_d) = d$ C'est contenu dans ce que nous avons fait dans la partie (2).

(4) **Si $d \mid n$ alors H_d est un sous-groupe de G** C'est un cas particulier de la partie (1).

(5) **Note** Le point (3) est prouvé. Cela ne contredit pas le fait que H_d soit un sous-groupe de G pour tout d, et pas seulement pour les d qui divisent n. En effet si d ne divise pas n, il existe d' divisant n tel que $H_d = H_{d'}$. Pas besoin de chercher une preuve de ce fait : la preuve est déjà faite. Il s'agit de dire que H_d est un sous-groupe de G pour tout d (partie (1)), et que tous les sous-groupes de G sont de la forme H_d avec $d \mid n$.

[7] Définition 2.149.
[8] Théorème de Lagrange 2.73(1).

(6) **Pour (4)** Soit un générateur g de G. Nous avons d'une part $g^{n/d} \in H_d$ parce que $(g^{n/d})^d = g^n = e$. D'autre part, les éléments

$$g^{n/d}, g^{2n/d}, \dots, g^{(d-1)n/d}, g^n = e \tag{5.70}$$

sont distincts. En effet si $g^{kn/d} = g^{ln/d}$ avec $0 < l < k < d$, alors $g^{(k-l)n/d} = e$. Comme $k - l < d$, nous avons $(k-l)n/d < n$ et donc $g^{(k-l)n/d} \neq e$ parce que g est générateur.

Bref, les $g^{kn/d}$ avec $k = 1, \dots, d$ sont d éléments distincts, tous dans H_d dont le cardinal est d. Donc

$$H_d = \{g^{kn/d}\}_{1,\dots,d}. \tag{5.71}$$

□

DEFooQDHPooCfDEuL

Définition 5.32.
*Soit G un groupe agissant sur un ensemble E. Nous disons que l'action est **transitive** si elle possède une seule orbite. L'action est **libre** si $g \cdot x = g' \cdot x$ implique $g = g'$.*

Chapitre 6

Espaces vectoriels (début)

6.1 Parties libres, génératrices, bases et dimension

NORMooANZNooTUhDdk

6.1.
Nous avons déjà défini (dans 3.96) un espace vectoriel comme étant un module sur un corps commutatif. En explicitant un peu, cela donne ceci[154].

Un espace vectoriel sur le corps $\mathbb{K}$ est un ensemble E muni de deux opérations :

- une loi de composition interne $+ : E \times E \to E$,
- une loi de composition externe $\cdot : \mathbb{K} \times E \to E$

telles que

(1) $(E, +)$ soit un groupe abélien,

(2) pour tout $u, v \in E$ et pour tout $k, k' \in \mathbb{K}$,

ITEMooYQMWooNNvHSb

(2a) $k(u + v) = (ku) + (kv)$
(2b) $(kk')u = k(k'u)$
(2c) $(k + k')u = (ku) + (k'u)$
(2d) $1u = u$

où 1 est le neutre de $\mathbb{K}$ et où nous avons directement adopté la notation ku pour $k \cdot u$.

Si $u \in E$, nous notons $-u$ l'inverse de u dans le groupe $(E, +)$.

DEFooDLHWooAvfhgc

Définition 6.2 (Partie libre)**.**
Si E est un espace vectoriel, une partie A de E est ***libre*** *si pour tout choix d'un nombre fini d'éléments $\{u_i\}_{i=1,\dots,n}$ de A, l'égalité*

$$a_1u_1 + \cdots + a_nu_n = 0 \tag{6.1}$$

implique $a_i = 0$ pour tout i (ici les a_i sont dans le corps de base).

Remarque 6.3.
Notons que le vecteur nul n'est dans aucune partie libre, ne fût-ce que parce que $a0 = 0$ n'implique pas $a = 0$.

Si A est une partie de l'espace vectoriel E, nous notons $\mathrm{Span}(A)$ l'ensemble des combinaisons linéaires finies d'éléments de A. Les coefficients de ces combinaisons linéaires sont dans le corps de base $\mathbb{K}$.

Définition 6.4 (Partie génératrice)**.**
Une partie B d'un espace vectoriel E est ***génératrice*** *si* $\mathrm{Span}(B) = E$.

Remarque 6.5.
Ces définitions demandent des commentaires en dimension infinie[1].

(1) Tout élément peut être écrit comme combinaison linéaire finie d'une partie génératrice. Cela ne signifie pas que nous pouvons extraire une partie finie qui convient pour tous les éléments à la fois. Lorsque l'espace est de dimension infinie, ceci est particulièrement important.

[1] Nous n'avons pas encore défini le concept de dimension, mais nous nous adressons au lecteur trop pressé.

(2) La définition séparée de liberté dans le cas des parties infinies a son importance lorsqu'on parle d'espaces vectoriels de dimension infinie (en dimension finie, aucune partie infinie n'est libre) parce que cela fera une différence entre une base algébrique et une base hilbertienne par exemple.

DEFooNGDSooEDAwTh

Définition 6.6 (Base)**.**
*Une **base** de l'espace vectoriel E est une partie à la fois génératrice et libre.*

NORMooJGRNooAKtvWt

6.7.
Supposons que la partie $\{u_1, u_2, u_2\}$ soit une base d'un espace vectoriel E. Un ensemble étant quelque chose de non ordonné, la partie $\{u_3, u_2, u_1\}$ est la même, et $\{u_1, u_1, u_2, u_2, u_3, u_4\}$ est encore la même.

Lorsque l'ordre dans lequel nous numérotons les vecteurs d'une base est important (par exemple pour écrire explicitement la matrice d'une application linéaire), nous devrions écrire (u_1, u_2, u_3). Nous pourrions définir le concept de *base ordonnée* en disant qu'une base ordonnée de E est une application $u\colon I \to E$ où I est un ensemble totalement ordonné et telle que $u(I)$ soit une base de E.

À partir de là, il ne serait plus autorisé de dire « la matrice de f dans une base ». Il faudrait dire « la matrice de f dans une base ordonnée ». Dans ce contexte, une matrice pour une application linéaire d'un espace réel serait une application $I \times I \to \mathbb{R}$.

Bref, tout ça pour dire qu'il y a clairement des incohérences de notations à ce niveau dans le Frido. Il sera souvent écrit $\{u_1, u_2\}$ au lieu de (u_1, u_2) ou, mieux, $u\colon I \to \mathbb{R}$, et il sera souvent dit « base » au lieu de « base ordonnée ».

Nous prouvons à présent que tout élément non nul d'un espace vectoriel possédant une base[2] se décompose de façon unique en combinaison linéaire finie d'éléments d'une base.

PROPooEIQIooXfWDDV

Proposition 6.8 ([1])**.**
Soient un espace vectoriel E sur $\mathbb{K}$ muni d'une base $\{e_i\}_{i\in I}$. Si $v \in E$, alors il existe un unique couple (J, c) où

(1) J est une partie finie de I ;

(2) $c\colon J \to \mathbb{K}$ est une application

(3) $v = \sum_{j\in J} c(j)e_j$.

Les éléments $c(i)$ seront notés v_i et sont les composantes de v dans la base. Sous-entendu, on prolonge c de J vers I par zéro sur $I \setminus J$.

Démonstration. Soit un espace vectoriel E et une base $\{e_i\}_{i\in I}$ où I est un ensemble à priori quelconque. Soit $v \in E$. Puisque $E = \text{Span}\{e_i\}_{i\in I}$, il existe une partie finie J de I et des coefficients $\{v_j\}_{j\in J}$ dans $\mathbb{K}$ tels que

$$v = \sum_{j\in J} v_j e_j. \tag{6.2}$$

Cela donne l'existence.

En ce qui concerne l'unicité, soient J et K des parties finies de I et des coefficients $\{v_j\}_{j\in J}$ et $\{w_k\}_{k\in K}$ tels que

EQooFKNEooICnVBP

$$v = \sum_{j\in J} v_j e_j = \sum_{k\in K} w_k e_k. \tag{6.3}$$

Nous posons $L = J \cup K$. Remarquez que les unions suivantes sont des unions disjointes :

$$L = (J \setminus K) \cup (J \cap K) \cup (K \setminus J) \tag{6.4a}$$
$$J = (J \setminus K) \cup (J \cap K) \tag{6.4b}$$
$$K = (K \cap J) \cup (K \setminus J). \tag{6.4c}$$

Écrivons $0 = v - v$ en utilisant les expressions de v de (6.3) et en décomposant les sommes :

$$0 = \sum_{j\in J} v_j e_j - \sum_{k\in K} w_k e_k \tag{6.5a}$$
$$= \sum_{j\in J\setminus K} v_j e_j + \sum_{j\in J\cap K} v_j e_j - \sum_{k\in K\cap J} w_k e_k - \sum_{k\in K\setminus J} w_k e_k \tag{6.5b}$$
$$= \sum_{j\in J\setminus K} v_j e_j + \sum_{j\in J\cap K} (v_j - w_j)e_j - \sum_{k\in K\setminus J} w_k e_k. \tag{6.5c}$$

[2]Nous n'avons pas démontré que tout espace vectoriel possède une base. Donc à notre niveau, il est possible que ce théorème soit sans objet pour beaucoup d'espaces.

Là-dessus, nous posons

$$\alpha_l = \begin{cases} v_l & \text{si } l \in J \setminus K \\ v_l - w_l & \text{si } l \in J \cap K \\ -w_l & \text{si } l \in K \setminus J. \end{cases} \tag{6.6}$$

Nous avons alors

$$\sum_{l \in L} \alpha_l e_l = 0. \tag{6.7}$$

EQooCTWRooZKyaup

Vu que $\{e_i\}_{i\in I}$ est libre, la partie $\{e_l\}_{l\in L}$ est également libre. Donc l'équation (6.7) implique que $\alpha_l = 0$ pour tout $l \in L$.

Nous devons prouver que

$$\{j \in J \text{ tel que } v_j \neq 0\} = \{k \in K \text{ tel que } w_k \neq 0\} \tag{6.8}$$

et que pour l dans cet ensemble, $v_l = w_l$.

Soit $j \in J$; il y a deux possibilités : soit $j \in J \setminus K$, soit $j \in J \cap K$. Dans le premier cas nous avons déjà vu que $\alpha_j = v_j = 0$. Dans le second cas, $\alpha_j = v_j - w_j = 0$, c'est-à-dire $v_j = w_j$.

Donc $j \in J$ vérifiant $v_j \neq 0$ implique $j \in J \cap K$ et l'égalité des coefficients. Idem avec $k \in K$ tel que $w_k \neq 0$ implique $k \in J \cap K$. □

LEMooDJSIooYcsvhO

Lemme 6.9 ([1]).
Soit un espace vectoriel admettant des bases. Un endomorphisme est une bijection si et seulement si il change toute base en une base.

Démonstration. En deux parties. Soit un espace vectoriel E possédant des bases et un endomorphisme $f : E \to E$.

(1) **Si f est bijective** Soit une base $\{v_i\}_{i\in I}$; nous devons voir que $\{f(v_i)\}_{i\in I}$ est une base.

(1a) **Libre** Si J est une partie finie de I et si les λ_j sont des scalaires tels que $\sum_{j\in J} \lambda_j f(v_j) = 0$, alors

$$0 = \sum_{j\in J} \lambda_j f(v_j) = f\big(\sum_{j\in J} \lambda_j v_j\big). \tag{6.9}$$

Mais comme f est bijective, cela implique que $\sum_{j\in J} \lambda_j v_j = 0$. En retour, parce que $\{v_i\}$ est une base, cela implique que $\lambda_j = 0$ pour tout j.

(1b) **Générateur** Soit $x \in E$. Puisque f est bijective, il existe un unique $y \in E$ tel que $x = f(y)$. Comme $\{v_i\}_{i\in I}$ est une base, il existe une partie finie $J \subset I$ et des scalaires $\{\lambda_j\}_{j\in J}$ tels que

$$y = \sum_{j\in J} \lambda_j v_j. \tag{6.10}$$

Nous avons alors

$$x = f(y) = \sum_{j\in J} \lambda_j f(v_j), \tag{6.11}$$

qui montre que $\{f(v_i)\}_{i\in I}$ est bien génératrice de E

(2) **Si f change les bases en bases** Soit un endomorphisme changeant toute base en une base. Nous devons prouver qu'il est bijectif.

(2a) **Injective** Nous considérons une base $\{v_i\}_{i\in I}$. La partie $\{f(v_i)\}_{i\in I}$ est par hypothèse également une base.

Soient $x, y \in E$ tels que $f(x) = f(y)$. Il existe J et K finis dans I qui permettent de décomposer x et y respectivement dans la base $\{f(v_i)\}_{i\in I}$. Quitte à poser $J' = J \cup K$, nous supposons que J suffit[3]. Il existe donc des scalaires $\{\lambda_j\}_{j\in J}$ et $\{\mu_j\}_{j\in J}$ tels que $x = \sum_{j\in J} \lambda_j f(v_j)$ et $y = \sum_{j\in J} \mu_j f(v_j)$.

La relation $f(x) = f(y)$ donne immédiatement, par la linéarité de f,

$$\sum_{j\in J} (\lambda_j - \mu_j) f(v_j) = 0. \tag{6.12}$$

Du fait que $\{f(v_i)\}_{i\in I}$ soit une base, nous déduisons que $\lambda_j - \mu_j = 0$ pour tout j. Donc $x = y$, et f est injective.

[3] Nous utilisons le fait que l'union de deux parties finies d'un ensemble est finie (lemme 2.29(2)).

(2b) **Surjective** Soit $x \in E$. Puisque $\{f(v_i)\}_{i\in I}$ est une base, il existe des scalaires λ_j tels que

$$x = \sum_{j\in J} \lambda_j f(v_j) = f\big(\sum_{j\in J} \lambda_j v_j\big). \tag{6.13}$$

Donc f est surjective.

□

PROPooVJFNooSbkzTF

Proposition 6.10 ([1]).
Soit un espace vectoriel E. Soit une partie $B \subset E$ telle que tout élément de E puisse être écrit de façon unique comme combinaison linéaire d'un nombre fini d'éléments de B. Alors B est une base.

LEMooRWQHooIxrQek

Lemme 6.11 ([1]).
Bases dans $\mathbb{R}^n$.

ITEMooKWULooCTmOqM

(1) Si v et w ne sont pas colinéaire dans $\mathbb{R}^2$, alors $\{v, w\}$ est une base de $\mathbb{R}^2$.

(2) Toute partie libre de $\mathbb{R}^n$ contenant n élément est une base.

Définition 6.12.
*Un espace vectoriel est **de type fini** si il contient une partie génératrice finie.*

Nous verrons dans les résultats qui suivent que cette définition est en réalité inutile parce qu'un espace vectoriel sera de type fini si et seulement si il est de dimension finie.

LemytHnlD

Lemme 6.13.
Si E a une famille génératrice de cardinal n, alors toute famille de $n+1$ éléments est liée.

Démonstration. Nous procédons par récurrence sur n. Pour $n = 1$, nous avons $E = \text{Span}(e)$ et donc si $v_1, v_2 \in E$ nous avons $v_1 = \lambda_1 e$, $v_2 = \lambda_2 e$ pour certains éléments non nuls λ_1, λ_2 du corps de base. Nous avons donc $\lambda_2 v_1 - \lambda_1 v_2 = 0$. Cela prouve que $\{v_1, v_2\}$ est liée.

Supposons maintenant que le résultat soit vrai pour $k < n$, c'est-à-dire que pour tout espace vectoriel contenant une partie génératrice de cardinal $k < n$, les parties de $k+1$ éléments sont liées. Soit maintenant un espace vectoriel muni d'une partie génératrice $G = \{e_1, \dots, e_n\}$ de n éléments, et montrons que toute partie $V = \{v_1, \dots, v_{n+1}\}$ contenant $n+1$ éléments est liée. Dans nos notations nous supposons que les e_i sont des vecteurs distincts et les v_i également. Nous les supposons également tous non nuls. Étant donné que $\{e_i\}$ est génératrice nous pouvons définir les nombres $\lambda_{i,k}$ par

$$v_i = \sum_{k=1}^{n} \lambda_{i,k} e_k \tag{6.14}$$

Puisque

$$v_{n+1} = \sum_{k=1}^{n} \lambda_{n+1,k} e_k \neq 0, \tag{6.15}$$

quitte à changer la numérotation des e_i, nous pouvons supposer que $\lambda_{n+1,n} \neq 0$. Nous considérons les vecteurs

$$w_i = \lambda_{n+1,n} v_i - \lambda_{i,n} v_{n+1}. \tag{6.16}$$

En calculant un peu,

$$w_i = \lambda_{n+1,n} \sum_{k=1}^{n} \lambda_{i,k} e_k - \lambda_{i,n} \sum_{k=1}^{n} \lambda_{n+1,k} e_k \tag{6.17a}$$

$$= \sum_{k=1}^{n-1} \big(\lambda_{n+1,n}\lambda_{i,k} - \lambda_{i,n}\lambda_{n+1,k}\big) e_k \tag{6.17b}$$

parce que les termes en e_n se sont simplifiés. Donc la famille $\{w_1, \dots, w_n\}$ est une famille de n vecteurs dans l'espace vectoriel $\text{Span}\{e_1, \dots, e_{n-1}\}$; elle est donc liée par l'hypothèse de récurrence. Il existe donc des nombres $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ non tous nuls, tels que

$$0 = \sum_{i=1}^{n} \alpha_i w_i = \sum_{i=1}^{n} \alpha_i \lambda_{n+1,n} v_i - \sum_{i=1}^{n} \alpha_i \lambda_{i,n} v_{n+1}. \tag{6.18}$$

EqOOGGoU

Vu que $\lambda_{n+1,n} \neq 0$ et que, parmi les α_i, au moins un est non nul, nous avons au moins un des produits $\alpha_i\lambda_{n+1,n}$ qui est non nul. Par conséquent (6.18) est une combinaison linéaire nulle non triviale des vecteurs de $\{v_1, \dots, v_{n+1}\}$. Cette partie est donc liée. □

LemkUfzHl

Lemme 6.14.
Soient L une partie libre et G une partie génératrice d'un espace vectoriel E. Si l'ensemble des parties libres L' telles que $L \subset L' \subset G$ possède un élément maximum[4]*, alors cet élément est une base.*

Qu'entend-on par « maximale » ? La partie B candidate, doit être libre, contenir L, être contenue dans G et de plus avoir la propriété que $\forall x \in G \setminus B$, la partie $B \cup \{x\}$ est liée.

Démonstration. D'abord si G est une base, alors toutes les parties de G sont libres et le maximum est $B = G$. Dans ce cas le résultat est évident. Nous supposons donc que G est liée.

La partie $B = \{b_1, \dots, b_l\}$ est libre parce qu'on l'a prise parmi les libres. Montrons que B est génératrice. Soit $x \in G \setminus B$; par hypothèse de maximalité, $B \cup \{x\}$ est liée, c'est-à-dire qu'il existe des nombres λ_i, λ_x non tous nuls tels que

$$\sum_{i=1}^{l} \lambda_i b_i + \lambda_x x = 0. \tag{6.19}$$

EqxfkeyM

Si $\lambda_x = 0$ alors un de λ_i doit être non nul et l'équation (6.19) devient une combinaison linéaire nulle non triviale des b_i, ce qui est impossible parce que B est libre. Donc $\lambda_x \neq 0$ et

$$x = -\frac{1}{\lambda_x} \sum_{i=1}^{l} \lambda_i b_i. \tag{6.20}$$

Donc tous les éléments de $G \setminus B$ sont des combinaisons linéaires des éléments de B, et par conséquent, G étant génératrice, tous les éléments de E sont combinaisons linéaires d'éléments de B. □

ThonmnWKs

Théorème 6.15 (Théorème de la base incomplète)**.**
Soit E un espace vectoriel de type fini sur le corps $\mathbb{K}$.

ItemBazxTZ

(1) Si L est une partie libre et si G est une partie génératrice contenant L, alors il existe une base B telle que $L \subset B \subset G$.

ITEMooFVJXooGzzpOu

(2) Toute partie libre peut être étendue en une base.

ITEMooFBUAooSSZxgx

(3) Toutes les bases sont finies et ont même cardinal.

ITEMooJIJSooGuJMdt

(4) Si V est un sous-espace vectoriel de E, et si L est une base de V, alors il existe une base de E qui contient L.

Démonstration. Point par point.

(1) Comme E est de type fini, il admet une partie génératrice G de cardinal fini n. Donc une partie libre est de cardinal au plus n par le lemme 6.13. Soit L, une partie libre contenue dans G (ça existe : par exemple $L = \varnothing$). La partie B maximalement libre contenue dans G et contenant L est une base par le lemme 6.14.

(2) Notons que puisque E lui-même est générateur, le point (1) implique que toute partie libre peut être étendue en une base.

(3) Soient B et B', deux bases. En particulier B est génératrice et B' est libre, donc le lemme 6.13 indique que $\mathrm{Card}(B') \leqslant \mathrm{Card}(B)$. Par symétrie on a l'inégalité inverse. Donc $\mathrm{Card}(B) = \mathrm{Card}(B')$.

(4) La partie L étant une base de V, elle est en particulier libre dans E. Par le point (2), L peut être étendue en une base.

□

REMooYGJEooEcZQKa

Remarque 6.16.
Le théorème de la base incomplète 6.15(2) est ce qui permet de construire une base d'un espace vectoriel en « commençant par » une base d'un sous-espace. En effet si H est un sous-espace de E, alors une base de H est une partie libre de E et donc, peut être étendue en une base de E.

[4] Encore une fois, à part quelques cas triviaux, il n'est pas clair à ce point que ce maximum existe.

DEFooWRLKooArTpgh

Définition 6.17.
*La **dimension** d'un espace vectoriel de type fini est le cardinal*[5] *d'une*[6] *de ses bases.*

Il existe une infinité de bases de $\mathbb{R}^m$. On peut démontrer que le cardinal de toute base de $\mathbb{R}^m$ est m, c'est-à-dire que toute base de $\mathbb{R}^m$ possède exactement m éléments.

Exemple 6.18.
La base de **canonique** de $\mathbb{R}^m$ est la partie $\{e_1, \dots, e_m\}$, où le vecteur e_j est

$$e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow \text{j-ème} \quad .$$

La composante numéro j de e_i est 1 si $i = j$ et 0 si $i \neq j$. Cela s'écrit $(e_i)_j = \delta_{i,j}$ où δ est le **symbole de Kronecker** défini par

$$\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \tag{6.21}$$

Les éléments de la base canonique de $\mathbb{R}^m$ peuvent donc être écrits $e_i = \sum_{k=1}^{m} \delta_{i,k} e_k$. △

Le théorème suivant est essentiellement une reformulation du théorème 6.15.

ThoMGQZooIgrXjy

Théorème 6.19.
Soit E un espace vectoriel de dimension finie et $\{e_i\}_{i\in I}$ une partie génératrice de E.

ITEMooTZUDooFEgymQ

(1) Il existe $J \subset I$ tel que $\{e_i\}_{i\in J}$ est une base. Autrement dit : de toute partie génératrice nous pouvons extraire une base.

ITEMooCJQGooXwjsfm

(2) Soit $\{f_1, \dots, f_l\}$ une partie libre. Alors nous pouvons la compléter en utilisant des éléments e_i. C'est-à-dire qu'il existe $J \subset I$ tel que $\{f_k\} \cup \{e_i\}_{i\in J}$ soit une base.

Démonstration. En deux parties.

(1) **Pour (1)** C'est le théorème 6.15(1). La partie $\{e_{i_0}\}$ est libre et la partie $\{e_i\}_{i\in I}$ est génératrice. Donc il existe une base B telle que $\{e_{i_0}\} \subset B \subset \{e_i\}_{i\in I}$. Si $B = \{e_i\}_{i\in J}$, alors J est fini[7] parce que toutes les bases d'un espace vectoriel de dimension finie ont le même nombre d'éléments.

(2) **Pour (2)** Utiliser le théorème 6.15(4) avec $V = \text{Span}\{f_1, \dots, f_l\}$.

□

PROPooVEVCooHkrldw

Proposition 6.20.
Si E est un espace vectoriel de dimension finie n, alors

ITEMooZNLDooBISkJyBS

(1) toute partie contenant $n+1$ éléments est liée.

ITEMooSGGCooOUsuBs

(2) toute partie libre contenant n éléments est une base,

(3) toute partie génératrice contenant n éléments est une base.

Démonstration. Soit une partie M contenant $n+1$ éléments. L'espace E possède une partie génératrice contenant n éléments (n'importe quelle base). Donc M est liée par le lemme 6.13.

Une partie libre contenant n éléments peut être étendue en une base ; si ladite extension est non triviale (c'est-à-dire qu'on ajoute vraiment au moins un élément) une telle base contiendra une partie de $n+1$ éléments qui serait liée par le lemme 6.13.

Pour la dernière assertion, soit une partie génératrice $\{v_i\}_{i\in I}$ où I contient n éléments. Par le théorème 6.19(1) nous pouvons en extraire une base : il existe $J \subset I$ tel que $\{v_j\}_{j\in J}$ soit une base. Si l'inclusion $J \subset I$ était stricte, alors la base $\{v_j\}_{j\in J}$ contiendrait moins de n éléments, ce qui serait en contradiction avec le théorème 6.15(3). □

[5] Définition 2.24.
[6] Le théorème de la base incomplète 6.15(3) montre que cette définition ne souffre d'aucune ambiguïté.
[7] Sauf si I est choisi de façon traitresse. Il se peut que $e_{i_1} = e_{i_2}$ avec $i_1 \neq i_2$.

DefCodimension

Définition 6.21.
*Soit F un sous-espace vectoriel de l'espace vectoriel E. La **codimension** de F dans E est*

$$\operatorname{codim}_E(F) = \dim(E/F). \tag{6.22}$$

LEMooGNDPooAhvIek

Lemme 6.22.
L'ensemble $\mathbb{Q}^n$ est un $\mathbb{Q}$-espace vectoriel de dimension n.

PROPooRKOVooBFRCKq

Proposition-Définition 6.23 (Supplémentaire vectoriel[1])**.**
Soit un espace vectoriel V et un sous-espace vectoriel V_1 dans V. Il existe un sous-espace vectoriel V_2 de V tel que

(1) $V_1 \cap V_2 = \{0\}$,

(2) pour tout $x \in V$, il existe un unique $(x_1, x_2) \in V_1 \times V_2$ satisfaisant $x = x_1 + x_2$.

*Une telle partie V_2 est dite **supplémentaire** de V_1 et on écrit parfois $V = V_1 \oplus V_2$*[8]*.*

Démonstration. La partie V_1 est un sous-espace vectoriel. Il possède donc une base $\mathcal{B}_1 = \{u_1, \dots, u_l\}$. Le théorème de la base incomplète 6.15(3) dit qu'il existe $\{v_1, \dots, v_k\}$ tels que $\mathcal{B} = \{u_1, \dots, u_l, v_1, \dots, v_k\}$ soit une base de V.

Nous posons alors $V_2 = \operatorname{Span}\{v_1, \dots, v_k\}$.

(1) $V_1 \cap V_2 = \{0\}$ Soit $x \in V_1 \cap V_2$. Étant donné que $x \in V_1$, il existe des a_i tels que $x = \sum_i a_i u_i$, et étant donné que $x \in V_2$ il existe des b_j tels que $x = \sum_j b_j v_j$. Nous avons donc $\sum_i a_i u_i - \sum_j b_j v_j = 0$ en tant que combinaison linéaire nulle d'éléments d'une base, les coefficients sont nuls[9] : $a_i = 0$ et $b_j = 0$ pour tout i et j. Donc $x = 0$.

(2) **Décomposition : existence** Si $x \in V$, il y a une décomposition dans la base $\mathcal{B}$: $x = \sum_{i=1}^{l} a_i u_i + \sum_{j=1}^{k} b_j v_j$. En posant $x_1 = \sum_i a_i u_i$ et $x_2 = \sum_j b_j v_j$, nous avons bien $x = x_1 + x_2$ avec $x_1 \in V_1$ et $x_2 \in V_2$.

(3) **Décomposition : unicité** Supposons $x = x_1 + x_2 = y_1 + y_2$ avec $x_1, y_1 \in V_1$ et $x_2, y_2 \in V_2$. Nous avons les décompositions $x_1 = \sum_i a_i u_i$, $x_2 = \sum_j b_j v_j$, $y_1 = \sum_i a'_i u_i$ et $y_2 = \sum_j b'_j v_j$. L'égalité $x_1 + x_2 = y_1 + y_2$ donne

$$\sum_i (a_i - a'_i) u_i + \sum_j (b_j - b'_j) v_j = 0. \tag{6.23}$$

Combinaison linéaire nulle d'éléments d'une base. Les coefficients son nuls, et donc $a_i - a'_i = 0$ et $b_j - b'_j = 0$. Nous en déduisons $x_1 = y_1$ et $x_2 = y_2$.

□

PROPooOMUHooYFXJSY

Proposition 6.24 ([1])**.**
Si E est un espace vectoriel de dimension d sur le corps $\mathbb{K}$, et si $\{e_1, \dots, e_d\}$ est une base, alors l'application

$$\begin{aligned} \varphi\colon \mathbb{K}^d &\to E \\ (x_1, \dots, x_d) &\mapsto \sum_i x_i e_i \end{aligned} \tag{6.24}$$

est une bijection linéaire.

6.1.1 Et en dimension infinie

Dans ZFC, en dimension infinie, il existe aussi une base pour tout espace vectoriel ainsi qu'un théorème de la base incomplète. Nous ne parlerons pas de ce qu'il se passe lorsque nous ne considérons que ZF[10].

LEMooSSRXooIyfgNz

Lemme 6.25 ([155])**.**
Soient un $\mathbb{K}$-espace vectoriel E et un sous-espace vectoriel V de E. Soient encore deux sous-espaces vectoriels W_1 et W_2 tels que

[8] Mais c'est un léger abus parce que $V_1 \oplus V_2$ est formellement $V_1 \times V_2$ (définition 6.156).
[9] C'est la définition 6.2 d'une partie libre.
[10] Si vous ne savez pas ce que signifient les sigles « ZF » et « ZFC » vous ne devriez pas être en train de lire ceci, et encore moins penser à le resservir à un jury d'agrégation.

(1) $V \cap W_1 = \{0\}$;

(2) $V + W_2 = E$.

Alors il existe un supplémentaire[11] W *de* V *tel que* $W_1 \subset W \subset W_2$.

Juste une remarque : dans le Frido le symbole « $\subset$ » ne signifie pas une inclusion stricte.

Démonstration. Nous utilisons le lemme de Zorn.

(1) **Un gros ensemble** Soit

$$\mathcal{A} = \left\{ S \subset E \text{ tel que } \begin{cases} S \text{ est un sous-espace vectoriel de } E \\ W_1 \subset S \subset W_2 \\ S \cap V = \{0\} \end{cases} \right\} \tag{6.25}$$

(2) **Non vide** Puisque $W_1 \in \mathcal{A}$, cet ensemble n'est pas vide.

(3) **Ordre** L'ensemble $\mathcal{A}$ est partiellement ordonné pour l'inclusion.

(4) **$\mathcal{A}$ est inductif** Nous prouvons maintenant que $\mathcal{A}$ est inductif[12]. Pour cela, soit une partie $\mathcal{A}'$ totalement ordonnée et $U = \bigcup_{A \in \mathcal{A}'} A$.

Alors, la partie U est un sous-espace vectoriel de E. En effet si $x, y \in U$, alors il existe $A_1, A_2 \in \mathcal{A}'$ tels que $x \in A_1$ et $y \in A_2$. Comme $\mathcal{A}'$ est totalement ordonné, l'un des ensembles parmi A_1 et A_2 est inclus dans l'autre. Sans perdre de généralité, disons $A_1 \subset A_2$. Alors les opérations s'effectuent dans A_2 : nous avons $x, y \in A_2$, et donc $\lambda x \in A_2 \subset U$ ainsi que $x + y \in A_2 \subset U$.

De plus, U contient W_1, et est contenu dans W_2. Ainsi, $U \in \mathcal{A}$ et majore $\mathcal{A}'$ pour l'inclusion. En bref, $\mathcal{A}$ est bien inductif.

(5) **Utilisation de Zorn** Le lemme de Zorn 1.42 nous donne alors un élément maximal W de $\mathcal{A}$. Cet élément vérifie

(5a) $W \cap V = \{0\}$,

(5b) $W_1 \subset W \subset W_2$,

(5c) pour tout $W' \in \mathcal{A}$, nous avons $W' \subset W$ par maximalité de W.

(6) **Supplémentaire** Montrons que ce W est un supplémentaire de V. Soit $x \in E$. Le but est de trouver une décomposition de x en somme d'un élément de W et un de V. Comme $V + W_2 = E$, nous avons $v \in V$ et $w_2 \in W_2$ tels que

$$x = v + w_2. \tag{6.26}$$

Si $w_2 \in W$ alors c'est fini. Sinon …

Soit $X = \text{Span}\{W, w_2\}$. Vu que X contient strictement W et que W est maximum dans $\mathcal{A}$, la partie X n'est pas un élément de $\mathcal{A}$. Comme X est un sous-espace vectoriel de E tel que $W_1 \subset X \subset W_2$, la seule possibilité pour que X ne soit pas dans $\mathcal{A}$ est que $X \cap V \neq \{0\}$. Soit donc $y \neq 0$ dans $X \cap V$. Par définition de X,

$$y = w' + \lambda w_2 \tag{6.27}$$

EqDecompo55.296

pour $w' \in W$, $w_2 \in W_2$ et $\lambda \in \mathbb{K}$. Nous avons $\lambda \neq 0$, sinon nous aurions $y \in W \cap V$ et donc $y = 0$ puisque W est dans $\mathcal{A}$. La décomposition (6.27) permet alors d'écrire $w_2 = (y - w')/\lambda$ et finalement

$$x = v + \frac{1}{\lambda}(y - w') = \underbrace{v + \frac{1}{\lambda} y}_{\in V} - \underbrace{\frac{1}{\lambda} w'}_{\in W}. \tag{6.28}$$

La somme d'espaces vectoriels $E = V + W$ est donc établie.

□

Corolaire 6.26.
Tout sous-espace vectoriel d'un espace vectoriel possède un supplémentaire.

[11] Définition 6.23.
[12] Définition 1.41.

Démonstration. Soit un espace vectoriel E ainsi qu'un sous-espace vectoriel V. Si $V = E$ nous sommes O.K. Sinon nous considérons $v \in E \setminus V$ et nous posons $W_1 = \mathbb{K}v$ et $W_2 = E$.

Vu que V et W_1 sont des espaces vectoriels, nous avons $V \cap W_1 = \{0\}$, et puisque $W_2 = E$, nous avons $V + W_2 = E$. Le lemme 6.25 nous donne alors un supplémentaire de V. □

PROPooHDCEooMhDjPi

Proposition 6.27 (Base incomplète)**.**
Tout espace vectoriel (non réduit à $\{0\}$) possède une base.

Démonstration. Soit $\mathcal{A}$ l'ensemble des familles libres de E. Il n'est pas vide parce que $\{v\}$ en est une dès que v est non nul dans E. Rapidement :

- l'ensemble $\mathcal{A}$ est ordonné pour l'inclusion,
- si $\mathcal{A}'$ est une partie totalement ordonnée, l'union est un majorant,
- donc $\mathcal{A}$ est inductif,
- soit un maximum F de $\mathcal{A}$.

La partie F est libre parce qu'elle est dans $\mathcal{A}$. Elle est génératrice parce que si v n'est pas dans $\text{Span}(F)$ alors la partie $F \cup \{v\}$ est encore libre, et majore strictement F pour l'inclusion, ce qui n'est pas possible.

Donc F est une base de E. □

THOooOQLQooHqEeDK

Théorème 6.28 (Base incomplète, dimension quelconque)**.**
Soit une partie $\{e_i\}_{i\in I}$ génératrice de l'espace vectoriel E (ici, I est un ensemble quelconque[13]). Soit $I_0 \subset I$ tel que $\{e_i\}_{i\in I_0}$ soit libre.

Alors il existe I_1 tel que $I_0 \subset I_1 \subset I$ tel que $\{e_i\}_{i\in I_1}$ soit une base de E.

Note : une telle partie I_0 existe en prenant un singleton. Mais l'existence n'est pas le sujet ici.

Démonstration. Soit $\mathcal{A}$ l'ensemble des parties J de I telles que $I_0 \subset J \subset I$ et telles que $\{e_i\}_{i\in J}$ soit libre.

Encore une fois, $\mathcal{A}$ est inductif pour l'ordre partiel donné par l'inclusion. Soit J un élément maximum par le lemme de Zorn 1.42. Puisque $J \in \mathcal{A}$, la partie $\{e_i\}_{i\in J}$ est libre. Mais elle est également génératrice parce que si e_k n'est pas dedans, J ne serait pas maximum, étant majorée par $J \cup \{k\}$.

Donc $\{e_i\}_{i\in J}$ engendre tous les e_i avec $i \in I$ et donc, tous les éléments de E. □

PROPooTSRCooOfTEmO

Proposition 6.29 ([1])**.**
L'ensemble des parties libres d'un espace vectoriel, muni de l'ordre de l'inclusion, est inductif[14].

Démonstration. Soit un espace vectoriel V. Soit un ensemble totalement ordonnée $\mathcal{L} = \{L_i\}_{i\in I}$ de parties libres de V. Nous posons $L = \bigcup_{i\in I} L_i$. Nous prouvons que L est libre, de telle sorte que ce soit un maximum de $\mathcal{L}$.

Soient $x_1, \dots, x_n \in L$. Il existe une partie finie $I_0 \subset I$ telle que $x_1, \dots, x_n \in \bigcup_{i\in I_0} L_i$. Mais toute partie finie d'un ensemble totalement ordonné a un maximum (lemme 2.31). Donc il existe $i_0 \in I_0$ tel que $x_1, \dots, n_n \in L_{i_0}$. Vu que L_0 est libre et que $\{x_1, \dots, n_n\} \subset L_{i_0}$, la partie $\{x_1, \dots, x_n\}$ est libre. □

NORMooREVQooEFJWta

6.30 ([18])**.**
Une preuve alternative du théorème de la base incomplète serait de dire que l'ensemble des parties libres est inductif (proposition 6.29). De ce fait, la proposition 1.43 permet de dire que toute partie libre peut être complétée en une base.

6.1.2 Espace librement engendré

DEFooCPNIooNxsYMY

Définition 6.31 ([156])**.**
Soient un ensemble S et un corps $\mathbb{K}$. L'espace vectoriel ***librement engendré*** *sur S, noté $F_{\mathbb{K}}(S)$ est l'ensemble des applications $S \to \mathbb{K}$ qui sont non-nulles en un nombre fini de points de S.*

Autrement dit, $\sigma : S \to \mathbb{K}$ est dans $F_{\mathbb{K}}(S)$ si $\{x \in S \text{ tel que } \sigma(x) \neq 0\}$ est fini[15].

Le lemme suivant donne tout son sens à l'expression « librement » engendré. Il dit que $F_{\mathbb{K}}(S)$ possède une base indexée par S lui-même.

[13] Un cas d'utilisation intéressant est de poser $I = E$ et $e_i = i$. Pensez-y.
[14] Définition 1.41.
[15] Parce que nous l'aimons bien, nous ne résistons pas à faire un renvoi vers la définition 1.74.

LEMooLOPAooUNQVku

Lemme 6.32.
L'ensemble des applications δ_s données par

$$\begin{aligned}\delta_s : S &\to \mathbb{K} \\ t &\mapsto \begin{cases} 1 & si\ t = s \\ 0 & sinon \end{cases}\end{aligned} \tag{6.29}$$

avec $s \in S$ forment une base[16] *de $F_{\mathbb{K}}(S)$.*

Démonstration. Pour prouver que les δ_s sont générateurs, nous considérons $g : S \to \mathbb{K}$ non nul sur la partie finie $\{s_i\}_{i\in I}$ de S. Alors nous avons

$$g = \sum_{i\in I} g(s_i)\delta_{s_i}. \tag{6.30}$$

Pour prouver que les δ_s forment une partie libre, nous supposons avoir $\lambda_i \in \mathbb{K}$ tels que

$$g = \sum_{i\in I} \lambda_i \delta_{s_i} = 0 \tag{6.31}$$

Soit $j \in I$. Nous avons

$$0 = f(s_j) = \sum_{i\in I} \lambda_i \underbrace{\delta_{s_i}(s_j)}_{=\delta_{i,j}} = \lambda_j. \tag{6.32}$$

Donc les coefficients λ_i sont tous nuls, et nous avons prouvé que la partie est libre. □

Il est parfois pratique d'écrire les éléments de $F_{\mathbb{K}}(S)$ comme sommes « formelles » d'éléments de S. Cela va encore lorsque S est un ensemble n'ayant aucune somme bien définie.

Mais attention : si $S = \mathbb{R}$, l'élément $4+7$ de $F_{\mathbb{R}}(\mathbb{R})$ n'est pas 11. L'élément 11 de $F_{\mathbb{R}}(\mathbb{R})$ est un élément complètement différent. Bref, il n'est pas judicieux d'écrire les éléments de $F_{\mathbb{K}}(S)$ comme des combinaisons linéaires d'éléments de S. Pour $x \in S$ il vaut mieux écrire explicitement δ_x que x. La somme $\delta_x + \delta_y$ est parfaitement bien définie dans l'ensemble des applications de S vers $\mathbb{K}$.

6.2 Applications linéaires

Le lien entre matrice et applications linéaires est la définition 6.78 et toutes les propriétés qui s'en suivent.

6.2.1 Définition

DEFooULVAooXJuRmr

Définition 6.33.
*Soient des espaces vectoriels E et F sur le corps $\mathbb{K}$. Soit un sous-corps $\mathbb{L}$ de $\mathbb{K}$. Une application $T : E \to F$ est dite $\mathbb{L}$-**linéaire** si*

- *$T(x+y) = T(x) + T(y)$ pour tout x et y dans E,*
- *$T(\lambda x) = \lambda T(x)$ pour tout λ dans $\mathbb{K}$ et x dans E.*

Nous noterons $\mathcal{L}_{\mathbb{L}}(E, F)$ l'espace des applications $\mathbb{L}$-linéaires de E vers F.

Si vous avez bien suivi, les égalités dans la définition 6.33 sont des égalités dans F.

6.34.
Le plus souvent, si E est un espace vectoriel sur $\mathbb{K}$, alors nous ne considérerons que les applications $\mathbb{K}$-linéaires. Autrement dit, nous écrirons le plus souvent simplement $\mathcal{L}(E, F)$ sans préciser le corps.

Il pourra pourtant arriver que, pour un espace vectoriel sur $\mathbb{C}$, nous considérions les applications seulement $\mathbb{R}$-linéaires. Ce sera le cas dans le lemme 29.160.

DefDQRooVGbzSm

Lemme-Définition 6.35.
L'ensemble de toutes les applications linéaires de E vers F est noté $\mathcal{L}(E, F)$ et devient un espace vectoriel sur $\mathbb{K}$ avec les définitions suivantes :

(1) $(T_1 + T_2)(x) = T_1(x) + T_2(x)$,

[16] Définition 6.6.

(2) $(\lambda T)(x) = \lambda T(x)$.

EXooMAWMooEaNWpl

Exemple 6.36.

△

PROPooEQYBooMYIFKR

Proposition 6.37.
Si V est un espace vectoriel sur le corps $\mathbb{K}$ et si $\lambda \in \mathbb{K}$, l'application

$$\begin{aligned} T_\lambda \colon V &\to V \\ x &\mapsto \lambda x \end{aligned} \tag{6.33}$$

est linéaire.

Démonstration. Soient $\lambda, \mu \in \mathbb{K}$ ainsi que $a, b \in V$. Nous avons

$$\begin{aligned} T_\lambda(a+b) &= \lambda(a+b) && && (6.34a)\\ &= \lambda a + \lambda b && \text{cf. 6.1(2a)} && (6.34b)\\ &= T_\lambda(a) + T_\lambda(b) && && (6.34c) \end{aligned}$$

et

$$\begin{aligned} T_\lambda(\mu a) &= \lambda(\mu a) && && (6.35a)\\ &= \mu(\lambda a) && \mathbb{K} \text{ est comm. et ass.} && (6.35b)\\ &= \mu T_\lambda(a). && && (6.35c) \end{aligned}$$

□

ex_affine

Exemple 6.38.
Soit $m \in \mathbb{N}$. On fixe λ dans $\mathbb{R}$ et v dans $\mathbb{R}^m$. L'application U_λ de $\mathbb{R}^m$ dans $\mathbb{R}^m$ définie par $U_\lambda(x) = \lambda x + v$ n'est pas une application linéaire lorsque $v \neq 0$, parce que si a est un réel différent de 0 et 1, alors $av \neq v$, d'où

$$U_\lambda(ax) = \lambda(ax) + v \neq a(\lambda x + v) = aU_\lambda(x).$$

△

exampleT_A

Exemple 6.39.
Soit A une matrice fixée de $\mathbb{M}(m \times n, \mathbb{R})$. La fonction $T_A \colon \mathbb{R}^m \to \mathbb{R}^n$ définie par $T_A(x) = Ax$ est une application linéaire. En effet,

- $T_A(x+y) = A(x+y) = Ax + Ay = T_A(x) + T_A(y)$,
- $T_A(ax) = A(ax) = a(Ax) = aT_A(x)$.

△

LEMooLGEHooVEEoiU

Lemme 6.40.
Si une application linéaire est inversible, alors son inverse est linéaire.

Démonstration. Soient une application linéaire inversible $f \colon E \to F$, ainsi que $x, y \in E$. Nous avons

$$f\big(f^{-1}(x) + f^{-1}(y)\big) = f\big(f^{-1}(x)\big) + f\big(f^{-1}(y)\big) = x + y = f\big(f^{-1}(x+y)\big). \tag{6.36}$$

En prenant f^{-1} des deux côtés, nous trouvons

$$f^{-1}(x) + f^{-1}(y) = f^{-1}(x+y). \tag{6.37}$$

De même :

$$f\big(\lambda f^{-1}(x)\big) = \lambda f\big(f^{-1}(x)\big) = \lambda x = f\big(f^{-1}(\lambda x)\big), \tag{6.38}$$

ce qui nous donne $\lambda f^{-1}(x) = f^{-1}(\lambda x)$. □

DEFooOAOGooKuJSup

Définition 6.41 (Quelques ensembles d'applications linéaires)**.**
Soient E et F des espaces vectoriels.

- *L'ensemble des applications linéaires de E vers F est noté $\mathcal{L}(E, F)$, comme déjà dit en 6.35.*

- *Une application linéaire $E \to E$ est un* ***endomorphisme*** *de E. L'ensemble des endomorphismes de E est noté* $\mathrm{End}(E)$.
- *Un endomorphisme bijectif est un* ***automorphisme***. *L'ensemble des automorphismes de E est noté* $\mathrm{Aut}(E)$.
- *Une application linéaire bijective $E \to F$ est un* ***isomorphisme*** *d'espace vectoriel. L'ensemble des isomorphismes de $E \to F$ est noté*[17] $\mathrm{GL}(E, F)$. *C'est un groupe par le lemme 6.40.*

Remarque 6.42.
Les ensembles définis en 6.41 concernent la structure d'espace vectoriel seulement. Lorsque nous verrons la notion d'espace vectoriel normé, nous demanderons de plus, la continuité, laquelle n'est pas automatique en dimension infinie. Voir aussi les définitions 12.331.

Définition 6.43.
Si E est un espace vectoriel, si X est un espace vectoriel, et si $f\colon X \to E$ est une application, le ***noyau*** *de f est le noyau de f lorsque E est vu comme un groupe pour l'addition*[18]*, c'est-à-dire la partie*

$$\ker(f) = \{x \in X \text{ tel que } f(x) = 0\}. \tag{6.39}$$

PROPooRLLPooKYzsJp

Proposition 6.44.
Le noyau d'une application linéaire est un sous-espace vectoriel.

Démonstration. Soit une application linéaire $f\colon E \to F$. Si $x, y \in \ker(f)$ et si $\lambda \in \mathbb{K}$ alors

$$f(x + y) = f(x) + f(y) = 0 + 0 = 0, \tag{6.40}$$

donc $x + y \in \ker(f)$, et

$$f(\lambda x) = \lambda f(x) = 0, \tag{6.41}$$

donc $\lambda x \in \ker(f)$. □

LEMooIQJMooJWRbub

Lemme 6.45 ([1]).
Soit une application linéaire $f\colon V \to W$. Si $b \in W$ et si $m \in f^{-1}(b)$, alors

$$f^{-1}(b) - m = \ker(f). \tag{6.42}$$

Démonstration. Si $x \in f^{-1}(b) - m$, il existe $\alpha \in f^{-1}(b)$ tel que $x = \alpha - m$. Alors

$$f(x) = f(\alpha) - f(m) = b - b = 0. \tag{6.43}$$

Pour l'inclusion dans l'autre sens, si $z \in \ker(f)$, alors $z = (z + m) - m$ avec $z + m \in f^{-1}(b)$ parce que

$$f(z + m) = f(z) + f(m) = 0 + b = b = . \tag{6.44}$$

□

Proposition 6.46.
Si E et F sont des espaces vectoriels de dimension n et si $\{e_i\}_{i=1,\dots,n}$ et $\{f_i\}_{i=1,\dots,n}$ sont des bases respectivement de E et F, alors il existe une unique application linéaire $T\colon E \to F$ telle que $T(e_i) = f_i$ pour tout i.

Démonstration. En deux parties.

(1) **Existence** Soit $v \in E$. Vu que $\{e_i\}$ est une base, v se décompose de façon unique en $v = \sum_i v_i e_i$. Alors la définition

$$T(v) = \sum_i v_i f_i \tag{6.45}$$

est une bonne définition et satisfait aux exigences.

(2) **Unicité** Soient T et U satisfaisant aux exigences. Alors pour tout i nous avons $T(e_i) = U(e_i)$. Si $v \in E$ s'écrit de la forme $v = \sum_i v_i e_i$ alors la linéarité impose $T(v) = \sum_i v_i T(e_i) = \sum_i v_i U(e_i) = U(v)$. Donc $T = U$.

[17] Le fait d'utiliser une notation similaire à celle des matrices inversibles n'est pas anodine : le lecteur en est sans doute conscient.
[18] Définition 2.19.

□

LEMooJXFIooKDzRWR

Lemme 6.47 ([1]).
Soient des espaces vectoriels V et W de dimension finie. Soient des bases $\{e_i\}$ de V et $\{f_\alpha\}$ de W. Nous posons

$$\begin{aligned}\varphi_{i\alpha}\colon V &\to W\\ v &\mapsto v_i f_\alpha\end{aligned} \tag{6.46}$$

où v_i est défini par la décomposition (unique) $v = \sum_i v_i e_i$.
Alors :

(1) La partie $\{\varphi_{i\alpha}\}$ est une base de $\mathcal{L}(V,W)$.

ITEMooPMLWooNbTyJI

(2) Au niveau des dimensions : $\dim\big(\mathcal{L}(V,W)\big) = \dim(V)\dim(W)$.

Démonstration. Il faut prouver que $\{\varphi_{i\alpha}\}$ est libre et générateur.

(1) **Générateur** Soit une application linéaire $b\colon V \to W$. En décomposant $b(v)$ dans la base $\{f_\alpha\}$, nous définissons $b_\alpha\colon V \to \mathbb{K}$ par

$$b(v) = \sum_\alpha b_\alpha(v) f_\alpha. \tag{6.47}$$

Nous posons $b_{\alpha i} = b_\alpha(e_i)$. Ainsi,

$$b(v) = \sum_\alpha v_i b_{\alpha i} f_\alpha = \sum_{\alpha i} b_{\alpha i}\varphi_{i\alpha}(v). \tag{6.48}$$

Donc b peut être écrit comme combinaison linéaire des $\varphi_{i\alpha}$.

(2) **Libre** Supposons que $\sum_{i\alpha} a_{i\alpha}\varphi_{i\alpha} = 0$ pour certains coefficients $a_{i\alpha} \in \mathbb{K}$. Nous avons, pour tout $v \in V$:

$$0 = \sum_{i\alpha} a_{i\alpha}\varphi_{i\alpha}(v) = \sum_{i\alpha} a_{i\alpha} v_i f_\alpha, \tag{6.49}$$

mais comme les f_α forment une base, chaque terme de la somme sur α est nul :

$$\sum_i a_{i\alpha} v_i = 0. \tag{6.50}$$

Et comme cela est valable pour tout v et donc, pour tout choix de v_i, nous avons $a_{i\alpha} = 0$ pour tout i et pour tout α.

La formule de dimension est simplement la cardinalité de la base trouvée ; c'est la définition 6.17. □

6.2.2 Linéarité et bases

Proposition 6.48 ([157]).
Soient deux espaces vectoriels E et F. Une application linéaire[19] *$f\colon E \to F$ est injective si et seulement si $\ker(f) = \{0\}$.*

Démonstration. Nous supposons que f est injective. Si $x \in \ker(f)$, alors $f(x) = 0$. Or f est linéaire, donc $f(0) = 0$. Nous avons donc $f(x) = f(0)$ et donc $x = 0$ parce que f est injective.

Dans l'autre sens, soient x, y tels que $f(x) = f(y)$. Par linéarité de f nous avons $f(x-y) = 0$, et donc $x - y = 0$ parce que $\ker(f) = \{0\}$. Donc $x = y$ et f est injective. □

PROPooZFKZooBGLSex

Proposition 6.49 ([157]).
Soit $f \in \mathcal{L}(E,F)$ où E et F sont deux espaces vectoriels.

ITEMooPPMEooIaZqtm

(1) Si f est injective et si $\{v_i\}_{i\in I}$ est libre, alors $\{f(v_i)\}_{i\in I}$ est libre.

ITEMooOZSPooQBrDGi

(2) Si f est surjective et si $\{v_i\}_{i\in I}$ est génératrice, alors $\{f(v_i)\}_{i\in I}$ est génératrice.

ITEMooOIEYooIfdFnv

(3) Si f est une bijection, alors l'image d'une base par f est une base.

Démonstration. En trois parties.

[19] Définition 6.33.

(1) **(1)** Nous devons montrer que $\{f(v_j)\}_{j\in J}$ est libre pour tout J fini dans I. Soit donc une partie finie $J \subset I$ et des scalaires[20] tels que $\sum_{j\in J} \lambda_j f(v_j) = 0$. La linéarité de f donne[21]

$$f\big(\sum_{j\in J} \lambda_j v_j\big) = 0. \tag{6.51}$$

Par injectivité de f nous avons alors $\sum_j \lambda_j v_j = 0$. Comme les v_j eux-même forment une partie libre, nous avons $\lambda_j = 0$ pour tout $j \in J$.

(2) **(2)** Soit $y \in F$. Puisque f est surjective, il existe $x \in E$ tel que $f(x) = y$. Étant donné que $\{v_i\}_{i\in I}$ est générateur, il existe une partie finie $J \subset I$ et des scalaires $\lambda_j \in \mathbb{K}$ tels que

$$x = \sum_{j\in J} \lambda_j v_j. \tag{6.52}$$

En appliquant f aux deux côtés, et en tenant compte de la linéarité de f,

$$y = f(x) = \sum_{j\in J} \lambda_j f(v_j), \tag{6.53}$$

ce qui prouve que y est une combinaison linéaire des $f(v_j)$.

(3) **(3)** Une base est à la fois libre et génératrice et une bijection est à la fois injective et surjective. Les deux premiers points permettent de conclure.

□

CORooXIPKooWThOsr

Corolaire 6.50 ([1]).
Si E et F sont des espaces vectoriels isomorphes de dimensions finies. Alors leurs dimensions sont égales.

Démonstration. Puisque E et F sont isomorphes, il existe une bijection $f\colon E \to F$. Par la proposition 6.49(3), l'image d'une base de E est une base de F. Donc les espaces E et F ont des bases contenant le même nombre d'éléments. □

6.2.3 Rang

La proposition 6.51 et le théorème 6.53 sont valables également en dimension infinie ; ce sera une des rares incursions en dimension infinie de ce chapitre.

DefALUAooSPcmyK

Proposition-Définition 6.51.
*L'image d'une application linéaire est un espace vectoriel. La dimension de cet espace est le **rang** de ladite application linéaire.*

Démonstration. Soit une application linéaire $f\colon E \to F$. Nous considérons v, w dans l'image de f ainsi que λ dans le corps de base commun à E et F.

Soient $v_0 \in E$ et $w_0 \in E$ tels que $v = f(v_0)$ et $w = f(w_0)$. Alors $v + w = f(v_0 + w_0)$ et $\lambda v = f(\lambda v_0)$. Donc l'image est bien un espace vectoriel. □

LEMooARZGooMOlgsl

Lemme 6.52 ([1]).
Soient des espaces vectoriels E, F avec $\dim(E) \geqslant \dim(F)$ et une application linéaire de rang maximum $f\colon E \to F$. Soit une base $\{e_1, \dots, e_m\}$ de E. Alors il existe une une application linéaire $\phi\colon E \to E$ qui

(1) est une permutation des vecteurs de base,

(2) $(f \circ \phi)\big(\operatorname{Span}\{e_1, \dots, e_n\}\big) = \mathbb{R}^n$.

ThoGkkffA

Théorème 6.53 (Théorème du rang).
Soient E et F deux espaces vectoriels (de dimensions finies ou non) et soit $f\colon E \to F$ une application linéaire.

Si $(u_s)_{s\in S}$ est une base de $\ker(f)$ et si $\big(f(v_t)\big)_{t\in T}$ est une base de $\operatorname{Image}(f)$ alors

$$(u_s)_{s\in s} \cup (v_t)_{t\in T} \tag{6.54}$$

[20] Des éléments du corps de base $\mathbb{K}$.
[21] Voir les propriétés de la définition 6.33.

est une base de E.

En dimension finie, nous avons en plus la formule suivante :

$$rang(f) + \dim(\ker f) = \dim E, \tag{6.55}$$

EQooUEOQooLySRiE

c'est-à-dire que le rang[22] *de f est égal à la codimension*[23] *du noyau.*

Démonstration. Nous devons montrer que

$$(u_s)_{s\in S} \cup (v_t)_{t\in T} \tag{6.56}$$

est libre et générateur.

Soit $x \in E$. Nous définissons les nombres x_t par la décomposition de $f(x)$ dans la base $\big(f(v_t)\big)$:

$$f(x) = \sum_{t\in T} x_t f(v_t). \tag{6.57}$$

Ensuite le vecteur $x - \sum_t x_t v_t$ est dans le noyau de f, par conséquent nous le décomposons dans la base (u_s) :

$$x - \sum_t x_t v_t = \sum_{s\in S} x_s u_s. \tag{6.58}$$

Par conséquent

$$x = \sum_s x_s u_s + \sum_t x_t v_t. \tag{6.59}$$

En ce qui concerne la liberté nous écrivons

$$\sum_t x_t v_t + \sum_s x_s u_s = 0. \tag{6.60}$$

En appliquant f nous trouvons que

$$\sum_t x_t f(v_t) = 0 \tag{6.61}$$

et donc que les x_t doivent être nuls. Nous restons avec $\sum_s x_s u_s = 0$ qui à son tour implique que $x_s = 0$. □

Un exemple d'utilisation de ce théorème en dimension infinie sera donné dans le cadre du théorème de Fréchet-Riesz, théorème 27.17.

LEMooOMZUooDvwbhf

Lemme 6.54 ([1])**.**
Soient des espaces vectoriels E et F de dimension finie. Si $f\colon E \to F$ est une application linéaire injective, alors

ITEMooSTNLooGfZYMp

(1) $rang(f) = \dim(E)$.

ITEMooTAONooSUTnHq

(2) $\dim(E) \leqslant \dim(F)$.

Démonstration. En deux parties.

(1) **Pour (1)** Soit une base $\{e_1, \dots, e_n\}$ de E. Étant donné que f est injective, la partie $\{f(e_1), \dots, f(e_n)\}$ est libre dans F. En effet si $\sum_i a_i f(e_i) = 0$ alors $f(\sum_i a_i e_i) = 0$ et donc $\sum_i a_i e_i = 0$ parce que f est injective. La dernière égalité implique que $a_i = 0$ parce que $\{e_i\}_{i=1,\dots,n}$ est libre.

Donc

$$rang(f) = \dim\big(f(E)\big) \geqslant n = \dim(E). \tag{6.62}$$

D'autre part le théorème du rang, sous forme de l'équation 6.55 dit que $rang(f) \leqslant \dim(E)$.

(2) **Pour (2)** Nous avons déjà prouvé que $\{f(e_i)\}_{i=1,\dots,n}$ est une partie libre de F. Le théorème de la base incomplète 6.28 dit alors qu'il existe une base de F contenant cette partie libre. Vu que $\text{Card}\big(\{f(e_i)\}_{i=1,\dots,n}\big) = n$, nous avons $\dim(F) \geqslant n$.

□

[22] Définition 6.51.
[23] Définition 6.21.

PROPooQCIXooHIyPPq

Proposition 6.55 ([158]).
Soit E, un espace vectoriel de dimension finie sur le corps $\mathbb{K}$. Soient V et W des sous-espaces vectoriels de E. Alors

$$\dim(V+W)=\dim(V)+\dim(W)-\dim(V\cap W). \tag{6.63}$$

Démonstration. Nous considérons l'application

$$\begin{aligned}\varphi\colon V\times W&\to E\\ (x,y)&\mapsto x+y.\end{aligned} \tag{6.64}$$

C'est une application linéaire dont l'image est $V+W$. Nous avons donc, pour commencer

$$\dim(V+W)=\dim\big(\text{Image}(\varphi)\big). \tag{6.65}$$

Nous appliquons à présent le théorème du rang 6.53 à l'application φ :

$$\begin{aligned}\dim(V+W)&=\dim\big(\text{Image}(\varphi)\big) &(6.66a)\\ &=\dim(V\times W)-\dim\big(\ker(\varphi)\big) &(6.66b)\\ &=\dim(V)+\dim(W)-\dim\big(\ker(\varphi)\big). &(6.66c)\end{aligned}$$

Nous devons maintenant étudier $\ker(\varphi)$. D'abord, $(v,w)\in V\times W$ appartient à $\ker(\varphi)$ si et seulement si $v+w=0$. Nous avons donc

$$\ker(\varphi)=\{(x,-x)\text{ tel que }x\in V\cap W\}. \tag{6.67}$$

Nous montrons à partir de cela que $\dim\big(\ker(\varphi)\big)=\dim(V\cap W)$ en montrant que l'application

$$\begin{aligned}\psi\colon V\cap W&\to\ker(\varphi)\\ x&\mapsto(x,-x)\end{aligned} \tag{6.68}$$

est un isomorphisme d'espaces vectoriels. D'abord ψ est injective parce que si $\psi(x)=\psi(y)$, alors $(x,-x)=(y,-y)$ et donc $x=y$. Ensuite, ψ est surjective parce qu'un élément générique de $\ker(\varphi)$ est $(x,-x)=\psi(x)$ avec $x\in V\cap W$. L'application ψ étant un isomorphisme d'espaces vectoriels, nous avons bien $\dim\big(\ker(\varphi)\big)=\dim(V\cap W)$. □

CORooCCXHooALmxKk

Corolaire 6.56.
Soient deux espaces vectoriels E et F de même dimension finie[24]*. Pour une application linéaire $f\colon E\to F$, les trois conditions suivantes sont équivalentes :*

(1) f est injective ;

(2) f est surjective ;

(3) f est bijective.

Démonstration. Si $f\colon E\to E$ est surjective, alors $rang(f)=\dim(E)$, ce qui donne, par le théorème du rang 6.53, $\dim\big(\ker(f)\big)=0$, c'est-à-dire que f est injectif.

De la même façon, si f est injective, alors $\dim\big(\ker(f)\big)=0$, ce qui donne $rang(f)=\dim(E)$ ou encore que f est surjective. □

Exemple 6.57.
Le corolaire 6.56 n'est pas correct en dimension infinie. Par exemple en prenant $f(e_1)=f(e_2)=e_1$ et ensuite $f(e_k)=e_{k-1}$ pour tout $k\geqslant 2$. Cette application est surjective mais pas injective. △

LEMooNNDDooKXdqud

Lemme 6.58 ([1]).
Soit un espace vectoriel E. Si $p\colon E\to E$ est un projecteur[25] *vérifiant $p(E)=E$, alors $p=\mathrm{Id}$.*

Démonstration. L'hypothèse est que p est surjective. Le corolaire 6.56 dit que p est alors bijective et donc inversible. En partant de $p^2(x)=p(x)$ et en appliquant p^{-1} est deux côtés nous trouvons $p(x)=x$. Donc $p=\mathrm{Id}$. □

PROPooKUAVooCbjDcR

Proposition 6.59 ([1]).
Soient des espaces vectoriels de dimension finie V et W vérifiant $\dim(V)>\dim(W)$. Si $f\colon V\to W$ est une application linéaire, alors $\dim\big(\ker(f)\big)\geqslant\dim(V)-\dim(W)$.

[24] Les deux mots sont importants : les dimensions doivent être égales et finies.
[25] Définition 3.107.

Démonstration. Il s'agit d'une conséquence du théorème du rang (6.55). Vu que $rang(f) \leqslant \dim(W)$, nous avons

$$\dim\big(\ker(f)\big) = \dim(V) - rang(f) \geqslant \dim(V) - \dim(W). \tag{6.69}$$

□

Une conséquence du théorème du rang est que les endomorphismes ont un inverse à gauche et à droite égaux (lorsqu'ils existent). En résumé, ce que le corolaire 6.60 dit est que si $AB = \mathbb{1}$, alors $BA = \mathbb{1}$.

CORooNFJLooJtzFwN

Corolaire 6.60.
Soit un endomorphisme f d'un espace vectoriel de dimension finie. Si f admet un inverse à gauche, alors

(1) f est bijective,

(2) f admet également un inverse à droite,

(3) les inverses à gauche et à droite sont égaux.

Tout cela tient également en remplaçant « gauche » par « droite ».

Démonstration. Soit g, un inverse à gauche de f : $gf = \mathrm{Id}$. Cela implique que f est injective et que g est surjective, et donc qu'elles sont toutes deux bijectives par le corolaire 6.56. Puisque f est bijective, elle admet également un inverse à droite, soit h. Nous avons : $gf = \mathrm{Id}$ et $fh = \mathrm{Id}$.

Alors $gfh = h$ parce que $gf = \mathrm{Id}$, mais également $gfh = g$ parce que $fh = \mathrm{Id}$. Donc $g = h$.[26] □

C'est ce corolaire qui nous permet d'écrire f^{-1} sans plus de précisions dès que f est une bijection.

Exemple 6.61 (Pas en dimension infinie)**.**
Tout cela ne fonctionne pas en dimension infinie. Par exemple avec une base $\{e_k\}_{k\in\mathbb{N}}$ nous pouvons considérer l'opérateur

$$f(e_k) = e_{k+1}. \tag{6.70}$$

Il est injectif, mais pas surjectif. Si on pose

$$g(e_k) = \begin{cases} e_{k-1} & \text{si } k \geqslant 1 \\ 0 & \text{si } k = 0 \end{cases} \tag{6.71}$$

alors nous avons $gf = \mathrm{Id}$, mais pas $fg = \mathrm{Id}$ parce que ce $(fg)(e_0) = 0$. △

LEMooRZDTooEuLTrO

Lemme 6.62.
Si E et F sont des espaces vectoriels et si $f\colon E \to F$ est une application linéaire inversible, alors son inverse est également linéaire.

Démonstration. Nous avons $f^{-1}(x + y) = f^{-1}(x) + f^{-1}(y)$. En effet,

$$f\big(f^{-1}(x) + f^{-1}(y)\big) = f\big(f^{-1}(x)\big) + f\big(f^{-1}(y)\big) = x + y. \tag{6.72}$$

De la même façon,

$$f\big(\lambda f^{-1}(x)\big) = \lambda x, \tag{6.73}$$

donc $f^{-1}(\lambda x) = \lambda f^{-1}(x)$. □

LEMooVGDDooRmUDUi

Lemme 6.63 ([1])**.**
Soient une application linéaire $f\colon E \to F$ ainsi que $v_1, \dots, v_2 \in E$. Alors

$$\mathrm{Span}\big(\{f(v_i)\}_{i=1,\dots,k}\big) = f\big(\mathrm{Span}(\{v_i\}_{i=1,\dots,k})\big). \tag{6.74}$$

Démonstration. Dans un sens, un élément générique de $\mathrm{Span}\big(\{f(v_i)\}_{i=1,\dots,k}\big)$ est

$$\sum_{i=1}^{k} a_j f(v_i) = f\Big(\sum_i a_i v_i\Big) \in f\big(\mathrm{Span}(\{v_i\}_{i=1,\dots,k})\big). \tag{6.75}$$

Dans l'autre sens, un élément générique de $f\big(\mathrm{Span}(\{v_i\}_{i=1,\dots,k})\big)$ est

$$f\Big(\sum_i a_i v_i\Big) = \sum_i a_i f(v_i) \in \mathrm{Span}\big(\{f(v_i)\}_{i=1,\dots,k}\big). \tag{6.76}$$

□

[26] C'est le même argument que celui employé pour la preuve du lemme 2.1 (2), à ceci près que nous devions montrer l'existence de l'inverse à droite.

PROPooHLUYooNsDgbn

Proposition 6.64.
Soient un espace vectoriel E de dimension finie, un endomorphisme $f\colon E\to E$ et une partie $\{v_i\}_{i\in I}$ tel que $\{f(v_i)\}_{i\in I}$ soit une base.
Alors $\{v_i\}_{i\in I}$ est une base.

Démonstration. Soit $x\in E$. Il existe une partie finie $J\subset I$ et des scalaires λ_j tels que

$$x=\sum_j\lambda_j f(v_j)=f\big(\sum_j\lambda_j v_j\big),\tag{6.77}$$

ce qui prouve que f est surjective. Le corolaire 6.56 nous dit alors que f est une bijection. L'application inverse est également linéaire par le lemme 6.62.

Une application linéaire bijective (comme f^{-1}) transforme une base en une base par la proposition 6.49. Donc

$$f^{-1}\big(\{f(v_i)\}\big)\tag{6.78}$$

est une base. □

PROPooADESooATJSrH

Proposition 6.65.
Soit un espace vectoriel E de dimension finie et deux applications linéaires $f,g\colon E\to E$ telles que $g\circ f=\mathrm{Id}$. Alors f et g sont bijectives.

Démonstration. En plusieurs étapes

(1) **f est injective** Si $f(x)=f(y)$, alors en appliquant g nous avons

$$g\big(f(x)\big)=g\big(f(y)\big),\tag{6.79}$$

ce qui donne $x=y$.

(2) **f est surjective** C'est maintenant le corolaire 6.56.

(3) **g est surjective** Pour tout $x\in E$ nous avons $g\big(f(x)\big)=x$. Donc l'image de $f(E)$ par g est E.

(4) **g est injective** C'est maintenant le corolaire 6.56.

□

LEMooDAACooElDsYb

Lemme 6.66 ([159]).
Soit une application linéaire $f\colon E\to F$.

ITEMooEZEWooZGoqsZ

(1) L'application f est injective si et seulement si il existe $g\colon F\to E$ telle que $g\circ f=\mathrm{Id}\,|_E$.

(2) L'application f est surjective si et seulement si il existe $g\colon F\to E$ telle que $f\circ g=\mathrm{Id}\,|_F$.

Démonstration. Nous démontrons séparément les deux affirmations.

(1) Si f est injective, alors $f\colon E\to\mathrm{Image}(f)$ est un isomorphisme. Si V est un supplémentaire de $\mathrm{Image}(f)$ dans F (c'est-à-dire $F=\mathrm{Image}(f)\oplus V$) alors nous pouvons poser $g(x+v)=f^{-1}(x)$ où $x+v$ est la décomposition (unique) d'un élément de F en $x\in\mathrm{Image}(f)$ et $v\in V$. Avec cela nous avons bien $g\circ f=\mathrm{Id}$.

Réciproquement, si il existe $g\colon F\to E$ telle que $g\circ f=\mathrm{Id}$ alors $f\colon E\to E$ doit être injective. Parce que si $f(x)=0$ avec $x\neq 0$ alors $(g\circ f)(x)=0\neq x$.

(2) Si f est surjective nous pouvons choisir des éléments $x_1,\dots,x_p$ dans E tels que $\{f(x_i)\}$ soit une base de F. Ensuite nous définissons

$$\begin{aligned}g\colon F&\to E\\ \sum_k a_k f(x_k)&\mapsto\sum_k a_k x_k.\end{aligned}\tag{6.80}$$

Cela donne $f\circ g=\mathrm{Id}\,|_F$ parce que si $v\in F$ alors $v=\sum_k v_k f(x_k)$ avec $v_k\in\mathbb{K}$, et nous avons

$$(f\circ g)(v)=\sum_k v_k(f\circ g)\big(f(x_k)\big)=f\left(\sum_k v_k x_k\right)=\sum_k v_k f(x_k)=v.\tag{6.81}$$

Réciproquement, si il existe $g\colon F\to E$ tel que $f\circ g=\mathrm{Id}$ alors f doit être surjective, parce que

$$F=\mathrm{Image}(f\circ g)=f\big(\mathrm{Image}(g)\big)\subset\mathrm{Image}(f).\tag{6.82}$$

□

6.3 Matrices

Les matrices et les applications linéaires sont deux choses différentes. Une application linéaire[27] est une application d'un espace vectoriel vers un autre, et une matrice est un simple tableau de nombres sur lesquels nous définissons des opérations, de telle sorte à fournir une structure d'espace vectoriel. Le lien entre ces opérations et les opérations correspondantes sur les applications linéaires sera fait plus tard. Voir la définition 6.78 et ce qui s'en suit.

6.3.1 Définitions

Les notions topologiques sur les espaces de matrices sont pour plus tard, à commencer par la définition 11.34.

Définition 6.67.
Soit un anneau $\mathbb{A}$ ainsi que des entiers m, n strictement positifs. L'ensemble $\mathbb{M}(n\times m,\mathbb{A})$ est l'ensemble des applications

$$\{1,\dots,n\}\times\{1,\dots,m\}\to\mathbb{A}, \tag{6.83}$$

*et est appelé ensemble des **matrices** $n\times m$ sur $\mathbb{A}$.*

Si A est une matrice, nous notons $A_{i,j}$ au lieu de $A(i,j)$ l'image de (i,j) par l'application A.

Définition 6.68.
Quelques ensembles de matrices particuliers.

(1) *Si $n=m$, alors :*

- *nous disons que la matrice est **carrée**,*
- *nous notons $\mathbb{M}(n,\mathbb{A})$ pour $\mathbb{M}(n\times n,\mathbb{A})$,*
- *n est appelée **ordre** de la matrice.*

(2) *Si $n=1$, alors la matrice est appelée **matrice-ligne**.*

(3) *Si $m=1$, alors la matrice est appelée **matrice-colonne**.*

6.69.
On note les isomorphismes naturels $\mathbb{M}(1\times m,\mathbb{A})\simeq\mathbb{A}^m$ et $\mathbb{M}(n\times 1,\mathbb{A})\simeq\mathbb{A}^n$.

LEMooYWTEooQyLxKv

Lemme-Définition 6.70.
Nous considérons les opérations suivantes sur $\mathbb{M}(n\times m,\mathbb{A})$:

Somme $(A+B)_{i,j}=A_{i,j}+B_{i,j}$,

Produit par un scalaire $(\lambda\cdot A)_{i,j}=\lambda A_{i,j}$ *pour tout $A,B\in\mathbb{M}(n\times m,\mathbb{A})$ et $\lambda\in\mathbb{A}$.*

Alors $\big(\mathbb{M}(n\times m,\mathbb{A}),+,\ \cdot\ \big)$ est un $\mathbb{A}$-module[28].

Démonstration. Plusieurs parties. Il faut vérifier les conditions de la définition 3.94.

(1) **Groupe** Le neutre est la matrice nulle $N_{ij}=0$. Nous avons $((A+B)+C)_{ij}=(A+B)_{ij}+C_{ij}=A_{ij}+B_{ij}+C_{ij}$. Et l'inverse de A est $B_{ij}=-A_{ij}$.

(2) **Autres propriétés** Nous n'allons pas toutes les faire. Par exemple

$$\begin{aligned}\lambda\big(\lambda(A+B)\big)_{ij}&=\lambda(A+B)_{ij} &(6.84a)\\ &=\lambda(A_{ij}+B_{ij}) &(6.84b)\\ &=\lambda A_{ij}+\lambda B_{ij} &(6.84c)\\ &=(\lambda A)_{ij}+(\lambda B)_{ij}. &(6.84d)\end{aligned}$$

Notez l'utilisation de $\lambda(x+y)=\lambda x+\lambda y$ lorsque $x,y\in\mathbb{A}$.

□

[27] Définition 6.33.
[28] Définition 3.94

LEMooMBZTooKdGvON

Lemme-Définition 6.71.
Avec la multiplication

$$\begin{aligned}\mathbb{M}(n\times p,\mathbb{A})\times\mathbb{M}(p\times m,\mathbb{A})&\to\mathbb{M}(n\times m,\mathbb{A})\\(A,B)&\mapsto(AB)_{i,j}=\sum_{k=1}^{p}A_{i,k}B_{k,j},\end{aligned}\tag{6.85}$$

l'espace $\mathbb{M}(n,\mathbb{K})$ *est une* $\mathbb{K}$*-algèbre*[29].

Démonstration. Il faut vérifier les trois formules de la définition 3.111.

(1) **Distribution (1)** Nous avons

$$\big((x+y)\times z\big)_{ij}=\sum_k(x+y)_{ik}z_k=\sum_k\big(x_{ik}z_kj+y_{ik}z_{kj}\big)=(xz)_{ij}+(yz)_{ij}.\tag{6.86}$$

(2) **Distribution (2)** Même calcul.

(3) **Multiplication par un scalaire** Encore le même genre de calculs, en partant de

$$\big((\alpha x)\times(\beta y)\big)_{ij}=\sum_k(\alpha x)_{ik}(\beta y)_{kj}.\tag{6.87}$$

□

Définition 6.72.
Pour un élément $A\in\mathbb{M}(n\times m,\mathbb{A})$ *nous définissons encore*

La transposée $A^t_{i,j}=A_{j,i}$,

La trace $\mathrm{Tr}(A)=\sum_i A_{i,i}$.

Remarque 6.73.
Quelques remarques directes sur les définitions.

(1) La motivation de cette définition pour le produit apparaîtra plus loin, mais le Frido n'étant pas un livre d'introduction, j'imagine que le lecteur a déjà une idée.

(2) Nous verrons plus loin en 10.11.4 que la définition de transposée d'une application linéaire n'est pas tout à fait évidente ; elle sera la définition 10.187.

Ici nous avons bien défini la transposée d'une matrice, pas d'une application linéaire.

Remarque 6.74.
Quelques remarques à propos de structures supplémentaires.

(1) Nous utiliserons (presque) tout le temps des matrices à coefficients dans un corps. Il est clair que, si $\mathbb{K}$ est un corps (commutatif), alors $\mathbb{M}(n\times m,\mathbb{K})$ a une structure d'espace vectoriel sur $\mathbb{K}$.

(2) Par ailleurs, sur les matrices carrées d'ordre n fixé, le produit de deux matrices est bien défini. Ainsi, $\mathbb{M}(n,\mathbb{A})$ se voit conférer une structure d'anneau, dont le neutre pour la multiplication est la matrice carrée $\mathbb{1}_n$ (notée aussi $\mathbb{1}$ lorsqu'il n'y a pas d'ambiguïté sur la taille), donnée par

$$\mathbb{1}_{i,j}=\begin{cases}1 & \text{si } i=j\\ 0 & \text{sinon.}\end{cases}\tag{6.88}$$

Il est vite vu que si A est une matrice carrée d'ordre n, alors $A\mathbb{1}=\mathbb{1}A=A$.

LEMooUXDRooWZbMVN

Lemme 6.75 ([1])**.**
Si A*,* B *et* C *sont des matrices, nous avons*

(1) $(AB)^t=B^tA^t$,

ITEMooXDYQooAlnArd

(2) $\mathrm{Tr}(ABC)=\mathrm{Tr}(CAB)$.

[29] Définition 3.111.

Démonstration. La première est un simple calcul :

$$(AB)^t_{i,j} = (AB)_{j,i} = \sum_k A_{j,k}B_{k,i} = \sum_k A^t_{k,j}B^t_{i,k} = (B^tA^t)_{i,j}. \tag{6.89}$$

Pour la seconde :

$$\mathrm{Tr}(ABC) = \sum_{ikl} A_{i,k}B_{k,l}C_{l,i} = \sum_{ikl} C_{l,i}A_{i,k}B_{k,l} = \sum_l (CAB)_{l,l} = \mathrm{Tr}(CAB). \tag{6.90}$$

□

6.76.
La seconde égalité est importante et est nommée **invariance cyclique** de la trace. Elle sert, entre autres nombreuses choses, à prouver que la trace d'une matrice d'une application linéaire ne dépend pas de la base choisie. Ce sera la proposition 10.205.

LEMooLXAHooPRyHaF

Lemme 6.77.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$. Si pour tout $x, y \in \mathbb{K}^n$ nous avons

$$\sum_{ij} A_{i,j}x_iy_j = \sum_{ij} B_{i,j}x_iy_j \tag{6.91}$$

alors $A = B$.

Démonstration. Il suffit de choisir $x_i = \delta_{i,k}$ et $y_j = \delta_{j,l}$ et d'effectuer les sommes ; par exemple

$$\sum_{ij} A_{i,j}\delta_{i,k}y_j = \sum_j A_{k,j}y_j. \tag{6.92}$$

Après avoir effectué toutes les sommes, nous nous retrouvons avec $A_{k,l} = B_{k,l}$, ce qui signifie $A = B$. □

6.3.2 Identifier matrices et applications linéaires

Voir dans l'index thématique, -1.1.1.

Soient deux espaces vectoriels de dimension finie E, F sur le corps $\mathbb{K}$. Nous considérons les bases[30] $\{e_i\}$ pour E et $\{f_\alpha\}$ pour F.

DEFooJVOAooUgGKme

Définition 6.78.
Nous considérons l'application

$$\begin{aligned}\psi\colon \mathbb{M}(n\times m, \mathbb{K}) &\to \mathcal{L}(E,F)\\ A &\mapsto f_A\end{aligned} \tag{6.93}$$

EQooVZQWooMxFFeO

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha,i}x_if_\alpha \tag{6.94}$$

EQooBVGHooJhFbMs

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

6.79.
Nous allons prouver un certain nombre de résultats montrant que cette application a toutes les propriétés imaginables permettant d'identifier les matrices aux applications linéaires : elle est un isomorphisme pour toutes les structures que vous pouvez raisonnablement imaginer.

À cette application ψ il manque cependant une propriété importante : elle n'est pas canonique. Elle dépend des bases choisies. Autrement dit : nous avons à priori autant d'applications ψ différentes qu'il y a de choix de bases sur E et F[31].

Nous allons prouver maintenant quelques résultats montrant que les matrices et les applications linéaires, dans le cas des espaces vectoriels $\mathbb{K}^n$ sont deux présentations de la même chose.

Le fait que ψ est continue sera la proposition 14.119.

[30] C'est le théorème 6.15 qui nous permet de considérer des bases. Et ce théorème ne fonctionne que parce que nous avons supposé une dimension finie.

[31] Bonne question. Est-ce qu'il y a moyen de construire deux choix de bases donnant la même application ψ ? Écrivez-moi si vous savez la réponse.

6.80.
Lorsque $A \in \mathbb{M}(n, \mathbb{K})$ est une matrice et $x \in \mathbb{K}^n$ un vecteur, nous notons Ax l'élément de $\mathbb{K}^n$ donné par

$$(Ax)_i = \sum_j A_{i,j} x_j. \tag{6.95}$$

Autrement dit, $Ax = f_A(x)$.

Cette convention et de nombreuses autres à propos de matrice sera rappelée dans -1.1.

Proposition-Définition 6.81.
Soient deux espaces vectoriels de dimension finie E, F sur le corps $\mathbb{K}$. Nous considérons les bases $\{e_i\}$ pour E et $\{f_\alpha\}$ pour F.

Nous considérons l'application

$$\begin{aligned} \psi \colon \mathbb{M}(n \times m, \mathbb{K}) &\to \mathcal{L}(E, F) \\ A &\mapsto f_A \end{aligned} \tag{6.96}$$

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha,i} x_i f_\alpha \tag{6.97}$$

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

Alors

(1) Nous avons

$$f_A(e_i)_\alpha = A_{\alpha,i}. \tag{6.98}$$

(2) Nous avons

$$f_A(e_i) = \sum_\alpha A_{\alpha,i} f_\alpha. \tag{6.99}$$

(3) Nous avons

$$\big(f_A(x)\big)_\alpha = \sum_i A_{\alpha,i} x_i. \tag{6.100}$$

(4) L'application ψ est une bijection.

*Si f est une application linéaire, alors la matrice $\psi^{-1}(f)$ est la **matrice associée** à f dans les bases choisies.*

Remarque : les bases ne sont supposées être canoniques en aucun sens du terme. Les dimensions de E et F ne sont pas non plus supposées identiques.

Démonstration. En nous rappelant que $(e_j)_i = \delta_{i,j}$ nous avons

$$f_A(e_j) = \sum_{i\alpha} A_{\alpha,i} (e_j)_i f_\alpha = \sum_\alpha A_{\alpha,j} f_\alpha, \tag{6.101}$$

donc $f_A(e_i)_\alpha = A_{\alpha,i}$. Cela prouve la formule du point (1).

Le point (2) est une simple somme sur α de (1).

La formule du point (3) est simplement la composante f_α de la définition 6.97.

Prouvons que ψ est injective. Si $f_A = f_B$, nous avons en particulier $f_A(e_i)_\alpha = f_B(e_i)_\alpha$ et donc $A_{\alpha,i} = B_{\alpha,i}$.

Prouvons que ψ est surjective. Pour cela nous considérons $f \in \mathcal{L}(E, F)$ et nous posons $A_{\alpha,i} = f(e_i)_\alpha$. Nous avons alors $f = f_A$ parce que

$$f_A(x) = \sum_{i\alpha} A_{\alpha,i} x_i f_\alpha = \sum_{i\alpha} f(e_i)_\alpha x_i f_\alpha = \sum_\alpha f(\sum_i x_i e_i)_\alpha f_\alpha = \sum_\alpha f(x)_\alpha f_\alpha = f(x). \tag{6.102}$$

□

La proposition suivante montre que le produit matriciel correspond à la composition d'applications linéaires, pourvu que l'on travaille avec les bases canoniques sur $\mathbb{K}^n$.

PROPooIYVQooOiuRhX

Proposition 6.82 ([1]).
Soit un corps commutatif $\mathbb{K}$. Nous considérons des espaces vectoriels E et F munis de bases $\{e_i\}_{i=1,\dots,n}$ et $\{f_\alpha\}_{\alpha=1,\dots,m}$.

L'application déjà définie[32]

$$\psi\colon \mathbb{M}(m\times n,\mathbb{K})\to\mathcal{L}(E,F) \tag{6.103}$$

est un isomorphisme d'espaces vectoriels.

Démonstration. Le fait que ψ soit une bijection est la proposition 6.81. Nous devons montrer que c'est une application linéaire.

Pour $\lambda\in\mathbb{K}$ nous avons le calcul

$$\psi(\lambda A)(e_k)=f_{\lambda A}(e_k)=\sum_{\alpha i}(\lambda A)_{\alpha,i}\underbrace{(e_k)_i}_{=\delta_{k,i}}f_\alpha=\lambda\sum_\alpha A_{\alpha,k}f_\alpha=\lambda f_A(e_k). \tag{6.104}$$

Donc $\psi(\lambda A)=\lambda\psi(A)$.

Si $A,B\in\mathbb{M}(n,\mathbb{K})$ nous avons de la même façon, $f_{A+B}=f_A+f_B$. □

PROPooCSJNooEqcmFm

Proposition 6.83.
Soient des espaces vectoriels E, F et G de dimensions n, m et p munis de bases[33] *$\{e_i\}$, $\{f_i\}$ et $\{g_i\}$. Nous considérons les applications*

$$\psi\colon \mathbb{M}(m\times n,\mathbb{K})\to\mathcal{L}(E,F) \tag{6.105a}$$
$$\psi\colon \mathbb{M}(p\times m,\mathbb{K})\to\mathcal{L}(F,G) \tag{6.105b}$$
$$\psi\colon \mathbb{M}(p\times n,\mathbb{K})\to\mathcal{L}(E,G). \tag{6.105c}$$

Nous avons

$$\psi(A)\circ\psi(B)=\psi(AB) \tag{6.106}$$

pour toutes matrices $A\in\mathbb{M}(p\times m,\mathbb{K})$ et $B\in\mathbb{M}(m\times n,\mathbb{K})$.

Démonstration. Nous considérons les applications linéaires associées à A et B : $f_A\colon F\to G$ et $f_B\colon E\to F$ et la composée $f_A\circ f_B\colon E\to G$. Et puis c'est le calcul :

$$(f_A\circ f_B)(e_k)=f_A\Big(\sum_{ij}B_{i,j}(e_k)_jf_i\Big) \tag{6.107a}$$
$$=\sum_i B_{i,k}f_A(f_i) \tag{6.107b}$$
$$=\sum_i B_{i,k}\sum_{rs}A_{r,s}(f_i)_sg_r \tag{6.107c}$$
$$=\sum_{ir}B_{i,k}A_{r,i}g_r \tag{6.107d}$$
$$=\sum_r(AB)_{r,k}g_r \tag{6.107e}$$
$$=f_{AB}(e_k). \tag{6.107f}$$

Donc $f_A\circ f_B=f_{AB}$ comme il se doit. □

Nous pouvons particulariser au cas où $E=F=G$.

PROPooFMBFooEVCLKA

Proposition 6.84.
Si E est un espace vectoriel muni d'une base $\{e_i\}$, alors l'application

$$\psi\colon \mathbb{M}(n,\mathbb{K})\to\mathrm{End}(E) \tag{6.108}$$

est un isomorphisme d'algèbre[34] *et d'anneaux*[35].

[32] Notez la position du n et du m. Sachez noter les bornes des sommes écrites dans la démonstration.
[33] Avec trois ensembles, nous renonçons à utiliser des alphabets différents pour numéroter les éléments des bases.
[34] Définition 3.111.
[35] Définition 1.106

Démonstration. Le fait que ψ soit un isomorphisme d'algèbre est juste la combinaison entre les propositions 6.82 et 6.83.

En ce qui concerne l'isomorphisme d'anneaux, il faut en plus identifier les neutres. Le neutre pour la composition d'applications linéaires est l'application identité et le neutre pour la multiplication de matrices est la matrice identité. Nous devons donc montrer que $\psi(\delta) = f_\delta = \mathrm{Id}$. Juste un calcul :

$$f_\delta(x) = \sum_{ij} \delta_{i,j} x_j e_i = \sum_i x_i e_i = x. \tag{6.109}$$

Donc oui, f_δ est l'identité. □

Le fait que ψ est continue sera la proposition 14.119.

Voilà. Soyez bien conscient que l'application ψ dont nous avons beaucoup parlé est surtout intéressante dans le cas des espaces de la forme $\mathbb{K}^n$. Dans ce cas, nous avons une identification canonique entre $\mathbb{M}(n, \mathbb{K})$ et $\mathrm{End}(\mathbb{K}^n)$ qui est un isomorphisme d'anneaux et d'algèbres.

Nous verrons que ce ψ respecte encore les inverses[36] et les déterminants[37].

6.85.
Il convient de ne pas confondre matrice et application linéaire (bien que nous le ferons sans vergogne). Une matrice est un bête tableau de nombres, tandis qu'une application linéaire est une application entre deux espaces vectoriels vérifiant certaines propriétés.

Cependant si les espaces vectoriels E et F sont munis de bases, alors il y a une application

$$\psi : \mathbb{M}(m \times n, \mathbb{K}) \to \mathcal{L}(E, F) \tag{6.110}$$

qui a toutes les propriétés imaginables[38].

Cette application dépend des bases choisies. Il n'y a donc pas de trucs comme « la matrice de telle application linéaire » ou comme « voici une matrice, nous considérons l'application linéaire associée ».

Cependant, sur des espaces comme $\mathbb{R}^n$ ou plus généralement sur $\mathbb{K}^n$, nous avons une base canonique et toute personne raisonnable utilise toujours la base canonique (sauf mention du contraire). Dans ces cas il est sans danger de dire « la matrice associée à telle application linéaire » sans préciser les bases.

Mais si un jour vous utilisez une base autre que la base canonique sur $\mathbb{R}^n$, précisez-le et plutôt deux fois qu'une[39].

6.86.
Tant que nous sommes à parler de matrice et d'applications linéaires, les plus acharnés anti-abus de language[40] remarqueront qu'il n'est pas vrai que « étant donné une base, une application linéaire a une matrice ».

En effet, une base est une partie libre et génératrice (définition 6.6). Or une partie d'un ensemble n'est pas muni d'un ordre. Toutes les permutations de colonnes de la matrice sont encore possible d'après l'ordre que l'on met sur les vecteurs de la base.

Encore une fois, la base canonique n'a pas de problème parce que les $\{e_i\}$ de $\mathbb{R}^n$ viennent avec un ordre indiscutable. Plus généralement, très souvent, lorsqu'on construit une base, la construction suggère un ordre.

6.3.3 Ensemble des applications linéaires

PROPooRIFBooGOvsfb

Proposition 6.87 ([1])**.**
Soient deux espaces vectoriels de dimension finie V et W. Soit des bases $\{e_i\}_{i\in I}$ de V et $\{e'_j\}_{j\in J}$ de W. Nous considérons les applications

EQooBMKQooCCypzP

$$\begin{aligned} f_{ij} &: V \to W \\ \sum_k x_k e_k &\mapsto x_i e'_j. \end{aligned} \tag{6.111}$$

Nous avons :

ITEMooSEMLooXuxrpk

(1) Ces applications sont linéaires.

(2) Elles forment une base de $\mathcal{L}(V, W)$.

(3) $\dim(V, W) = \dim(V)\dim(W)$.

[36] Proposition 6.107.
[37] Proposition 10.16.
[38] Et elle en aura encore plus lorsque nous aurons vu les déterminants.
[39] Au passage, non, les coordonnées polaires ne sont pas une base de $\mathbb{R}^2$. C'est un système de coordonnées, et ce n'est pas la même chose.
[40] Dont l'auteur de ces lignes fait partie.

Démonstration. Pas de preuve pour le moment. Vous pouvez aider en m'envoyant une preuve. □

PROPooPNQNooAZpojm

Proposition 6.88 ([1]).
Soient des bases $\{e_i\}$ et $\{e'_j)\}$ des espaces vectoriels V et W. Soit une application linéaire $A \in \mathrm{End}(V, W)$. Alors

$$A = \sum_{ij} A_{ji} f_{ij} \tag{6.112}$$

où les f_{ij} sont les éléments de bases définis en (6.111) et A_{ji} sont les éléments de matrices définis par la proposition 6.81.

Démonstration. Il s'agit d'un calcul. En appliquant à e_k, nous avons

$$\sum_{ij} A_{ji} f_{ij}(e_k) = \sum_{ij} A_{ji} \delta_{ik} e'_j = \sum_j A_{jk} e'_j. \tag{6.113}$$

En comparant avec la formule de la proposition 6.81(1), nous avons le résultat. □

6.3.4 Déterminant

DEFooYCKRooTrajdP

Définition 6.89.
*Si $A \in \mathbb{M}(n, \mathbb{K})$ nous définissons le **déterminant** de A par la formule*

$$\det(A) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{6.114}$$

où la somme est effectuée sur tous les éléments du groupe symétrique[41] S_n et où $(-1)^\sigma$ représente la parité de la permutation σ.

En se souvenant que $|S_n| = n!$, nous sommes frappés de stupeur devant le fait que le nombre de termes dans la somme croît de façon factorielle (c'est plus qu'exponentiel, pour info) en la taille de la matrice. Cette formule est donc sans espoir pour une matrice plus grande que 3×3 ou à la rigueur 4×4 à la main. À l'ordinateur, il est possible de monter plus haut, mais pas tellement.

6.3.5 Déterminant en petite dimension

En dimension deux, le déterminant de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est le nombre

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb. \tag{6.115}$$

EQooQRGVooChwRMd

Ce nombre détermine entre autres le nombre de solutions que va avoir le système d'équations linéaires associé à la matrice.

Pour une matrice 3×3, nous avons le même concept, mais un peu plus compliqué ; nous avons la formule

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}. \tag{6.116}$$

6.3.6 Manipulations de lignes et de colonnes

Nous voudrions savoir ce qu'il se passe avec le déterminant d'une matrice lorsque nous substituons à une ligne ou une colonne, une combinaison des autres lignes et colonnes. Lorsqu'une matrice est donnée, nous notons C_j sa j^{e} colonne.

LEMooRSJTooQEoOtN

Lemme 6.90 ([1]).
Si A et B sont des matrices, alors

$$(AB)^t = B^t A^t. \tag{6.117}$$

[41] Pour le groupe symétrique, c'est la définition 2.2, le fait que ce soit un groupe fini est le lemme 2.97, et pour la somme sur un groupe fini c'est la définition 2.129.

Démonstration. Il suffit de calculer les éléments de matrice :

$$(AB)^t_{i,j} = (AB)_{j,i} = \sum_k A_{j,k}B_{k,i} = \sum_k B^t_{i,k}A^t_{k,j} = (B^tA^t)_{i,j}. \tag{6.118}$$

□

LEMooCEQYooYAbctZ

Lemme 6.91 ([1, 160])**.**
Si A est une matrice, alors $\det(A) = \det(A^t)$.

Démonstration. Nous commençons par écrire la définition du déterminant :

$$\det(A^t) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^n (A^t)_{i,\sigma(i)} = \sum_\sigma \epsilon(\sigma)\prod_i A_{\sigma(i),i}. \tag{6.119}$$

Pour chaque σ séparément, en utilisant la proposition 2.130 pour ré-indexer le produit :

$$\prod_i A_{\sigma(i),i} = \prod_i A_{i,\sigma^{-1}(i)}. \tag{6.120}$$

Nous profitons du fait que l'application $\varphi\colon S_n \to S_n$ donnée par $\varphi(\sigma) = \sigma^{-1}$ soit une permutation de S_n pour appliquer la définition 2.129 et faire la somme sur σ^{-1} :

$$\det(A^t) = \sum_\sigma \epsilon(\sigma)\prod_i A_{i,\sigma^{-1}(i)} = \sum_\sigma \epsilon(\sigma^{-1})\prod_i A_{i,\sigma(i)} = \det(A) \tag{6.121}$$

où nous avons utilisé le fait que $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$ (corolaire 2.125). □

Le fait que $\det(A) = \det(A^t)$ permet, dans toutes les propositions du type « ce qui arrive au déterminant si on change telle ligne ou colonne » de ne donner qu'une preuve pour la partie « ligne » et déduire automatiquement le cas « colonne ». Le lemme suivant donne un exemple d'utilisation.

LEMooWMQWooGWFlmC

Lemme 6.92 ([1])**.**
Soit une matrice A. Nous considérons la matrice B obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$ ainsi que la matrice C obtenue à partir de A^t par la permutation de colonnes $C_k \leftrightarrow C_l$.
Alors $C^t = B$.

Démonstration. Calculons les éléments de matrice de C :

$$C_{i,j} = \begin{cases} (A^t)_{i,j} & \text{si } j\neq k, j\neq l \\ (A^t)_{i,k} & \text{si } j = l \\ (A^t)_{i,l} & \text{si } j = k \end{cases} = \begin{cases} A_{j,i} & \text{si } j\neq k, j\neq l \\ A_{k,i} & \text{si } j = l \\ A_{l,i} & \text{si } j = k. \end{cases} \tag{6.122}$$

Ensuite nous prouvons que $C^t = B$ en écrivant les éléments de C^t :

$$(C^t)_{i,j} = C_{j,i} = \begin{cases} A_{i,j} & \text{si } i\neq k, i\neq l \\ A_{k,j} & \text{si } i = l \\ A_{l,j} & \text{si } i = k. \end{cases} \tag{6.123}$$

Cette dernière expression est la matrice A après permutation des lignes $L_k \leftrightarrow L_l$, c'est-à-dire la matrice B. □

Pour la suite nous écrivons δ la matrice « identité », c'est-à-dire celle dont les entrées sont précisément les $\delta_{i,k}$. Nous écrivons également $E_{i,j}$ la matrice contenant des zéros partout sauf en (i,j) où elle a un 1, c'est-à-dire

$$(E_{i,j})_{k,l} = \delta_{i,k}\delta_{j,l}. \tag{6.124}$$

PROPooFQRDooRPfuxk

Proposition 6.93 (Permuter des lignes ou des colonnes $L_k \leftrightarrow L_l$[161, 1])**.**
Soient une matrice $A \in \mathbb{M}(n,\mathbb{K})$, deux entiers $k \neq l$ inférieurs ou égaux à n.

ITEMooAIHWooHXzeys

(1) Si B est la matrice obtenue à partir de A en permutant deux lignes ou deux colonnes, alors

$$\det(A) = -\det(B). \tag{6.125}$$

ITEMooDNHWooOMgmxa

(2) *Si B est la matrice obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$. Alors*

$$B = SA \tag{6.126}$$

avec $S = \delta + E_{k,l} + E_{l,k} - E_{k,k} - E_{l,l}$.

Autrement dit : la matrice S est une matrice de permutations de lignes.

ITEMooSHRQooQrqVdO

(3) *La matrice S vérifie $\det(S) = -1$*

ITEMooQXSEooMWiKbL

(4) *Nous avons*

$$\det(SA) = \det(S)\det(A). \tag{6.127}$$

Démonstration. Point par point

(1) **(1) pour les colonnes**

Soient k et l fixés, et considérons la permutation des colonnes C_k et C_l. Nous notons α la permutation (k, l) dans S_n (groupe symétrique, définition 2.2). Nous avons

$$B_{i,j} = A_{i,\alpha(j)}, \tag{6.128}$$

ou encore : $A_{i,j} = B_{i,\alpha(j)}$. Par définition,

$$\det(A) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{6.129}$$

C'est le moment d'utiliser la proposition 2.136 à propos de somme sur des groupes avec $G = S_n$, $h = \alpha$ et

$$f(\sigma) = \epsilon(\sigma) \prod_i A_{i,\sigma(i)}. \tag{6.130}$$

Nous savons que $\epsilon(\alpha) = -1$ et que ϵ est un morphisme par la proposition 2.124(1), donc

$$f(\alpha\sigma) = \epsilon(\alpha\sigma) \prod_i A_{i,(\alpha\sigma)(i)} = -\epsilon(\sigma) \prod_i B_{i,\sigma(i)}. \tag{6.131}$$

Avec ça, nous concluons :

$$\det(A) = \sum_{\sigma\in S_n} f(\sigma) = \sum_{\sigma} f(\alpha\sigma) = -\sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} B_{i,\sigma(i)} = -\det(B). \tag{6.132}$$

(2) **(1) pour les lignes** Que se passe-t-il si nous permutons les lignes L_k et L_l ? Si nous notons B' la matrice obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$, et C celle obtenue de A^t après permutation de colonnes $C_k \leftrightarrow C_l$ alors nous avons $C^t = B'$. Le lemme 6.92 nous dit que $C^t = B'$. En utilisant le lemme 6.91 sur le déterminant de la transposée,

$$\det(B') = \det(C^t) = \det(C) = -\det(A^t) = -\det(A). \tag{6.133}$$

Voilà qui prouve le résultat pour les permutations de lignes.

(3) **(2)** Si $k = l$, il n'y a pas de permutation, et il est vite vu que la matrice S est l'identité parce qu'il y a quatre fois le terme $E_{k,k}$. Nous supposons donc que $k \neq l$; en particulier $\delta_{k,l} = 0$.

Il s'agit surtout d'un beau calcul :

$$(SA)_{i,j} = \sum_m S_{i,m}A_{m,j} = A_{i,j} + \sum_m (\delta_{k,i}\delta_{l,m} + \delta_{l,i}\delta_{l,m} - \delta_{k,i}\delta_{k,m} - \delta_{l,i}\delta_{l,m})A_{m,j} \tag{6.134a}$$

$$= A_{i,j} + \delta_{k,i}A_{l,j} + \delta_{l,i}A_{k,j} - \delta_{k,i}A_{k,j} - \delta_{l,i}A_{l,j}. \tag{6.134b}$$

Si $i \neq j$ et $i \neq l$, alors $(SA)_{i,j} = A_{i,j}$. Si $i = k$, alors

$$(SA)_{k,j} = A_{k,j} + A_{l,j} - A_{k,j} = A_{l,j}, \tag{6.135}$$

c'est-à-dire que la k^{e} ligne de SA est la l^{e} ligne de A.

Avec $i = l$ nous obtenons la k^{e} ligne de A.

Tout cela montre que SA est la matrice A dans laquelle les lignes k et l ont été échangées, c'est-à-dire $SA = B$.

(4) **(3)** En utilisant la définition du déterminant,

$$\det(S) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} S_{i,\sigma(i)} \tag{6.136a}$$

$$= \sum_{\sigma} \epsilon(\sigma) \prod_{i} \big(\delta_{i,\sigma(i)} + \delta_{k,i}\delta_{l,\sigma(i)} + \delta_{l,i}\delta_{k,\sigma(i)} - \delta_{k,i}\delta_{k,\sigma(i)} - \delta_{l,i}\delta_{l,\sigma(i)}\big). \tag{6.136b}$$

Nous utilisons l'associativité et la commutativité du produit pour séparer les facteurs $i = k$ et $i = l$ des autres :

$$\det(S) = \sum_{\sigma} \epsilon(\sigma) \prod_{\substack{i\neq k\\ i\neq l}} \delta_{i,\sigma(i)}(\delta_{k,\sigma(k)} + \delta_{l,\sigma(k)} - \delta_{k,\sigma(k)})(\delta_{l,\sigma(l)} + \delta_{k,\sigma(l)} - \delta_{l,\sigma(l)}). \tag{6.137}$$

À cause des facteurs $i \neq k$ et $i \neq l$, les σ pour lesquels le tout n'est pas nul doivent vérifier $\delta_{i,\sigma(i)} = 1$ pour tout i différent de k et l. Les deux seuls sont donc $\sigma = \mathrm{Id}$ et la permutation $\sigma = (k, l)$. Pour $\sigma = \mathrm{Id}$, nous avons

$$\prod_{\substack{i\neq k\\ i\neq l}} \delta_{i,i}(\delta_{k,k} + \delta_{l,k} - \delta_{k,k})(\delta_{l,l} + \delta_{k,l} - \delta_{l,l}) = 0. \tag{6.138}$$

Dernier espoir : $\sigma = (k, l)$. Pour ce terme nous avons $\epsilon(\sigma) = -1$ et

$$\prod_{\substack{i\neq k\\ i\neq l}} \delta_{i,i}(\delta_{k,l} + \delta_{l,l} - \delta_{k,l})(\delta_{l,k} + \delta_{k,k} - \delta_{l,k}) = 1. \tag{6.139}$$

Au final dans $\det(S)$, il n'y a que le terme $\sigma = (k, l)$ qui est non nul, et il vaut -1. Donc

$$\det(S) = -1. \tag{6.140}$$

(5) **(4)** Il s'agit de mettre bout à bout les points déjà prouvés :

$$\det(SA) = -\det(A) = \det(S)\det(A). \tag{6.141}$$

□

CORooAZFCooSYINvBl

Corolaire 6.94 ([161]).
Soit une matrice $A \in \mathbb{M}(n, \mathbb{K})$. Si deux lignes ou deux colonnes de A sont égales, alors $\det(A) = 0$.

Démonstration. Si deux colonnes sont égales, la matrice ne change pas lorsqu'on les permute, alors que le déterminant change de signe. La seule possibilité est que $\det(A) = -\det(A)$, ce qui signifie que $\det(A) = 0$. □

Notons que si pour $k \neq l$ nous avons $C_k = \lambda C_l$, alors nous avons aussi $\det(A) = 0$.

La réciproque n'est pas vraie : il existe des matrices dont le déterminant est nul et dont aucune entrée n'est nulle. Par exemple

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}. \tag{6.142}$$

PROPooNGZJooHjtMyn

Proposition 6.95 ([161]).
Soient $A \in \mathbb{M}(n, \mathbb{K})$, et $v \in \mathbb{K}^n$. Si B est la matrice A avec la substitution $L_j \to L_j + v$ et C est la matrice A avec la substitution $L_j \to v$, alors

$$\det(B) = \det(A) + \det(C). \tag{6.143}$$

Démonstration. En utilisant l'associativité de la multiplication,

$$\det(B) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n} B_{i,\sigma(i)} \tag{6.144a}$$
$$= \sum_{\sigma} \epsilon(\sigma)\big(\prod_{i\neq j} B_{i,\sigma(i)}\big)B_{j,\sigma(j)} \tag{6.144b}$$
$$= \sum_{\sigma} \epsilon(\sigma)\big(\prod_{i\neq j} A_{i,\sigma(i)}\big)(A_{j,\sigma(j)} + v_{\sigma(j)}) \tag{6.144c}$$
$$= \sum_{\sigma} \epsilon(\sigma)\prod_{i} A_{i,\sigma(i)} + \sum_{\sigma} \epsilon(\sigma)\prod_{i\neq j} C_{i,\sigma(i)}v_{\sigma(j)} \tag{6.144d}$$
$$= \det(A) + \sum_{\sigma} \epsilon(\sigma)\prod_{i\neq j} C_{i,\sigma(i)}C_{j,\sigma(j)} \tag{6.144e}$$
$$= \det(A) + \det(C). \tag{6.144f}$$

Justifications :

- 6.144d parce que pour $i \neq j$ nous avons $A_{i,\sigma(i)} = C_{i,\sigma(i)}$
- 6.144e parce que $v_{\sigma(j)} = C_{j,\sigma(j)}$.

□

Proposition 6.96 (Combinaison de lignes ou colonnes $L_k \to L_k + \lambda L_l$[161])**.**
Soient une matrice $A \in \mathbb{M}(n,\mathbb{K})$, deux entiers $k \neq l$ inférieurs ou égaux à n.

(1) Si B est la matrice obtenue à partir de A par la substitution $L_k \to L_k + \lambda L_l$ ou $C_k \to C_k + \lambda C_l$, alors

$$\det(A) = \det(B). \tag{6.145}$$

(2) Si B est la matrice A dans laquelle nous avons opéré la substitution $L_k \to L_k + \lambda L_l$, alors

$$B = UA \tag{6.146}$$

avec $U = \delta + \lambda E_{k,l}$, c'est-à-dire que U est une matrice de combinaison de lignes.

(3) La matrice U vérifie $\det(U) = 1$.

(4) Nous avons

$$\det(UA) = \det(U)\det(A). \tag{6.147}$$

Démonstration. Point par point.

(1) **(1)** Soit la matrice C obtenue à partir de A par $L_k \to \lambda L_l$. En considérant le vecteur $v = \lambda L_l$, nous sommes dans la situation de la proposition 6.95. Donc

$$\det(B) = \det(A) + \det(C). \tag{6.148}$$

Mais dans la matrice C, nous avons $L_k = \lambda L_l$, ce qui implique $\det(C) = 0$ par le corolaire 6.94. Donc $\det(A) = \det(B)$ comme il se devait.

(2) **(2)** Encore un calcul :

$$(UA)_{i,j} = \sum_m \big(\delta_{i,m} + \lambda(E_{k,l})_{i,m}\big)A_{m,j} = A_{i,j} + \lambda\sum_m \delta_{k,i}\delta_{l,m}A_{m,j} = A_{i,j} + \lambda\delta_{l,i}A_{k,j}. \tag{6.149}$$

Cela donne, pour $i = k$ la ligne

$$(UA)_{k,j} = A_{k,j} + \lambda A_{l,j}, \tag{6.150}$$

ce qui correspond bien à $L_k \to L_k + \lambda L_l$.

(3) **(3)** Nous calculons le déterminant de $U = \delta + \lambda E_{k,l}$ avec $k \neq l$. Nous avons dans un premier temps :

$$\det(U) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n}(\delta_{i,\sigma(i)} + \lambda\delta_{k,i}\delta_{l,\sigma(i)}). \tag{6.151}$$

Puisque nous avons toujours $\delta_{k,i}\delta_{l,i}=0$, le terme $\sigma=\mathrm{Id}$ donne 1.

Pour les $\sigma\neq\mathrm{Id}$, le facteur $\lambda\delta_{k,i}\delta_{l,\sigma(i)}$ ne s'annule pas, uniquement si $i=k$ et $\sigma(i)=l$. Donc le seul terme non nul autre que $\sigma=\mathrm{Id}$ peut provenir de $\sigma=(k,l)$. Pour ce terme, nous isolons les termes $i=l$ et $i=k$:

$$(\delta_{k,\sigma(k)}+\lambda\delta_{k,k}\delta_{k,\sigma(k)})(\delta_{l,\sigma(l)}+\lambda\delta_{k,l}\delta_{k,\sigma(l)}).\tag{6.152}$$

Le dernier facteur est nul.

(4) (4) En mettant bout à bout les résultats prouvés,

$$\det(UA)=\det(A)=\det(U)\det(A).\tag{6.153}$$

□

PROPooXUFKooOaPnna

Proposition 6.97 (Multiplication par un scalaire d'une ligne ou colonne $L_k\to\lambda L_k$[161])**.**
Soient une matrice $A\in\mathbb{M}(n,\mathbb{K})$, un entier $k\leqslant n$. Soit la matrice B obtenue à partir de A en multipliant la ligne L_k par $\lambda\in\mathbb{K}$.

ITEMooBKIGooCDQEDt

(1) $\det(B)=\lambda\det(A)$

ITEMooWRRCooFXkRNW

(2) En considérant la matrice $T=\delta+(\lambda-1)E_{k,k}$, nous avons

$$B=TA,\tag{6.154}$$

c'est-à-dire que la matrice T est une matrice de multiplication de ligne par un scalaire.

ITEMooOGGDooPVVRzk

(3) Nous avons $\det(T)=\lambda$.

ITEMooIFRVooWQYgkK

(4) Et aussi : $\det(TA)=\det(T)\det(A)$

Démonstration. Point par point.

(1) (1) La matrice B est donnée par les éléments

$$B_{i,j}=\begin{cases}A_{i,j} & \text{si } i\neq k\\ \lambda A_{i,j} & \text{si } i=k\end{cases}\tag{6.155}$$

c'est-à-dire $B_{i,j}=\big(1+(\lambda-1)\delta_{i,k}\big)A_{i,j}$. Nous mettons cela dans la définition du déterminant de B :

$$\det(B)=\sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n}B_{i,\sigma(i)}=\sum_{\sigma}\prod_{i}\big(1+(\lambda-1)\delta_{\sigma(i),k}A_{i,\sigma(i)}\big).\tag{6.156}$$

EQooGVMTooPutKcw

L'associativité du produit dans $\mathbb{K}$ nous permet de séparer le produit de la façon suivante :

$$\prod_{i=1}^{n}\big(1+(\lambda-1)\delta_{\sigma(i),k}\big)A_{i,\sigma(i)}=\prod_{i}\big(1+(\lambda-1)\delta_{\sigma(i),k}\big)\prod_{i}A_{i,\sigma(i)}=\lambda\prod_{i}A_{i,\sigma(i)}.\tag{6.157}$$

En remettant dans (6.156), nous trouvons $\det(B)=\det(A)$.

(2) (2) C'est un cas particulier de la proposition 6.96(2) en prenant $k=l$ et en adaptant le λ.

(3) (3) Nous calculons le déterminant de la matrice $T=\delta+(\lambda-1)E_{k,k}$. La formule du déterminant donne

$$\det(T)=\sum_{\sigma}\epsilon(\sigma)\prod_{i=1}^{n}\big(\delta_{i,\sigma(i)}+(\lambda-1)\delta_{k,i}\delta_{k,\sigma(i)}\big).\tag{6.158}$$

Si $i\neq\sigma(i)$, alors non seulement $\delta_{i,\sigma(i)}=0$, mais en plus $\delta_{k,i}\delta_{k,\sigma(i)}=0$. Donc seul $\sigma=\mathrm{Id}$ reste dans la somme sur $\sigma\in S_n$. Il reste donc

$$\det(T)=\prod_{i=1}^{n}\big(1+(\lambda-1)\delta_{k,i}\big)=\left(\prod_{i\neq k}1\right)(1+(\lambda-1))=\lambda\tag{6.159}$$

où nous avons utilisé encore l'associativité pour isoler le facteur $i=k$.

(4) (4) Il faut mettre bout à bout les résultats déjà établis :

$$\det(TA)=\lambda\det(A)=\det(T)\det(A).\tag{6.160}$$

□

6.3.7 Réduction de Gauss

DEFooKJNNooOcIJuu

Définition 6.98.
Nous avons vu les matrices d'opérations élémentaire sur les lignes :

- *Permutation de lignes $L_k \leftrightarrow L_l$: $S(n;k,l) = \delta + E_{k,l} + E_{l,k} - E_{k,k} - E_{l,l}$, proposition 6.93.*
- *Combinaisons de lignes $L_k \to L_k + \lambda L_l$: $U(n;k,l,\lambda) = \delta + \lambda E_{k,l}$, proposition 6.96.*
- *Multiplication d'une ligne par un scalaire $L_k \to \lambda L_k$: $T(n;k,\lambda) = \delta + (\lambda - 1)E_{k,k}$, proposition 6.97.*

Les matrices $S(n;k,l)$, $U(n;k,l)$ et $T(n;k,\lambda)$ sont les ***matrices de manipulation de lignes****.*

NORMooDXYZooEdnztA

6.99.
Il existe également des matrices pour faire les mêmes opérations, mais sur les colonnes. Ces matrices doivent toutefois multiplier à droite et non à gauche. Par exemple il existe une matrice $C(n,k,l)$ telle que $AC(n,k,l)$ soit la matrice A, avec les colonnes k et l inversées.

LEMooDXSZooVpbCRj

Lemme 6.100.
Si G est une matrice de manipulation de lignes, alors

EQooLQTVooBYiVYl

$$\det(GA) = \det(G)\det(A) \tag{6.161}$$

pour toute matrice A.

Si H est une matrice de manipulation de colonnes, alors

$$\det(AH) = \det(A)\det(H) \tag{6.162}$$

pour toute matrice A.

Démonstration. En ce qui concerne les manipulations de ligne, nous avons déjà tout fait dans les propositions 6.93(4), 6.96(4) et 6.97(4).

□

PROPooJBTZooNLobpf

Proposition 6.101 (Réduction de Gauss[1])**.**
Soit une matrice $A \in \mathbb{M}(n,\mathbb{K})$ de déterminant non nul : $\det(A) \neq 0$*. Alors il existe des matrices $G_1,\dots,G_N$ toutes de type S, U ou T telles que*

$$G_1 \dots G_N A = \delta. \tag{6.163}$$

Démonstration. Nous procédons par récurrence sur n. D'abord pour $n = 1$, la matrice A contient un seul élément $A_{1,1}$ qui est non nul par hypothèse. Nous pouvons multiplier sa ligne par $1/A_{1,1}$ pour obtenir le résultat. Plus précisément, nous avons l'égalité

$$T(1;1,\frac{1}{A_{1,1}})A = \delta \tag{6.164}$$

dans $\mathbb{M}(1,\mathbb{K})$. Notons que $\mathbb{K}$ est un corps (donc $A_{1,1}$ est inversible) commutatif, ce qui permet d'écrire $1/A_{1,1}$ sans ambiguïté.

Supposons le résultat prouvé pour n, et voyons ce qu'il se passe pour $n+1$. Puisque $\det(A) \neq 0$, aucune de ses colonnes n'est nulle (corolaire 6.94). Il existe donc un k tel que $A_{k,1} \neq 0$.

Par la proposition 6.93, la matrice

$$B^{(1)} = S(n+1;k,1)A \tag{6.165}$$

est une matrice telle que $B^{(1)}_{1,1} = A_{k,1} \neq 0$. Ensuite, par la proposition 6.97 la matrice

$$B^{(2)} = T(n+1;1,\frac{1}{A_{k,1}})B^{(1)} \tag{6.166}$$

vérifie $B^{(2)}_{1,1} = 1$.

Puisque la multiplication par la matrice $U(n+1;k;l;\lambda)$ réalise, par la proposition 6.96, la substitution $L_k \to L_k + \lambda L_l$, la matrice

$$B^{(3)} = \prod_{k=2}^{n+1} U(n+1;k,1,-B^{(1)}_{k,1})B^{(1)} \tag{6.167}$$

a toute sa première colonne nulle à l'exception de $B^{(3)}_{1,1} = 1$.

Nous n'avons pas donné de nom ni démontré de théorèmes à propos de la substitution $C_k \to C_k + \lambda C_l$. En passant éventuellement par les transposées et en utilisant les lemmes 6.90 et 6.91 nous obtenons une matrice $U'(n+1;k,l,\lambda)$ ayant la propriété que la matrice

$$B^{(4)} = \prod_{k=2}^{n+1} U'(n+1;k,1,-B^{(3)}_{1,k})B^{(3)} \tag{6.168}$$

vérifie $B^{(4)}_{1,j} = B^{(4)}_{j,1} = 0$ pour tout j sauf $j=1$. En d'autres termes, la matrice $B^{(4)}$ est de la forme

$$B^{(4)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix} \tag{6.169}$$

où A' est une matrice de taille n.

Voyons quelques propriétés de A'. Nous savons que

$$B^{(4)} = \prod_i G_i A \tag{6.170}$$

où les G_i sont de type S, T ou U. Puisque $\det(SA) = \det(S)\det(A)$ (et idem pour T et U), nous avons

$$\det(B^{(4)}) = \prod_i \det(G_i)\det(A), \tag{6.171}$$

et comme aucun des $\det(G_i)$ n'est nul, nous avons encore $\det(B^{(4)}) \neq 0$, ce qui implique $\det(A') \neq 0$.

La récurrence peut avoir lieu. Il existe des matrices G'_i telles que

$$G'_1 \dots G'_M A' = \delta \tag{6.172}$$

où les G'_i sont de taille n, ainsi que le δ. En remarquant que

$$S(n+1;k,l) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & S(n;k-1,l-1) & \\ 0 & & & \end{pmatrix}, \tag{6.173}$$

et pareillement pour les matrices T et U, nous voyons qu'en prenant

$$G_i = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & G'_i & \\ 0 & & & \end{pmatrix}, \tag{6.174}$$

nous avons

$$\prod_{i=1}^{M} G_i B^{(3)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \prod_{i=1}^{M} G'_i A' & \\ 0 & & & \end{pmatrix} = \delta_{n+1} \tag{6.175}$$

où nous avons mis un indice sur le dernier δ pour être plus explicite. □

6.3.8 Matrices inversibles

PROPooMLWRooRWfZXE

Proposition-Définition 6.102.
Soit une matrice $A \in \mathbb{M}(n,\mathbb{K})$. Si les matrices B_1 et B_2 de $\mathbb{M}(n,\mathbb{K})$ vérifient

$$AB_1 = B_1 A = \delta \tag{6.176}$$

et

$$AB_2 = B_2 A = \delta, \tag{6.177}$$

alors $B_1 = B_2$. Dans ce cas, nous disons que A est inversible et nous notons A^{-1} l'unique matrice telle que $AA^{-1} = A^{-1}A = \delta$.

Démonstration. La preuve est réalisée dans le cas général par le lemme 2.1. Mais si vous en voulez une preuve avec les notations d'ici, en voici une.

Nous avons $AB_1 = AB_2$. En multipliant à gauche par B_1, nous trouvons $B_1AB_1 = B_1AB_2$. En remplaçant B_1A par δ des deux côtés, il reste $B_1 = B_2$. □

LEMooGZCTooQigDvC

Lemme 6.103 ([161]).
Si $A \in \mathbb{M}(n, \mathbb{K})$, alors il existe au plus une matrice $B \in \mathbb{M}(n, \mathbb{K})$ telle que $AB = \delta$.

Démonstration. Soient des matrices $B, C \in \mathbb{M}(n, \mathbb{K})$ telles que $AB = AC = \delta$. Nous allons montrer que $B = C$.

Pour cela nous considérons les applications linéaires $f_A, f_B, f_C \in \mathrm{End}(\mathbb{K}^n)$ associées par la proposition 6.81. Puisque $AB = \delta$, par la proposition 6.83, nous avons $f_A \circ f_B = f_{AB} = \mathrm{Id}$. La proposition 6.65 nous dit alors que f_A et f_B sont bijectives.

En particulier, comme $\{e_i\}$ est une base, son image par f_B est une base par la proposition 6.49. La proposition 6.64 dit alors que $\{f_B(e_i)\}$ est une base. Nous décomposons $f_B(e_k) - f_C(e_k)$ dans cette base :

$$f_B(e_k) - f_C(e_k) = \sum_j \alpha_j f_B(e_j) \tag{6.178}$$

où les α_j dépendent à priori de k. Puisque $f_A \circ (f_B - f_C) = 0$, nous avons

$$0 = f_A\big(f_B(e_k) - f_C(e_k)\big) = \sum_j (f_A \circ f_B)(e_j) = \sum_j \alpha_j e_j. \tag{6.179}$$

Donc les α_j sont tous nuls.

Nous en déduisons que $f_B(e_k) = f_C(e_k)$, et donc $f_B = f_C$. Cela implique que $B = C$ par la proposition 6.81(4). □

PROPooECIIooVMCIwz

Proposition 6.104 ([161]).
Si $A, B \in \mathbb{M}(n, \mathbb{K})$ vérifient $AB = \delta$, alors $BA = \delta$.

Démonstration. L'astuce est de poser $C = BA - \delta + B$ et de montrer que $C = B$. Pour cela, un rapide calcul commence par montrer que

$$AC = ABA - A + AB = AB = \delta. \tag{6.180}$$

Donc C est également un inverse à droite de A. Le lemme 6.103 donne alors $C = B$. □

CORooBQLXooTeVfgb

Corolaire 6.105.
Soit $A \in \mathbb{M}(n, \mathbb{K})$. Si il existe $B \in \mathbb{M}(n, \mathbb{K})$ tel que $AB = \delta$, alors A est inversible et son inverse est B.

Démonstration. Il s'agit d'une paraphrase de la proposition 6.104 et de la définition 6.102. □

LEMooZDNVooArIXzC

Lemme 6.106.
Si une matrice A n'est pas inversible, alors le produit AB n'est inversible pour aucune matrice B.

Démonstration. Soient une matrice non inversible A, ainsi qu'une matrice quelconque B. Supposons que AB soit inversible. Alors

$$AB(AB)^{-1} = \delta. \tag{6.181}$$

Donc la matrice $B(AB)^{-1}$ est un inverse de A. Contradiction. □

PROPooNPMCooPmaCwu

Proposition 6.107.
Une matrice est inversible si et seulement si son application linéaire associée est inversible. Dans ce cas, nous avons

$$f_A^{-1} = f_{A^{-1}}. \tag{6.182}$$

Démonstration. Dans le sens direct, si A est inversible nous avons $AA^{-1} = \delta$. Donc

$$f_A \circ f_{A^{-1}} = f_{AA^{-1}} = f_\delta = \mathrm{Id} \tag{6.183}$$

EQooQQOSooBKVqXb

où nous avons utilisé la proposition 6.83 pour la composition et la proposition 6.84 pour l'identité. L'égalité (6.183) indique que f_A est inversible et que son inverse est $f_{A^{-1}}$.

Dans l'autre sens, l'application f_A^{-1} existe. Soit $B \in \mathbb{M}(n, \mathbb{K})$ sa matrice. Alors nous avons

$$f_\delta = \mathrm{Id} = f_A \circ f_B = f_{AB}. \tag{6.184}$$

Le fait que l'application $\psi\colon A \to f_A$ soit une bijection[42] implique que $AB = \delta$, c'est-à-dire que A est inversible et que $B = A^{-1}$. □

6.3.9 Inversibilité et déterminant

PROPooAVIXooMtVCet

Proposition 6.108.
Une matrice au déterminant non nul est inversible.

Démonstration. Si A est une matrice telle que $\det(A) \neq 0$, alors la proposition 6.101 nous donne des matrices $G_1, \dots, G_N$ telles que

$$G_1 \dots G_N A = \delta. \tag{6.185}$$

Donc la matrice $G_1 \dots G_N$ est un inverse de A par le corolaire 6.105. □

PROPooEOKBooKUROFg

Proposition 6.109.
Si une matrice A a une ligne ou une colonne de zéros, alors

(1) $\det(A) = 0$,

(2) A n'est pas inversible.

Démonstration. Par définition, nous avons

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)}. \tag{6.186}$$

Si la k^{e} ligne est nulle, alors $A_{k,\sigma(k)} = 0$ pour tout σ. Donc tous les produits contiennent un facteur nul. Donc $\det(A) = 0$.

Pour toute matrice B nous avons

$$(AB)_{k,k} = \sum_{l} A_{k,l} B_{l,k}. \tag{6.187}$$

Si la k^{e} ligne de A est nulle nous avons $(AB)_{k,k} = 0$ et donc pas $AB = \delta$. Donc A n'est pas inversible. □

6.3.10 Quelques ensembles de matrices particuliers

Certains ensembles de matrices ont une importance particulière, que nous développerons plus tard.

Définition 6.110 (Groupe linéaire de matrices)**.**
On note $\mathrm{GL}(n, \mathbb{A})$ *l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{A}$, qui sont inversibles. En d'autres termes,* $\mathrm{GL}(n, \mathbb{A}) = U(\mathbb{M}(n, \mathbb{A}))$.

DefMatriceOrthogonale

Définition 6.111 (Groupe orthogonal de matrices)**.**
On dit qu'une matrice A est ***orthogonale*** *si son inverse est sa transposée, c'est-à-dire si $A^{-1} = A^t$. On note* $\mathrm{O}(n, \mathbb{A})$ *l'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{A}$, qui sont orthogonales.*

6.3.11 Déterminant et combinaisons de lignes et colonnes

SUBSPROPooMSZVooBKlwQh

Proposition 6.112.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ telles que $\det(A) \neq 0$ *et* $\det(B) \neq 0$. *Alors*

$$\det(AB) = \det(A)\det(B). \tag{6.188}$$

Démonstration. La proposition 6.101 nous donne des matrices de permutations de lignes et de colonnes $G_1, \dots, G_N$ et $G'_1, \dots, G'_N$ telles que[43] EQooDNZUooHBhcZj

$$G_1 \dots G_N A = \delta \tag{6.189a}$$
$$G'_1 \dots G'_N B = \delta. \tag{6.189b}$$

Nous avons

$$(G'_1 \dots G'_N) \underbrace{(G_1 \dots G_N) A}_{=\delta} B = \delta. \tag{6.190}$$

[42] Proposition 6.81(4).

[43] Les plus acharnés préciseront que pour avoir le même N des deux côtés, il a fallu compléter avec des matrices δ là où il y en avait le moins.

En prenant le déterminant des deux côtés et en tenant compte de (6.161),

$$1 = \det(\delta) = \det\left(G'_1 \dots G'_N G_1 \dots G_N AB\right) = \det(G'_1 \dots G'_N)\det(G_1 \dots G_N)\det(AB). \tag{6.191}$$

Mais en même temps, les équations 6.189 donnent

$$\det(G_1 \dots G_N) = \det(A)^{-1} \tag{6.192a}$$
$$\det(G'_1 \dots G'_N) = \det(B)^{-1}. \tag{6.192b}$$

Cela pour dire que

$$1 = \det(A)^{-1}\det(B)^{-1}\det(AB), \tag{6.193}$$

et donc ce qu'il nous fallait. □

PROPooWVJFooTmqoec

Proposition 6.113.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ telles que $\det(A) = 0$ et $\det(B) \neq 0$. Alors

$$\det(AB) = \det(BA) = \det(A)\det(B) = 0. \tag{6.194}$$

Démonstration. Il existe des matrices de manipulations de lignes et de colonnes $G_1, \dots, G_N$ telles que $G_1 \dots G_N B = \delta$. Donc

$$0 = \det(A) = \det(G_1 \dots G_N BA) = \det(G_1 \dots G_N)\det(BA). \tag{6.195}$$

Donc $\det(BA) = 0$. □

6.3.12 Transvections

Nous nommons $E_{i,j}$ la matrice remplie de zéros sauf à la case i, j qui vaut 1. Autrement dit

$$(E_{i,j})_{k,l} = \delta_{i,k}\delta_{j,l}. \tag{6.196}$$

Définition 6.114.
*Une **matrice de transvection** est une matrice de la forme*

$$T_{i,j}(\lambda) = \mathrm{Id} + \lambda E_{i,j} \tag{6.197}$$

avec $i \neq j$.

*Une **matrice de dilatation** est une matrice de la forme*

$$D_i(\lambda) = \mathrm{Id} + (\lambda - 1)E_{i,i}. \tag{6.198}$$

Ici le $(\lambda - 1)$ sert à avoir λ et non $1 + \lambda$. C'est donc une matrice qui dilate d'un facteur λ la direction i, tout en laissant le reste inchangé.

*Si σ est une permutation (un élément du groupe symétrique S_n) alors la **matrice de permutation** associée est la matrice d'entrées*

$$(P_\sigma)_{i,j} = \delta_{i,\sigma(j)}. \tag{6.199}$$

LemyrAXQs

Lemme 6.115.
La matrice $T_{i,j}(\lambda)A = (\mathbb{1} + \lambda E_{i,j})A$ est la matrice A à qui on a effectué la substitution

$$L_i \to L_i + \lambda L_j. \tag{6.200}$$

La matrice $AT_{i,j}(\lambda)$ est la substitution

$$C_j \to C_j + \lambda C_i. \tag{6.201}$$

La matrice AP_σ est la matrice A dans laquelle nous avons permuté les colonnes avec σ.
La matrice $P_\sigma A$ est la matrice A dans laquelle nous avons permuté les lignes avec σ^{-1}.

Démonstration. Calculons la composante k, l de la matrice $E_{i,j}A$:

$$(E_{i,j}A)_{k,l} = \sum_m (E_{i,j})_{k,m}A_{m,l} \tag{6.202a}$$
$$= \sum_m \delta_{i,k}\delta_{j,m}A_{m,l} \tag{6.202b}$$
$$= \delta_{i,k}A_{j,l}. \tag{6.202c}$$

C'est donc la matrice pleine de zéros, sauf la ligne i qui est donnée par la ligne j de A. Donc effectivement la matrice

$$A + \lambda E_{i,j} A \tag{6.203}$$

est la matrice A à laquelle on a substitué la ligne i par la ligne i plus λ fois la ligne j.

En ce qui concerne l'autre assertion sur les transvections, le calcul est le même et nous obtenons

$$(AE_{i,j}) = A_{k,i}\delta_{j,l}. \tag{6.204}$$

Pour les matrices de permutation, nous avons

$$(AP_\sigma)_{k,l} = A_{k,\sigma(l)} \tag{6.205}$$

et

$$(P_\sigma A)_{k,l} = \sum_m \delta_{k,\sigma(m)} A_{m,l} = \sum_m \delta_{\sigma^{-1}(k),m} A_{m,l} = A_{\sigma^{-1}(k),l}. \tag{6.206}$$

□

6.3.13 Mineur, rang

Pour la définition du rang d'une matrice, nous en donnons une qui est clairement inspirée de l'application linéaire associée.

DEFooCSGXooFRzLRj

Définition 6.116 ([161]).
*Le **rang** d'une matrice de $\mathbb{M}(n,\mathbb{K})$ est la dimension de la partie de $\mathbb{K}^n$ engendrée par ses colonnes.*

Il est possible d'exprimer le rang d'une matrice de façon plus « intrinsèque » via le concept de mineur.

Définition 6.117 ([162]).
Les mineurs d'une matrice sont les déterminants de ses sous-matrices carrées.

Dans la suite nous désignerons souvent par le mot « mineur » la sous-matrice carrée elle-même au lieu de son déterminant.

Lorsque A est une matrice, nous notons f_A l'application linéaire associée à la matrice A par l'application (6.93).

LEMVecsaRgFixe

Lemme 6.118.
Soit $\mathbb{K}$ un corps commutatif[44]*. Si A est une matrice carrée d'ordre n et de rang r à coefficients dans $\mathbb{K}$, alors il existe des vecteurs $(x_i)_{i=1,\dots,n}$ formant une base de $\mathbb{K}^n$ tels que*

$$f_A(x_i) \neq 0 \tag{6.207}$$

pour $i \leqslant r$ et

$$f_A(x_i) = 0 \tag{6.208}$$

pour $i > r$.

Démonstration. Soit V le sous-espace de $\mathbb{K}^n$ engendré par les colonnes de A. Nous considérons la base canonique $\{e_i\}$ de $\mathbb{K}^n$, ainsi que v_i le vecteur créé par la i^{e} colonne de A. Nous avons

$$v_i = f_A(e_i). \tag{6.209}$$

Les vecteurs v_i engendrent V, donc nous pouvons en extraire une base par le théorème 6.19(1). Soit donc $\{v_j\}_{i\in J}$ une base de V avec $J \subset \{1,\dots,n\}$.

La base de $\mathbb{K}^n$ que nous cherchons commence par les vecteurs $\{e_j\}_{j\in J}$. Ces vecteurs vérifient $f_A(e_j) = v_j \neq 0$ parce que des vecteurs d'une base ne sont jamais nuls.

Pour la suite de la base, nous pourrions penser au théorème de la base incomplète[45], mais les vecteurs ainsi complétant la base ne sont pas garantis de s'annuler par f_A. Voir l'exemple 6.119.

L'idée est d'utiliser le noyau de f_A qui est un sous-espace vectoriel par la proposition 6.44. Soit une base[46] $\{z_k\}$ de $\ker(f)$. Les vecteurs $\{e_j\}_{j\in J}$ forment une base de $\text{Image}(f_A)$. Puisque les z_i forment une base de $\ker(f_A)$, le théorème du rang 6.53 dit alors que $\{e_j\}_{j\in J} \cup \{z_k\}$ est une base de $\mathbb{K}^n$.

Il y a r éléments dans J parce que l'espace engendré par les colonnes de A est de dimension r par hypothèse. Donc il y a $n-r$ éléments dans les $\{z_k\}$ pour que le tout ait le bon nombre d'éléments. □

[44] Comme toujours.
[45] Théorème 6.15(2).
[46] Cette base contient $n-r$ éléments, mais ce n'est pas très important pour la suite.

EXooRKVQooZOGDEf

Exemple 6.119.
Soit la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}. \tag{6.210}$$

Elle est de rang 1. En suivant l'idée de la démonstration, nous commençons la base de $\mathbb{R}^2$ par le vecteur e_1 qui vérifie

$$f_A(e_1) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}. \tag{6.211}$$

L'utilisation du théorème de la base incomplète ne permet pas de trouver un second vecteur de base v tel que $f_A(v) = 0$. En effet ce théorème donne juste l'existence d'une completion de la base, mais pas de propriétés particulières de la base obtenue. Elle pourrait donner $v = e_2$ comme second vecteur de base. Mais alors

$$f_A(v) = f_A(e_2) = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq 0. \tag{6.212}$$

Au contraire, le noyau de f_A est donné par le sous-espace engendré par $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Une base convenable est donc $\{e_1, e_1 - e_2\}$. △

PROPooEGNBooIffJXc

Proposition 6.120.
Le rang d'une application linéaire[47] *est égal au rang de sa matrice*[48] *dans n'importe quelle base.*

Démonstration. Soient deux espaces vectoriels V de dimension n et W de dimension m. Nous considérons les bases $\{e_i\}_{i=1,\dots,n}$ de V et $\{f_j\}_{j=1,\dots,m}$ de W. Soit une application linéaire $\alpha\colon V \to W$. La matrice de α est donnée par $A_{ji} = \alpha(e_i)j$. Nous considérons les applications linéaires

$$\begin{aligned} \beta\colon V &\to \mathbb{K}^m \\ e_i &\mapsto \big(\alpha(e_i)_1, \dots, \alpha(e_i)_m\big). \end{aligned} \tag{6.213}$$

et

$$\begin{aligned} \gamma\colon \mathbb{K}^m &\to W \\ (x_1, \dots, x_m) &\mapsto \sum_{k=1}^{m} x_k f_k. \end{aligned} \tag{6.214}$$

L'espace de $\mathbb{K}^m$ engendré par les colonnes de A est

$$S = \text{Span}\{\beta(e_i)\}_{i=1,\dots,n}. \tag{6.215}$$

Nous allons montrer que γ est un isomorphisme entre S et $\text{Image}(\alpha)$. Pour cela nous commençons par remarquer que

$$\beta(e_i)_k = \alpha(e_i)_k \tag{6.216}$$

et donc que

$$\alpha(e_i) = \sum_k \alpha(e_i)_k f_k \tag{6.217a}$$

$$= \sum_k \beta(e_i)_k f_k \tag{6.217b}$$

$$= \gamma\big(\beta(e_i)\big). \tag{6.217c}$$

Cela montre que $\gamma(S) = \text{Image}(\alpha)$. □

PROPooAPYRooGQxGoj

Proposition 6.121 ([1])**.**
Une matrice inversible est de rang maximum.

PropEJBZooTNFPRj

Proposition 6.122.
Si A est la matrice d'une application linéaire, alors le rang de cette application linéaire est égal au rang de A, c'est-à-dire à la taille de la plus grande matrice carrée de déterminant non nul contenue dans A.

[47] Définition 6.51.
[48] Définition 6.116.

PROPooRYWLooZmsxFS

Proposition 6.123 ([1]).
Soit une matrice $A \in \mathbb{M}(n, \mathbb{K})$ de rang r. Si nous notons v_i le vecteur de $\mathbb{K}^n$ formé par la i-ième colonne de A, alors

$$\dim\big(\text{Span}(v_1, \dots, v_n)\big) = r \tag{6.218}$$

Le lemme suivant dit que si une matrice est inversible, à permutation près des colonnes, on peut supposer que le carré $r \times r$ du au-dessus à gauche est inversible.

LEMooMCIDooYBHrbq

Lemme 6.124 ([1, 3]).
Soient une matrice inversible $A \in \mathbb{M}(n, \mathbb{K})$ et $r \leqslant n$. Il existe une permutation $\sigma \in S_n$ telle que la matrice $a \in \mathbb{M}(r, \mathbb{K})$ donnée par

$$a_{i,j} = A_{i,\sigma(j)} \tag{6.219}$$

soit inversible.

Démonstration. Nous considérons l'application linéaire

$$\begin{aligned} \pi\colon \mathbb{K}^n &\to \mathbb{K}^r \\ (x_1, \dots, x_n) &\mapsto (x_1, \dots, x_r). \end{aligned} \tag{6.220}$$

D'autre part, nous notons v_i le vecteur de $\mathbb{K}^n$ formé par la i-ième colonne de la matrice A. Nous utilisons le lemme 6.63 pour dire que

$$\text{Span}\big(\pi(v_1), \dots, \pi(v_n)\big) = \pi\Big(\text{Span}\big(\{v_1, \dots, v_n\}\big)\Big). \tag{6.221}$$

Étant donné que A est inversible, son rang est n par la proposition 6.121. Alors la proposition 6.123 donne $\text{Span}\big(\{v_1, \dots, v_n\}\big) = \mathbb{R}^n$. Nous avons donc

$$\text{Span}\big(\{\pi(v_1), \dots, \pi(v_n)\}\big) = \mathbb{K}^r. \tag{6.222}$$

Il existe donc $i_1, \dots, i_r$ tels que

$$\text{Span}\big(\pi(v_{i_1}), \dots, \pi(v_{i_r})\big) = \mathbb{K}^r. \tag{6.223}$$

Il suffit maintenant de prendre la permutation σ qui permute$k$ avec i_k. □

THOooSEAZooOYSsmP

Théorème 6.125 (Théorème du rang constant[163]).
Soient un ouvert U de $\mathbb{R}^m$ et une application $f\colon U \to \mathbb{R}^n$ de classe C^1. Nous supposons que $df\colon U \to \mathcal{L}(\mathbb{R}^m, \mathbb{R}^n)$ est de rang constant r sur U.

Alors il existe un ouvert V de $\mathbb{R}^n$ contenant $f(U)$ et un C^1-difféomorphisme $\theta\colon V \to \mathbb{R}^n$ tel que

$$(\theta \circ f)(x_1, \dots, x_m) = (x_1, \dots, x_r, 0, \dots, 0) \tag{6.224}$$

pour tout $x \in U$.

6.3.14 Matrices équivalentes et semblables

DefBLELooTvlHoB

Proposition-Définition 6.126.
Deux relations d'équivalence[49] entre les matrices.

ItemPFXCooOUbSCt

*(1) Deux matrices A et B sont **équivalentes** dans $\mathbb{M}(n, \mathbb{K})$ si il existe $P, Q \in \text{GL}(n, \mathbb{K})$ telles que $A = PBQ^{-1}$.*

*(2) Deux matrices sont **semblables** si il existe une matrice $P \in \text{GL}(n, \mathbb{K})$ telle que $A = PBP^{-1}$.*

LemZMxxnfM

Lemme 6.127.
Une matrice de rang[50] r dans $\mathbb{M}(n, \mathbb{K})$ est équivalente à la matrice par blocs

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{6.225}$$

[49] Définition 1.55.
[50] Définition 6.116.

Démonstration. Nous devons prouver que pour toute matrice $A \in \mathbb{M}(n,\mathbb{K})$ de rang r, il existe $P,Q \in \mathrm{GL}(n,\mathbb{K})$ telles que $QAP = J_r$. Soit $\{e_i\}$ la base canonique de $\mathbb{K}^n$, puis $\{f_i\}$ une base telle que $Af_i = 0$ dès que $i > r$, qui existe par le lemme 6.118.

Nous considérons la matrice inversible P telle que $Pe_i = f_i$; ses colonnes sont donc précisément les f_i, si bien que

$$APe_i = Af_i = \begin{cases} 0 & \text{si } i > r \\ \neq 0 & \text{sinon.} \end{cases} \tag{6.226}$$

La matrice AP se présente donc sous la forme

$$AP = \begin{pmatrix} M & 0 \\ * & 0 \end{pmatrix} \tag{6.227}$$

où M est une matrice $r \times r$. Nous considérons maintenant une base $\{g_i\}_{i=1,\dots,n}$ dont les r premiers éléments sont les r premières colonnes de AP et une matrice inversible Q telle que $Qg_i = e_i$. Alors

$$QAPe_i = \begin{cases} e_i & \text{si } i < r \\ 0 & \text{sinon.} \end{cases}. \tag{6.228}$$

Cela signifie que QAP est la matrice J_r. □

CorGOUYooErfOIe

Corolaire 6.128 (Équivalence et rang)**.**
Deux matrices sont équivalentes[51] *si et seulement si elles sont de même rang.*

Démonstration. D'abord il y a des implicites dans l'énoncé. Puisque nous voulons, soit par hypothèse, soit par conclusion, que les matrices A et B soient équivalentes, nous supposons qu'elles ont même dimension. Soient donc A et B deux matrices carrées d'ordre n.

Par le lemme 6.127, deux matrices de même rang r sont équivalentes à J_r. Elles sont donc équivalentes entre elles.

Inversement, supposons que A et B soient deux matrices équivalentes[52] : $A = PBQ^{-1}$ avec P et Q inversibles. Alors

$$\begin{aligned} \mathrm{Image}(PBQ^{-1}) &= \{PBQ^{-1}v \text{ tel que } v \in \mathbb{K}^n\} && \text{(6.229a)} \\ &= PB\underbrace{\{Q^{-1}v \text{ tel que } v \in \mathbb{K}^n\}}_{=\mathbb{K}^n} && \text{(6.229b)} \\ &= P\big(B(\mathbb{K}^n)\big). && \text{(6.229c)} \end{aligned}$$

L'ensemble $B(\mathbb{K}^n)$ est un sous-espace vectoriel de $\mathbb{K}^n$. Comme le rang de P est maximum, la dimension de $P\big(B(\mathbb{K}^n)\big)$ est la même que celle de $B(\mathbb{K}^n)$. Par conséquent

$$\dim\Big(\mathrm{Image}(PBQ^{-1})\Big) = \dim\big(B(\mathbb{K}^n)\big) = rang(B). \tag{6.230}$$

Le membre de gauche de cela n'est autre que $rang(A) = \dim\big(\mathrm{Image}(PBQ^{-1})\big)$. □

6.3.15 Algorithme des facteurs invariants

PropPDfCqee

Proposition 6.129 (Algorithme des facteurs invariants[112])**.**
Soit $(\mathbb{A},\delta)$ un anneau euclidien muni de son stathme et $U \in \mathbb{M}(n \times m,\mathbb{A})$. Alors il existe $d_1,\dots,d_s \in \mathbb{A}^*$ et des matrices $P \in \mathrm{GL}(m,\mathbb{A})$, $Q \in \mathrm{GL}(n,\mathbb{A})$ tels que nous ayons

$$U = P\begin{pmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_s & \\ & 0 & & 0 \end{pmatrix}Q \tag{6.231}$$

avec $d_i \mid d_{i+1}$ pour tout i.

[51] Définition 6.126(1).
[52] Définition 6.126.

Démonstration. Nous allons donner la preuve plus ou moins sous forme d'algorithme.

D'abord si $U = 0$ c'est bon, on a la réponse. Sinon, nous prenons l'élément (i_0, j_0) dont le stathme est le plus petit et nous l'amenons en $(1, 1)$ par les permutations

$$\begin{aligned} C_1 &\leftrightarrow C_{j_0} \\ L_1 &\leftrightarrow L_{i_0} \end{aligned} \tag{6.232}$$

Ensuite nous traitons la première colonne jusqu'à amener des zéros partout en dessous de $u_{1,1}$ de la façon suivante : pour chaque ligne successivement nous calculons la division euclidienne

$$u_{i,1} = qu_{1,1} + r_i, \tag{6.233}$$

et nous faisons

$$L_i \to L_i - qL_1, \tag{6.234}$$

c'est-à-dire que nous enlevons le maximum possible et il reste seulement r_i en u_{i1}. Vu que le but est de ne laisser que des zéros dans la première colonne, si le reste n'est pas zéro, nous ne sommes pas contents[53]. Dans ce cas nous permutons $L_1 \leftrightarrow L_i$, ce qui aura pour effet de strictement diminuer le stathme de $u_{1,1}$ parce qu'on va mettre en $u_{1,1}$ le nombre r_i dont le stathme est strictement plus petit que celui de $u_{1,1}$.

En faisant ce jeu de division euclidienne puis échange, on diminue toujours le stathme de $u_{1,1}$, donc ça finit par s'arrêter, c'est-à-dire qu'à un certain moment, la division euclidienne de $u_{i,1}$ par $u_{1,1}$ va donner un reste nul et nous serons contents.

Une fois la première colonne ramenée à la forme

$$C_1 = \begin{pmatrix} u_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{6.235}$$

nous faisons tout le même jeu avec la première ligne, en faisant maintenant des sommes divisions et permutations de colonnes. Notons que ce faisant, nous ne changeons plus la première colonne.

En fin de compte, nous trouvons une matrice[54]

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix} \tag{6.236}$$

Si l'élément $u_{1,1}$ ne divise pas un des éléments de A, disons $a_{i,j}$, alors nous opérons

$$C_1 \to C_1 - C_j. \tag{6.237}$$

Cela nous détruit un peu la première colonne, mais ne change pas $u_{1,1}$. Nous avons maintenant

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ * & & & \\ u_{i,j} & & A & \\ * & & & \\ 0 & & & \end{pmatrix} \tag{6.238}$$

Et nous refaisons tout le jeu depuis le début. Cependant, lorsque nous allons nous attaquer à la ligne i, $u_{1,1}$ ne divisera pas $u_{i,j}$, ce qui donnera lieu à une division euclidienne et un échange $L_1 \leftrightarrow L_i$. L'échange consistant à mettre r_i à la place de $u_{1,1}$ et réciproquement, diminuera encore strictement le stathme. Encore une fois, nous allons travailler jusqu'à avoir la matrice sous la forme

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}, \tag{6.239}$$

EqADcNVgI

[53] Si il est zéro, nous passons à la ligne suivante

[54] Nous nommons toujours par la même lettre U la matrice originale et la matrice modifiée, comme il est d'usage en informatique.

sauf que cette fois, le stathme de $u_{1,1}$ est strictement plus petit que la fois précédente. Si $u_{1,1}$ ne divise toujours pas tous les éléments de A, nous recommençons encore et encore. En fin de compte, nous finissons par avoir une matrice de la forme (6.239) avec $u_{1,1}$ qui divise tous les éléments de A.

Une fois que cela est fait, il faut continuer en recommençant tout sur la matrice A. Nous avons maintenant

$$U = \begin{pmatrix} u_{1,1} & & 0 \\ & u_{2,2} & \\ 0 & & B \end{pmatrix}. \tag{6.240}$$

Sous cette forme nous avons $u_{1,1} \mid u_{2,2}$ et $u_{1,1}$ divise tous les éléments de B. En effet $u_{1,1}$ divisant tous les éléments de A, il divise toutes les combinaisons de ces éléments. Or tout l'algorithme ne consiste qu'à prendre des combinaisons d'éléments.

Nous finissons donc bien sur une matrice comme annoncée. De plus, n'ayant effectué que des combinaisons de lignes, nous avons seulement multiplié par des matrices inversibles (lemme 6.115). □

6.4 Changement de base

Soit un espace vectoriel E muni de deux bases $(e_i)_{i=1,\dots,n}$ et $(f_\alpha)_{\alpha=1,\dots,n}$. Les deux bases sont liées entre elles par

EQooFRQRooSMsQQB
$$f_\alpha = \sum_i Q_{i,\alpha} e_i. \tag{6.241}$$

Ici Q n'est pas une application linéaire $E \to E$: Q est seulement un tableau de nombres, donnant les coordonnées des vecteurs f_α dans la base de e_i. Éventuellement Q peut être vu comme une application linéaire $\mathbb{K}^n \to \mathbb{K}^n$.

Dans la suite nous nommerons Q^{-1} la matrice inverse de Q. Inverse au sens des bêtes tableaux de nombres, sans interprétation en tant qu'application linéaire. De même pour Q^t qui est la transposée de Q.

6.4.1 Changement de base : vecteurs de base

LEMooIHZGooOZoYZd

Lemme 6.130.
Soit un espace vectoriel E sur $\mathbb{K}$ ainsi que deux bases $(e_i)_{i=1,\dots,n}$, $(f_\alpha)_{\alpha=1,\dots,n}$ de E liées par $f_\alpha = \sum_i Q_{i,\alpha} e_i$. Alors

EQooZQPAooAbKAdg
$$e_i = \sum_\alpha Q^{-1}_{\alpha,i} f_\alpha. \tag{6.242}$$

Démonstration. Nous multiplions l'égalité $f_\alpha = \sum_i Q_{i,\alpha} e_i$ par le nombre[55] $Q^{-1}_{\alpha,j} \in \mathbb{K}$ et nous sommons sur α :

$$\sum_\alpha Q^{-1}_{\alpha,j} f_\alpha = \sum_{i\alpha} (A_{i,\alpha} Q^{-1}_{\alpha,j}) e_i = e_j. \tag{6.243}$$

□

6.4.2 Changement de base : coordonnées

PROPooNYYOooHqHryX

Proposition 6.131.
Soit un espace vectoriel E sur $\mathbb{K}$. Soient deux bases $(e_i)_{i=1,\dots,n}$ et $(f_\alpha)_{\alpha=1,\dots,n}$ liées par $f_\alpha = \sum_i Q_{i,\alpha} e_i$. Nous considérons un même vecteur dans les deux bases : $\sum_i x_i e_i = \sum_\alpha y_\alpha f_\alpha$. Alors

ITEMooIBAEooNaUnPD
(1) $y_\alpha = \sum_i Q^{-1}_{\alpha,i} x_i$

ITEMooKPWTooMwdbPu
(2) $x_i = \sum_\alpha Q_{i,\alpha} y_\alpha$.

Démonstration. Soit un vecteur $x \in E$. Il peut être écrit dans les deux bases :

EQooGSJMooGQstMx
$$x = \sum_i x_i e_i = \sum_\alpha y_\alpha f_\alpha. \tag{6.244}$$

En remplaçant e_i par sa valeur (6.242) nous avons l'égalité

$$\sum_{i\alpha} x_i Q^{-1}_{\alpha,i} f_\alpha = \sum_\alpha y_\alpha f_\alpha. \tag{6.245}$$

[55] Attention à la bonne interprétation de ce nombre : on fait bien référence à l'élément situé en (α, j) de la matrice Q^{-1}, et pas autre chose.

Puisque les f_α sont linéairement indépendants, l'égalité des sommes donne l'égalité de chacun des termes :

$$y_\alpha = \sum_i x_i Q^{-1}_{\alpha,i}. \tag{6.246}$$

En identifiant $x \in E$ au vecteur dans $\mathbb{K}^n$ de ses coordonnées dans la base $\{e_i\}$ nous pouvons écrire

$$y_\alpha = (Q^{-1}x)_\alpha, \tag{6.247}$$

Le point (1) est prouvé.

En ce qui concerne le point (2), nous repartons encore de (6.244), mais nous y substituons la définition des f_α :

$$\sum_i x_i e_i = \sum_{\alpha i} y_\alpha Q_{i,\alpha} e_i. \tag{6.248}$$

Vous voulez des détails ? Allez, une étape de plus que le strict nécessaire : nous écrivons

$$\sum_i \big(x_i - \sum_\alpha y_\alpha Q_{i,\alpha}\big)e_i = 0. \tag{6.249}$$

Par linéaire indépendance des e_i, nous avons annulation de tous les coefficients, c'est-à-dire

$$x_i = \sum_\alpha Q_{i,\alpha} y_\alpha, \tag{6.250}$$

comme annoncé. □

6.132.
Attention à l'ordre des indices dans la dernière égalité : la matrice Q vient avec les indices dans l'ordre i, α, tandis que la matrice Q^{-1} vient avec les indices dans l'ordre opposé : α, i. C'est pour cela qu'il est intéressant de noter avec des lettres latines les indices se rapportant à la première base, et avec des lettres grecques ceux se rapportant à la seconde base.

NORMooNWKZooPMwYTO

6.133.
Les formules de changement de coordonnées de la proposition 6.131 s'écrivent souvent de la façon suivante :

ITEMooLHQCooBRvSlp

(1) $y_\alpha = (Q^{-1}x)_\alpha$

ITEMooNXUGooJIeoBf

(2) $y = Q^{-1}x$.

ITEMooEFILooNENamW

(3) $x_i = (Qy)_i$

ITEMooMOKHooFEJvIW

(4) $x = Qy$

Ces égalités reposent sur un petit paquet d'abus de notations qu'il convient de bien comprendre. Ici, x et y sont les éléments de $\mathbb{K}^n$ donnés par les composantes de x dans les bases $\{e_i\}$ et $\{f_\alpha\}$, et Q est vu comme une matrice, un opérateur linéaire sur $\mathbb{K}^n$. Autrement dit, le choix des bases permet d'identifier E avec $\mathbb{K}^n$ et la matrice Q avec l'application linéaire f_Q de la proposition 6.81.

6.4.3 Changement de base : matrice d'une application linéaire

PROPooNZBEooWyCXTw

Proposition 6.134.
Soit une application linéaire $t\colon E \to E$ de matrices A et B dans les bases $\{e_i\}$ et $\{f_\alpha\}$. Si les bases sont liées par

$$f_\alpha = \sum_i Q_{i,\alpha} e_i, \tag{6.251}$$

alors les matrices A et B sont liées par

$$B = Q^{-1}AQ. \tag{6.252}$$

Démonstration. L'hypothèse sur le fait que A et B sont les matrices de t signifie que pour tout $x \in E$,

$$t(x) = \sum_{ij} A_{j,i} x_i e_j = \sum_{\alpha\beta} B_{\alpha,\beta} y_\beta f_\alpha. \tag{6.253}$$

En remplaçant e_j par son expression (6.242) en termes des f_α et x_i par son expression $x_i = (Qy)_i$ (proposition 6.131), nous avons

$$(By)_\alpha = \sum_{ij\alpha} A_{j,i}(Qy)_i Q^{-1}_{\alpha,j} f_\alpha \tag{6.254a}$$
$$= \sum_{i\alpha} (Q^{-1}A)_{\alpha,i}(Qy)_i f_\alpha \tag{6.254b}$$
$$= \sum_{\alpha} (Q^{-1}AQy)_\alpha f_\alpha. \tag{6.254c}$$

Puisque les f_α forment une base, nous en déduisons $Q^{-1}AQy = By$. Et comme y est un élément quelconque de $\mathbb{K}^n$, nous en déduisons l'égalité de matrices

$$B = Q^{-1}AQ. \tag{6.255}$$

ooWKTYooQJfclT

□

Il s'agit bien d'une égalité de matrices ou, à la limite, d'applications linéaires sur $\mathbb{K}^n$, et non d'une égalité d'application linéaire sur E.

6.4.4 Déterminant de Vandermonde

PropnuUvtj

Proposition 6.135 ([121]).
*Le **déterminant de Vandermonde** est le polynôme en n variables donné par*

$$V(T_1, \dots, T_n) = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ T_1 & T_2 & \dots & T_n \\ \vdots & \ddots & \ddots & \vdots \\ T_1^{n-1} & T_2^{n-1} & \dots & T_n^{n-1} \end{pmatrix} = \prod_{1 \leqslant i < j \leqslant n} (T_j - T_i). \tag{6.256}$$

Notez que l'inégalité du milieu est stricte (sinon d'ailleurs l'expression serait nulle).

Démonstration. Nous considérons le polynôme

$$f(X) = V(T_1, \dots, T_{n-1}, X) \in \big(\mathbb{K}[T_1, \dots, T_{n-1}]\big)[X]. \tag{6.257}$$

C'est un polynôme de degré au plus $n-1$ en X et il s'annule aux points $T_1, \dots, T_{n-1}$. Par conséquent[56] nous pouvons factoriser les $X - T_i$, c'est-à-dire qu'il existe $\alpha \in \mathbb{K}[T_1, \dots, T_{n-1}]$ tel que

$$f = \alpha \prod_{i=1}^{n-1} (X - T_i). \tag{6.258}$$

EqeVxBwQ

Nous trouvons α en écrivant $f(0)$. D'une part la formule (6.258) nous donne

$$f(0) = \alpha(-1)^{n-1} T_1 \dots T_{n-1}. \tag{6.259}$$

EqblwWMj

D'autre part la définition donne

$$f(0) = \det \begin{pmatrix} 1 & \cdots & 1 & 1 \\ T_1 & & T_{n-1} & 0 \\ \vdots & & \vdots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} & 0 \end{pmatrix} \tag{6.260a}$$
$$= (-1)^{n-1} \det \begin{pmatrix} T_1 & \dots & T_{n-1} \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} \end{pmatrix} \tag{6.260b}$$
$$= (-1)^{n-1} T_1 \dots T_{n-1} \det \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} \end{pmatrix} \tag{6.260c}$$
$$= (-1)^{n-1} T_1 \dots T_{n-1} V(T_1, \dots, T_{n-1}) \tag{6.260d}$$

[56] Proposition 3.279.

En égalisant avec (6.259), nous trouvons $\alpha = V(T_1, \dots, T_{n-1})$, et donc

$$f = V(T_1, \dots, T_{n-1}) \prod_{j \leqslant n-1} (X - T_j) \tag{6.261}$$

Enfin, une récurrence montre que

$$\begin{aligned} V(T_1, \dots, T_n) &= f(T_n) && \text{(6.262a)}\\ &= V(T_1, \dots, T_{n-1}) \prod_{j \leqslant n-1} (T_n - T_j) && \text{(6.262b)}\\ &= \prod_{k \leqslant n} \prod_{j \leqslant k-1} (T_k - T_j) && \text{(6.262c)}\\ &= \prod_{1 \leqslant j < k \leqslant n} (T_i - T_j). && \text{(6.262d)} \end{aligned}$$

□

PROPooNVXIooXJKplZ

Proposition 6.136 ([1]).
Soient des $a_i \in \mathbb{R}$ tels que

$$f(x) = \sum_{k=0}^{n} a_k x^k \tag{6.263}$$

ait $n+1$ racines distinctes dans $\mathbb{R}$. Alors

(1) $f = 0$

(2) $a_k = 0$ *pour tout k.*

Démonstration. Nous nommons $(r_i)_{i=1,\dots,n+1}$ les racines de f. L'équation $f(x) = 0$ s'écrit

$$(1, x, \dots, x^n) \cdot (a_0, \dots, a_n) = 0. \tag{6.264}$$

Le système $f(r_i) = 0$ (vu comme système d'équation pour les a_i) pour tout i s'écrit

$$\begin{pmatrix} 1 & r_1 & \dots & r_1^n \\ 1 & r_2 & \dots & r_2^n \\ \vdots & \vdots & & \vdots \\ 1 & r_n & \dots & r_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = 0. \tag{6.265}$$

La proposition 6.135 nous dit que le déterminant de ce système est non nul. Donc il existe une solution unique. Cette unique solution est manifestement $(a_0, \dots, a_n) = (0, \dots, 0)$. □

6.5 Espaces de polynômes

SecEspacePolynomes

Attention : les polynômes en-soi, font l'objet de la définition 3.228.

Pour chaque $k > 0$ donné, nous définissons

$$\mathcal{P}_{\mathbb{R}}^k = \{p : \mathbb{R} \to \mathbb{R} \,|\, p : x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k,\ a_i \in \mathbb{R},\ \forall i = 0, \dots, k\}. \tag{6.266}$$

Il est facile de se convaincre que la somme de deux polynômes de degré inférieur ou égal à k est encore un polynôme de degré inférieur ou égal à k. En outre il est clair que la multiplication par un scalaire ne peut pas augmenter le degré d'un polynôme. L'ensemble $\mathcal{P}_{\mathbb{R}}^k$ est donc un espace vectoriel muni des opérations héritées de $\mathcal{P}_{\mathbb{R}}$.

PROPooWOMFooLpTKgG

Proposition 6.137 ([1]).
Les polynômes $x \mapsto x^k$ avec $k = 0, \dots, n$ forment une base de $\mathcal{P}_{\mathbb{R}}^k$.

Démonstration. Si nous notons $e_i(x) = x^i$, et si P est un polynôme, alors il existe des a_i tels que $P(x) = \sum_{i=0}^n a_i x^i$. Dans ce cas, $P = \sum_i a_i e_i$. Cela prouver que $\{e_i\}_{i=0,\dots,n}$ est générateur.

Pour montrer que c'est libre, nous supposons que $\sum_{i=0}^n a_i e_i = 0$. En particulier le polynôme $P(x) = \sum_i a_i x^i$ a plein de racines distinctes et la proposition 6.136 implique que $a_i = 0$ pour tout i. □

Nous allons maintenant étudier trois applications linéaires de $\mathcal{P}_{\mathbb{R}}^k$ vers d'autres espaces vectoriels.

L'isomorphisme canonique $\phi : \mathcal{P}^k_{\mathbb{R}} \to \mathbb{R}^{k+1}$ Nous définissons ϕ par les relations suivantes

$$\phi(x^j) = e_{j+1}, \qquad \forall j \in \{0, \dots, k\}.$$

Cela veut dire que pour tout p dans $\mathcal{P}^k_{\mathbb{R}}$, avec $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$, l'image de p par ϕ est

$$\phi(p) = \phi\left(\sum_{j=0}^{k} a_j x^j\right) = \sum_{j=0}^{k} a_j e_{j+1}.$$

Exemple 6.138.
Soit $k = 5$ on a

$$\phi(-8 - 7x - 4x^2 + 4x^3 + 2x^5) = \begin{pmatrix} -8 \\ -7 \\ -4 \\ 4 \\ 0 \\ 2 \end{pmatrix}. \tag{6.267}$$

△

Cette application est clairement bijective et respecte les opérations d'espace vectoriel, donc c'est un isomorphisme d'espaces vectoriels. L'existence d'un isomorphisme entre $\mathcal{P}^k_{\mathbb{R}}$ et $\mathbb{R}^{k+1}$ est un cas particulier du théorème qui dit que pour chaque m dans $\mathbb{N}_0$ fixée, tous les espaces vectoriels sur $\mathbb{R}$ de dimension m sont isomorphes à $\mathbb{R}^m$. Vous connaissez peut être déjà ce théorème depuis votre cours d'algèbre linéaire.

La dérivation $d : \mathcal{P}^k_{\mathbb{R}} \to \mathcal{P}^{k-1}_{\mathbb{R}}$ L'application de dérivation d fait exactement ce qu'on attend d'elle

$$d(x^0) = d(1) = 0, \qquad d(x^j) = jx^{j-1}, \quad \forall j \in \{1, \dots, k\}.$$

Cette application n'est pas injective, parce que l'image de p ne dépend pas de la valeur de a_0, donc si deux polynômes sont les mêmes à une constante près ils auront la même image par d.

Exemple 6.139.
Soit $k = 3$ on a

$$d(-8 - 12x + 4x^3) = -12(1) + 4(3x^2) = -12 + 12x^2. \tag{6.268}$$

Noter que $d(-30 - 12x + 4x^3) = d(-8 - 12x + 4x^3)$. Cela confirme, comme mentionné plus haut, que la dérivée n'est pas injective. △

L'intégration $I : \mathcal{P}^k_{\mathbb{R}} \to \mathcal{P}^{k+1}_{\mathbb{R}}$ Nous pouvons définir une application qui est « à une constante près » l'application réciproque de la dérivation. Cette application est définie sur les éléments de base par

$$I(x^j) = \frac{x^{j+1}}{j+1}. \tag{6.269}$$

Bien entendu, la raison d'être et la motivation de cette définition apparaîtront lorsque nous développerons une théorie générale de l'intégration.

Exemple 6.140.
Soit $k = 4$ on a

$$I(6 + 2x + x^2 + x^4) = 6x + x^2 + \frac{x^3}{3} + \frac{x^5}{5}. \tag{6.270}$$

△

Remarque : étant donné que dans la définition de I nous avons décidé d'intégrer entre zéro et x, tous les polynômes dans $\mathcal{P}^{k+1}_{\mathbb{R}}$ qui sont l'image par I d'un polynôme de $\mathcal{P}^k_{\mathbb{R}}$ ont $a_0 = 0$. Cela veut dire que nous pouvons générer toute l'image de I en utilisant un sous-ensemble de la base canonique de $\mathcal{P}^{k+1}_{\mathbb{R}}$, en particulier $\mathcal{B}_1 = \{x \mapsto x^j \,|\, j = 1, \dots, k\} \subset \mathcal{B}$ nous suffira. Cela n'est guère surprenant, parce que l'image par une application linéaire d'un espace vectoriel de dimension finie ne peut pas être un espace de dimension supérieure.

Les applications de dérivation et intégration correspondent évidemment à des applications linéaires de $\mathcal{P}_{\mathbb{R}}$ dans lui-même.

L'espace de tous les polynômes étant de dimension infinie, il peut servir de contre-exemple assez simple. Dans la sous-section 12.5.2, nous verrons que toutes les normes ne sont pas équivalentes sur l'espace des polynômes.

6.6 Projection et orthogonalité

PropProjScal

Proposition 6.141.
Si nous écrivons $\mathbf{proj}_Y$ l'opération de projection sur la droite qui sous-tend Y, alors nous avons

$$\| \mathbf{proj}_Y X\| = \frac{X \cdot Y}{\|Y\|}. \tag{6.271}$$

Démonstration. Les vecteurs X et Y sont des flèches dans l'espace. Nous pouvons choisir un système d'axe orthogonal tel que les coordonnées de X et Y soient

$$X = \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}, \quad Y = \begin{pmatrix} l \\ 0 \\ 0 \end{pmatrix} \tag{6.272}$$

où l est la longueur du vecteur Y. Pour ce faire, il suffit de mettre le premier axe le long de Y, le second dans le plan qui contient X et Y, et enfin le troisième axe dans le plan perpendiculaire aux deux premiers.

Un simple calcul montre que $X \cdot Y = xl + y \cdot 0 + 0 \cdot 0 = xl$. Par ailleurs, nous avons $\| \mathrm{proj}_Y X\| = x$. Par conséquent,

$$\| \mathrm{proj}_Y X\| = \frac{X \cdot Y}{l} = \frac{X \cdot Y}{\|Y\|}. \tag{6.273}$$

□

Corolaire 6.142.
Si la norme de Y est 1, alors le nombre $X \cdot Y$ est la longueur de la projection de X sur Y.

Démonstration. Poser $\|Y\| = 1$ dans la proposition 6.141. □

6.7 Dualité

DefJPGSHpn

Définition 6.143.
Soit E un espace vectoriel sur $\mathbb{K}$.

(1) *Une **forme linéaire** sur E est une application linéaire de E sur son corps de base $\mathbb{K}$.*

(2) *Le **dual algébrique** de E, noté E^*, est l'ensemble des formes linéaires sur E. Autrement dit : $E^* = \mathcal{L}(E, \mathbb{K})$.*

Nous verrons les formes multilinéaires en la définition 10.1.

Nous verrons plus tard qu'en dimension infinie, les applications linéaires ne sont pas toujours continues. Nous définirons donc aussi un concept de dual topologique. Voir la proposition 12.98, la remarque 12.101 et la définition 9.338.

DEFooTMSEooZFtsqa

Lemme-Définition 6.144.
Si E est un espace vectoriel et si $\{b_i\}$ est une base de E, alors nous définissons

$$\begin{aligned} b_i^* \colon E &\to \mathbb{K} \\ b_j &\mapsto \delta_{ij}, \end{aligned} \tag{6.274}$$

*et sa prolongation par linéarité. Ces éléments du dual E^* forment une base appelée **base duale**.*

En particulier nous avons

$$\dim(E) = \dim(E^*). \tag{6.275}$$

Démonstration. Notons pour commencer que $b_i^*\big(\sum_i x_i b_i\big) = x_i$.

(1) **Générateur** Soit $\varphi \in E^*$. Nous avons

$$\varphi(x) = \sum_i x_i \varphi(b_i) = \sum_i \varphi(b_i) b_i^*(x), \tag{6.276}$$

ce qui signifie que $\varphi = \sum_i \varphi(b_i) b_i^*$.

(2) **Libre** Si $\sum_i a_i b_i^* = 0$, alors en particulier en appliquant à b_k nous avons

$$0 = \big(\sum_i a_i b_i^*\big)(b_k) = \sum_i a_i \delta_{ik} = a_k. \tag{6.277}$$

Donc tous les coefficients sont nuls et $\{b_i^*\}_{i=1,\dots,n}$ est libre.

□

Notons que si $v \in E$ est un vecteur, ça n'a aucun sens à priori de parler de v^*. Il s'agit bien de définir *toute* la base $\{e_i^*\}$ à partir de toute la base $\{e_i\}$.

LEMooSVRIooFbxfue

Lemme 6.145 (Changement de base duale[1])**.**
Soient un espace vectoriel V de dimension finie, une base $\{e_i\}_{i=1,\dots,n}$ et sa base duale $\{\alpha_i\}_{i=1,\dots,n}$. Soit une bijection linéaire $A\colon V \to V$. Nous considérons $\{\beta_i\}_{i=1,\dots,n}$ la base duale de la base $\{Ae_i\}$.

Alors

$$\beta_i = \sum_j A_{ij}^{-1}\alpha_j. \tag{6.278}$$

Démonstration. Par définition d'une base duale, il faut $\beta_i(Ae_k) = \delta_{ik}$. Vu que $\{\alpha_i\}$ est une base, nous pouvons décomposer β_i de la façon suivante : $\beta_i = \sum_j B_{ij}\alpha_j$. Il nous reste à prouver que $B = A^{-1}$.

Pour cela nous calculons un peu :

$$\delta_{ik} = \beta_i(Ae_k) = \sum_j B_{ij}\alpha_j(Ae_k) = \sum_{lj} B_{ij}A_{lk}\underbrace{\alpha_j(e_l)}_{=\delta_{jl}} = \sum_l B_{il}A_{lk} = (BA)_{ik}. \tag{6.279}$$

Nous avons donc $\delta_{ik} = (BA)_{ik}$, c'est-à-dire $BA = \mathbb{1}$ ou encore $B = A^{-1}$. □

LEMooQLWNooYUpGdo

Lemme 6.146 ([164])**.**
Soit un espace vectoriel E de dimension finie.

ITEMooHHTLooNCjgfn

(1) Si α est une forme linéaire non nulle sur E, alors il existe $x \in E$ tel que $\alpha(x) = 1$.

ITEMooBYAAooUWBKDk

(2) Si $x \neq 0$ dans E, alors il existe une forme linéaire α sur E telle que $\alpha(x) = 1$.

Démonstration. En deux parties.

(1) **Pour (1)** Puisque α est non nulle, nous pouvons considérer $v \in E$ tel que $\alpha(v) \neq 0$. Alors en posant $x = \alpha(v)^{-1}v$, nous avons le résultat.

(2) **Pour (2)** Soit un vecteur non nul que nous écrivons sous la forme $x = \sum_{i=1}^n x_i e_i$ (pour une certaine base $\{e_i\}_{i=1,\dots,n}$ de E). Supposons que $x_k \neq 0$. Alors la forme

$$\begin{aligned}\alpha\colon E &\to \mathbb{K}\\ y &\mapsto y_k/x_k\end{aligned} \tag{6.280}$$

fait l'affaire.

□

LEMooKTREooBrnWVz

Lemme 6.147.
Soit un espace vectoriel de dimension finie E sur le corps $\mathbb{K}$. Si $\{\alpha_1, \dots, \alpha_n\}$ est une base de E^*, alors l'application

$$\begin{aligned}\Phi\colon E &\to \mathbb{K}^n\\ x &\mapsto \big(\alpha_1(x), \dots, \alpha_n(x)\big)\end{aligned} \tag{6.281}$$

est un isomorphisme d'espaces vectoriels.

Démonstration. En deux parties.

(1) **Φ est injective** Soit $z \in \ker(\Phi)$. Nous avons $\alpha_i(z) = 0$ pour tout i. Si $z \neq 0$, alors le lemme 6.146 dit qu'il existe $\beta \in E^*$ tel que $\beta(z) \neq 0$.

Décomposons un tel β dans la base de $\{\alpha_i\}$:

$$\beta = \sum_{i=1}^n \beta_i\alpha_i. \tag{6.282}$$

Alors nous avons

$$0 \neq \beta(z) = \sum_{i=1}^n \beta_i \underbrace{\alpha_i(z)}_{=0} = 0. \tag{6.283}$$

Contradiction. Donc $\ker(\Phi) = \{0\}$ et Φ est injective.

(2) **Φ est surjective** Les espaces vectoriels E, E^* et $\mathbb{K}^n$ ont tout trois, une dimension n. Donc Φ est une application linéaire injective entre deux espaces de même dimension. Elle est donc surjective par le corolaire 6.56.

□

PROPooDBPGooPagbEB

Proposition-Définition 6.148 ([164]).
*Soit un espace vectoriel E de dimension finie sur le corps $\mathbb{K}$. Toute base du dual E^* est duale d'une unique base de E. Cette base est dite **préduale**.*

Démonstration. Nous considérons une base $\mathcal{F} = \{\alpha_1, \dots, \alpha_n\}$ de E^*. Nous devons prouver qu'il existe une unique base de E dont la base duale est $\mathcal{F}$.

(1) **Existence** Le lemme 6.147 nous indique que l'application

$$\begin{aligned}\Phi\colon E &\to \mathbb{K}^n \\ x &\mapsto \big(\alpha_1(x), \dots, \alpha_n(x)\big)\end{aligned} \tag{6.284}$$

est un isomorphisme d'espaces vectoriels.

Soit la base canonique de $\mathbb{K}^n$: $(\epsilon_1, \dots, \epsilon_n)$. Puisque Φ est un isomorphisme, $\big(\Phi^{-1}(\epsilon_i)\big)_{i=1,\dots,n}$ est une base de E. Nous allons montrer qu'elle est préduale de (α_i). Nous posons $e_i = \Phi^{-1}(\epsilon_i)$ et nous calculons :

$$\alpha_i(e_j) = \alpha_i\big(\Phi^{-1}(\epsilon_j)\big) \tag{6.285a}$$
$$= \Phi\big(\Phi^{-1}(\epsilon_j)\big)_i \tag{6.285b}$$
SUBEQooACVAooVNwzMq
$$= (\epsilon_i)_j \tag{6.285c}$$
$$= \delta_{i,j} \tag{6.285d}$$
SUBEQooOYNHooSVOOyz

Justifications :

- Pour 6.285b, nous remarquons que $\alpha_i(x) = \Phi(x)_i$.
- Pour 6.285d, nous utilisons le fait que les ϵ_j forment la base canonique de $\mathbb{K}^n$.

(2) **Unicité** Soit une base préduale (e_i) de (α_i). Nous avons, par définition, que $\alpha_i(e_j) = \delta_{i,j}$. Donc

$$\big(\alpha_1(e_j), \dots, \alpha_n(e_j)\big) = \epsilon_j. \tag{6.286}$$

Nous appliquons Φ^{-1} à cette dernière équation pour obtenir $e_j = \Phi^{-1}(\epsilon_j)$. Donc les e_j sont déterminés de façon unique à partir des α_i.

□

Si u et v sont des vecteurs de $\mathbb{K}^n$, alors nous notons uv^* l'application linéaire

$$\begin{aligned}uv^*\colon \mathbb{K}^n &\to \mathbb{K}^n \\ x &\mapsto uv^*(x).\end{aligned} \tag{6.287}$$

LEMooJVDHooONXNAh

Lemme 6.149 (Lemme des déterminants[165]).
Soit une application linéaire $A \in \mathrm{End}(\mathbb{K}^n)$ ainsi que $u, v \in \mathbb{K}^n$. Nous avons

(1) $\det(A + uv^*) = (1 + v \cdot Au)\det(A)$

ITEMooGJOZooVLfZcX

(2) $\det(\mathbb{1} + af) = 1 + f(a)$.

6.7.1 Changement de base duale

PROPooDOEYooDpUbnc

Proposition 6.150 ([1]).
Soient deux bases $\{e_i\}$ et $\{e'j\}$ de l'espace vectoriel V. Nous notons $\{\alpha_i\}$ et $\{\alpha'_i\}$ les bases duales. Si $e'_j = \sum_i A_{ij} e_i$, alors

$$\alpha'_j = \sum_k A^{-1}_{jk} \alpha_k. \tag{6.288}$$

Démonstration. Nous posons $\alpha'_j = \sum_k B_{kj}\alpha_k$ et nous appliquons ça à e'_i. À gauche nous avons $\alpha'_j(e'_i) = \delta_{ij}$, et à droite,

$$\sum_k B_{kj}\alpha_k(e'_i) = \sum_k B_{kj}\alpha_k\big(\sum_l A_{li}e_l\big) \tag{6.289a}$$
$$= \sum_{kl} B_{kj}A_{li}\delta_{kl} \tag{6.289b}$$
$$= \sum_l B_{lj}A_{li} \tag{6.289c}$$
$$= (B^tA)_{ji}. \tag{6.289d}$$

Nous avons donc montré que $B^tA = \mathbb{1}$, ou encore que $B^t = A^{-1}$, ce qu'il fallait. □

6.7.2 Orthogonal

DEFooEQSMooHVzbfz

Définition 6.151.
*Soit E, un espace vectoriel, et F un sous-espace de E. L'**orthogonal** de F est la partie $F^\perp \subset E^*$ donnée par*

$$F^\perp = \{\alpha \in E^* \text{ tel que } \forall x \in F, \alpha(x) = 0\}. \tag{6.290}$$

Eqiyple

Cette définition d'orthogonal via le dual n'est pas du pur snobisme. En effet, la définition « usuelle » qui ne parle pas de dual,

$$F^\perp = \{y \in E \text{ tel que } \forall x \in F, y \cdot x = 0\}, \tag{6.291}$$

demande la donnée d'un produit scalaire. Évidemment dans le cas de $\mathbb{R}^n$ muni du produit scalaire usuel et de l'identification usuelle entre $\mathbb{R}^n$ et $(\mathbb{R}^n)^*$ via une base, les deux notions d'orthogonal coïncident.

La définition 6.151, au contraire, est intrinsèque : elle ne dépend que de la structure d'espace vectoriel.

Si $B \subset E^*$, on note B^o son orthogonal :

$$B^o = \{x \in E \text{ tel que } \omega(x) = 0, \forall \omega \in B\}. \tag{6.292}$$

Notons qu'on le note B^o et non $B^\perp$ parce qu'on veut un peu s'abstraire du fait que $(E^*)^* = E$. Du coup on impose que B soit dans un dual, et on prend une notation précise pour dire qu'on remonte au pré-dual, et non qu'on va au dual du dual.

PropXrTDIi

Proposition 6.152.
Soient un espace vectoriel E et F, un sous-espace vectoriel de E. Nous avons

$$\dim F + \dim F^\perp = \dim E. \tag{6.293}$$

Démonstration. Soit $\{e_1, \dots, e_p\}$ une base de F que nous complétons en une base $\{e_1, \dots, e_n\}$ de E par le théorème 6.15. Soit $\{e_1^*, \dots, e_n^*\}$ la base duale. Alors nous prouvons que $\{e_{p+1}^*, \dots, e_n^*\}$ est une base de $F^\perp$.

D'abord, ce sont des éléments de $F^\perp$, parce que si $i \leqslant p$ et si $k \geqslant 1$, nous avons $e_{p+k}^*(e_i) = 0$; donc oui, $e_{p+k}^* \in F^\perp$.

Ensuite, en tant que partie d'une base de F^*, c'est une partie libre. Il reste à montrer que c'est générateur.

Enfin $F^\perp \subset \text{Span}\{e_k^*, k \in \{p+1, \dots, n\}\}$ parce que si $\omega = \sum_{k=1}^n \omega_k e_k^*$, alors $\omega(e_i) = \omega_i$, mais nous savons que si $\omega \in F^\perp$, alors $\omega(e_i) = 0$ pour $i \leqslant p$. Donc $\omega = \sum_{k=p+1}^n \omega_k e_k^*$. □

La proposition 10.183 donnera une version plus terre à terre de la proposition 6.152 en disant que si nous avons un produit scalaire, alors $E = F \oplus F^\perp$ où $F^\perp$ est cette fois défini comme l'orthogonal pour le produit scalaire.

6.8 Représentation de groupe

DEFooXVMSooXDIfZV

Définition 6.153 (Représentation)**.**
*Soit un groupe G. Une **représentation** de G est un couple (E, ρ) où E est un espace vectoriel et ρ est une application $\rho\colon G \to \mathrm{GL}(E)$ vérifiant*

$$\rho(g) \circ \rho(h) = \rho(gh). \tag{6.294}$$

pour tout $g, h \in G$.

Définition 6.154.
Une représentation[57] $\rho\colon G \to \mathrm{GL}(E)$ *est* ***fidèle*** *si elle est injective*
La dimension de E est le ***degré*** *de la représentation (E, ρ).*

Le fait que la représentation $\rho\colon G \to \mathrm{GL}(E)$ soit fidèle ne dit pas que chacun des $\rho(g)$ est injectif.

PROPooHNQOooSzeEFG

Proposition 6.155.
Soit un corps $\mathbb{K}$. Si G est un groupe dans $\mathbb{M}(n, \mathbb{K})$ (c'est-à-dire un groupe de matrices $n \times n$ à coefficients dans $\mathbb{K}$), alors l'application

$$\begin{aligned} \rho\colon G &\to \mathrm{GL}(\mathbb{K}^n) \\ A &\mapsto f_A \end{aligned} \tag{6.295}$$

où f_A est l'application linéaire associée à A, est une représentation de G.

Démonstration. La représentation dont nous parons n'est autre que l'application ψ de la définition 6.78, dont nous connaissons beaucoup de propriétés. La proposition 6.84 dit, entre autres, que $\psi(AB) = \psi(A)\psi(B)$, c'est-à-dire que $\rho(AB) = \rho(A)\rho(B)$, et donc que ρ est une représentation. □

6.9 Somme directe d'espaces vectoriels

Si V et W sont des espaces vectoriels, ce que nous notons $V \oplus W$ n'est rien d'autre que l'espace vectoriel de l'ensemble $V \times W$.

DEFooJKAWooKkkkwm

Proposition-Définition 6.156 ([166, 167])**.**
Si V et W sont des espaces vectoriels sur le même corps $\mathbb{K}$, alors les définitions

(1) $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$

(2) $\lambda(v, w) = (\lambda v, \lambda w)$

donnent une structure d'espace vectoriel sur $V \times W$.
Cet espace sera noté $V \oplus W$ et est appelé ***somme directe*** *de V et W.*

DEFooIJDNooRUDUYF

Définition 6.157 (Sous-espaces en somme directe[168])**.**
Soient un espace vectoriel E sur $\mathbb{K}$ ainsi que des sous-espaces vectoriels $\{F_i\}_{i\in I}$ (I est un ensemble fini ou infini). Nous disons que les F_i sont ***en somme directe*** *si pour tout élément $u \in \sum_{i\in I} F_i$, il existe un unique ensemble $\{u_i\}_{i\in I}$ de vecteurs tel que*

(1) $u = \sum_{i\in I} u_i$

(2) $u_i \in F_i$ *pour tout i,*

(3) $\{j \in I \text{ tel que } u_j \neq 0\}$ *est fini.*

Si l'espace vectoriel E est un espace vectoriel topologique, nous avons la définition 9.248 qui donne des conditions de compatibilité entre les topologies.

LEMooHWRVooLedAmF

Lemme 6.158 (Décomposition suivant une somme directe)**.**
Soit un espace vectoriel E et deux sous-espaces F_1, F_2 en somme directe : $E = F_1 \oplus F_2$. Alors l'application

$$\begin{aligned} \psi\colon F_1 \times F_2 &\to E \\ (x, y) &\mapsto x + y \end{aligned} \tag{6.296}$$

est une bijection.

Démonstration. L'application est injective parce que si $\psi(x_1, x_2) = \psi(y_1, y_2)$, alors $x_1 + x_2 = y_1 + y_2$. Nommons u ce vecteur. Par unicité de l'ensemble $\{u_1, u_2\}$ tel que $u = u_1 + u_2$, nous avons automatiquement $\{x_1, x_2\} = \{y_1, y_2\}$ et donc $x_1 = y_1$ et $x_2 = y_2$.

En ce qui concerne la surjectivité, si $u \in E$, il existe un ensemble $\{u_1, u_2\}$ avec $u_i \in F_i$ tel que $u = u_1 + u_2 = \psi(u_1, u_2)$. □

LEMooDQMQooInVVDY

Lemme 6.159 ([1, 168])**.**
Soient un espace vectoriel E ainsi que des sous-espaces vectoriels F_i. Nous avons équivalence entre les assertions suivantes.

[57] Définition 6.153.

ITEMooHJXIooQKAfBe

(1) *Les F_i sont en somme directe*[58].

ITEMooJFOFooGDlwUz

(2) *Si $\sum_{i\in I} u_i = 0$ avec $u_i \in F_i$ et si $\{j \in I \text{ tel que } u_j \neq 0\}$ est fini, alors tous les u_i sont nuls.*

ITEMooNFWVooNdhhid

(3) *Chaque espace F_k est en somme directe avec la somme des précédents, c'est-à-dire que pour tout k,*

$$\left(\sum_{i=1}^{k-1} F_i\right) \cap F_k = \{0\}. \tag{6.297}$$

ITEMooPLXGooCOQgen

(4) *Pour tout k,*

$$F_k \cap \left(\sum_{i\neq k} F_i\right) = \{0\}. \tag{6.298}$$

Notez qu'ici $\sum_{i\neq k} F_i$ signifie l'ensemble des $x \in V$ pouvant être écrit comme une combinaison linéaire finie d'éléments des F_i avec $i \neq k$.

Démonstration. En plusieurs parties.

(1) **(1) implique (2)** Par définition de la somme directe, le vecteur 0 de E peut être écrit de façon unique sous la forme $\sum_i u_i$, et cette façon est avec $u_i = 0$ pour tout i.

(2) **(2) implique (3)** Supposons que $\sum_{i=1}^{k-1} u_i = u_k$ avec $u_j \in F_j$ pour tout j. Alors en posant $v_i = u_i$ (i=1,...,k-1) et $v_k = -u_k$ nous avons $\sum_{i=1}^{k} v_i = 0$, ce qui, en vertu de (2) donne $v_i = 0$ pour tout i.

(3) **(3) implique (4)** Supposons avoir

$$u_k = \sum_{i\in J} u_i \tag{6.299}$$

où J est fini dans $\mathbb{N} \setminus \{k\}$. Donc $J = \{1, \dots, n\} \setminus \{k\}$ pour un certain n. En réarrangeant la somme nous avons

$$u_n = \sum_{i=1}^{n-1} u_i, \tag{6.300}$$

et donc tous les u_i sont nuls par (3).

(4) **(4) implique (1)** Soit un élément $x \in \sum_{i\in I} F_i$. Nous l'écrivons de deux façons

$$x = \sum_{i\in J_1} u_i = \sum_{i\in J_2} v_i \tag{6.301}$$

où J_1 et J_2 sont finis. Nous posons $J = J_1 \cup J_2$ et $u_j = 0$ pour $j \in J \setminus J_1$ et $v_j = 0$ pour $j \in J \setminus J_2$. Ainsi $\sum_{i\in J} u_i = \sum_{i\in J} v_j$ et donc

$$\sum_{i\in J} (i_i - v_i) = 0. \tag{6.302}$$

Soit $k \in J$. Nous avons

$$u_k - v_k = \sum_{i\in J\setminus\{k\}} (u_i - v_i). \tag{6.303}$$

En vertu de (4), tout est nul et en particulier $v_i = u_i$ pour tout i.

□

PROPooCASNooEqisqa

Proposition 6.160 ([169]).
Soient E un espace vectoriel de dimension finie, et deux sous-espaces F_1 et F_2 satisfaisant

(1) $F_1 \cap F_2 = \{0\}$,

(2) $\dim(F_1) + \dim(F_2) \geqslant \dim(E)$.

Alors $E = F_1 \oplus F_2$.

[58] Définition 6.157.

Démonstration. Soient une base $\{e_i\}_{i\in I}$ de F_1 et $\{f_\alpha\}$ de F_2. Nous commençons par prouver que la partie $B = \{e_i\} \cup \{f_\alpha\}$ est libre.

Supposons en effet, avoir des coefficients a_i et b_α tels que

$$\sum_i a_i e_i + \sum_\alpha b_\alpha f_\alpha = 0. \tag{6.304}$$

Cela implique que $\sum_i a_i e_i = -\sum_\alpha b_\alpha f_\alpha$. Or $\sum_i a_i e_i \in F_1$ et $-\sum_\alpha b_\alpha f_\alpha \in F_2$. Donc les éléments $\sum_i a_i e_i$ et $\sum_\alpha b_\alpha f_\alpha$ sont dans $F_1 \cap F_2 = \{0\}$. Nous avons alors les égalités

$$\sum_i a_i e_i = 0 \tag{6.305}$$

et

$$\sum_\alpha b_\alpha f_\alpha = 0. \tag{6.306}$$

La première implique $a_i = 0$ pour tout i et la seconde implique $b_\alpha = 0$ pour tout α.

Donc B est une partie libre de E contenant $\dim(F_1) + \dim(F_2) \geqslant \dim(E)$ éléments. La proposition 6.20(1) nous indique alors qu'en réalité $\dim(F_1) + \dim(F_2) = \dim(E)$. Comme B est une partie libre contenant $\dim(E)$ éléments, c'est une base par la proposition 6.20(2). □

DEFooYQZHooCDuhDU

Définition 6.161 (Projection parallèle)**.**
Si nous avons une somme directe d'espaces vectoriels[59] $E = \bigoplus_{k=1}^n E_k$ *alors le* ***projecteur sur*** E_i ***parallèlement*** *aux autres* E_i *est l'application*

$$\begin{aligned} p_i \colon E &\to E \\ x_1 + \ldots + x_n &\mapsto x_i \end{aligned} \tag{6.307}$$

où $(x_1, \ldots, x_n)$ *est la décomposition*[60] *de* x *selon les espaces* E_i.

Cette application est un projecteur au sens de la définition 3.107.

LEMooCFDYooHTroSi

Lemme 6.162 ([1])**.**
Soit une somme directe d'espaces vectoriels[61] $E = \bigoplus_{i=1}^n E_i$. *Si une application linéaire* $p \colon E \to E$ *vérifie*

ITEMooCDFXooKZJvON

(1) $p(E_i) = \{0\}$,

ITEMooJKLVooLbSljW

(2) $p(x) = x$ *pour tout* $x \in E_k$,

alors p *est la projection sur* E_k *parallèle*[62] *aux autres* E_i.

Démonstration. Soit $x \in E$ et décomposons-le selon le lemme 6.157 : $x = x_1 + \ldots + x_n$. Alors

$$\begin{aligned} p(x) &= p(x_1) + \ldots + p(x_n) && p \text{ est linéaire} && (6.308a)\\ &= p(x_k) && \text{hyp. (1)} && (6.308b)\\ &= x_k && \text{hyp. (2)} && (6.308c)\\ & && && (6.308d) \end{aligned}$$

□

6.9.1 Structure réelle

DEFooCIFSooVmcNtE

Proposition-Définition 6.163 ([170, 167, 1])**.**
Soit un espace vectoriel E *sur* $\mathbb{C}$. *Il existe une application* $\sigma \colon E \to E$ *telle que*

(1) $\sigma^2 = \mathrm{Id}_E$

(2) Pour tout $\alpha, \beta \in \mathbb{R}$, $f(\alpha x + \beta y) = \bar{\alpha}\sigma(x) + \bar{\beta}\sigma(y)$.

Une telle application est une ***structure réelle*** *sur* E.

[59] Définition 6.157.
[60] Lemme 6.157.
[61] Définition 6.157.
[62] Définition 6.161.

Démonstration. La proposition 6.27 nous permet de considérer une base $\{e_i\}_{i\in I}$ de E. Alors, nous définissons

$$\sigma\big(\sum_{i\in I}\lambda_i e_i\big)=\sum_{i\in I}\bar{\lambda}_i e_i. \tag{6.309}$$

Notez que la somme est toujours finie. □

PROPooPZHPooNdarzg

Proposition 6.164.
Soit un espace vectoriel E sur $\mathbb{C}$ et une structure réelle[63] *σ sur E. Nous posons*

$$E_{\mathbb{R}}=\{v\in E \text{ tel que } \sigma(v)=v\}. \tag{6.310}$$

Alors

(1) *La partie $E_{\mathbb{R}}$ est un espace vectoriel réel.*

(2) *Nous avons la décomposition en somme directe*[64]

$$E=E_{\mathbb{R}}\oplus iE_{\mathbb{R}}. \tag{6.311}$$

Démonstration. En plusieurs parties.

(1) **Espace vectoriel réel** Si $v,w\in E_{\mathbb{R}}$, alors

$$\sigma(v+w)=\sigma(v)+\sigma(w)=v+w, \tag{6.312}$$

et si $\lambda\in\mathbb{R}$,

$$\sigma(\lambda x)=\lambda\sigma(x)=\lambda x. \tag{6.313}$$

Donc $E_{\mathbb{R}}$ est un espace vectoriel réel.

(2) **Première somme directe** Nous définissons

$$E^+=\{v\in E \text{ tel que } \sigma(v)=v\}, \tag{6.314a}$$
$$E^-=\{v\in E \text{ tel que } \sigma(v)=-v\} \tag{6.314b}$$

Nous prouvons que

$$\begin{aligned}\psi\colon E^+\times E^-&\to E\\ (a,b)&\mapsto a+b\end{aligned} \tag{6.315}$$

est un isomorphisme d'espaces vectoriels.

Puisque ψ est linéaire, il suffit de prouver qu'elle est bijective.

(2a) **Surjectif** Si $v\in E$, alors en posant $v_+=\frac{1}{2}\big(v+\sigma(v)\big)$, $v_-=\frac{1}{2}\big(v-\sigma(v)\big)$, nous avons

$$v=v_++v_-,\quad v_+\in E^+,\quad v_-\in E^-, \tag{6.316}$$

et donc $v=\psi(v_+,v_-)$.

(2b) **Injectif** Supposons $\psi(a,b)=\psi(\alpha,\beta)$. Alors $a+b=\alpha+\beta$ et donc $a-\alpha=\beta-b$. Comme $a-\alpha\in E^+$ et $\beta-b\in E^-$, nous savons que $a-\alpha=\beta-b\in E^+\cap E^-$. Étant donné que $E^+\cap E^-=\{0\}$, nous avons $a-\alpha=\beta-b=0$.

Nous avons donc la somme directe $E=E^+\oplus E^-$.

(3) **Conclusion** Par définition, $E^+=E_{\mathbb{R}}$. Il nous reste à voir que $E^-=iE^+$. Nous prouvons les inclusions dans les deux sens.

(3a) $E^-\subset iE^+$ Soit $v\in E^-$. Nous avons $iv\in E^+$; en effet

$$\sigma(iv)=\bar{i}\sigma(v)=-i\sigma(v)=iv. \tag{6.317}$$

Donc $iv\in E^+$ pour $v\in E^-$.

(3b) $iE^+\subset E^-$ Soit $v\in E^+$, et voyons que $iv\in E^-$. En effet,

$$\sigma(iv)=-i\sigma(v)=-iv. \tag{6.318}$$

[63] Définition 6.163.
[64] Définition 6.156.

□

6.165.
Lorsque nous avons une structure réelle σ sur un espace vectoriel complexe E, nous écrivons $E = E_{\mathbb{R}} \oplus iE_{\mathbb{R}}$ sans préciser dans la notation « $E_{\mathbb{R}}$ » que cet ensemble dépend du choix de σ. En particulier si F est un sous-espace vectoriel de E, nous utiliserons la notation $F_{\mathbb{R}}$ relativement à la même involution que celle utilisée pour E.

Lemme 6.166.
Soit un espace vectoriel complexe E muni d'une structure réelle σ. Si F est un sous-espace de E alors $F_{\mathbb{R}} = E_{\mathbb{R}} \cap F$.

Démonstration. Par définition,

$$F_{\mathbb{R}} = \{v \in F \text{ tel que } \sigma(v) = v\}. \tag{6.319}$$

(1) $\underline{F_{\mathbb{R}} \subset F}$ C'est dans la définition de $F_{\mathbb{R}}$ (sous-ensemble de F).

(2) $\underline{F_{\mathbb{R}} \subset E_{\mathbb{R}}}$ Si $v \in F_{\mathbb{R}}$, alors $\sigma(v) = v$. Mais cette égalité est précisément celle qui permet d'être dans $E_{\mathbb{R}}$.

□

Vous remarquerez que ce lemme ne fonctionne que parce que nous avons choisi la même structure réelle sur F que sur E.

Chapitre 7

Classification de certains groupes

7.1 Théorèmes de Sylow

Lemme 7.1.
Soient H et K des sous-groupes finis de G. Alors

$$\text{Card}(HK) = \frac{|H| \cdot |K|}{|H \cap K|}. \tag{7.1}$$

Attention : dans ce lemme, l'ensemble HK n'est pas spécialement un groupe. Ce serait le cas si H normalisait K, c'est-à-dire si nous avions $hkh^{-1} \in K$, $\forall (h,k) \in H \times K$.

ThoCauchyGpFini

Théorème 7.2 (Théorème de Cauchy[171])**.**
Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors

(1) G contient un élément d'ordre p.

(2) Si G est un p-groupe, il existe un élément central d'ordre p dans G.

ThoIfdlEB

Lemme 7.3 (Théorème de Cayley)**.**
Si G est un groupe d'ordre n alors il est isomorphe à un sous-groupe du groupe symétrique S_n.

Démonstration. L'action à gauche de G sur lui-même

$$\begin{aligned} \varphi\colon G &\to S_n \\ \varphi(x)g &\mapsto xg \end{aligned} \tag{7.2}$$

est une permutation des éléments de G. Cela donne un morphisme injectif parce que si $\varphi(x) = \varphi(y)$ nous avons $xg = yg$ pour tout g et en particulier pour $g = e$ nous trouvons $x = y$. □

Pour rappel, lorsque p est premier, nous notons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

LemaQxjcm

Lemme 7.4.
Soit p un diviseur premier de n. Alors il existe un morphisme injectif du groupe symétrique S_n dans $\text{GL}(n, \mathbb{F}_p)$.

Démonstration. Soit $\{e_i\}$ la base canonique de $\mathbb{F}_p^n$. Par exemple $e_1 = \big([1]_p, [0]_p, \dots, [0]_p\big)$. Nous avons le morphisme injectif $\varphi\colon S_n \to \text{GL}(n, \mathbb{F}_p)$ donné par $\varphi(\sigma)e_i = e_{\sigma(i)}$. □

RemFzxxst

Remarque 7.5.
En mettant bout à bout les lemmes 7.3 et 7.4, nous trouvons que si p est un diviseur premier de $|G|$, alors G peut être vu comme un sous-groupe de $\text{GL}(n, \mathbb{F}_p)$.

DEFooPRCHooVZdwST

Définition 7.6.
*Soit p un nombre premier. Un p-**groupe** est un groupe dont tous les éléments sont d'ordre p^m pour un certain m (dépendant de l'élément).*

*Soit G un groupe fini et p, un diviseur premier de $|G|$. Un p-**Sylow** dans G est un p-sous-groupe d'ordre p^n où p^n est la plus grande puissance de p divisant $|G|$.*

Notons que si p est un nombre premier, alors tout groupe d'ordre p^m est un p-groupe.

Lemme 7.7.
Soit G un groupe fini et P, Q des p-sous-groupes. Nous supposons que Q normalise P. Alors PQ est un p-sous-groupe de G.

Si S est un p-Sylow, alors p ne divise pas le nombre $|G : S| = |G|/|S|$.

Propvocmon

Proposition 7.8.
Soit le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p premier). Soit T le sous-ensemble de $\mathrm{GL}_n(\mathbb{F}_p)$ formé des matrices triangulaires supérieures de rang[1] n et dont les éléments diagonaux sont 1. Alors T est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

Démonstration. Nous commençons par étudier le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$. Pour la première colonne, la seule contrainte à vérifier est qu'elle ne soit pas nulle. Il y a donc $p^n - 1$ possibilités. Pour la seconde, il faut ne pas être multiple de la première. Il y a donc $p^n - p$ possibilités (parce qu'il y a p multiples possibles de la premières colonne). Pour la k-ième colonne, il faut éviter toutes les combinaisons linéaires des $(k-1)$ premières colonnes. Il y a p^{k-1} telles combinaisons et donc $p^n - p^{k-1}$ possibilités pour la k-ième colonne. Nous avons donc

$$\begin{aligned}\mathrm{Card}\big(\mathrm{GL}(n,\mathbb{F}_p)\big) &= (p^n-1)(p^n-p)\dots(p^n-p^{n-1}) && (7.3a)\\ &= p\cdot p^2\cdots p^{n-1}(p^n-1)(p^{n-1}-1)\dots(p-1) && (7.3b)\\ &= p^{\frac{n(n-1)}{2}}m && (7.3c)\end{aligned}$$

où m est un entier qui ne divise pas p.

En ce qui concerne le cardinal de T, le calcul est plus simple : pour la première ligne nous avons p^{n-1} choix (parce qu'il y a un 1 qui est imposé sur la diagonale), pour la seconde p^{n-2}, etc. En tout nous avons alors

$$|T| = p^{\frac{n(n-1)}{2}}, \tag{7.4}$$

et T est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. □

Proposition 7.9.
Soit p un nombre premier. Un groupe fini G est un p-groupe si et seulement l'ordre de G est p^n pour un certain n.

Démonstration. Supposons que G est un p-groupe. Soit q un nombre premier divisant $|G|$. Par le théorème de Cauchy (7.2), le groupe G contient un élément d'ordre q, soit g un tel élément. Étant donné que G est un p-groupe, $g^{p^n} = g^q = e$ pour un certain n. Donc $q = p^n$ et $q = p$ parce que q est premier. Nous venons de prouver que p est le seul nombre premier qui divise $|G|$. L'ordre de G est par conséquent une puissance de p.

Nous nous intéressons maintenant à l'implication inverse. Nous supposons que $|G| = p^n$ pour un certain entier $n \geqslant 0$. Soit $g \in G$; nous notons r l'ordre de G. Le sous-groupe $\mathrm{gr}(g)$ est d'ordre r, donc r divise $|G|$ (par le théorème 2.73 de Lagrange). Le nombre r est alors une puissance de p. □

LemwDYQMg

Lemme 7.10.
Soit G, un groupe fini de cardinal $|G| = n$ et p, un diviseur premier de n. Nous notons $n = p^m \cdot r$ où p ne divise pas r. Soit H un sous-groupe de G et S, un p-Sylow de G. Alors il existe $g \in G$ tel que

$$gSg^{-1} \cap H \tag{7.5}$$

soit un p-Sylow de H.

Démonstration. Nous considérons l'ensemble G/S sur lequel H agit. Si $a \in G$, le stabilisateur de $[a]$ dans G/S est

$$\begin{aligned}\mathrm{Fix}\big([a]\big) &= \{h \in H \text{ tel que } [ha] = [a]\} && (7.6a)\\ &= \{h \in H \text{ tel que } a^{-1}ha \in S\} && (7.6b)\\ &= aSa^{-1} \cap H. && (7.6c)\end{aligned}$$

Nous cherchons $a \in G$ tel que l'entier

$$\frac{\mathrm{Card}(H)}{\mathrm{Card}\big(aSa^{-1} \cap H\big)} \tag{7.7}$$

EqZpUbWx

[1] Définition 6.51.

soit premier avec p. En effet, dans ce cas le groupe $\mathrm{Fix}([a])$ est un p-Sylow de H parce que $|H : aSa^{-1} \cap H|$ ne divise pas p. La formule des orbites (équation (5.45)) nous dit que

$$\frac{|H|}{|aSa^{-1} \cap H|} = \mathrm{Card}\left(\mathcal{O}_{[a]}\right). \tag{7.8}$$

Supposons que toutes les orbites aient un cardinal divisible par p. Étant donné que G/S est une réunion disjointe de ses orbites, nous aurions

$$p \mid \mathrm{Card}(G/S) = \frac{|G|}{|S|} \tag{7.9}$$

alors que S étant un p-Sylow, p ne peut pas diviser $|G|/|S|$. Toutes les orbites n'ont donc pas un cardinal divisible par p, et il existe un $a \in G$ tel que (7.7) soit vérifiée. □

ThoUkPDXf

Théorème 7.11 (Théorème de Sylow)**.**
Soit G un groupe fini et p, un diviseur premier de $|G|$. Alors

ITEMooETYHooXlUMQZ

(1) G possède au moins un p-Sylow[2]*.*

(2) Tout p-sous-groupe de G est contenu dans un p-Sylow.

ItemMzNRVf

(3) Les p-Sylow de G sont conjugués.

ItemkYbdzZ

(4) Si n_p est le nombre de p-Sylow de G, alors n_p divise $|G|$ et $n_p \in [1]_p$.

Démonstration. En plusieurs points.

(1) Nous savons de la remarque 7.5 que G est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ et que ce dernier a un p-Sylow par la proposition 7.8. Par conséquent G possède un p-Sylow par le lemme 7.10.

(2) Soit H un p-sous-groupe de G et S, un p-Sylow de G (qui existe par le point précédent). Par le lemme 7.10 il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais H est un p-groupe et un p-Sylow dans un p-groupe est automatiquement le groupe entier. Par conséquent,

$$H = aSa^{-1} \cap H \tag{7.10}$$

et $H \subset aSa^{-1}$, ce qui signifie que H est inclus dans un p-Sylow.

(3) Soit H un p-Sylow. Nous venons de voir que si S est un p-Sylow quelconque, alors H est inclus au p-Sylow aSa^{-1} pour un certain $a \in G$. Donc H est un p-Sylow inclus dans le p-Sylow aSa^{-1}, donc $H = aSa^{-1}$.

(4) Le fait que n_p divise n vient du fait que tous les p-Sylow ont le même nombre d'éléments (ils sont conjugués) et sont deux à deux disjoints. Donc ils forment une partition de G et $|G| = n_p|S|$ si S est un p-Sylow quelconque.

Montrons maintenant que n_p est congru à un modulo p. Soit E l'ensemble des p-Sylow de G. Le groupe G agit sur E par conjugaison. Soit S un p-Sylow et considérons l'ensemble

$$E_S = \{T \in E \text{ tel que } s \cdot T = T, \forall s \in S\}. \tag{7.11}$$

où l'action est celle par conjugaison. C'est l'ensemble des points fixes de E sous l'action de S. L'ensemble E est la réunion des orbites sous S et chacune de ces orbites a un cardinal qui divise $|S| = p^m$. Par conséquent $|\mathcal{O}_T|$ vaut 1 lorsque $T \in E_S$ et est un multiple de p sinon. Nous avons donc

$$|E| \equiv |E_S| \mod p. \tag{7.12}$$

Nous voulons obtenir $|E_S| = 1$. Évidemment $S \in E_S$ parce que si $s \in S$ alors $sSs^{-1} = S$. Nous voudrions montrer que S est le seul élément de E_S. Soit $T \in E_S$, c'est-à-dire que T est un p-Sylow de G tel que

$$sTs^{-1} = T \tag{7.13}$$

pour tout $s \in S$. Soit N le groupe engendré par S et T. Montrons que T est normal dans N. Un élément g dans N s'écrit

$$g = s_1 t_1 \cdots s_r t_r \tag{7.14}$$

[2] Définition 7.6.

avec $s_i \in S$ et $t_i \in T$. Si $t \in T$, en utilisant le fait que T est un groupe et le fait que S le normalise, nous avons

$$gtg^{-1} = s_1 t_1 \dots s_r t_r t t_r^{-1} s_r^{-1} \dots t_1^{-1} s_1^{-1} \in T. \tag{7.15}$$

Donc T est un sous-groupe normal de N. Mais S et T sont conjugués dans N (parce qu'ils sont des p-Sylow de N), donc il existe un élément $a \in N$ tel que $aTa^{-1} = S$. Mais étant donné que T est normal,

$$S = aTa^{-1} = T. \tag{7.16}$$

Ceci achève la démonstration des théorèmes de Sylow.

□

Proposition 7.12.
Si S est un p-Sylow dans le groupe G alors pour tout $g \in G$, l'ensemble gSg^{-1} est encore un p-groupe.

Démonstration. Si les éléments de S sont d'ordre p^n, alors nous avons

$$(gsg^{-1})^q = gs^q g^{-1} = e. \tag{7.17}$$

Pour avoir $gs^q g^{-1} = e$, il faut et suffit que $gs^q = g$, alors $s^q = e$, c'est-à-dire $q = p^n$. Donc gSg^{-1} est encore un p-Sylow. □

Lemcmbzum

Lemme 7.13 ([172])**.**
Soit G, un groupe fini et p, un nombre premier. Si H et K sont des groupes distincts d'ordre p, alors $H \cap K = \{e\}$.

Démonstration. L'ensemble $H \cap K$ est un sous-groupe de H. Par conséquent son ordre divise celui de H qui est un nombre premier. Par conséquent soit $|H \cap K| = 1$, soit $|H \cap K| = |H|$. Dans le second cas nous aurions $H = K$, alors que nous avons supposé que H et K étaient distincts. □

PropyfhTmf

Proposition 7.14 ([172])**.**
Soit G un groupe fini et n le nombre de sous-groupes d'ordre p dans G. Alors le nombre d'éléments d'ordre p dans G vaut $n(p-1)$.

Démonstration. Si g est un élément d'ordre p dans G, le groupe H engendré par g est d'ordre p. Réciproquement si H est un groupe d'ordre p, tous les éléments de $H \setminus \{e\}$ sont d'ordre p (parce que l'ordre d'un élément divise l'ordre du groupe). Donc l'ensemble des éléments d'ordre p dans G est la réunion des ensembles $H \setminus \{e\}$ où H parcourt les sous-groupes d'ordre p dans G. Chacun de ces ensembles possède $p-1$ éléments et le lemme 7.13 nous assure qu'ils sont disjoints. Par conséquent nous avons $n(p-1)$ éléments d'ordre p dans G. □

Corolaire 7.15.
Un groupe d'ordre premier est cyclique.

Démonstration. Soit p l'ordre de G. Le nombre de sous-groupes d'ordre p est $n = 1$ (et c'est G lui-même). La proposition 7.14 nous dit alors que le nombre d'éléments d'ordre p dans G est $p-1$. Donc tout élément est générateur. □

7.2 Groupe monogène

SECooXIHPooWVSjhT

Groupe monogène : définition 2.148 ; groupe cyclique : définition 2.149.

Le théorème suivant donne quelques informations à propos des groupes monogènes. Il impliquera dans le corolaire 7.41 qu'un groupe monogène d'ordre n possède $\varphi(n)$ générateurs où φ est la fonction indicatrice d'Euler définie en 7.29.

THOooDOMZooOEYHAe

Théorème 7.16.
Un groupe monogène est abélien. Plus précisément,

(1) un groupe monogène infini est isomorphe à $\mathbb{Z}$,

(2) un groupe monogène fini est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain n.

Démonstration. Le groupe est abélien parce que $g = a^n$, $g' = a^{n'}$ implique $gg' = q^{n+n'} = g'g$. Nous considérons un générateur a de G (qui existe parce que G est monogène) et le morphisme surjectif

$$\begin{aligned} f\colon \mathbb{Z} &\to G \\ p &\mapsto a^p. \end{aligned} \tag{7.18}$$

Si G est infini, alors f est injective parce que si $a^n = a^{n'}$, alors $a^{n-n'} = e$, ce qui rendrait G cyclique et par conséquent non infini. Nous concluons que si G est infini, alors f est une bijection et donc un isomorphisme $\mathbb{Z} \simeq G$.

Si G est fini, alors f n'est pas injective et a un noyau $\ker f$. Étant donné que $\ker f$ est un sous-groupe de G, il existe un (unique) n tel que $\ker f = n\mathbb{Z}$ et le premier théorème d'isomorphisme (théorème 2.20) nous indique que

$$\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} = \text{Image } f = G. \tag{7.19}$$

□

Le lemme suivant donne une démonstration alternative, avec une construction plus explicite de l'isomorphisme.

LemZhxMit

Lemme 7.17 ([1])**.**
À propos de groupes monogènes[3] *et cycliques.*

(1) *Soit un groupe cyclique G de cardinal n dont g est un générateur. Alors il existe un isomorphisme*

$$\phi\colon G \to (\mathbb{Z}/n\mathbb{Z}, +) \tag{7.20}$$

tel que $\phi(g) = 1$.

(2) *Si G est un groupe monogène d'ordre infini et si g est un générateur, alors il existe un isomorphisme*

$$\phi\colon G \to (\mathbb{Z}, +) \tag{7.21}$$

tel que $\phi(g) = 1$.

(3) *Soient G et H deux groupes monogènes de même ordre. Soient g un générateur de G et h, un générateur de H. Il existe un isomorphisme de G sur H qui envoie g sur h.*

Démonstration. Commençons par enfoncer une porte ouverte : comme le groupe est monogène, l'ordre du groupe est égal à l'ordre de son générateur. Nous séparons les cas selon que l'ordre soit fini ou non.

(1) **L'ordre de G est fini et vaut n** Si $k \in \mathbb{Z}$, nous notons $[k]_n$ la classe de k modulo n, c'est-à-dire l'ensemble $\{k + pn \text{ tel que } p \in \mathbb{Z}\}$.

Nous construisons l'isomorphisme $\phi\colon G \to \mathbb{Z}/n\mathbb{Z}$ de la façon suivante :

$$\phi(g^m) = [m]_n. \tag{7.22}$$

Cela est une bonne définition parce qu'une égalité du type $g^m = g^{m'}$ implique que m et m' soient dans la même classe modulo n. Nous vérifions que cela est un isomorphisme entre G et $\mathbb{Z}/n\mathbb{Z}$.

(1a) **Morphisme** Pour l'identité, si $x = e$ alors $m = 0$ et $\phi(e) = [0]_n$. Et si $x = g^k$, $y = g^l$ alors $\phi(xy) = \phi(g^{k+l}) = [k + l]_n = [k]_n + [l]_n = \phi(x) + \phi(y)$.

(1b) **Injectif** Supposons $\phi(g^k) = \phi(g^l)$ avec $k \geqslant l$. Nous avons $h^k = h^l$, donc $h^{k-l} = e$, ce qui donne $k - l \in [0]_n$ ou encore $[k]_n = [l]_n$. En particulier $g^k = g^l$.

(1c) **Surjectif** La classe $[k]_n$ est l'image de g^k.

(2) **L'ordre de G est infini**

Si l'ordre de G est infini alors un élément $x \in G$ s'écrit de façon unique sous la forme $x = g^m$ avec $m \in \mathbb{Z}$. Dans ce cas nous définissons directement $\phi(g^m) = m$.

Le reste de la preuve est alors identique au cas d'ordre fini, mais sans les complications liées au modulo.

La dernière assertion s'obtient des précédentes par composition d'isomorphismes.

□

[3] Définition 2.148.

7.3 Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$

Notons que $\mathbb{Z}/n\mathbb{Z} = \mathbb{F}_n$ est un groupe pour l'addition tandis que $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe pour la multiplication. Il ne peut donc pas y avoir d'équivoque.

ThoozyeSn

Théorème 7.18 ([173]).
Pour chaque $x \in (\mathbb{Z}/n\mathbb{Z})^*$ nous considérons l'application

$$\begin{aligned}\sigma_x\colon \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}\\ y &\mapsto xy.\end{aligned} \tag{7.23}$$

L'application

$$\sigma\colon \big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big) \to \operatorname{Aut}\big(\mathbb{Z}/n\mathbb{Z},+\big) \tag{7.24}$$

ainsi définie est un isomorphisme de groupes.

L'énoncé de ce théorème s'écrit souvent rapidement par

$$\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*, \tag{7.25}$$

mais il faut bien garder à l'esprit qu'à gauche on considère le groupe additif et à droite celui multiplicatif.

Démonstration. Nous notons $[x]$ la classe de x dans $\mathbb{Z}/n\mathbb{Z}$. Nous avons $\mathbb{Z}/n\mathbb{Z} = [1]$. Soit f un automorphisme de $(\mathbb{Z}/n\mathbb{Z},+)$; pour tout $r \in \mathbb{Z}$ nous avons

$$f([r]) = f(r[1]) = rf([1]) = [r]f([1]). \tag{7.26}$$

En particulier, puisque f est surjective, il existe un r tel que $f([r]) = [1]$. Pour un tel r nous avons $[1] = [r]f([1])$, c'est-à-dire que nous avons montré que $f([1])$ est inversible dans $\big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big)$. Nous montrons à présent que[4]

$$\begin{aligned}\sigma\colon \operatorname{Aut}((\mathbb{Z}/n\mathbb{Z},+)) &\to \big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big)\\ f &\mapsto f([1])\end{aligned} \tag{7.27}$$

est un isomorphisme.

Nous commençons par la surjectivité. Soit $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. Les éléments $[a]$ et $[1]$ étant tous deux des générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$, il existe un automorphisme de $\mathbb{Z}/n\mathbb{Z}$ qui envoie $[1]$ sur $[a]$ par le lemme 7.17. Cela prouve la surjectivité de σ.

En ce qui concerne l'injectivité, considérons des automorphismes f_1 et f_2 de $(\mathbb{Z}/n\mathbb{Z},+)$ tels que $f_1([1]) = f_2([1])$. Les automorphismes f_1 et f_2 prennent la même valeur sur un générateur et donc sur tout le groupe. Donc $f_1 = f_2$.

Enfin nous prouvons que σ est un morphisme, c'est-à-dire que $\sigma(f\circ g) = \sigma(f)\sigma(g)$. Nous avons

$$f\big(g([1])\big) = f\big(g([1])[1]\big) = g([1])f([1]) = \sigma(f)\sigma(g). \tag{7.28a}$$

□

Ce dernier résultat s'étend aux groupes cycliques.

PROPooBZOMooVOHoYf

Proposition 7.19.
Si G est un groupe cyclique[5] *d'ordre n, alors*

$$\operatorname{Aut}(G) = \big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big). \tag{7.29}$$

Démonstration. Vu que G est cyclique, le lemme 7.17 nous dit que G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}),+$. Maintenant le théorème 7.18 nous indique que

Les égalités suivantes sont en réalité des isomorphismes de groupes :

$$\begin{aligned}\operatorname{Aut}(G) &= \operatorname{Aut}\Big(\mathbb{Z}/n\mathbb{Z},+\Big) && \text{(7.30a)}\\ &= \Big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \Big) && \text{(7.30b)}\end{aligned}$$

SUBEQooBNGBooEKRZUn
SUBEQooZBMEooBSGPUB

Jusitifications.

[4] Le σ donné ici est l'inverse de celui donné dans l'énoncé. Cela ne change évidemment rien à la validité de l'énoncé et de la preuve.

[5] Définition 2.149.

- Pour (7.30a). Le lemme 7.17 nous dit que G est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$, et le lemme 1.99 dit que des groupes isomorphes ont des groupes d'isomorphismes isomorphes.
- Pour (7.30b). C'est le théorème 7.18.

□

CorwgmoTK

Corolaire 7.20.
Si p divise $q-1$ alors $\mathrm{Aut}(\mathbb{F}_q)$ possède un unique sous-groupe d'ordre p.

Démonstration. Si a est un générateur de $\mathbb{F}_q^*$ alors le groupe

$$\mathrm{gr}\left(a^{\frac{q-1}{p}}\right) \tag{7.31}$$

EqAdGiil

est un sous-groupe d'ordre p. En ce qui concerne l'unicité, soit S un sous-groupe d'ordre p. Il est donc d'indice $(q-1)/p$ dans $\mathbb{F}_q^*$ et le lemme 3.167 nous enseigne que le groupe donné en (7.31) est contenu dans S. Il est donc égal à S parce qu'il a l'ordre de S. Le fait que S soit normal est dû au fait que $\mathbb{F}_q^*$ est abélien. □

7.4 Groupes abéliens finis

Nous rappelons que l'exposant d'un groupe fini est le ppcm des ordres de ses éléments. Dans le cas des groupes abéliens finis, l'exposant joue un rôle important du fait qu'il existe un élément dont l'ordre est l'exposant. C'est le théorème suivant.

Théorème 7.21 (Exposant dans un groupe abélien fini)**.**
Un groupe abélien fini contient un élément dont l'ordre est l'exposant du groupe.

Démonstration. Soit G un groupe abélien fini et $x\in G$, un élément d'ordre maximum m. Nous montrons par l'absurde que l'ordre de tous les éléments de G divise m. Soit donc $y\in G$, un élément dont l'ordre ne divise pas m ; nous notons q son ordre. Vu que q ne divise pas m, le nombre q possède au moins un facteur premier plus de fois que m : soit p premier tel que la décomposition de q contienne p^β et celle de m contienne p^α avec $\beta>\alpha$. Autrement dit,

$$m=p^\alpha m' \tag{7.32a}$$
$$q=p^\beta q' \tag{7.32b}$$

où m' et q' ne contiennent plus le facteur p. L'élément x étant d'ordre m, l'élément x^{p^α} est d'ordre m'. De la même manière, l'élément $y^{q'}$ est d'ordre p^β. Étant donné que p^β et m' sont premiers entre eux, l'élément $x^{p^\alpha}y^{q'}$ est d'ordre $p^\alpha m'>m$. D'où une contradiction avec le fait que x était d'ordre maximal.

Par conséquent l'ordre de tous les éléments de G divise celui de x qui est alors le ppcm des ordres de tous les éléments de G, c'est-à-dire l'exposant de G. □

PropfPRVxi

Proposition 7.22.
Soit G un groupe abélien fini et $x\in G$, un élément d'ordre maximum. Alors

(1) Il existe un morphisme $\varphi\colon G\to\mathrm{gr}(x)$ tel que $\varphi(x)=x$.

ItemKRYwjU

(2) Il existe un sous-groupe K de G tel que $G=\mathrm{gr}(x)\oplus K$.

Démonstration. Nous notons a l'ordre de x qui est également l'exposant du groupe G.

Nous allons prouver la première partie par récurrence sur l'ordre du groupe. Si $G=\mathrm{gr}(x)$, alors c'est évident. Soit H un sous-groupe propre de G contenant x et tel que le problème soit déjà résolu pour H : il existe un morphisme $\varphi\colon H\to\mathrm{gr}(x)$ tel que $\varphi(x)=x$. Soit $y\in G\setminus H$, d'ordre b. Nous allons trouver un morphisme $\hat{\varphi}\colon \mathrm{gr}(H,y)\to\mathrm{gr}(x)$ telle que $\hat{\varphi}(x)=x$.

Pour cela nous commençons par construire les applications suivantes :

$$\begin{aligned}\tilde{\varphi}\colon \mathbb{Z}/b\mathbb{Z}\times H&\to\mathrm{gr}(x)\\ (\bar{k},h)&\mapsto x^{kl}\varphi(h)\end{aligned} \tag{7.33}$$

où l est encore à déterminer, et

$$\begin{aligned}p\colon \mathbb{Z}/b\mathbb{Z}\times H&\to\mathrm{gr}(y,H)\\ (\bar{k},h)&\mapsto y^k h.\end{aligned} \tag{7.34}$$

Pour que $\tilde{\varphi}$ soit bien définie, il faut que a divise bl. L'application p est bien définie parce que $\bar{k}$ est pris dans $\mathbb{Z}/b\mathbb{Z}$ et que b est l'ordre de y.

Nous allons construire le morphisme $\hat{\varphi}$ en considérant le diagramme

$$\begin{array}{ccccc} \ker(p) & \hookrightarrow & \mathbb{Z}/b\mathbb{Z}\times H & \xrightarrow{p} & \operatorname{gr}(y,H) \\ & & \downarrow{\scriptstyle\tilde{\varphi}} & \swarrow{\scriptstyle\hat{\varphi}} & \\ & & \operatorname{gr}(x) & & \end{array} \tag{7.35}$$

que l'on voudra être commutatif. Puisque p est surjective, les théorèmes d'isomorphismes nous disent que

$$\operatorname{gr}(y,H)\simeq\frac{\mathbb{Z}/b\mathbb{Z}\times H}{\ker p}. \tag{7.36}$$

Si $[\bar{k},h]$ est la classe de $(\bar{k},h)$ modulo $\ker(p)$ alors nous voudrions définir $\hat{\varphi}$ par

$$\hat{\varphi}\big([\bar{k},h]\big)=\tilde{\varphi}(\bar{k},h). \tag{7.37}$$

Pour que cela soit bien défini, il faut que si $(\bar{r},z)\in\ker p$, alors,

$$\hat{\varphi}\big([\bar{k}\bar{r},hz]\big)=\hat{\varphi}\big([\bar{k},h]\big), \tag{7.38}$$

c'est-à-dire que $\tilde{\varphi}(\bar{r},z)=e$. Du coup la définition (7.37) n'est bonne que si et seulement si

$$\ker(p)\subset\ker(\tilde{\varphi}). \tag{7.39}$$

Nous pouvons obtenir cela en choisissant bien l.

Déterminons d'abord le noyau de p. Pour cela nous considérons un nombre β divisant b tel que $\operatorname{gr}(y)\cap H=\operatorname{gr}(y^\beta)$. Nous aurons $p(\bar{k},h)=e$ si et seulement si $y^h=e$. En particulier $h=y^{-k}\in\operatorname{gr}(y)\cap H=\operatorname{gr}(y^\beta)$. Si $h=(y^\beta)^m=y^{m\beta}$, alors $k=-m\beta$ et nous avons

$$\ker(p)=\{(-m\beta,y^{m\beta})\text{ tel que }m\in\mathbb{Z}\}. \tag{7.40}$$

En plus court : $\ker(p)=\operatorname{gr}(\beta,y^{-\beta})$. Nous devons donc fixer l de telle sorte que $\tilde{\varphi}(\beta,y^{-\beta})=e$. Étant donné que φ prend ses valeurs dans $\operatorname{gr}(x)$, il existe un entier α tel que $\varphi(y^{-\beta})=x^\alpha$; en utilisant cet α, nous écrivons

$$\tilde{\varphi}(\beta,y^{-\beta})=x^{\beta l}\varphi(y^{-\beta})=x^{\beta l+\alpha}. \tag{7.41}$$

Par conséquent nous choisissons $l=-\alpha/\beta$. Nous devons maintenant vérifier que ce choix est légitime, c'est-à-dire que a divise bl et que α/β est un entier.

Étant donné que y est d'ordre b,

$$e=\varphi(y^b)=\varphi(y^{-\beta b/\beta})=\varphi(y^{-\beta})^{b/\beta}=x^{b\beta/\alpha}. \tag{7.42}$$

Par conséquent a divise $\frac{b\alpha}{\beta}=-bl$.

Pour voir que l est entier, nous nous rappelons que a est l'exposant de G (parce que x est d'ordre maximum) et que par conséquent b divise a. Mais a divise $\alpha\frac{b}{\beta}$. Donc α/β est entier.

Nous passons maintenant à la seconde partie de la preuve. Nous considérons un morphisme $\varphi\colon G\to\operatorname{gr}(x)$ tel que $\varphi(x)=x$. La première partie nous en assure l'existence. Nous montrons que

$$\begin{aligned}\psi\colon G&\to\operatorname{gr}(x)\oplus\ker(\varphi)\\ g&\mapsto\big(\varphi(g),g\varphi(g)^{-1}\big)\end{aligned} \tag{7.43}$$

est un isomorphisme. D'abord $g\varphi(g)^{-1}$ est dans le noyau de φ parce que $\varphi(g)^{-1}$ étant dans $\operatorname{gr}(x)$, et φ étant un morphisme,

$$\varphi\big(g\varphi(g)^{-1}\big)=\varphi(g)\varphi(g)^{-1}=e. \tag{7.44}$$

L'application ψ est un morphisme parce que, en utilisant le fait que G est abélien,

$$\psi(g_1g_2)=\big(\varphi(g_1g_2),g_1g_2\varphi(g_1g_2)^{-1}\big) \tag{7.45a}$$
$$=\big(\varphi(g_1)\varphi(g_2),g_1\varphi(g_1)^{-1}g_2\varphi(g_2)^{-1}\big) \tag{7.45b}$$
$$=\psi(g_1)\psi(g_2). \tag{7.45c}$$

L'application ψ est injective parce que si $\psi(g)=(e,e)$ alors $\varphi(g)=e$ et $g\varphi(g)^{-1}=e$, ce qui implique $g=e$.

Enfin ψ est surjective parce qu'elle est injective et que les ensembles de départ et d'arrivée ont même cardinal. En effet par le premier théorème d'isomorphisme (théorème 2.20) appliqué à φ nous avons

$$|G|=|\operatorname{gr}(x)|\cdot|\ker(\varphi)|. \tag{7.46}$$

□

ThoRJWVJd

Théorème 7.23.
Si G est un groupe abélien fini non trivial, il exise un unique $r > 0$ et une unique liste de naturels $(d_1, \dots, d_r)$ tels que

(1) $G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_r\mathbb{Z}$

(2) $d_1 \geqslant 1$

(3) d_i *divise* d_{i+1} *pour tout* $i = 1, \dots, r-1$.

Démonstration. Soit x_1 un élément d'ordre maximal dans G. Soit n_1 son ordre et

$$H_1 = \mathrm{gr}(x_1) = \mathbb{F}_{n_1}. \tag{7.47}$$

D'après la proposition 7.22(2), il existe un supplémentaire K_1 tel que $G = \mathbb{F}_{n_1} \oplus K_1$. Si $K_1 = \{e\}$ on s'arrête et on garde $G = \mathbb{F}_{n_1}$. Sinon on continue de la sorte en prenant x_2 d'ordre maximal dans K_1 etc.

Nous devons maintenant prouver l'unicité de cette décomposition. Supposons deux décompositions avec les nombres $(d_1, \dots, d_r)$ et $(s_1, \dots, s_q)$:

$$G = \mathbb{F}_{d_1} \oplus \dots \oplus \mathbb{F}_{d_r} = \mathbb{F}_{s_1} \oplus \dots \oplus \mathbb{F}_{s_q}. \tag{7.48}$$

L'exposant de G est d_r et s_q. Donc $d_r = s_q$. Les complémentaires étant égaux nous avons

$$\mathbb{F}_{d_1} \oplus \dots \oplus \mathbb{F}_{d_{r-1}} = \mathbb{F}_{s_1} \oplus \dots \oplus \mathbb{F}_{s_{q-1}}. \tag{7.49}$$

En continuant nous trouvons $r = q$ et $d_i = s_i$. □

7.5 Groupes d'ordre pq

Lemme 7.24.
Soit G un groupe d'ordre pq où p et q sont des nombres premiers distincts. Nous supposons que $p < q$.

(1) Le groupe G possède un unique q-Sylow.

(2) Cet unique q-Sylow est normal dans G.

(3) Il n'est ni $\{e\}$ ni G.

(4) Le groupe G n'est pas un groupe simple[6].

Démonstration. Soit n_q le nombre de q-Sylow ; par le théorème de Sylow 7.11(1) le groupe G possède des q-Sylow et par 7.11(4),

$$n_q \in [1]_q. \tag{7.50}$$

De plus le nombre n_q divise $|G| = pq$. Donc n_q vaut p, q ou 1. Avoir $n_q = p$ n'est pas possible parce que $n_q \in [1]_q$ et $p < q$. Avoir $n_q = q$ n'est pas possible non plus, pour la même raison. Donc $n_q = 1$. Notons H l'unique q-Sylow de G.

Le fait que H soit normal est une conséquence de 7.11(3) parce que le conjugué de H est encore un q-Sylow alors que H est l'unique q-Sylow.

Vu que

$$1 < p = |H| < pq = |G|, \tag{7.51}$$

le sous-groupe H n'est ni réduit à l'identité ni le groupe entier.

Par conséquent G n'est pas simple parce qu'il contient un sous-groupe normal non trivial. □

Avant de lire le théorème suivant, n'oubliez pas de lire la définition d'un produit semi-direct 2.158.

ThoLnTMBy

Théorème 7.25 ([174]).
Soient deux nombres premiers distincts[7] *p et q avec $q > p$.*

(1) Si p ne divise pas $q-1$ alors tout groupe d'ordre pq est cyclique et plus précisément le seul groupe (à isomorphisme près) d'ordre pq est $\mathbb{Z}/pq\mathbb{Z}$.

ITEMooFQXIooFLAiUD

(2) Si $p \mid q-1$, alors il n'existe que deux groupes d'ordre pq :

[6] Pas de sous-groupes normaux non triviaux, 2.75.
[7] Le cas $p = q$ sera traité par la proposition 7.28.

- *Le groupe abélien et cyclique* $\mathbb{Z}/pq\mathbb{Z}$.
- *Le produit semi-direct non abélien*

$$G = \mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z} \tag{7.52}$$

où $\varphi(\bar{1})$ *est d'ordre* p *dans* $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

(3) Si p *et* q *sont premiers entre eux, le produit est direct*[8].

Démonstration. Division de la preuve en plusieurs parties.

(1) **Préliminaires avec Sylow**

Soit un groupe G d'ordre pq. Soient H, un q-Sylow et K, un p-Sylow de G. Ils existent parce que p et q sont des diviseurs premiers de $|G|$ (théorème de Sylow 7.11). Si n_q est le nombre de q-Sylow dans G alors n_q divise $|G|$ et $n_q = 1 \mod q$. Donc d'abord n_q vaut 1, p ou q. Ensuite $n_q = q$ est exclu par la condition $n_q = 1 \mod q$; la possibilité $n_q = p$ est également impossible parce que $p = 1 \mod q$ est impossible avec $p < q$. Donc $n_q = 1$ et H est normal dans G.

L'ensemble $H \cap K$ est un sous-groupe à la fois de H et de K, ce qui entraine que (théorème de Lagrange 2.73) $|H \cap K|$ divise à la fois p et q. Nous en déduisons que $|H \cap K| = 1$ et donc que $H \cap K = \{e\}$.

Étant donné que H est normal, l'ensemble HK est un sous-groupe de G. De plus l'application

$$\begin{aligned} \psi\colon H \times K &\to HK \\ (h,k) &\mapsto hk \end{aligned} \tag{7.53}$$

est un bijection. Nous ne devons vérifier seulement l'injectivité. Supposons que $hk = h'k'$. Alors $e = h^{-1}h'k'k^{-1}$, et donc

$$h^{-1}h' = (k'k^{-1})^{-1} \in H \cap K = \{e\}. \tag{7.54}$$

Par conséquent $|pq| = |H \times K| = |HK|$, et $HK = G$. Le corolaire 2.161 nous indique que

$$G = H \times_\varphi K \tag{7.55}$$

où φ est l'action adjointe. Nous devons maintenant identifier cette action. En d'autres termes, nous savons que $H = \mathbb{Z}/q\mathbb{Z}$ et $K = \mathbb{Z}/p\mathbb{Z}$ et que $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme. Nous devons déterminer les possibilités pour φ.

Soit n_p le nombre de p-Sylow de G. Comme précédemment, n_p vaut 1, p ou q et la possibilité $n_p = p$ est exclue. Donc n_p est 1 ou q.

(2) **Si** p **ne divise pas** $q-1$

Si p ne divise pas $q-1$ alors il n'est pas possible d'avoir $n_p = q$ parce que $n_p \in [1]_p$. Or dire $n_p = q$ demanderait $q \in [1]_p$, c'est-à-dire $q = kp + 1$, qui impliquerait que p divise $q - 1$.

La seule possibilité est que $n_p = 1$. Dans ce cas, K est également normal dans G. Du coup le produit semi-direct (7.55) est en réalité un produit direct (φ est triviale) et nous avons

$$G = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/pq\mathbb{Z}. \tag{7.56}$$

(3) **Si** p **divise** $q-1$

Cette fois $n_p = 1$ et $n_p = q$ sont tous deux possibles. Ce que nous savons est que $\varphi(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Par le premier théorème d'isomorphisme 2.20, nous avons

$$|\varphi(\mathbb{Z}/p\mathbb{Z})| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\ker\varphi|}, \tag{7.57}$$

ce qui signifie que $|\varphi(\mathbb{Z}/p\mathbb{Z})|$ divise $|\mathbb{Z}/p\mathbb{Z}| = p$. Par conséquent, $|\varphi(\mathbb{Z}/p\mathbb{Z})|$ est égal à 1 ou p. Si c'est 1, alors l'action est triviale et le produit est direct.

Nous supposons que $|\varphi(\mathbb{Z}/p\mathbb{Z})| = p$. Le corolaire 7.20 nous indique que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ possède un unique sous-groupe d'ordre p que nous notons Γ ; c'est-à-dire que $\Gamma = \mathrm{Image}(\varphi)$. Vu que $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme, Γ est généré par $\varphi(\bar{1})$ qui est alors un élément d'ordre p, comme annoncé.

[8] Cette affirmation me semble très bizarre. Comment deux nombres premiers distincts pourraient ne pas être premiers entre eux ???

(4) **Unicité** Nous nous attaquons maintenant à l'unicité. Soient φ et φ' deux morphismes non triviaux $\mathbb{Z}/p\mathbb{Z} \to \text{Aut}(\mathbb{Z}/q\mathbb{Z})$. Étant donné que $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ ne possède qu'un seul sous-groupe d'ordre p, nous savons que $\text{Image}(\varphi) = \text{Image}(\varphi') = \Gamma$. Nous pouvons donc parler de φ'^{-1} en tant qu'application de $\mathbb{Z}/p\mathbb{Z}$ dans Γ. Nous montrons que

$$\begin{aligned} f\colon \mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/q\mathbb{Z} \times_{\varphi'} \mathbb{Z}/p\mathbb{Z} \\ (h,k) &\mapsto (h, \alpha(k)) \end{aligned} \tag{7.58}$$

où $\alpha = \varphi'^{-1} \circ \varphi$ est un isomorphisme de groupes. Le calcul est immédiat :

$$f(h_1,k_1)f(h_2mk_2) = \big(h_1,\alpha(k_1)\big)(h_2,\alpha(k_2)) \tag{7.59a}$$
$$= \big(h_1\varphi'(\alpha(k_1))h_2m\alpha(k_1k_2)\big) \tag{7.59b}$$
$$= f\big(h_1\varphi(k_1)h_2, k_1k_2\big) \tag{7.59c}$$
$$= f\big((h_1,k_1),(h_2,k_2)\big). \tag{7.59d}$$

Par conséquent $\mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \times_{\varphi'} \mathbb{Z}/p\mathbb{Z}$.

□

Note : il existe des nombres premiers p et q tels que $q = 1 \mod p$. Par exemple $7 = 1 \mod 3$.

PROPooNSRYooEodtUl

Proposition 7.26 ([57]).
Soit G un groupe fini d'ordre pq où p et q sont deux nombres premiers distincts vérifiant

$$\begin{cases} p \neq 1 \mod q & (7.60a) \\ q \neq 1 \mod p. & (7.60b) \end{cases}$$

Alors G est cyclique, abélien et

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \tag{7.61}$$

Démonstration. Soient n_p et n_q les nombres de p-Sylow et q-Sylow. Par le théorème de Sylow 7.11, n_p divise pq et $n_p = 1 \mod p$. Le second point empêche n_p de diviser p. Par conséquent n_p divise q et donc n_p vaut 1 ou q. La possibilité $n_p = q$ est exclue par l'hypothèse $q \neq 1 \mod p$. Donc $n_p = 1$, et de la même façon nous obtenons $n_q = 1$.

Soient S l'unique p-Sylow et T, l'unique q-Sylow. Pour les mêmes raisons que celles exposées plus haut, ce sont deux sous-groupes normaux dans G. Étant donné que S est d'ordre p^n pour un certain n et que l'ordre de S doit diviser celui de G, nous avons $|S| = p$. De la même façon, $|T| = q$. Par conséquent S est un groupe cyclique d'ordre p et nous considérons x, un de ses générateurs. De la même façon soit y, un générateur de T.

Nous montrons maintenant que x et y commutent, puis que xy engendre G. Nous savons que $S \cap T$ est un sous-groupe à la fois de S et de T, de telle façon que $|S \cap T|$ divise à la fois $|S| = p$ et $|T| = q$. Nous avons donc $|S \cap T| = 1$ et donc $S \cap T$ se réduit au neutre. Par ailleurs, S et T sont normaux, donc

$$(xyx^{-1})y^{-1} \in T \tag{7.62a}$$
$$x(yx^{-1}y^{-1}) \in S, \tag{7.62b}$$

donc $xyx^{-1}y^{-1} = e$, ce qui montre que $xy = yx$.

Montrons que xy engendre G. Soit $m > 0$ tel que $(xy)^m = e$. Pour ce m nous avons $x^m = y^{-m}$ et $y^{-m} = x^m$, ce qui signifie que x^m et y^m appartiennent à $S \cap T$ et donc $x^m = y^m = e$. Les nombres p et q divisent donc tous deux m ; par conséquent $\text{ppcm}(p,q) = pq$ divise m. Nous en concluons que xy est d'ordre pq (il ne peut pas être plus) et qu'il est alors générateur.

Pour la suite nous allons d'abord prouver que $G = ST$ puis que $G \simeq S \times T$. Nous savons déjà que $|S \cap T| = 1$, ce qui nous amène à dire que $|ST| = |S||T|$. En effet si $s, s' \in S$ et $t, t' \in t$ et si $st = s't'$, alors $t = s^{-1}s't'$, ce qui voudrait dire que $s^{-1}s' \in T$ et donc que $s^{-1}s' = e$. Au final nous avons

$$|ST| = |S||T| = pq = |G|. \tag{7.63}$$

Par conséquent $G = ST$. En nous rappelant que $S \cap T = \{e\}$ et que S et T sont normaux, le lemme 3.138 nous dit que $G \simeq S \times T$. Le groupe S étant cyclique d'ordre p nous avons $S = \mathbb{Z}/p\mathbb{Z}$ et pour T, nous avons la même chose : $T = \mathbb{Z}/q\mathbb{Z}$. Nous concluons que

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \tag{7.64}$$

□

ThoImkljy

Théorème 7.27 (Théorème de Burnside[150]).
Le centre d'un p-groupe non trivial est non trivial.

Démonstration. Soit G un p-groupe non trivial. Nous considérons l'action adjointe G sur lui-même. Les points fixes de cette action sont les éléments du centre :

$$\mathcal{Z}_G = \{z \in G \text{ tel que } \sigma_x(z) = z, \forall x \in G\} = \mathrm{Fix}_G(G). \tag{7.65}$$

Nous utilisons l'équation aux classes (5.25) pour dire que $|G| = |\mathcal{Z}_G| \mod p$. Mais $|\mathcal{Z}_G|$ n'est pas vide parce qu'il contient l'identité. Donc $|\mathcal{Z}_G|$ est au moins d'ordre p. □

PropssttFK

Proposition 7.28.
Si p est un nombre premier, tout groupe d'ordre p ou p^2 est abélien.

Rappel : un groupe d'ordre p ou p^2 est automatiquement un p-groupe.

Démonstration. Si $|G| = p$, alors le théorème de Cauchy 7.2 nous donne l'existence d'un élément d'ordre p. Cet élément est alors automatiquement générateur, G est cyclique et donc abélien.

Si par contre G est d'ordre p^2, alors les choses se compliquent (un peu). D'après le théorème de Burnside 7.27, le centre $\mathcal{Z}$ n'est pas trivial ; il est alors d'ordre p ou p^2. Supposons qu'il soit d'ordre p et prenons $x \in G \setminus \mathcal{Z}$. Alors le stabilisateur de x pour l'action adjointe contient au moins $\mathcal{Z}$ et x, c'est-à-dire que $|\mathrm{Fix}_G(x)| \geqslant p + 1$. Étant donné que $\mathrm{Fix}_G(x)$ est un sous-groupe, son ordre est automatiquement 1, p ou p^2. En l'occurrence, il doit être p^2 (parce que plus grand que p), et donc x doit être central, ce qui est une contradiction. □

7.5.1 Fonction indicatrice d'Euler

DEFooZRYMooZCozga

Définition 7.29.
*La **fonction indicatrice d'Euler** est l'application*

$$\begin{aligned} \varphi\colon \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto \mathrm{Card}\Big(\{m \in \mathbb{N}^* \text{ tel que } 1 \leqslant m \leqslant n, \mathrm{pgcd}(m,n) = 1\}\Big). \end{aligned} \tag{7.66}$$

7.30.
Quelques notes.

(1) Cette fonction est nommée « totient » en anglais.

(2) Voir le thème 11 pour des formules concernant l'indicatrice d'Euler.

(3) Une vidéo de 3Blue1Brown : https://www.youtube.com/watch?v=EK32jo7i5LQ.

LEMooVGDHooStUaKH

Lemme 7.31 ([175]).
L'élément $[m]_n$ est inversible dans le groupe $\big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big)$ si et seulement si $\mathrm{pgcd}(m,n) = 1$.

Démonstration. Dans les deux sens.

(1) $\Rightarrow$ Si $[m_n]$ est inversible, il existe $u \in \mathbb{Z}$ tel que $[u]_n[m]_n = [1]_n$. Cela donne $[um]_n = [1]_n$ ou encore $um \in [1]_n$, c'est-à-dire $um = 1 + vn$. Le théorème de Bézout 3.46 conclut que $\mathrm{pgcd}(m,n) = 1$.

(2) $\Leftarrow$ Si $\mathrm{pgcd}(m,n) = 1$, alors le théorème de Bézout 3.46 nous dit qu'il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$. Cela donne directement $um = 1 - vn \in [1]_n$ et donc $[u]_n$ est un inverse de $[m]_n$ dans le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}$.

□

LEMooCLYEooONhWKs

Lemme 7.32.
Nous avons

$$\varphi(n) = \mathrm{Card}\big((\mathbb{Z}/n\mathbb{Z})^\times\big) \tag{7.67}$$

où $A^\times$ est le groupe des inversibles (pour la multiplication) dans l'anneau A.

Démonstration. En utilisant le lemme 7.31,

$$\begin{aligned}\big(\mathbb{Z}/n\mathbb{Z}\big)^{\times} &= \{[m]_n \text{ tel que } \operatorname{pgcd}(m,n)=1\} &(7.68a)\\ &= \{[m]_n \text{ tel que } 1\leqslant m\leqslant n, \operatorname{pgcd}(m,n)=1\} &(7.68b)\end{aligned}$$

Comme deux entiers différents entre 1 et n ne peuvent pas être dans la même classe modulo n, il y a bijection entre le dernier ensemble et $\{1\leqslant m\leqslant n \text{ tel que } \operatorname{pgcd}(m,n)=1\}$. Donc

$$\varphi(n)=\operatorname{Card}\big(\{[m]_n \text{ tel que } 1\leqslant m\leqslant n, \operatorname{pgcd}(m,n)=1\}\big)=\operatorname{Card}\big((\mathbb{Z}/n\mathbb{Z})^{\times}\big). \tag{7.69}$$

□

LEMooRGIYooRxgyCO

Lemme 7.33 ([176]).
Soit $n,d\in\mathbb{N}$ tels que $d\mid n$. Nous notons $q=n/d$ et $G=\{k[q]_n \text{ tel que } 0\leqslant k\leqslant d-1\}$. Alors, pour $r\in\mathbb{Z}$ nous avons $d[r]_n=[0]_n$ si et seulement si $[r]_n\in G$.

Démonstration. Dans les deux sens.

(1) $\Rightarrow$ Nous supposons que $d[r]_n=[0]_n$. Étant donné que $n=dq$ nous avons les implications suivantes :

$$d[r]_n=[0]_n\Rightarrow d\mid dr\Rightarrow dq\mid dr\Rightarrow q\mid r. \tag{7.70}$$

Nous avons donc $r=kq$ pour un certain $k\in\mathbb{Z}$. Par la division euclidienne 3.40, il existe $s,t\in\mathbb{N}$ tels que $k=sd+t$ avec $t<d$. Avec ça, nous avons le calcul

$$[r]_n=k[q]_n=sd[q]_n+t[q]_n=\underbrace{s[dq]_n}_{=[0]_n}+t[q]_n\in G. \tag{7.71}$$

(2) $\Leftarrow$ Si $[r]_n\in G$, il existe $0\leqslant k\leqslant d-1$ tel que $[r]_n=k[q]_n$. De ce fait,

$$d[r]_n=dk[q]_n=k[dq]_n=[0]_n. \tag{7.72}$$

Et voilà.

□

La proposition suivante est un pas important dans l'algorithme de Shor permettant aux ordinateurs quantiques de factoriser rapidement des grands nombres[177].

THOooXMBSooXrrfOP

Théorème 7.34 (Euler-Fermat[178]).
Deux énoncés très similaires.

(1) Soient a,n premiers entre eux dans $\mathbb{N}$. Alors Nous avons la formule

$$a^{\varphi(n)}\in[1]_n. \tag{7.73}$$

ITEMooJHZBooXVKMlT

(2) Soient $A,B\in\mathbb{N}$ premiers entre eux. Alors il existe $p,m\in\mathbb{N}$ tels que

$$A^p=mB+1. \tag{7.74}$$

Démonstration. Vu que $\operatorname{pgcd}(a,n)=1$, le théorème de Bézout 3.46 donne $ua+vn=1$, c'est-à-dire $u[a]_n\in[1]_n$. Autrement dit, $[a]_n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. De ce fait l'application

$$\begin{aligned}f\colon (\mathbb{Z}/n\mathbb{Z})^{\times}&\to(\mathbb{Z}/n\mathbb{Z})^{\times}\\ x&\mapsto[a]_nx\end{aligned} \tag{7.75}$$

est une bijection.

Un produit peut être réindexé par une bijection[9]. En posant $P = \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x$, nous avons

$$\begin{aligned}
P &= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x && (7.76a)\\
&= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} f(x) && (7.76b)\\
&= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} [a]_n x && (7.76c)\\
&= \Big(\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} [a]_n\Big)\Big(\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x\Big) && (7.76d)\\
&= [a]_n^{\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)} P && (7.76e)
\end{aligned}$$

En simplifiant par P dans $\mathbb{Z}/n\mathbb{Z}$ nous trouvons

$$[a]_n^{\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)} = [1]_n. \tag{7.77}$$

Et comme le lemme 7.32 donne $\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right) = \varphi(n)$, nous avons trouvé $[a]_n^{\varphi(n)} = [1]_n$. Autrement dit,

$$a^{\varphi(n)} \in [1]_n. \tag{7.78}$$

Le point (2) n'est qu'une reformulation. Vu que A et B sont premiers entre eux, nous venons de voir que $A^{\varphi(B)} \in [1]_B$. Il existe donc $m \in \mathbb{Z}$ tel que $A^{\varphi(B)} = 1 + mB$. Vu que A et B sont dans $\mathbb{N}$, le nombre m est contraint d'être positif, c'est-à-dire $m \in \mathbb{N}$. □

LEMooKPKBooPbrHkI

Lemme 7.35 ([176]).
Soient $d \mid n$ dans $\mathbb{N}^*$. Nous considérons le groupe additif $G_d = \{k[q]_n \text{ tel que } 0 \leqslant k \leqslant d-1\}$. Les éléments d'ordre[10] d dans $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les générateurs de G_d.

Démonstration. Les générateurs de G_d sont d'ordre d parce que $|G_d| = d$. Ça, c'était le sens facile. Dans l'autre sens, si $[r]_n$ est d'ordre d, alors $d[r]_n = [0]_n$. D'après le lemme 7.33, cela prouve que $[r]_n \in G_d$.

Comme le groupe engendré par $[r]_n$ est d'ordre d, il est tout G_d. Donc $[r]_n$ est générateur de G_d. □

LEMooQGGLooDkkmcF

Lemme 7.36 ([179]).
L'ensemble des générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ est $(\mathbb{Z}/n\mathbb{Z})^\times$.

Démonstration. Si $[r]_n$ est générateur de $\mathbb{Z}/n\mathbb{Z}$, il existe k tel que $k[r]_n = [1]_n$. Dans ce cas, $[k]_n$ est l'inverse de $[r]_n$ pour la multiplication. Donc $[r]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$.

À l'inverse, si $[r]_n$ est inversible, alors il existe k tel que $k[r]_n = [1]_n$. Dans ce cas, $[t]_n = kt[r]_n$, ce qui montre que $[r]_n$ est générateur (pour l'addition). □

LEMooRMWRooRSjGPL

Lemme 7.37 ([179]).
Si G est un groupe cyclique d'ordre n, alors G possède $\varphi(n)$ générateurs.

Démonstration. Vu que tous les groupes cycliques d'ordre n sont isomorphes à $(\mathbb{Z}/n\mathbb{Z}), +$, nous nous contentons de prouver le résultat pour ce groupe. Le lemme 7.36 montre que $(\mathbb{Z}/n\mathbb{Z}, +)$ possède $\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)$ générateurs.

Mais le lemme 7.32 assure que $\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right) = \varphi(n)$. □

PROPooYHUDooUROTiN

Proposition 7.38.
Nous avons la formule

$$n = \sum_{d\mid n} \varphi(d). \tag{7.79}$$

EqTPHqgJ

Démonstration. Nous notons H_d la partie de $(\mathbb{Z}/n\mathbb{Z}, +)$ composée des éléments d'ordre d. Nous avons vu dans le lemme 7.35 que H_d sont justement les générateurs de G_d – voir le lemme pour la notation. Mais comme G_d est un groupe cyclique d'ordre d, il contient $\varphi(d)$ générateurs (lemme 7.37) : $\text{Card}(H_d) = \varphi(d)$.

[9] Proposition 2.129. Pour rappel, le produit n'est rien d'autre qu'une somme pour un groupe dont la loi est notée multiplicativement.

[10] Ordre d'un élément, définition 2.68.

Vu que tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ ont un ordre qui divise n (corolaire 2.74), nous avons l'union disjointe

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n} H_d, \tag{7.80}$$

et donc au niveau des cardinals,

$$n = \mathrm{Card}(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \mathrm{Card}(H_d) = \sum_{d|n} \varphi(d). \tag{7.81}$$

□

LEMooBEJOooDqTirj

Lemme 7.39 ([180])**.**
Si p est un nombre premier, alors $\varphi(p^n) = p^n - p^{n-1}$.

Démonstration. Les éléments de $\{1, \dots, p^n\}$ qui ont un pgcd différent de 1 avec p^n sont des nombres qui s'écrivent sous la forme qp avec $q \leqslant p^{n-1}$ (corolaire 3.161). Il y a évidemment p^{n-1} tels nombres.

Donc les éléments de $\{1, \dots, p^n\}$ qui sont relativement premiers à p^n sont au nombre de $p^n - p^{n-1}$ (tous sauf les p^{n-1} dont on vient de parler). □

7.5.2 Générateurs

PropZnmuphiGensn

Proposition 7.40.
Soit $n \in \mathbb{N} \setminus \{0\}$ et le groupe (additif) $\mathbb{Z}/n\mathbb{Z}$. L'élément $[x]_n$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $x \in P_n$. En particulier $\mathbb{Z}/n\mathbb{Z}$ est un groupe contenant $\varphi(n)$ générateurs.

Démonstration. Nous avons $\mathrm{gr}\big([1]_n\big) = \mathbb{Z}/n\mathbb{Z}$. L'élément $[x]_n$ sera générateur si et seulement si il génère $[1]_n$, c'est-à-dire si il existe u tel que $u[x]_n = [1]_n$. Cette dernière égalité étant une égalité de classes dans $\mathbb{Z}/n\mathbb{Z}$, elle sera vraie si et seulement si il existe v tel que

$$ux + vn = 1. \tag{7.82}$$

Cela signifie entre autres que[11] $x\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$, et aussi que $\mathrm{pgcd}(x, n) = 1$ par le théorème de Bézout 3.46, et donc que $x \in P_n$. □

CORooMBLSooMHKmAq

Corolaire 7.41.
Un groupe monogène d'ordre n possède $\varphi(n)$ générateurs, où φ est la fonction indicatrice d'Euler définie en 7.29.

Démonstration. Le théorème 7.16 nous dit qu'un groupe monogène d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. La proposition 7.40 nous indique que $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(n)$ générateurs. □

7.5.3 Fonction indicatrice d'Euler (propriétés)

subSecKGDFonAbEffjs

Corolaire 7.42.
Deux propriétés.

(1) L'indicatrice d'Euler est multiplicative : si p est premier avec q, alors

$$\varphi(pq) = \varphi(p)\varphi(q). \tag{7.83}$$

(2) Si p est un nombre premier,

$$\varphi(p) = (p - 1). \tag{7.84}$$

Démonstration. Nous savons que si p et q sont premiers entre eux, alors le théorème 7.25 nous donne l'isomorphisme de groupe

$$(\mathbb{Z}/pq\mathbb{Z}, +) \simeq (\mathbb{Z}/p\mathbb{Z}, +) \times (\mathbb{Z}/q\mathbb{Z}, +). \tag{7.85}$$

Un élément (x, y) est générateur du produit si et seulement si x est générateur de $\mathbb{Z}/p\mathbb{Z}$ et y est générateur de $\mathbb{Z}/q\mathbb{Z}$. Par la proposition 7.40, il y a $\varphi(p)\varphi(q)$ tels éléments. Par ailleurs le nombre de générateurs de $\mathbb{Z}/pq\mathbb{Z}$ est $\varphi(pq)$, d'où l'égalité.

Si p est premier, nous avons $\varphi(p) = p - 1$ parce que tous les entiers de $\{1, \dots, p - 1\}$ sont premiers avec p. □

[11] Corolaire 3.47

7.6 Groupe symétrique, groupe alterné

SECooZFYQooFfopMa

La définition des permutations et du groupe symétrique sont 2.2. Voir aussi le thème 8.

7.6.1 Le groupe alterné

DEFooEIVIooFvVkHH

Définition 7.43.
Le groupe A_n des permutations paires[12] *dans S_n est le* ***groupe alterné****.*

PROPooCPXOooVxPAij

Proposition 7.44.
À propos du groupe alterné dans le groupe symétrique.

(1) *Le groupe alterné A_n est un sous-groupe caractéristique*[13] *de S_n*

ITEMooWXXUooOWvFgE

(2) *Le sous-groupe A_n est d'indice 2 dans S_n.*

ITEMooGGAHooRYgNqq

(3) *Le sous-groupe A_n est l'unique sous-groupe d'indice*[14] *2 de S_n.*

Démonstration. Soit $\alpha \in \mathrm{Aut}(S_n)$. Étant donné que $\epsilon \circ \alpha$ est un homomorphisme[15] surjectif sur $\{-1,1\}$, par unicité de cet homomorphisme, nous avons $\epsilon \circ \alpha = \epsilon$, et donc $\alpha(A_n) = A_n$. Par le premier théorème d'isomorphisme 2.20, il existe un isomorphisme

$$f\colon S_n/\ker(\epsilon) \to \mathrm{Image}(\epsilon). \tag{7.86}$$

En égalant le nombre d'éléments nous avons $|S_n : \ker\epsilon| = |S_n : A_n| = 2$.

Nous prouvons maintenant l'unicité. Soit H un sous-groupe d'indice 2 dans S_n. Par le lemme 3.166, H est distingué et nous pouvons considérer le groupe S_n/H. Ce dernier ayant 2 éléments, il est isomorphe à $\{-1,1\}$. Soit θ l'isomorphisme. On note φ le morphisme canonique $\varphi\colon S_n \to S_n/H$:

$$S_n \xrightarrow{\varphi} S_n/H \xrightarrow{\theta} \{-1,1\}. \tag{7.87}$$

EqSZBPTR

La composition $\theta\circ\varphi$ est alors un homomorphisme[16] surjectif de S_n sur $\{-1,1\}$ et nous avons $\theta\circ\varphi = \epsilon$ par la proposition 2.124. L'enchainement (7.87) nous montre que $H = \ker(\theta\circ\varphi) = \ker(\epsilon) = A_n$. □

PROPooPSZVooSmAgPA

Proposition 7.45 ([181])**.**
Le groupe symétrique S_n peut être écrit comme un produit semi-direct[17] *du groupe alterné :*

$$S_n = A_n \times_\varphi \mathbb{Z}/2\mathbb{Z} \tag{7.88}$$

où l'action de $\mathbb{Z}/2\mathbb{Z}$ sur A_n est la conjugaison par $\sigma = (12)$, c'est-à-dire $\rho(-1)\tau = \sigma\tau\sigma^{-1}$.

Démonstration. Nous avons la suite exacte

$$1 \xrightarrow{i} A_n \xrightarrow{i} S_n \xrightarrow{\epsilon} \{\pm 1\} \longrightarrow 1 \tag{7.89}$$

où les i représentent des inclusions et ϵ est la signature définie en 2.117. Grâce à cette suite et au fait que la signature soit un isomorphisme à partir de la partie $\{\mathrm{Id},\sigma\}$ (pour σ d'ordre 2, par exemple $\sigma = (12)$), le théorème 2.160 nous dit que

$$S_n \simeq A_n \times_\varphi \{\mathrm{Id},\sigma\} \tag{7.90}$$

où φ est l'action adjointe de $\{\mathrm{Id},\sigma\}$ sur A_n. □

PROPooZOWBooIMxxlj

Proposition 7.46.
Si $\beta \in S_n$ est une transposition, nous avons les égalités suivantes d'ensembles :

$$S_n = A_n \cup A_n\beta = A_n \cup \beta A_n. \tag{7.91}$$

Démonstration. Les parties A_n et βA_n ont le même nombre d'éléments. En effet, l'application

$$\begin{aligned}\varphi\colon A_n &\to A_n\beta\\ \sigma &\mapsto \sigma\beta\end{aligned} \tag{7.92}$$

est une bijection.

De plus ces deux ensembles sont disjoints à cause de la proposition 2.124. En effet si $\sigma \in A_n$, alors $\epsilon(\sigma) = 1$. Mais un élément de $A_n\beta$ est de la forme $\sigma\beta$ avec $\sigma \in A_n$. Or ϵ est un homomorphisme[18], donc

[12] Définition 2.120.
[13] Définition 2.11.
[14] Définition 2.72.
[15] Voir -1.1.
[16] Voir -1.1.
[17] Définition 2.158.
[18] Voir -1.1.

$\epsilon(\sigma\beta) = \epsilon(\sigma)\epsilon(\beta) = -1$.

Enfin, la proposition 7.44(2) dit que A_n est d'indice deux dans S_n. Donc la partie

$$A_n \cup A_n\beta \tag{7.93}$$

contient $|S_n|/2 + |S_n|/2 = |S_n|$ éléments. C'est donc S_n. □

LemiApyfp

Lemme 7.47.
Le groupe dérivé du groupe symétrique est le groupe alterné : $D(S_n) = A_n$.

Démonstration. Tout élément de $D(S_n)$ s'écrit sous la forme $ghg^{-1}h^{-1}$. Quel que soit le nombre de transpositions dans g et h, le nombre de transpositions dans $[g, h]$ est pair. □

PropsHlmvv

Proposition 7.48 ([182]).
Soit $n \geqslant 3$. Les 3-cycles $c_i = (1, 2, i)$ avec $i = 3, \dots, n$ engendrent le groupe alterné A_n.

Démonstration. Soit H, le groupe engendré par les c_i. D'abord nous avons

$$c_i = (1, 2, i) = (1, 2)(2, i), \tag{7.94}$$

de telle sorte que $\epsilon(c_i) = 1$. Par conséquent nous avons $H \subset A_n$. Nous montrons par récurrence que $A_n \subset H$.

Pour $n = 3$ il suffit de vérifier que $A_3 = \{\mathrm{Id}, c_3, c_3^2\}$. Supposons avoir obtenu le résultat pour A_{n-1}, et prouvons le pour A_n. Soit $s \in A_n$.

Si $s(n) = n$, alors s se décompose de la même manière que sa restriction s' à $\{1, \dots, n-1\}$. Par l'hypothèse de récurrence, cette restriction, appartenant à A_{n-1}, se décompose en produit des $c_3, \dots, c_{n-1}$ et de leurs inverses.

Si $s(n) = k$ alors nous considérons l'élément $c_n^2 c_k s$. Cet élément envoie n sur n et peut donc être décomposé avec les c_i $(i = 1, \dots, n-1)$ en vertu du point précédent. □

PropiodtBG

Proposition 7.49.
Lorsque $n \geqslant 5$, tous les 3-cycles de A_n sont conjugués. Autrement dit, la classe de conjugaison d'un 3-cycle est l'ensemble des 3-cycles.

Démonstration. Soient les 3-cycles $\sigma = (i_1, i_2, i_3)$ et $\varphi = (j_1, j_2, j_3)$. Nous considérons une bijection α de $\{1, \dots, n\}$ telle que $\alpha(i_s) = j_s$. Nous avons immédiatement que $\alpha \in S_n$ et que $\alpha\sigma\alpha^{-1} = \varphi$. Donc les 3-cycles sont conjugués dans S_n. Il reste à prouver qu'ils le sont dans A_n.

Si α est une permutation paire, la preuve est terminée. Si α est impaire, alors nous devons un peu la modifier. Comme $n \geqslant 5$, nous pouvons prendre s et t, des éléments distincts dans $\{1, \dots, n\} \setminus \{j_1, j_2, j_3\}$ et poser $\tau = (st)$. Puisque la signature est un homomorphisme[19] et que τ et α sont impairs, l'élément $\tau\alpha$ est pair (lemme et proposition 2.123 et 2.116) et est donc dans A_n. Les supports de τ et φ étant disjoints, ces derniers commutent et nous avons

$$(\tau\alpha)\sigma(\tau\alpha)^{-1} = \tau(\alpha\sigma\alpha^{-1})\tau^{-1} = \tau\varphi\tau^{-1} = \varphi. \tag{7.95}$$

Donc σ et φ sont conjugués par $\tau\alpha$ qui est dans A_n. □

ThoURfSUXP

Théorème 7.50 ([57]).
Le groupe alterné A_n est simple[20] pour $n \geqslant 5$.

Démonstration. Soit N, un sous-groupe normal de A_n non réduit à l'identité. Étant donné que les 3-cycles engendrent A_n (proposition 7.48) et que tous les 3-cycles sont conjugués dans A_n (proposition 7.49), il suffit de montrer que N contient un 3-cycle. En effet si N contient un 3-cycle, le fait qu'il soit normal implique (par conjugaison) qu'il les contienne tous et donc qu'il contient une partie génératrice de A_n.

Soit donc $\sigma \in N$ différent de l'identité. Nous prenons i dans le support de σ et $j = \sigma(i)$. Nous choisissons ensuite $k \in \{1, \dots, n\} \setminus \{i, j, \sigma^{-1}(i)\}$ et $m = \sigma(k)$. Nous considérons la permutation $\alpha = (ijk)$. Étant donné que N est normal, l'élément

$$\theta = (\alpha^{-1}\sigma\alpha)\sigma^{-1} \tag{7.96}$$

est dans N. De plus en utilisant le lemme 2.110 et le fait que $\alpha^{-1} = (ikj)$ nous avons

$$\theta = (ikj)(j\sigma(j)m). \tag{7.97}$$

Cela n'est pas spécialement un 3-cycle, mais nous allons en construire un. Nous allons déterminer que θ est soit un 5-cycle, soit un 3-cycle , soit un 2×2-cycle suivant les valeurs de $\sigma(j)$ et m.

Souvenons-nous que nous avons :

[19] Voir -1.1.
[20] Pas de sous-groupes normaux non triviaux, définition 2.75.

- $i \neq j = \sigma(i)$, puisque i est dans le support de σ ;
- $k \neq i$ et $k \neq j$, par définition de k (rappelons aussi que $k \neq \sigma^{-1}(i)$) ;
- $m \neq i$, $m \neq j$ et $m \neq \sigma(j)$ puisque $m = \sigma(k)$.

Il ne nous reste alors seulement les deux possibilités suivantes :

(1) soit $m = k$, soit $m \neq k$, d'une part ;

(2) soit $\sigma(j) = i$, soit $\sigma(j) = k$, soit $\sigma(j)$ n'est ni i, ni k, ni m, d'autre part.

Supposons dans un premier temps que $m = k$; alors

$$\theta = (ik)(j\sigma(j)). \tag{7.98}$$

C'est à priori un 2×2-cycle. Mais si de plus $\sigma(j) = i$, alors

$$\theta = (ijk) \tag{7.99}$$

qui est un 3-cycle ; et si $\sigma(j) = k$, alors

$$\theta = (ikj) \tag{7.100}$$

qui est un autre 3-cycle.

Supposons à présent que $m \neq k$. Si $\sigma(j)$ n'est ni i, ni k, ni m, alors i, j, k, $\sigma(j)$ et m sont cinq nombres différents, et

$$\theta = (i, j, \sigma(j), m, k) \tag{7.101}$$

est un 5-cycle. Si $\sigma(j) = i$, alors

$$\theta = (ikj)(jim) = (imk) \tag{7.102}$$

qui est un 3-cycle. Si $\sigma(j) = k$, alors

$$\theta = (ikj)(jkm) = (ikm) \tag{7.103}$$

qui est encore un 3-cycle.

Bref nous avons montré que θ est soit un 3-cycle, soit un 5-cycle, soit un 2×2-cycle. Si θ est un 3-cycle, la preuve est terminée.

Si $\theta = (ab)(cd)$, alors on considère $e \in \{1, \dots, n\} \setminus \{a, b, c, d\}$ et nous avons

$$\underbrace{(abe)^{-1}\theta(abe)}_{\in N}\theta^{-1} = (aeb)(ab)(cd)(abe)(an)(cd) = (abe) \in N. \tag{7.104}$$

Si θ est le 5-cycle $(abcde)$, alors l'élément suivant est dans N :

$$(abc)^{-1}\theta(abc)\theta^{-1} = (acb)(abcde)(abc)(aedcb) = (acd). \tag{7.105}$$

Dans tous les cas nous avons trouvé un 3-cycle dans N et nous avons par conséquent $N = A_n$, ce qui fait que A_n ne contient pas de sous-groupes normaux non triviaux. Le groupe alterné A_n est donc simple. □

Nous en déduisons immédiatement que si $n \geqslant 5$, le groupe dérivé de A_n est A_n parce que A_n ne contient pas d'autres sous-groupes non triviaux.

LEMooICEHooGSSpkq

Lemme 7.51.
Le groupe alterné[21] A_6 *n'accepte pas de sous-groupes normaux d'ordre* 60.

Démonstration. Soit G normal dans A_6, et a, un élément d'ordre 5 dans G (qui existe parce que 5 divise 60). Soit aussi un élément b d'ordre 5 dans A_6. Les groupes $\text{gr}(a)$ et $\text{gr}(b)$ sont deux 5-Sylow dans A_6. En effet, 5 est un nombre premier, et est la plus grande puissance de 5 dans la décomposition de 60 ; donc $\text{gr}(a)$ est un 5-Sylow dans G. D'autre part, l'ordre de A_6 (qui est $\frac{1}{2} \cdot 6!$) ne possède également que 5 à la puissance 1 dans sa décomposition.

En vertu du théorème de Sylow 7.11(3), les 5-Sylow $\text{gr}(a)$ et $\text{gr}(b)$ sont conjugués et il existe $\tau \in A_6$ tel que $b = \tau a \tau^{-1}$. Mais G étant normal dans A_6, l'élément $\tau a \tau^{-1}$ est encore dans G, de telle sorte que $b \in G$. Du coup G doit contenir tous les éléments d'ordre 5 de A_6.

Les éléments d'ordre 5 de A_6 doivent fixer un des points de $\{1, 2, 3, 4, 5, 6\}$ puis permuter les autres de façon à n'avoir qu'un seul cycle. Un cycle correspond à écrire les nombres $1, 2, 3, 4, 5$ dans un certain ordre. Ce faisant, le premier n'a pas d'importance parce qu'on considère la permutation cyclique, par exemple $(3, 5, 2, 1, 4)$ est la même chose que $(5, 2, 1, 4, 3)$. Le nombre de cycles sur $\{1, 2, 3, 4, 5\}$ est donc de 4!, et par conséquent le nombre d'éléments d'ordre 5 dans A_6 est $6 \cdot 4! = 144$.

Le groupe G doit contenir au moins 144 éléments alors que par hypothèse il en contient 60 ; contradiction. □

[21] Définition 7.43.

Le théorème suivant montre que tout groupe peut être vu, en agissant sur lui-même, comme une partie du groupe symétrique.

Théorème 7.52.
Un groupe G est isomorphe à un sous-groupe de son groupe symétrique $S(G)$.

Démonstration. Nous considérons φ, la translation à gauche :

$$\begin{aligned}\varphi\colon G &\to S(G)\\ g &\mapsto t_g\end{aligned} \tag{7.106}$$

où $f_g(h) = gh$. Étant donné que

$$\varphi(gh) = ghx = g(t_h x) = t_g \circ t_h(x), \tag{7.107}$$

l'application φ est un morphisme de groupes. Il est injectif parce que si $gx = hx$ pour tout x, en particulier pour $x = e$ nous trouvons $g = h$.

De la même manière, $\varphi(g)x = \varphi(g)y$ implique $x = y$. Cela montre que l'image est bien dans le groupe symétrique.

L'ensemble Image(φ) est donc un sous-groupe de $S(G)$, et φ est un isomorphisme vers ce groupe. □

LEMooMVUGooRiDaDz

Lemme 7.53.
Si $n \geqslant 3$, alors

(1) Le centre de S_n est trivial.

(2) Le groupe S_n est non abélien.

Démonstration. Soit $s \in Z(S_n)$ et trois éléments distincts a, b et c de $\{1, \dots, n\}$. Nous posons $\tau = (ab)$ et nous avons $s\tau = \tau s$. En notant $a' = s(a)$ et $b' = s(b)$ nous avons

$$a' = s(a) = (\tau s \tau^{-1})(a) = (\tau s)(b) = \tau(b') \tag{7.108a}$$

$$b' = s(b) = (\tau s \tau^{-1})(b) = (\tau s)(a) = \tau(a'). \tag{7.108b}$$

Donc τ permute a' et b'. Mais comme τ ne permute que a et b, en tant qu'ensembles, $\{a, b\} = \{s(a), s(b)\}$. Le même raisonnement sur $\{b, c\}$ donne $\{b, c\} = \{s(b), s(c)\}$. Et puisque a, b et c sont distincts,

$$\{b\} = \{b, c\} \cap \{a, b\} = \{s(b)\}. \tag{7.109}$$

Cela montre que $s(b) = b$, et donc que le centre de S_n est réduit à la permutation identité.

En ce qui concerne le fait que S_n est non abélien, si nous avions $st = ts$ pour tout $s, t \in S_n$ alors $s = tst^{-1}$ pour tout t. Alors s serait dans le centre de S_n. En bref, si S_n était abélien, son centre serait S_n et non $\{\mathrm{Id}\}$.

□

PROPooUBIWooTrfCat

Proposition 7.54 ([183, 172])**.**
Tout groupe simple[22] *d'ordre 60 est isomorphe au groupe alterné A_5.*

Démonstration. Nous avons la décomposition en nombres premiers $60 = 2^2 \cdot 3 \cdot 5$. Déterminons pour commencer le nombre n_5 de 5-Sylow dans G. Le théorème de Sylow 7.11(4) nous renseigne que n_5 doit diviser 60 et doit être égal à $1 \mod 5$. Les deux seules possibilités sont $n_5 = 1$ et $n_5 = 6$. Étant donné que tous les p-Sylow sont conjugués, si $n_5 = 1$ alors le 5-Sylow serait un sous-groupe invariant à l'intérieur de G, ce qui est impossible vu que G est simple. Donc $n_5 = 6$.

Par le point (3) du théorème de Sylow, le groupe G agit transitivement sur l'ensemble des 5-Sylow par l'action adjointe :

$$g \cdot S = gSg^{-1}. \tag{7.110}$$

Cela donne donc un morphisme $\theta\colon G \to S_6$. Le noyau de θ est un sous-groupe normal. En effet si $k \in \ker\theta$ et si $g \in G$ nous avons

$$(gkg^{-1}) \cdot S = gkg^{-1}Ggk^{-1}g^{-1} \tag{7.111a}$$

$$= gkTk^{-1}g^{-1} \tag{7.111b}$$

$$= gTg^{-1} \tag{7.111c}$$

$$= S \tag{7.111d}$$

[22] Définition 2.75.

où T est le Sylow $T = g^{-1}Sg$. Étant donné que $k \in \ker\theta$ nous avons utilisé $kTk^{-1} = aT$. Au final $gkg^{-1} \cdot S = S$, ce qui prouve que $gkg^{-1} \in \ker\theta$.

Étant donné que $\ker\theta$ est normal dans G, soit il est réduit à $\{e\}$ soit il vaut G. La seconde possibilité est exclue parce qu'elle reviendrait à dire que G agit trivialement, ce qui n'est pas correct étant donné qu'il agit transitivement. Nous en déduisons que $\ker\theta = \{e\}$, que θ est injective et que G est isomorphe à un sous-groupe de S_6.

Par ailleurs le groupe dérivé de G est un sous-groupe normal (et non réduit à l'identité parce que G est non commutatif). Donc $D(G) = G$. Étant donné que $G \subset S_6$, nous avons

$$G = D(G) \subset D(S_6) = A_6 \tag{7.112}$$

parce que le groupe dérivé du groupe symétrique est le groupe alterné (lemme 7.47).

L'ensemble $\theta^{-1}(A_6)$ est distingué dans G. En effet si $\sigma \in A_6$ et si $g \in G$ nous avons

$$\theta\big(g\theta^{-1}(\sigma)g^{-1}\big) = \theta(g)\sigma\theta(g)^{-1} \in A_6. \tag{7.113}$$

Nous en déduisons que $\theta^{-1}(A_6)$ est soit G entier soit réduit à $\{e\}$. Si $\theta^{-1}(A_6) = \{e\}$, alors pour tout $g \in G$ nous aurions $g^2 = e$ parce que $\theta(g^2) \in A_6$. L'ordre de G étant 60, il n'est pas possible que tous ses éléments soient d'ordre 2. Nous en déduisons que $\theta(G) \subset A_6$.

Nous nommons $H = \theta(G)$ et nous considérons l'ensemble $X = A_6/H$ où les classes sont prises à gauche, c'est-à-dire

$$[\sigma] = \{h\sigma \text{ tel que } h \in H\}. \tag{7.114}$$

Évidemment A_6 agit sur X de façon naturelle. Au niveau de la cardinalité,

$$\mathrm{Card}(X) = \frac{|A_6|}{|G|} = \frac{360}{60} = 6. \tag{7.115}$$

Le groupe A_6 agit sur X qui a 6 éléments. Nous avons donc une application $\varphi\colon A_6 \to A_6$. Encore une fois, la simplicité de A_6 montre que $\varphi(A_6) = A_6$.

Nous étudions maintenant $\varphi(H)$ agissant sur X. Un élément $x \in A_6$ fixe la classe de l'unité $[e]$ si et seulement si $x \in H$ et par conséquent $\varphi(H)$ est le fixateur de $[e]$ dans X. À la renumérotation près, nous pouvons identifier $\varphi(H)$ au sous-groupe de A_6 agissant sur $\{1, \dots, 6\}$ et fixant 6. Nous avons alors $\varphi(H) = S_5 \cap A_6 = A_5$. Nous venons de prouver que φ fournit un isomorphisme entre A_5 et H. Étant donné que H était isomorphe à G, nous concluons que G est isomorphe à A_6. □

7.6.2 Sous-groupes normaux

NORMooQAZTooBQLqDn

7.55 ([184]).
Soit le groupe V_4 engendré par les doubles transpositions de S_4. Nous savons de l'exemple 2.114(6) que ce groupe contient exactement 3 éléments non triviaux et l'identité. De plus, comme c'est une classe de conjugaison, V_4 est normal dans S_4.

Lemme 7.56.
Les sous-groupes $\mathrm{Fix}_{S_n}(a)$ *(avec* $a \in \{1, \dots, n\}$*) sont conjugués entre eux.*

Démonstration. Soit $\sigma \in \mathrm{Fix}(a)$ et $s \in S_n$ nous devons prouver que $s\sigma s^{-1}$ est le fixateur d'un élément de $\{1, \dots, n\}$. Nous notons $s(a) = b$. Alors

$$(s\sigma s^{-1})(b) = (s\sigma)(a) = s(a) = b. \tag{7.116}$$

Donc $s\,\mathrm{Fix}(a)s^{-1} \subset \mathrm{Fix}(b)$.

Dans l'autre sens, si $\sigma \in \mathrm{Fix}(b)$ alors $s^{-1}\sigma s \in \mathrm{Fix}(a)$. Mais $\sigma = s(s^{-1}\sigma s)s^{-1}$, donc $\sigma \in s\,\mathrm{Fix}(a)s^{-1}$. □

PROPooOTJAooUbzGZm

Proposition 7.57 (Sous-groupes normaux de S_n [184]).
Les sous-groupes normaux de S_n *ne sont pas légions.*

(1) Pour $n = 4$*, les sous-groupes normaux de* S_4 *sont* $\{\mathrm{Id}\}$*,* V_4*,* A_4 *et* S_4*.*

(2) Pour $n \neq 4$*, les sous-groupes normaux de* S_n *sont* $\{\mathrm{Id}\}$*,* A_n *et* S_n*.*

Démonstration. Les cas $n \leqslant 2$ sont un peu triviaux, donc nous faisons $n \geqslant 3$. Soit H normal dans S_n et $s \neq \mathrm{Id}$ dans H ; par le lemme 7.53, s n'est pas dans le centre de S_n et il existe $u \in S_n$ tel que $us \neq su$. Comme u est un produit de transpositions (proposition 2.116), il existe une transposition t telle que $st \neq ts$. Le sous-groupe H est normal et puisque $s \in H$ nous avons aussi $ts^{-1}t^{-1} \in H$. Mais en même temps,

la combinaison sts^{-1} est le conjugué d'une transposition et est donc également une transposition (classe de conjugaison de S_4 dans 2.114). Nous en concluons que $sts^{-1}t^{-1}$ est un produit de deux transpositions appartenant à H.

Nous venons de prouver que H contient au moins un produit de deux transpositions. Et ce produit est différent de Id parce que $sts^{-1}t^{-1} = \text{Id}$ impliquerait $st = ts$.

Soient donc deux transpositions $t_1, t_2 \in H$ telles que $t_1t_2 \neq \text{Id}$. Les supports de t_1 et t_2 ont soit 1 soit aucun élément communs.

(1) **Premier cas**

Supposons $t_1 = (a, b)$, $t_2 = (b, c)$ avec a, b, c distincts dans $\{1, \dots, n\}$. Dans ce cas $t_1t_2 = (a, b, c)$ et H contient un cycle de longueur 3. Puisque H est normal et que les cycles de longueur trois sont une classe de conjugaison (exemple 2.114) et que A_n est engendré par ceux-ci (proposition 7.48), $A_n \subset H$. Mais A_n est d'indice deux dans S_n (proposition (2)(2)). Quel nombre plus grand que $n!/2$ divise $n!$? Seulement n lui-même. Donc H est soit A_n soit S_n.

(2) **Second cas**

Le groupe H contient un élément de la forme $(ab)(cd)$ avec a, b, c, d distincts dans $\{1, \dots, n\}$.

(2a) **Si $n = 3$**

Impossible parce que avec $n = 3$ nous n'avons pas quatre éléments distincts.

(2b) **Si $n = 4$**

Le sous-groupe H de S_4 contient un élément de V_4 qui n'est pas l'identité. Par normalité et classes de conjugaison, H contient V_4. Nous devons maintenant prouver que si H n'est pas V_4 alors H est A_4 ou S_4. Nous avons les inclusions $V_4 \subset H \subset S_4$ et donc les inégalités

$$4 \leqslant |H| \leqslant 24. \tag{7.117}$$

Donc le nombre $|H|$ est un multiple de 4 qui divise 24. Les possibilités sont $|H| = 4, 8, 12, 24$. La possibilité $|H| = 4$ donne $H = V_4$; si $|H| = 24$ alors $H = S_4$; si $|H| = 12$ alors H est d'indice 2 dans S_4 et $H = A_n$ (proposition 7.44(3)). Quid de $|H| = 8$?

D'après le corolaire 2.74 au théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe. Soit x dans H mais pas dans V_4. L'ordre de x peut être 1, 2, 4 ou 8. Ordre 1 serait $x = \text{Id}$. Ordre 8, pas possible parce que S_4 n'a pas d'éléments d'ordre 8.

(2b.i) **x d'ordre 2**

Prenons la décomposition de x en cycles disjoints. Puisqu'on est dans S_4, ces cycles ne peuvent être que des transpositions. Soit il y en a un (alors H contient une transposition et donc $H = S_4$), soit il y en a deux et alors x est dans V_4.

(2b.ii) **x d'ordre 4**

L'élément x est alors un cycle de longueur 4, et H contient tous les cycles de longueur 4 ; par exemple, le produit $(abcd)(bacd) = (adc)$. Le sous-groupe H contient alors A_4 (parce qu'il contient tous les 3-cycles).

(2c) **Si $n \geqslant 5$**

Soit un élément e[23] distinct de a, b, c et d. Par notre liste préférée des classes de conjugaison (exemple 2.114(6)), le 2-cycle $(c, e)(a, b)$ est conjugué à $(a, b)(c, d)$ et appartient donc à H. Mais alors le produit suivant est également dans H :

$$(ce)(ab)(ab)(cd) = (ce)(cd) = (ecd). \tag{7.118}$$

Donc H contient un 3-cycle, et par conséquent tous les 3-cycles. Encore une fois, cela prouve que H est soit A_n soit S_n.

(2d) **Pourquoi $n = 4$ est spécial ?**

Dans le premier cas, nous montrons tout de suite que $H = V_4$ n'est pas possible. Dans le deuxième cas, nous montrons que, grâce à un élément différent de a, b, c et d, la possibilité $H = V_4$ est exclue. La possibilité $H = V_4$ n'existe que pour $n = 4$.

□

[23] e n'est pas l'élément neutre ici

7.6.3 Indice

THOooXDRNooIyaGlv

Théorème 7.58.
Tout sous-groupe d'indice n dans S_n est isomorphe à S_{n-1}.

Démonstration. Pour $n = 1$, il n'y a pas de sous-groupe. Pour $n = 2$, un sous-groupe d'indice 2 ne peut contenir que 1 élément, qui est donc l'identité. Ok pour que $\{\mathrm{Id}\}$ soit égal à S_1 ?

Pour les autres, il y a un peu plus de travail.

(1) **Pour $n = 3$**

Nous avons $|S_3| = 6$. Donc un sous-groupe d'indice 3 dans S_3 contient exactement 2 éléments. Il contient Id et un autre élément $\sigma \in S_3$ qui doit vérifier $\sigma^2 = \mathrm{Id}$ ou $\sigma^2 = \sigma$. Aucun élément de S_3 ne vérifie $\sigma^2 = \sigma$ (à part l'identité). Donc $\sigma^2 = \mathrm{Id}$, ce qui implique que σ est une transposition. Donc

$$H = \{\mathrm{Id}, (12)\} \tag{7.119}$$

ou l'identité avec (23), ou avec (13). Dans tous les cas c'est isomorphe à S_2.

(2) **Pour $n = 4$**

Nous avons $|S_4 : H| = 4$, donc $|H| = 6$. Mais $6 = 2 \times 3$ et $2 \mid 3 - 1$, donc le théorème 7.25 nous dit que H est soit cyclique[24] (et donc abélien), soit un produit semi-direct. Vu que S_4 n'a pas d'éléments d'ordre 6, aucun sous-groupe d'ordre 6 ne peut être cyclique. Nous sommes donc dans le cas du produit semi-direct

EQooSHWGooEMNRvf

$$H = \mathbb{Z}_3 \times_\varphi \mathbb{Z}_2 \tag{7.120}$$

où $\varphi\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ et $\varphi(1)$ est d'ordre 2 dans $\mathrm{Aut}(\mathbb{Z}_3)$. Il convient de nous attarder un peu pour être sûr d'avoir bien compris tout ce qui se trouve dans l'identification (7.120). D'abord un point de notations : ici nous considérons les groupes $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ munis de l'addition. Donc 1 n'est pas le neutre. Ensuite nous savons du théorème 7.18 que $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = (\mathbb{Z}/3\mathbb{Z})^*$, et que via cette identification, $\varphi(1) = 2 \in (\mathbb{Z}/3\mathbb{Z})^*$ au sens où $\varphi(1)x = 2x$. Nous avons alors $\varphi(1)^2 x = 4x = x$ dans $\mathbb{Z}/3\mathbb{Z}$. Cela montre bien que $\varphi(1)$ est d'ordre 2.

Par rapport à la proposition 7.45, ici nous écrivons $\mathbb{Z}_2 = \big(\{0, 1\}, +\big)$ alors que là nous écrivons $\mathbb{Z}_2 = \big(\{-1, 1\}, \cdot\big)$. Ce sont les mêmes groupes, mais il convient de remarquer que le 1 ici est le -1 là.

Nous savons par la proposition 7.45 que $S_n = A_n \times_\varphi \mathbb{Z}_2$; en comparant avec (7.120) nous voyons qu'il suffit de prouver que $A_3 = \mathbb{Z}/3\mathbb{Z}$ pour avoir $H = S_3$.

Le groupe A_3 possède $|S_3|/2 = 3$ éléments. Il est vite vu que $A_3 = \{\mathrm{Id}, (12)(31), (12)(32)\}$: ce sont trois éléments de signature paire dans S_3 ; donc c'est S_3. La correspondance $\mathrm{Id} \mapsto 0$, $(12)(13) \mapsto 1$, $(13)(12) \mapsto 2$ donne un isomorphisme avec $(\mathbb{Z}_3, +)$.

(3) **Pour $n \geqslant 5$**

Soit un sous-groupe H d'indice n dans S_n et l'action à gauche de S_n sur $E = S_n/H$ (qui n'est à priori pas un groupe) donnée par $g \cdot [s] = [gs]$.

(3a) **Morphisme $\varphi\colon S_n \to S_E$**

Le φ défini par l'action est un morphisme parce que

$$\varphi(g_1 g_2)[s] = [g_1 g_2 s] = \varphi(g_1)[g_2 s] = \varphi(g_1)\varphi(g_2)[s]. \tag{7.121}$$

Mais il faut également vérifier que pour chaque $g \in G$, l'application $\varphi(g)\colon E \to E$ est bien une permutation. Pour l'injectivité, si $\varphi(g)[s_1] = \varphi(g)[s_2]$ alors $[gs_1] = [gs_2]$, donc il existe $h \in H$ tel que $gs_1 = gs_2 h$, ce qui prouve que $s_1 = s_2 h$ et donc que $[s_1] = [s_2]$. Pour la surjectivité, soit $[t] \in S_n/H$ et résolvons $\varphi(g)[s] = [t]$ par rapport à s. L'élément $s = g^{-1}t$ convient.

(3b) **$\ker(\varphi)$ est normal**

Soit $z \in \ker(\varphi)$, c'est-à-dire que $\varphi(z) = \mathrm{Id}_E$. Alors pour $\sigma \in S_n$ nous avons $\varphi(\sigma z \sigma^{-1}) = \varphi(\sigma)\varphi(z)\varphi(\sigma^{-1}) = \mathrm{Id}_E$.

(3c) **$\ker(\varphi) = \bigcap_{g \in S_n} gHg^{-1}$**

Supposons que $z \in gHg^{-1}$ pour tout g, et calculons $\varphi(z)[s]$. D'abord par hypothèse il existe $h \in H$ tel que $z = shs^{-1}$, donc

$$\varphi(z)[s] = [zs] = [shs^{-1}s] = [sh] = [s], \tag{7.122}$$

[24] Définition 2.149.

ce qui prouve que $\varphi(z) = \mathrm{Id}$.

Dans l'autre sens, soit $z \in \ker(\varphi)$. Donc $\varphi(z)[s] = [s]$. Il existe donc $h \in H$ tel que $zs = sh$, c'est-à-dire tel que $z = shs^{-1}$. La formule demandée est donc prouvée.

(3d) **Questions d'ordre**

Nous savons que $|H| = (n-1)!$ alors que $|A_n| = \frac{n!}{2}$. Donc $|H| < |A_n|$ avec une inégalité stricte. En même temps nous avons $|\ker(\varphi)| \leqslant |H|$ parce que $\ker(\varphi)$ est une intersection dont un des termes est H lui-même. Nous avons alors les inégalités

$$|\ker(\varphi)| \leqslant |H| = (n-1)! < |A_n|. \tag{7.123}$$

Mais les seuls sous-groupes normaux de S_n sont A_n, S_n et $\{\mathrm{Id}\}$ (proposition 7.57). Donc $\ker(\varphi) = \mathrm{Id}$ et φ est une injection entre deux ensembles finis de même cardinalité. Cela fait de φ une bijection et donc un isomorphisme de groupes

$$\varphi\colon S_n \to S_E. \tag{7.124}$$

Soit une fonction de numérotation $\psi\colon E \to \{1, \ldots, n\}$. Avec cela nous définissons un isomorphisme de groupes

$$\begin{aligned} \tilde{\psi}\colon S_E &\to S_n \\ \sigma &\mapsto \psi\sigma\psi^{-1}. \end{aligned} \tag{7.125}$$

(3e) **Fixateur**

Nous montrons à présent que $(\tilde{\psi} \circ \varphi)(H) = \mathrm{Fix}\big(\psi[\mathrm{Id}]\big)$ où le stabilisateur est pris dans S_n. Pour la première inclusion, soit $h \in H$. Nous avons $(\tilde{\psi} \circ \varphi)(h) = \psi \circ \varphi(h)\psi^{-1}$, qui nous appliquons à $\psi[\mathrm{Id}]$:

$$(\tilde{\psi} \circ \varphi)(h)\psi[\mathrm{Id}] = \psi \circ \varphi(h)[\mathrm{Id}] = \psi[h] = \psi[\mathrm{Id}]. \tag{7.126}$$

Donc $(\tilde{\psi} \circ \varphi)(H) \subset \mathrm{Fix}\big(\psi[\mathrm{Id}]\big)$.

Pour l'autre inclusion, soit $\sigma \in S_n$ tel que $\sigma\psi[\mathrm{Id}] = \psi[\mathrm{Id}]$. Puisque $\sigma \in S_n$ nous avons $s \in S_E$ tel que $\sigma = \tilde{\psi}(s)$. Pour ce s nous avons donc

$$\big(\tilde{\psi}(s) \circ \psi\big)[\mathrm{Id}] = \psi[\mathrm{Id}], \tag{7.127}$$

d'où nous déduisons $s[\mathrm{Id}] = [\mathrm{Id}]$. Cela prouve que s stabilise $[\mathrm{Id}]$ dans S_E. Donc $s = \varphi(h)$ pour un certain $h \in H$, et au final $\sigma = \tilde{\psi}\big(\varphi(h)\big)$.

(3f) **Conclusion**

L'application $\tilde{\psi} \circ \varphi\colon H \to S_n$ est une application dont l'image est le fixateur d'un point. Plus précisément,

$$\tilde{\psi} \circ \varphi\colon H \to \mathrm{Fix}\big(\psi[\mathrm{Id}]\big) \tag{7.128}$$

est un isomorphisme de groupe. Mais le stabilisateur d'un point dans S_n est S_{n-1}.

□

7.7 Isométries du cube

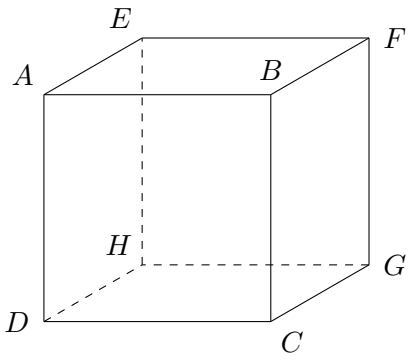
SecPVCmkxM

Les isométries du cube proviennent de [112].

Nous considérons le cube centré en l'origine de $\mathbb{R}^3$ et G, le groupe des isométries de $\mathbb{R}^3$ préservant ce cube. Nous notons aussi G^+ le sous-groupe de G constitué des éléments de déterminant positif. Nous notons

$$\mathcal{D} = \{D_1, \ldots, D_4\} \tag{7.129}$$

l'ensemble des grandes diagonales, c'est-à-dire les segments $[AG]$, $[EC]$, $[FD]$, et $[BH]$. Nous savons que G préserve les longueurs et que ces segments sont les plus longs possibles à l'intérieur du cube. Donc G agit sur $\mathcal{D}$ parce qu'il ne peut transformer une grande diagonale qu'en une autre grande diagonale. Nous avons donc un morphisme de groupes



$$\rho\colon G \to S_4. \tag{7.130}$$

Nous montrons que ce morphisme est surjectif en montrant qu'il contient les transpositions. Le groupe G contient la symétrie axiale passant par le milieu M de $[A,E]$ et le milieu N de $[C,G]$. Il est facile de voir que cette symétrie permute $[AG]$ avec $[EC]$. De plus elle laisse $[FD]$ inchangée. En effet, aussi incroyable que cela paraisse en regardant le dessin, nous avons $FD \perp MN$, parce qu'en termes de vecteurs directeurs,

$$\overrightarrow{ON} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \quad \overrightarrow{OF} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}. \tag{7.131}$$

Étudions à présent le noyau $\ker(\rho)$. Si $f \in \ker(\rho)$ n'est pas l'identité, alors $f(D_i) = D_i$ pour tout i, mais au moins pour une des diagonales les sommets sont inversés. Quitte à renommer les sommets du cube nous supposons que la diagonale $[AG]$ est retournée : $f(A) = G$ et $f(G) = A$. Regardons où peut partir B sous l'effet de f. Étant donné que f préserve les diagonales, $f(B) \in \{B, C\}$, mais étant donné que f est une isométrie, $d\big(f(B), f(G)\big) = d(B,G)$, et nous concluons que $f(B) = H$. Donc la diagonale $[BH]$ est retournée sous l'effet de f. En raisonnant de même, nous voyons que f retourne toutes les diagonales. Donc les éléments non triviaux de $\ker(\rho)$ retournent toutes les diagonales ; il n'y en a donc qu'un seul et c'est la symétrie centrale :

$$\ker(\rho) = \{\mathrm{Id}, s_0\}. \tag{7.132}$$

Le premier théorème d'isomorphisme 2.20 nous permet d'écrire le quotient de groupes :

$$\frac{G}{\{\mathrm{Id}, s_0\}} \simeq S_4. \tag{7.133}$$

Une classe d'équivalence modulo $\ker(\rho)$ dans G est donc toujours de la forme $\{f, f \circ s_0\}$. Et comme s_0 est de déterminant -1, une classe contient toujours exactement un élément de déterminant 1 et un de déterminant -1.

D'autre part, $\ker(\rho)$ est normal dans G parce qu'en tant que matrice, $s_0 = -\mathbb{1}$, donc les problèmes de commutativité ne se posent pas. L'application

$$\begin{aligned} \varphi\colon \frac{G}{\{\mathrm{Id}, s_0\}} &\to G^+ \\ [g] &\mapsto \begin{cases} g & \text{si } \det(g) > 0 \\ g \circ s_0 & \text{sinon} \end{cases} \end{aligned} \tag{7.134}$$

est un isomorphisme de groupes. Et enfin nous pouvons écrire

$$G^+ \simeq S_4. \tag{7.135}$$

Nous allons maintenant utiliser le corolaire 2.161 pour montrer que $G = G^+ \times_\sigma \ker(\rho)$. Les conditions sont remplies :

- $\ker(\rho)$ normalise G^+ parce que $\ker(\rho)$ ne contient que $\pm\mathbb{1}$.
- $\ker(\rho) \cap G^+ = \{\mathrm{Id}\}$.
- $\ker(\rho)G^+ = G$ parce que les classes d'équivalence de G modulo $\ker(\rho)$ sont composées de $\{f, f \circ s_0\}$.

Puisque $G^+ \simeq S_4$ et $\ker(\rho) \simeq \mathbb{Z}/2\mathbb{Z}$ nous pouvons écrire de façon plus brillante que

$$G \simeq S_4 \times_\sigma \mathbb{Z}/2\mathbb{Z}. \tag{7.136}$$

Mais étant donné que la conjugaison par s_0 est triviale, le produit semi-direct est un produit direct :

$$G \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}. \tag{7.137}$$

Il est maintenant du meilleur gout de pouvoir identifier géométriquement ces éléments. Les éléments de $\mathbb{Z}/2\mathbb{Z} = \{\mathrm{Id}, s_0\}$ ne font pas de mystère. Dans S_4 nous avons les classes de conjugaison des éléments Id, (12), (123), (1234) et (12)(34) déterminées durant l'exemple 2.114.

(1) L'élément (12) consiste à permuter deux diagonales et laisser les autres en place. Nous avons déjà vu que c'était une symétrie axiale passant par les milieux de deux côtés opposés. Cela fait 6 axes d'ordre 2.

(2) L'élément (123) fixe une des diagonales. C'est donc la symétrie axiale le long de la diagonale fixée. Par exemple la symétrie d'axe (AG) fait bouger le point B de la façon suivante :

$$B \to D \to E \to B. \tag{7.138}$$

C'est une rotation d'angle $\frac{2\pi}{3}$. En tout, nous avons donc 8 rotations d'ordre 3.

Notons à ce propos que la différence entre (234) et (243) est que la première réalise une rotation d'angle $2\pi/3$ tandis que la seconde, une rotation d'angle $-2\pi/3$.

(3) L'élément (1234) ne maintient aucune des diagonales et est d'ordre 4. C'est donc la rotation d'angle $\pi/2$ ou $-\pi/2$ autour de l'axe passant par les milieux de deux faces opposées. Il y en a 6 comme ça (3 paires de faces puis pour chaque il y a $\pi/2$ et $-\pi/2$), et ça tombe bien 6 est justement la taille de la classe de conjugaison de (1234) dans S_4.

(4) L'élément (12)(34) est le carré de la précédente[25], c'est-à-dire les rotations d'angle π autour des mêmes axes. Cela fait 3 éléments d'ordre 2.

[25] En fait c'est (13)(24), le carré de la précédente, mais c'est la même classe de conjugaison.

Chapitre 8

Corps

8.1 Généralités

NORMooGPWRooIKJqqw

8.1.
Nous trouvons parfois le terme **anneau à division**. Cela provient du fait que dans beaucoup de cas on considère uniquement des corps commutatifs ; donc on voudrait une façon de parler d'un anneau dont tous les éléments non nuls sont inversibles. Dans ce cadre on dit :

- Un anneau à division est un anneau dont tous les éléments non nuls sont inversibles,
- Un corps est un anneau à division commutatif.

Pour prendre un exemple de cette différence, le théorème de Wedderburn 21.31 est énoncé ici sous les termes « Tout corps fini est commutatif ». Sous-entendu : la commutativité ne fait pas partie de la définition d'un corps. Par contre dans [112] il est énoncé sous les termes « Tout anneau à division fini est un corps ». Chez lui, un corps est toujours commutatif et un anneau à division est ce que nous appelons ici un corps.

8.1.1 Corps ordonnés

Nous avons vu la définition de corps totalement ordonné en 3.249.

Définition 8.2 ([34]).
Un corps est ***formellement réel*** *si -1 n'est pas une somme de carrés.*

Proposition 8.3.
Un corps totalement ordonné est formellement réel.

Démonstration. Soit un corps totalement ordonné $(\mathbb{K}, \leqslant)$ et $a \in \mathbb{K}$ alors $a^2 \geqslant 0$. En effet si $a \geqslant 0$ alors $a^2 = a \times a \geqslant 0$ directement par la définition 3.249(2). Si $a \leqslant 0$ alors $-a \geqslant 0$ et

$$a^2 = (-a)^2 \geqslant 0. \tag{8.1}$$

Comme $-1 < 0$, il ne peut donc pas être écrit comme un carré. A fortiori comme somme de carrés. □

8.1.2 Automorphismes de $\mathbb{R}$ et $\mathbb{C}$

PROPooLLPMooIVanaO

Proposition 8.4 ([185, 1]).
L'identité est l'unique automorphisme du corps $\mathbb{R}$.

Démonstration. Soit un automorphisme $\sigma : \mathbb{R} \to \mathbb{R}$. Comme pour tout automorphisme,

$$\sigma(a) = \sigma(1a) = \sigma(1)\sigma(a). \tag{8.2}$$

Donc $\sigma(1) = 1$.

(1) **Identité sur les rationnels** De plus

$$\sigma(n) = \sigma(1 + \ldots + 1) = \sigma(1) + \ldots + \sigma(1) = n, \tag{8.3}$$

et

$$\sigma\left(\frac{1}{n}\right) + \ldots + \sigma\left(\frac{1}{n}\right) = \sigma\left(\frac{1}{n} + \ldots + \frac{1}{n}\right) = \sigma(1) = 1. \tag{8.4}$$

Donc $\sigma(1/n) = 1/n$.

Nous en déduisons que pour tout $q \in \mathbb{Q}$, $\sigma(q) = q$. Cela ne suffit pas pour déduire $\sigma(x) = x$ pour tout $x \in \mathbb{R}$ parce que rien n'indique que σ soit continue.

(2) **Positive sur les positifs**

Si $x > 0$ alors $\sigma(x) = \sigma(\sqrt{x})^2 > 0$.

(3) **Croissance**

Si $x > y$ alors $x - y > 0$ et $\sigma(x - y) > 0$. Cela donne $\sigma(x) > \sigma(y)$.

(4) **Identité sur les réels**

Soit un irrationnel $x \in \mathbb{R}$ et une suite (q_i) dans $\mathbb{Q}$ qui converge de façon croissante vers x. Soit $\epsilon > 0$ dans $\mathbb{Q}$. Il existe N tel que si $i > N$ alors $q_i + \epsilon > x$; en appliquant σ à cette inégalité et en se souvenant que σ est l'identité sur $\mathbb{Q}$,

$$q_i + \epsilon > \sigma(x). \tag{8.5}$$

Mais de plus, $q_i < x$ donne $\sigma(q_i) < \sigma(x)$, c'est-à-dire $q_i < \sigma(x)$. En regroupant ces deux inégalités,

$$q_i < \sigma(x) < q_i + \epsilon \tag{8.6}$$

EQooLZOUooPhUNTI

pour tout $\epsilon > 0$ dans $\mathbb{Q}$ et $i > N$. Ce ϵ étant fixé nous pouvons prendre la limite des inégalités (8.6) :

$$x \leqslant \sigma(x) \leqslant x + \epsilon. \tag{8.7}$$

Cela étant valable pour tout $\epsilon > 0$ dans $\mathbb{Q}$, nous avons bien $x = \sigma(x)$.

□

REMooGHEDooOYYUPk

Remarque 8.5.
Certains[185] pensent que l'énoncé de cette proposition, ne parlant que de *corps* $\mathbb{R}$ n'autorise pas l'utilisation d'autre structure réelle que celle de corps. Du coup il faut reconstruire la notion d'ordre à partir seulement du langage des corps. Par exemple en disant que $a > b$ si et seulement si il existe k tel que $a = b + k^2$.

On peut s'en sortir en donnant l'énoncé suivant : « Si $\mathbb{K}$ est un corps isomorphe (en tant que corps) à $\mathbb{R}$ alors son unique automorphisme est l'identité ». Cela se démontre immédiatement en disant que si f est un automorphisme de $\mathbb{K}$ et si ϕ est un isomorphisme $\mathbb{K} \to \mathbb{R}$ alors $\phi \circ f \circ \phi^{-1}$ est un automorphisme de $\mathbb{R}$. Donc il est l'identité et f l'est également.

Attention cependant à prouver que ϕ^{-1} est un morphisme. En effet en posant $\phi^{-1}(x) = a$ et $\phi^{-1}(y) = b$ nous avons

$$\phi\big(\phi^{-1}(x) + \phi^{-1}(y)\big) = x + y \tag{8.8}$$

parce que ϕ est un morphisme. D'autre part,

$$\phi\big(\phi^{-1}(x) + \phi^{-1}(y)\big) = \phi(a + b). \tag{8.9}$$

Donc

$$\phi^{-1}(x + y) = \phi^{-1}\big(\phi(a) + \phi(b)\big) = \phi^{-1}\big(\phi(a + b)\big) = a + b = \phi^{-1}(x) + \phi^{-1}(y). \tag{8.10}$$

PROPooEATMooIPPrRV

Proposition 8.6.
Un automorphisme du corps $\mathbb{C}$ qui fixe $\mathbb{R}$ est soit l'identité soit la conjugaison complexe[1].

Démonstration. Soit un automorphisme σ vérifiant la condition de fixer $\mathbb{R}$. Alors la restriction de σ à $\mathbb{R}$ est un automorphisme de $\mathbb{R}$ et y est donc l'identité par la proposition 8.4.

En ce qui concerne les imaginaires purs,

$$-1 = \sigma(-1) = \sigma(ii) = \sigma(i)^2. \tag{8.11}$$

Donc $\sigma(i)$ est un élément de $\mathbb{C}$ vérifiant $\sigma(i)^2 = -1$. C'est-à-dire $\sigma(i) = \pm i$.

Si $\sigma(i) = i$ alors $\sigma = \mathrm{Id}$. Si $\sigma(i) = -i$ alors σ est la conjugaison complexe. □

[1] Par « fixer $\mathbb{R}$ » nous entendons que $\sigma(\mathbb{R}) = \mathbb{R}$, pas spécialement que $\sigma(x) = x$ pour tout $x \in \mathbb{R}$

8.1.3 Corps premier

DEFooQSOFenIeSKjq

Définition 8.7.
*Un corps est **premier** si il est son seul sous-corps. Le **sous-corps premier** d'un corps est l'intersection de tous ses sous-corps.*

LEMooPOGUooATyqcf

Lemme 8.8.
Le sous corps premier d'un corps est un corps.

Démonstration. Soit un corps $\mathbb{K}$ et son sous-corps premier $\mathbb{P}$. Si $x, y \in \mathbb{P}$, alors pour tout sous-corps $\mathbb{L}$ de $\mathbb{K}$ nous avons $x, y \in \mathbb{L}$ et donc $xy \in \mathbb{L} \subset \mathbb{P}$. Même type de vérification pour les autres propriétés d'un corps. □

Lemme 8.9.
Un corps premier est commutatif.

Démonstration. Le centre d'un corps est certainement un sous-corps. Par conséquent un corps premier doit être contenu dans son propre centre, c'est-à-dire être commutatif. □

DefXIHLooBAcqYH

Définition 8.10.
Soit p un nombre premier. Nous notons $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Nous verrons plus loin (section 21.4) comment nous pouvons définir $\mathbb{F}_{p^n}$ lorsque p est premier, ainsi que l'unicité d'un tel corps.

Nous avons par exemple

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\} \tag{8.12}$$

avec la loi $2 = 0$.

Notons que $\mathbb{F}_p$ est un corps[2] possédant p éléments. L'ensemble $\mathbb{F}_p^*$ est un groupe d'ordre $p - 1$.

Lemme 8.11.
Les corps $\mathbb{Q}$ et $\mathbb{Z}/p\mathbb{Z}$ (avec p premier) sont premiers.

Démonstration. Tout sous-corps de $\mathbb{Q}$ doit contenir 1, et par conséquent $\mathbb{Z}$. Devant également contenir tous les inverses, il contient $\mathbb{Q}$.

Tout sous-corps de $\mathbb{F}_p$ doit contenir 1 et donc $\mathbb{F}_p$ en entier. Par ailleurs nous savons de la proposition 3.193 que $\mathbb{F}_p$ est un corps lorsque p est premier. □

LEMooCGIYooSwOmHG

Lemme 8.12.
Si $k \in \mathbb{Z}$, nous notons $k_{\mathbb{K}}$ l'élément $k \cdot 1_{\mathbb{K}} = \sum_{i=1}^{k} 1_{\mathbb{K}}$. L'application

$$\begin{aligned} s\colon \mathbb{Z} &\to \mathbb{K} \\ k &\mapsto k_{\mathbb{K}} \end{aligned} \tag{8.13}$$

est un morphisme d'anneaux.

Si la caractéristique de $\mathbb{K}$ est 0, alors s est injective.

PROPooXLLOooIAhEue

Proposition 8.13 (Sous-corps premier[186])**.**
Soit $\mathbb{K}$, un corps[3] de caractéristique p.

(1) Si $p > 0$ alors le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}$.

(2) Si $p = 0$ alors le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$.

Démonstration. Pour les besoins de notations, dans la suite si $k \in \mathbb{Z}$, nous notons $k_{\mathbb{K}}$ l'élément $k \cdot 1_{\mathbb{K}} = \sum_{i=1}^{k} 1_{\mathbb{K}}$. Notons aussi $\mathbb{P}$ le sous-corps premier de $\mathbb{K}$.

Étant donné que $1_{\mathbb{K}}$ est dans tout sous-corps, nous devons avoir $\mathbb{Z}1_{\mathbb{K}} \subseteq \mathbb{P}$. Nous avons donc toujours

$$\mathbb{Z}1_{\mathbb{K}} \subset \mathbb{P} \subset \mathbb{K}. \tag{8.14}$$

Maintenant, le lemme 3.116 nous dit la nature de $\mathbb{Z}1_{\mathbb{K}}$ en tant qu'anneaux, et nous pouvons séparer les cas en fonction de la caractéristique.

[2] Quand p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, proposition 3.193.

[3] Je rappelle que tous les corps du Frido sont commutatifs, sauf mention explicite du contraire.

(1) **Si $p > 0$** Nous avons $\mathbb{Z}1_{\mathbb{K}} \simeq \mathbb{Z}/p\mathbb{Z}$ par le lemme 3.116. L'ensemble $\mathbb{Z}/p\mathbb{Z}$ étant un corps, $\mathbb{Z}1_{\mathbb{K}}$ est un corps et c'est donc le corps premier de $\mathbb{K}$.

(2) **Si $p = 0$** Si $p = 0$, alors $\mathbb{Z}1 \simeq \mathbb{Z}$ en tant qu'anneaux. Dommage que $\mathbb{Z}$ ne soit pas un corps.

Soit $n \in \mathbb{Z}1_{\mathbb{K}}$ et $m \in (\mathbb{Z}1_{\mathbb{K}})^*$. L'élément $nm^{-1} \in \mathbb{K}$ est dans $\mathbb{P}$ parce que $\mathbb{P}$ est un corps. Donc l'application

$$\begin{aligned} \psi\colon \mathbb{Q} &\to \mathbb{P} \\ ab^{-1} &\mapsto a_{\mathbb{K}} b_{\mathbb{K}}^{-1} \end{aligned} \tag{8.15}$$

prend bien ses valeurs dans $\mathbb{P}$ et est un morphisme de corps.

La surjectivité de ψ est ce dont nous venons de parler. En ce qui concerne l'injectivité, si $\psi(ab^{-1}) = \psi(xy^{-1})$, alors $a_{\mathbb{K}} b_{\mathbb{K}}^{-1} = x_{\mathbb{K}} y_{\mathbb{K}}^{-1}$ et la commutativité de $\mathbb{K}$ nous permet d'écrire

$$a_{\mathbb{K}} y_{\mathbb{K}} = x_{\mathbb{K}} b_{\mathbb{K}}. \tag{8.16}$$

Étant donné le lemme 8.12, nous déduisons que $(ay - xb)_{\mathbb{K}} = 0$. Et comme $z \mapsto z_{\mathbb{K}}$ est injective, nous en déduisons que $ay - xb = 0$ dans $\mathbb{Z}$, et donc que $ab^{-1} = xy^{-1}$ dans $\mathbb{Q}$ par le lemme 3.245.

□

PropqPPrgJ

Proposition 8.14.
Soit $\mathbb{K}$ un corps et $\mathbb{P}$ son sous-corps premier[4]*. Si $\sigma \in \mathrm{Aut}(\mathbb{K})$ alors $\sigma|_{\mathbb{P}} = \mathrm{Id}$, c'est-à-dire que $\sigma(x) = x$ pour tout $x \in \mathbb{P}$.*

Démonstration. Soit $\mathbb{P}$ le sous-corps premier de $\mathbb{K}$. La proposition 8.13 nous dit que $\mathbb{P}$ est soit $\mathbb{Z}$ soit $\mathbb{Q}$ en fonction de la caractéristique de $\mathbb{K}$. Nous allons faire le cas de caractéristique nulle, c'est-à-dire $\mathbb{P} \simeq \mathbb{Q}$.

Tout élément de $\mathbb{P}$ peut être écrit sous la forme $k_{\mathbb{K}} l_{\mathbb{K}}^{-1}$ pour des $k, l \in \mathbb{Z}$. Nous calculons la valeur de σ sur ces éléments. D'abord σ satisfait $\sigma(1_{\mathbb{K}})$ et préserve la somme, dont $\sigma(k_{\mathbb{K}}) = k_{\mathbb{K}}$ pour tout $k \in \mathbb{Z}$[5]. Étant donné que σ préserve également l'inverse et le produit,

$$\sigma(k_{\mathbb{K}} l_{\mathbb{K}}^{-1}) = \sigma(k_{\mathbb{K}})\sigma(l_{\mathbb{K}})^{-1} = k_{\mathbb{K}} l_{\mathbb{K}}^{-1}. \tag{8.17}$$

Et voilà. □

8.1.4 Petit théorème de Fermat

ThoOPQOiO

Théorème 8.15 (Petit théorème de Fermat)**.**
Soit p un nombre premier.

(1) Si $x \in \mathbb{Z}/p\mathbb{Z}$ alors $x^p = x$.

(2) Si $x \in (\mathbb{Z}/p\mathbb{Z})^*$, alors $x^{p-1} = 1$.

(3) Si $x \in (\mathbb{Z}/p\mathbb{Z})^*$ alors $x^{-1} = x^{p-2}$.

ITEMooRNIVooOIzqgc

(4) Si x est premier avec p, alors $x^{p-1} \in [1]_p$.

Démonstration. Étant donné que $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif et que p est premier, la proposition 3.119 nous indique que $\sigma(x) = x^p$ est un automorphisme. La proposition 8.14 nous indique alors que

$$a^p = a. \tag{8.18}$$

Si a est inversible alors $a^{p-1} = a^p a^{-1} = 1$.

Pour (4). Le nombre x n'est pas premier avec p uniquement lorsque x est multiple de p. Dans ce cas c'est $[a]_p = 0$ dans $\mathbb{Z}/p\mathbb{Z}$ et donc $a^{p-1} = 0$. □

Exemple 8.16.
Soit $\mathbb{K} = \mathbb{F}_{29}$. Le nombre 29 étant premier, $\mathbb{K}$ est un corps. C'est le corps des entiers modulo 29. Nous avons donc

$$-142 = -113 = -84 = -55 = -26 = 3 = 32 = 61 = 90 = 119. \tag{8.19}$$

[4] Définition 8.7.
[5] Dans le cas de caractéristique non nulle, $\mathbb{P} = \mathbb{Z}$ et vous pouvez vous arrêter ici.

Le petit théorème de Fermat nous permet aussi de calculer des exposants et des inverses. En effet, puisque $1 = x^{28}$ pour tout $x \in \mathbb{F}_{29}^*$, nous avons $x^{-1} = x^{27}$, et par suite, pour tout entier a,

$$x^{-a} = (x^a)^{27} = x^{27a}. \tag{8.20}$$

Le nombre $27a$ peut être grand par rapport à 29. Mais en réutilisant le fait que $1 = x^{28}$, on obtient

$$x^{-a} = x^{[27a]_{28}}. \tag{8.21}$$

Cette expression doit être comprise comme disant que pour tout $k \in [27a]_{28}$ nous avons $x^{-a} = x^k$.

Chose à retenir : dans les exposants nous calculons modulo 28. △

8.1.5 Nombres de Sophie Germain

DEFooCVFJooKCdVVD

Définition 8.17.
*Un nombre premier p est de **Sophie Germain** si $p > 2$ et si le nombre $q = 2p + 1$ est également premier.*

Notons qu'il existe des nombres premiers de Sophie Germain. Par exemple $p = 3$ donne $q = 2 \times 3 + 1 = 7$. Comme 7 est un nombre premier, le nombre 3 est de Sophie Germain. D'après Wikipédia[187], l'existence d'une infinité de nombres premiers de Sophie Germain est encore une question ouverte[6].

LEMooIYIKooGkoqRJ

Lemme 8.18 ([188, 189]).
Soit p, un nombre premier de Sophie Germain. Si $m \in \mathbb{Z}$ n'est pas divisible par q, alors $m^p \in [\pm 1]_q$ où $q = 2p + 1$.

Démonstration. Le petit théorème de Fermat 8.15 nous dit que $m^{q-1} \in [1]_q$. Mais $m^{q-1} = m^{2p} = (m^p)^2$. Donc

$$(m^p)^2 \in [1]_q. \tag{8.22}$$

Puisque q est premier, l'anneau $\mathbb{Z}/q\mathbb{Z}$ est intègre par le corolaire 3.123. Comme $1 \neq -1$, la proposition 3.289 s'applique et nous avons $m^p \in [\pm 1]_q$. □

THOooSZXWooVeHdrh

Théorème 8.19 ([188, 189, 190]).
Soit un nombre premier de Sophie Germain (définition 8.17). Il n'existe pas de solution (x, y, z) dans $\mathbb{Z}^3$ au système

$$\begin{cases} x^p + y^p + z^p = 0 \\ [xyz]_p \neq 0. \end{cases} \tag{8.23}$$

Démonstration. Nous supposons que $(x, y, z) \in \mathbb{Z}^3$ est une solution telle que $\operatorname{pgcd}(x, y, z) = 1$.

(1) **x, y et z sont premiers deux à deux** Supposons que k soit un diviseur premier commun à x et y. Alors il existe $\alpha, \beta \in \mathbb{Z}$ tels que $x = k\alpha$ et $y = k\beta$. Du coup on aurait $z^p = -k^p(\alpha^p + \beta^p)$. Donc k divise z^p. Le lemme 3.64 nous indique qu'alors k divise z. Donc $k = 1$ parce que k diviserait x, y et z.

Ce qui est vrai pour le couple (x, y) est encore vrai pour (x, z) et pour (y, z).

(2) **Le fameux u** Nous introduisons à présent une nouvelle variable intermédiaire qui va beaucoup nous aider. En utilisant le lemme 3.77,

$$-x^p = y^p + z^p = (y + z)\sum_{k=0}^{p-1} y^k(-z)^{p-1-k} = (y + z)u \tag{8.24}$$

où nous avons posé $u = \sum_{k=0}^{p-1} y^k(-z)^{p-1-k}$.

(3) **$\operatorname{pgcd}(u, y + z) = 1$** Soit α un nombre premier qui divise u et $y + z$.

D'abord α divise x^p et donc x (lemme 3.64). Autrement dit : $[x]_\alpha = 0$.

Ensuite, $0 = [x + z]_\alpha$, de telle sorte que

$$[y]_\alpha = -[z]_\alpha \tag{8.25}$$

EQooPTICooBNDwpx

[6] Si vous lisez ce paragraphe dans un futur où la question est tranchée, n'hésitez pas à m'écrire pour mettre à jour.

Enfin, en prenant la classe de u modulo α, et en substituant (8.25) :

$$0 = [u]_\alpha = \Big[\sum_{k=0}^{p-1} y^k(-z)^{p-1-k}\Big]_\alpha \tag{8.26a}$$
$$= \sum_{k=0}^{p-1}[y^k]_\alpha[y^{p-1-k}]_\alpha \tag{8.26b}$$
$$= \sum_{k=0}^{p-1}[y]_\alpha^{p-1} \tag{8.26c}$$
$$= p[y]_\alpha^{p-1}. \tag{8.26d}$$

Nous avons donc $p[y]_\alpha^{p-1} = 0$. Mais $\mathbb{Z}/\alpha\mathbb{Z}$ est un anneau intègre[7]. Donc la règle du produit nul s'applique[8] et nous avons deux possibilités : $[p]_\alpha = 0$ ou $[y]_\alpha^{p-1} = 0$.

D'abord α divise déjà x. Or $\text{pgcd}(x, y) = 1$. Donc α ne peut pas diviser y (à part si $\alpha = 1$ évidemment), et à fortiori pas y^{p-1} non plus. Nous en déduisons que $[p]_\alpha = 0$. Puisque p est premier, nous avons $p = \alpha$.

Mais nous avons déjà vu que α divisait x. Donc $0 = [x]_\alpha = [x]_p$. Cela n'est pas possible parce que $[xyz]_p \neq 0$.

Nous avons donc prouvé que $\text{pgcd}(u, y + z) = 1$.

(4) **Utilisation d'un lemme**

Pour rappel, p est impair. Nous avons $(-x)^p = (y+z)u$. Le lemme 3.159 nous dit qu'il existe $a, \alpha \in \mathbb{Z}$ tels que

$$\begin{cases} y + z = a^p \\ u = \alpha^p. \end{cases} \tag{8.27}$$

EQooKMPZooCShJIT

Ce que nous venons de faire pour $y + z$ peut être fait pour les autres couples. Donc il existe $a, b, c \in \mathbb{Z}$ tels que

$$y + z = a^p \tag{8.28a}$$
$$x + z = b^p \tag{8.28b}$$
$$x + y = c^p. \tag{8.28c}$$

(5) **q divise un et un seul des x, y ou z** Supposons que q ne divise ni x, ni y ni z. Alors le lemme 8.18 dit que $x^p \in [\pm1]_q$, $y^p \in [\pm1]_q$ et $z^p \in [\pm1]_q$. Donc les valeurs possibles pour $[x^p + y^p + z^p]_q$ sont $[\pm3]_q$ et $[\pm1]_q$.

Mais nous avons supposé que $x^p + y^p + z^p = 0$ et que $q \geq 5$ de telle sorte que $[\pm3]_q \neq 0$. Contradiction. Donc q divise au moins un des trois x, y ou z.

Nous avons déjà montré que x, y et z étaient deux à deux premiers entre eux. Donc q ne peut diviser qu'un seul des trois.

(6) **q divise x** Jusqu'à présent x, y et z avaient des rôles symétriques. Maintenant nous supposons que q divise x.

(7) **$[y^p]_q = [\pm1]_q$** Nous savons que $c^p = x + y$. En passant aux classes modulo q, nous avons

$$[c^p]_q = [x]_q + [y]_q = [y]_q \tag{8.29}$$

parce que nous avons choisi que q divise x. Nous avons maintenant les implications suivantes :

q ne divise pas y.
$\Rightarrow$ q ne divise pas c^p parce que $[y]_q = [c^p]_q$.
$\Rightarrow$ q ne divise pas c par le lemme 3.64.
$\Rightarrow$ $c^p \in [\pm1]_q$ par le lemme 8.18.
$\Rightarrow$ $y \in [\pm1]_q$ toujours parce que $[y]_q = [c^p]_q$.

(8) **$[z^p]_q = [\pm1]_q$** Parce que les rôles de y et z sont symétriques. Donc ce que nous avons fait pour obtenir $[y^p]_q = [\pm1]_q$ tient pour avoir $[z^p]_q = [\pm1]_q$.

[7] Corolaire 3.123.
[8] Proposition 3.22.

(9) **q divise $y+z$** Nous avons dit que q divisait x. Il divise donc aussi $2x$. Nous avons :

$$2x = (x+y)+(x+z)-(y+z) = c^p + b^p - a^p. \tag{8.30}$$

En passant au modulo q, à gauche nous avons $[2x]_q = 0$. Donc

$$\begin{aligned}
[a^p]_q &= [c^p]_q + [b^p]_q && (8.31a)\\
&= [y]_q + [z]_q && (8.31b)\\
&= [\pm 1]_q + [\pm 1]_q && (8.31c)\\
&\in \{[2]_q, [-2]_q, [0]_q\}. && (8.31d)
\end{aligned}$$

En tout état de cause, $[a^p]_q$ n'est pas $[\pm 1]_q$. La contraposée du lemme 8.18 nous dit alors que q divise $a^p = y+z$.

(10) **$[y]_q = [-z]_q$** Il s'agit seulement du fait que q divise $y+z$.

(11) **$[u]_q = [p]_q$** Par définition, $u = \sum_{k=0}^{p-1} y^k (-z)^{p-1-k}$. On passe au modulo q, en substituant $[-z]_q$ par $[y]_q$:

$$[u]_q = \sum_{k=0}^{p-1} [y]_q^k [y]_q^{p-1-k} = \sum_{k=0}^{p-1} [y]_q^{p-1} = p[y]_q^{p-1} = [p]_q \tag{8.32}$$

La dernière égalité est le fait que $[y]_q = [\pm 1]_q$ et que $p-1$ est pair.

(12) **La contradiction** Vous vous souvenez de (8.27) qui disait que $u = \alpha^p$ pour un certain p ? Nous avons les implications suivantes :

$[\alpha^p]_q = [p]_q \neq 0 \Rightarrow q$ ne divise pas α^p.
$\Rightarrow q$ ne divise pas α.
$\Rightarrow \alpha^p \in [\pm 1]_q$.
$\Rightarrow [p]_q \in [\pm 1]_q$.

La dernière ligne est clairement fausse parce que $q > p$ et p n'est certainement pas égal à 1 ou -1.

Nous avons prouvé le théorème pour les triples (x,y,z) sans facteur commun. Si k était un diviseur commun de x, y et z, alors $(x/k, y/k, z/k)$ serait encore une solution, ce qui n'est pas le cas. □

8.2 Théorème des deux carrés

PropleGdaT

Proposition 8.20.
Soit p un nombre premier et P un élément de $\mathbb{F}_p[X]$. L'anneau $\mathbb{F}_p[X]/(P)$ est intègre si et seulement si P est irréductible dans $\mathbb{F}_p[X]$.

Démonstration. Supposons que P soit réductible dans $\mathbb{F}_p[X]$, c'est-à-dire qu'il existe $Q, R \in \mathbb{F}_p[X]$ tels que $P = QR$. Dans ce cas, $\bar{Q}$ est diviseur de zéro dans $\mathbb{F}_p[X]/(P)$ parce que $\bar{Q}\bar{R} = 0$.

Nous supposons maintenant que $\mathbb{F}_p[X]/(P)$ ne soit pas intègre : il existe des polynômes $R, Q \in \mathbb{F}_p[X]$ tels que $\bar{Q}\bar{R} = 0$. Dans ce cas le polynôme QR est le produit de P par un polynôme : $QR = PA$. Tous les facteurs irréductibles de A étant soit dans Q soit dans R, il est possible de modifier un peu Q et R pour obtenir $QR = P$, ce qui signifie que P n'est pas irréductible. □

8.2.1 Un peu de structure dans $\mathbb{Z}[i]$

LemSCAlICY

Lemme 8.21.
L'application

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{N} \\ a+bi &\mapsto a^2+b^2 \end{aligned} \tag{8.33}$$

est un stathme euclidien pour $\mathbb{Z}[i]$.

Démonstration. Soient $t, z \in \mathbb{Z}[i] \setminus \{0\}$ dont le quotient s'écrit

$$\frac{z}{t} = x + iy \tag{8.34}$$

dans $\mathbb{C}$. Nous considérons $q = a + bi$ où a et b sont les entiers les plus proches de x et y. Si il y a *ex aequo*, on prend au hasard[9]. Alors nous avons

$$|\frac{z}{t} - q| \leqslant \frac{|1+i|}{2} = \frac{\sqrt{2}}{2} < 1. \tag{8.35}$$

On pose $r = z - qt$ qui est bien un élément de $\mathbb{Z}[i]$. De plus

$$|r| = |z - qt| = |t||\frac{z}{t} - q| < |t|, \tag{8.36}$$

c'est-à-dire que $|r|^2 < |t|^2$ et donc $N(r) < N(t)$. □

Étant donné que $\mathbb{Z}[i]$ est euclidien, il est principal (proposition 3.38).

LemBMEIiiV

Lemme 8.22.
Les éléments inversibles de $\mathbb{Z}[i]$ sont $\{\pm 1, \pm i\}$.

Démonstration. Déterminons les éléments inversibles de $\mathbb{Z}[i]$. Si $z \in \mathbb{Z}[i]^*$, alors il existe $z' \in \mathbb{Z}[i]^*$ tel que $zz' = 1$. Dans ce cas nous aurions

$$1 = N(zz') = N(z)N(z'), \tag{8.37}$$

ce qui est uniquement possible avec $N(z) = N(z') = 1$, c'est-à-dire $z = \pm 1$ ou $z = \pm i$. Nous avons donc

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}. \tag{8.38}$$

□

DEFooUCSHooJqGuVB

Définition 8.23 ([191])**.**
*Un **monoïde** est un triplet $(E, *, e)$ où E est un ensemble, e est un élément de E et $*\colon E \times E \to E$ est une loi de composition telle que pour tout $x, y \in E$,*

(1) $x * (y * z) = (x * y) * z$ (associativité)

(2) $e * x = x * e = x$ (e est un neutre).

Nous notons $\Sigma = \{a^2 + b^2 \text{ tel que } a, b \in \mathbb{N}\}$.

LemIBDPzMB

Lemme 8.24.
L'ensemble $\Sigma = \{a^2 + b^2 \text{ tel que } a, b \in \mathbb{N}\}$ est un sous-monoïde[10] de $\mathbb{N}$.

Démonstration. Il suffit de prouver que si $m, n \in \Sigma$, alors le produit mn est également dans Σ. Soit N, le stathme euclidien sur $\mathbb{Z}[i]$ (celui donné par le lemme 8.21). Vu que $n \in \Sigma$, il existe $z \in \mathbb{Z}[i]$ tel que $N(z) = n$. Idem pour m : il existe $z' \in \mathbb{Z}[i]$ tel que $N(z') = m$. Nous avons évidemment $zz' \in \mathbb{Z}[i]$, et

$$N(zz') = N(z)N(z') = nm. \tag{8.39}$$

Donc nm est l'image de zz' par N, ce qui prouve que $nm \in \Sigma$. □

ThospaAEI

Théorème 8.25 (Théorème des deux carrés, version faible)**.**
Un nombre premier est somme de deux carrés si et seulement si $p = 2$ ou $p \in [1]_4$.

Démonstration. Soit p un nombre premier dans Σ. Si $a = 2k$, alors $a^2 = 4k^2$ et $a^2 = 0 \mod 4$. Si au contraire a est impair, $a = 2k + 1$ et $a^2 = 4k^2 + 1 + 4k = 1 \mod 4$. La même chose est valable pour b. Par conséquent, $a^2 + b^2$ est automatiquement $[0]_4$, $[1]_4$ ou $[2]_4$. Évidemment les nombres de la forme $0 \mod 4$ ne sont pas premiers ; parmi les $2 \mod 4$, seul $p = 2$ est premier (et vaut $1^2 + 1^2$).

Nous avons démontré que les seuls premiers de la forme $a^2 + b^2$ sont $p = 2$ et les $p = 1 \mod 4$. Il reste à faire le contraire : démontrer que si un nombre premier p vaut $1 \mod 4$, alors il est premier. Nous considérons l'anneau

$$\mathbb{Z}[i] = \{a + bi \text{ tel que } a, b \in \mathbb{Z}\}. \tag{8.40}$$

puis l'application

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{N} \\ a + bi &\mapsto a^2 + b^2. \end{aligned} \tag{8.41}$$

[9] Dans l'exemple 3.35, nous prenions toujours l'inférieur parce que le stathme tenait compte de la positivité.
[10] Définition 8.23.

Un peu de calcul dans $\mathbb{C}$ montre que pour tout $z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.

Nous savons que les éléments inversibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$ (lemme 8.22).

Le lemme 8.21 montre que $\mathbb{Z}[i]$ est un anneau euclidien parce que N est un stathme. L'anneau $\mathbb{Z}[i]$ étant euclidien, il est principal (proposition 3.38).

Pour la suite, nous allons d'abord montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$, puis nous allons voir quels sont les irréductibles de $\mathbb{Z}[i]$.

Soit p, un nombre premier dans Σ. Si $p = a^2 + b^2$, alors nous avons $p = (a + ib)(a - bi)$, mais étant donné que p est premier, nous avons $a \neq 0$ et $b \neq 0$. Du coup p n'est pas inversible dans $\mathbb{Z}[i]$, mais il peut être écrit comme le produit de deux non inversibles. Le nombre p est donc non irréductible dans $\mathbb{Z}[i]$.

Dans l'autre sens, nous supposons que p est un nombre premier non irréductible dans $\mathbb{Z}[i]$. Nous avons alors $p = zz'$ avec ni z ni z' dans $\{\pm 1, \pm i\}$. En appliquant N nous avons

$$p^2 = N(p) = N(z)N(z'). \tag{8.42}$$

Comme p est premier par hypothèse, c'est uniquement possible avec $N(z) = N(z') = p$ (avoir $N(z) = 1$ est impossible parce que cela signifirait que z est inversible). Si $z = a + ib$, alors $p = N(z) = a^2 + b^2$, et donc $p \in \Sigma$.

Nous savons déjà que $\mathbb{Z}[i]$ est un anneau principal et n'est pas un corps ; la proposition 3.126 s'applique donc et p sera non irréductible si et seulement si l'idéal (p) est non premier. Le fait que (p) soit un idéal non premier implique que le quotient $\mathbb{Z}[i]/(p)$ est non intègre (c'est la définition d'un idéal premier). Nous cherchons donc les nombres premiers pour lesquels le quotient $\mathbb{Z}[i]/(p)$ n'est pas intègre.

Nous commençons par écrire le quotient $\mathbb{Z}[i]/(p)$ sous d'autres formes. D'abord en remarquant que si I et J sont deux idéaux, on a $(\mathbb{A}/I)/J \simeq (\mathbb{A}/J)/I$. Par conséquent, en tenant compte du fait que $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2 + 1)$, nous avons

$$\mathbb{Z}[i]/(p) = (\mathbb{Z}[X]/(p))/(X^2 + 1) = \mathbb{F}_p[X]/(X^2 + 1). \tag{8.43}$$

Nous avons donc équivalence des propositions suivantes :

$$p \in \Sigma \tag{8.44a}$$
$$\mathbb{F}_p[X]/(X^2 + 1) \text{ n'est pas intègre} \tag{8.44b}$$
$$X^2 + 1 \text{ n'est pas irréductible dans } \mathbb{F}_p \tag{8.44c}$$
$$X^2 + 1 \text{ admet une racine dans } \mathbb{F}_p \tag{8.44d}$$
$$-1 \in (\mathbb{F}_p^*)^2 \tag{8.44e}$$
$$\exists y \in \mathbb{F}_p^* \text{ tel que } y^2 = -1. \tag{8.44f}$$

Le point (8.44c) vient de la proposition 8.20. Maintenant nous utilisons le fait que p soit un premier impair (parce que le cas de $p = 2$ est déjà complètement traité), donc $(p-1)/2 \in \mathbb{N}$ et nous avons, pour le y de la dernière ligne,

$$(-1)^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1 \tag{8.45}$$

parce que dans $\mathbb{F}_p$ nous avons $y^{(p-1)} = 1$ par le petit théorème de Fermat (théorème 8.15). Ainsi p doit vérifier

$$1 = (-1)^{(p-1)/2}, \tag{8.46}$$

c'est-à-dire $\frac{p-1}{2} = 0 \mod 2$ ou encore $p = 1 \mod 4$. □

Remarque 8.26.
Il n'est pas dit que les nombres dans $[1]_4$ sont premiers ($9 = 8 + 1$ ne l'est pas par exemple). Le théorème signifie que (à part 2), si un nombre premier est dans $[1]_4$ alors il est somme de deux carrés, et inversement, si un nombre premier est somme de deux carrés, il est dans $[1]_4$.

Théorème 8.27 (Théorème des deux carrés[112])**.**
Soit $n \geqslant 2$ un nombre dont nous notons

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \tag{8.47}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers. Alors $n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P} \cap [3]_4$, nous avons $v_p(n) \in [0]_2$ (c'est-à-dire $v_p(n)$ est pair).

Démonstration. (1) **Condition suffisante.**

Le produit (8.47) est évidemment un produit fini que nous pouvons alors regrouper en quatre parties : $\mathcal{P} \cap [0]_4$, $\mathcal{P} \cap [1]_4$, $\mathcal{P} \cap [2]_4$ et $\mathcal{P} \cap [3]_4$.

- Il n'y a pas de nombres premiers dans $[0]_4$.
- Les nombres premiers de $[1]_4$ sont dans Σ. Le produit d'éléments de Σ étant dans Σ, nous avons
$$\prod_{p\in\mathcal{P}\cap[1]_4} p^{v_p(n)} \in \Sigma. \tag{8.48}$$
- Le seul nombre premier dans $[2]_4$ est 2. C'est un élément de Σ.
- Le produit
$$\prod_{p\in\mathcal{P}\cap[3]_4} p^{v_p(n)} \tag{8.49}$$
est par hypothèse un produit de carrés ($v_p(n)$ est pair), et est donc un carré.

Au final le produit $\prod_{p\in\mathcal{P}} p^{v_p(n)}$ est un produit d'un carré par un élément de Σ, ce qui est encore un élément de Σ.

Pour cette partie, nous avons utilisé et réutilisé le lemme 8.24.

(2) **Condition nécessaire.**

Soit p, un nombre premier. Nous voulons montrer que
$$\{v_p(n) \text{ tel que } n \in \Sigma\} \subset [2]_2. \tag{8.50}$$
Pour montrer cela nous allons procéder par récurrence sur les ensembles
$$E_k = \{v_p(n) \text{ tel que } n \in \Sigma\} \cap \{0,\dots,k\}. \tag{8.51}$$
Il est évident que les éléments de E_0 sont pairs, puisqu'il n'y a que zéro, qui est pair.

Supposons que $E_k \subset [0]_2$, et montrons que $E_{k+1} \subset [0]_2$. Soit un élément de E_{k+1}, c'est-à-dire $v_p(n) \leqslant k+1$ avec $n = a^2+b^2$. Si $v_p(n) = 0$ alors l'affaire est réglée ; sinon c'est que p divise n. Mais dans $\mathbb{Z}[i]$ nous avons
$$n = a^2 + b^2 = (a+bi)(a-bi) \tag{8.52}$$
Comme $\mathbb{Z}[i]$ est principal, le lemme de Gauss 3.201 nous dit que si p divise n, alors il doit diviser soit $a+bi$, soit $a-bi$ (et en fait, les deux). Nous avons alors $p \mid a$ et $p \mid b$ en même temps. Et donc
$$p^2 \mid a^2 + b^2 = n. \tag{8.53}$$
Posons $a = pa'$ et $b = pb'$ avec $a', b' \in \mathbb{N}$. Nous avons
$$\frac{n}{p^2} = \frac{p^2a'^2 + p^2b'^2}{p^2} = a'^2 + b'^2 \in \Sigma. \tag{8.54}$$
Mais par construction,
$$v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 < k. \tag{8.55}$$
Donc $v_p(\frac{n}{p^2})$ est pair et par conséquent, $v_p(n)$ doit également être pair.

□

8.2.2 Résultats chinois

Nous allons maintenant parler du système d'équations [SUBEQooHVCTooGXvbAH]
$$\begin{cases} x = a_1 \mod p & \text{(8.56a)} \\ x = a_2 \mod q & \text{(8.56b)} \end{cases}$$
avec a_1, a_2 donnés dans $\mathbb{Z}$ et p, q des entiers premiers entre eux. Le lemme chinois nous donne la liste des solutions ainsi qu'une manière de les construire. Le théorème chinois en sera une espèce de corolaire qui établira l'isomorphisme d'anneaux $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Voir [192].

Notons que le système (8.56), en suivant les notations usuelles du Frido s'écrit plutôt
$$x \in [a_1]_p \cap [a_2]_q. \tag{8.57}$$

LemCtUeGA

Lemme 8.28 (Lemme chinois [193]).
Soient n_1, n_2 deux entiers premiers entre eux[11]*. Soient $a_1, a_2 \in \mathbb{Z}$.*

ITEMooZVUSooGoplQW

(1) Il existe $u_1, u_2 \in \mathbb{Z}$ tels que

EQooIJXOooNEfCBo

$$u_1 n_1 + u_2 n_2 = 1. \tag{8.58}$$

ITEMooFMFEooQHNLFc

(2) Nous posons

$$a = a_1 u_2 n_2 + a_2 n_1 u_1. \tag{8.59}$$

Nous avons

$$[a_1]_{n_1} \cap [a_2]_{n_2} = [a]_{n_1 n_2}. \tag{8.60}$$

Démonstration. En plusieurs points.

(1) **Pour (1)** Il suffit d'utiliser le théorème de Bézout 3.46

(2) **Pour (2) première inclusion** Soit $x \in [a]_{n_1 n_2}$, et vérifions que $x \in [a_1]_{n_1}$. Il existe $k \in \mathbb{Z}$ tel que

$$x = a_1 u_2 n_2 + a_2 n_1 u_1 + k n_1 n_2. \tag{8.61}$$

En remplaçant $u_2 n_2$ par $1 - u_1 n_1$, nous avons

$$x = a_1(1 - u_1 n_1) + a_2 n_1 u_1 + k n_1 n_2 \in [a_1]_{n_1} \tag{8.62}$$

parce qu'il n'y a que le tout premier terme qui ne contient pas de facteur n_1.

Le fait que $x \in [a_2]_{n_2}$ se vérifie de même[12].

(3) **Pour (2) seconde inclusion** Soit $x \in [a_1]_{n_1} \cap [a_2]_{n_2}$. Il existe $k \in \mathbb{Z}$ tel que $x = a_1 + k n_2$. Donc

$$\begin{aligned} x - a &= a_1 + k n_1 - (a_1 u_2 n_2 + a_2 n_1 u_1) && \text{(8.63a)} \\ &= a_1 - a_1 u_2 n_2 + k' n_1 && \text{(8.63b)} \\ &= a_1 \underbrace{(1 - u_2 n_2)}_{=u_1 n_1} + k' n_1 && \text{(8.63c)} \\ &= a_1 u_1 n_1 + k' n_1, && \text{(8.63d)} \end{aligned}$$

ce qui signifie que n_1 divise $x - a$..

De même nous prouvons que n_2 divise $x - a$. Il existe $k, l \in \mathbb{Z}$ tels que

EQooFMWBooTpqppj

$$x - a = k n_1 = l n_2. \tag{8.64}$$

En particulier n_1 divise $l n_2$ alors que n_1 et n_2 sont premiers entre eux. Le lemme de Gauss 3.201 dit alors que n_1 divise l. Il existe donc $s \in \mathbb{Z}$ tel que $l = s n_1$. En remettant ce l dans (8.64), nous trouvons

$$x - a = l n_1 = s n_1 n_2, \tag{8.65}$$

et donc $x - a$ est divisible en $n_1 n_2$, c'est-à-dire

$$x \in [a]_{n_1 n_2}, \tag{8.66}$$

ce qu'il fallait prouver.

□

THOooQHYLooVMBAfe

Théorème 8.29 (Théorème chinois[194]).
Soient p, q deux naturels premiers entre eux. Si $p, q \geqslant 2$ alors l'application

$$\begin{aligned} \phi\colon \mathbb{Z}/pq\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ [x]_{pq} &\mapsto \big([x]_p, [x]_q\big) \end{aligned} \tag{8.67}$$

est un isomorphisme d'anneaux.

[11] Définition 3.52.
[12] Je dis ça au hasard ; je n'ai pas vérifié. Faites-moi signe si c'est bon.

Démonstration. Nous devons prouver que l'application ϕ respecte la somme, le produit et qu'elle est bijective. En ce qui concerne la somme,

$$\begin{aligned}\phi([q]_{pq}+[y]_{pq}) &= \phi\big((x+y) \mod pq\big) && (8.68a)\\ &= \big([x+y]_p,[x+y]_q\big) && (8.68b)\\ &= \big([x]_p+[y]_p,[x]_q+[y]_q\big) && (8.68c)\\ &= \big([x]_p,[x]_q\big)+\big([y]_p,[y]_q\big) && (8.68d)\\ &= \phi(x)+\phi(y). && (8.68e)\end{aligned}$$

En ce qui concerne le produit, c'est le même jeu : nous obtenons

$$\phi\big([xy]_{pq}\big)=\phi([x]_{pq}])\phi([y]_{pq}) \tag{8.69}$$

en utilisant le fait que $[xy]_p=[x]_p[y]_p$.

Montrons maintenant que ϕ est surjective. Soient $y_1,y_2\in\mathbb{Z}$ et $x\in\mathbb{Z}$. Demander

$$\phi([x]_{pq})=\big([y_1]_p,[y_2]_q\big) \tag{8.70}$$

revient à demander de résoudre le système

$$\begin{cases}[x]_p=[y_1]_p & (8.71a)\\ [x]_q=[y_2]_q & (8.71b)\end{cases}$$

pour l'inconnue $x\in\mathbb{Z}$. Le lemme chinois 8.28 nous assure qu'une solution existe.

En ce qui concerne l'injectivité, nous supposons que x et y soient deux entiers tels que

$$\phi([x]_{pq})=\phi([y]_{pq}). \tag{8.72}$$

Nous en déduisons le système

$$\begin{cases}[x]_p=[y]_p & (8.73a)\\ [x]_q=[y]_q & (8.73b)\end{cases}$$

c'est-à-dire qu'il existe des entiers k et l tels que $x=y+kp$ et $x=y+lq$ ou encore tels que

$$kp+lq=0. \tag{8.74}$$

Étant donné que p et q sont premiers entre eux, le lemme de Gauss 3.58 implique que p divise l : il existe $l'\in\mathbb{Z}$ tel que $lp'=l$. En injectant cela dans $x=y+lq$, nous trouvons $x=y+l'pq$. Donc $[x]_{pq}=[y]_{pq}$, ce qu'il fallait. □

THOooVIGQooUhwBLS

Théorème 8.30 (Théorème chinois[1])**.**
Soit A un anneau commutatif. Soient $n\geqslant 2$, des éléments $x_1,\dots,x_n$ dans A et des idéaux $I_1,\dots,I_n$ tels que $I_i+I_j=A$ pour tout $i\neq j$.

Alors il existe un $x\in A$ tel que $x-x_i\in I_i$ pour tout $1\leqslant i\leqslant n$.

Démonstration. En plusieurs points.

(1) **Définition de J_k**
Pour $k\in\{1,\dots,n\}$ nous notons J_k le produit $J_k=\prod_{l\neq k}I_l$.

(2) **Si $k\neq i$ alors $J_k\subset I_i$** Un élément de J_k est de la forme

$$\prod_{l\neq k}a_j=a_i\prod_{\substack{l\neq k\\ l\neq i}}a_l \tag{8.75}$$

EQooLVTXooIrdWbH

avec $a_l\in I_l$. Vu que a_i est dans I_i qui est un idéal, tout le produit (8.75) est dans I_i.

(3) **$I_i+J_i=A$** En effet, soit $k\neq i$. Nous avons $J_i\subset I_k$ et donc

$$I_i+J_i\subset I_i+I_k=A. \tag{8.76}$$

(4) **Des α et des β**
Soit $i \in \{1, \dots, n\}$. Puisque $I_i + J_i = A$, nous pouvons donc prendre $\alpha_i \in I_i$ et $\beta_i \in J_i$ tels que

$$\alpha_i + \beta_i = 1. \tag{8.77}$$

(5) **Et enfin** Nous posons $x = \sum_{i=1}^{n} \beta_i x_i$. Pour chaque k nous avons

$$x - x_k = \sum_{i=1}^{n} \beta_i x_i - x_k \tag{8.78a}$$
$$= \sum_{i \neq k} \beta_i x_i + (\beta_k - 1)x_k \tag{8.78b}$$
$$= \sum_{i \neq k} \beta_i x_i - \alpha_k x_k. \tag{8.78c}$$

Les deux termes sont dans I_k. En effet, d'une part $\beta_i \in J_i \subset I_k$ et I_k est un idéal, donc $\beta_i x_i \in I_k$, et d'autre part $\alpha_k \in I_k$, donc $\alpha_k x_k \in I_k$.

Un idéal étant stable par somme, la somme du tout est dans I_k.

□

Remarque 8.31.
Ce théorème chinois est bien une généralisation du lemme chinois 8.28. En effet, l'élément x dont il est question est solution du problème $x = x_i \mod I_i$. L'hypothèse $I_i + I_j = A$ n'est pas nouvelle non plus étant donné que si p et q sont des entiers premiers entre eux nous avons $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$ par le corolaire 3.47.

8.3 Polynômes à coefficients dans un corps

SECooFYOGooQHitgE
Nous supposons que $\mathbb{K}$ est un corps commutatif, et nous étudions l'anneau $\mathbb{K}[X]$, défini en 3.228.

LEMooKSTIooSTxAll
Lemme 8.32 ([129]).
Soit un anneau factoriel A, ainsi que son corps des fraction[13] *$\mathbb{K}$. Si $P \in \mathbb{K}[X]$ est de degré $\geqslant 1$, nous pouvons écrire $P = qP_1$ où*

(1) $q \in \mathbb{K}^\times$

(2) $P_1 \in A[X]$ est primitif[14].

Démonstration. Nous considérons le polynôme $P = \sum_{j=0}^{n} \frac{a_j}{s_j} X^j$ avec $n \geqslant 1$, $a_j \in A$, $s_j \in A^*$ et $a_n \neq 0$. Si $s \in \text{ppcm}(\{s_j\}_{j=1,\dots,n})$, nous avons

$$P = \frac{1}{s} \sum_{j=1}^{n} a'_j X^j \tag{8.79}$$

avec $a'_j \in A$.
Si $d \in \text{pgcd}(\{a'_j\})$, nous pouvons écrire $a'_j = db_j$ où les $b_j \in A$ sont premiers entre eux. Avec tout ça,

$$P = \frac{d}{s} \sum_{j} b_j X^j. \tag{8.80}$$

Maintenant en posant $q = d/s$ et $P_1 = \sum_j b_j X^j$ nous avons ce qu'il faut parce que $d/s \in \mathbb{K}^\times$ et P_1 est primitif. □

LEMooGTPJooPWkffg
Lemme 8.33 ([72]).
Soit un polynôme primitif $P \in A[X]$ sur l'anneau factoriel A. Nous notons $\mathbb{K}$ le corps des fractions de A Soient $Q, R \in \mathbb{K}[X]$ tels que $P = QR$. Il existe $q, r \in \mathbb{K}$ tels que

$$P = (qQ)(rR) \tag{8.81}$$

avec qQ, rR dans $A[X]$.

[13] Définition 3.239.
[14] Définition 3.271(1).

Démonstration. En utilisant le lemme 8.32, nous considérons $qQ = Q_1$ et $rR = R_1$ avec Q_1 et R_1 primitifs dans $A[X]$. Avec ces éléments nous avons

$$R_1Q_1 = rqPQ = qrP. \tag{8.82}$$

EQooMGXYooIAFBgx

À priori q et p sont dans $\mathbb{K}$. Nous allons prouver que $qr = 1$ … pas tout à fait. Nous allons prouver que qr est inversible. Ensuite il faudra choisir les q et r un peu autrement.

(1) $qr \in A$ Posons $P = \sum_i a_iX^i$ ainsi que $qr = s/t$ avec $s, t \in A$. Nous supposons que s/t est une fraction irréductible. L'équation (8.82) nous dit que le polynôme qrP est R_1Q_1 et donc à coefficients dans A. Pour chaque i, il existe donc $b_i \in A$ tel que

$$\frac{sa_i}{t} = b_i, \tag{8.83}$$

ou encore $sa_i = tb_i$. Donc nous avons $t \mid sa_i$ pour tout i. Vu que la fraction $\operatorname{pgcd}(t, s) = 1$, le lemme de Gauss 3.201 nous indique que t divise a_i. Donc si $\delta \in \operatorname{pgcd}(\{a_i\}_{i=1,\dots,n})$, alors $t \mid \delta$. Vu que P est primitif, δ est inversible, et donc t l'est aussi. Nous avons alors le calcul

$$\frac{s}{t} = \frac{st^{-1}}{tt^{-1}} = st^{-1} \in A. \tag{8.84}$$

Nous avons prouvé que $qr \in A$.

(2) qr **est inversible**

Comme qr est dans A nous pouvons l'utiliser dans le lemme 3.27. Nous savons que $c(P)$ est inversible, disons $c(P) = u$. Nous avons donc, en utilisant le lemme 3.275,

$$qru = qr\,c(P) = u\,c(qrP) = u\,c(Q_1R_1) = uv\,c(Q_1)c(R_1) \in A^\times \tag{8.85}$$

pour un certain inversible $v \in A^\times$. Donc qru est inversible et comme u est inversible, qr est inversible.

(3) **Conclusion**

Nous avions $P = QR$, et nous avions posé $qQ = Q_1$, $rR = R_1$. Maintenant, en posant $u = (qr)^{-1}$ nous avons

$$(uqQ)(rR) = uqrQR = P. \tag{8.86}$$

En même temps, $uqQ = uQ_1 \in A[X]$ et $rR = R_1 \in A[X]$. Donc les polynômes qui satisfont la demande sont uqQ et rR.

□

THOooJESZooNqScLF

Théorème 8.34 ([72])**.**
Soient un anneau factoriel A et son corps des fractions $\mathbb{K}$. Les irréductibles[15] *dans $A[X]$ sont :*

(1) les polynômes de degré zéro dont l'unique coefficient est un élément irréductible de A (polynômes constants),

ITEMooVKOOooDeGYYz

(2) les polynômes de $A[X]$ qui sont de degré $\geqslant 1$, primitifs dans $A[X]$ et irréductibles dans $\mathbb{K}[X]$.

Démonstration. Un polynôme est soit de degré zéro soit de degré $\geqslant 1$.

(1) **Degré zéro, $\Rightarrow$**

Soit un polynôme irréductible[16] $P \in \mathcal{P}_0(A)$.

Si nous notons $a \in A$ l'unique coefficient de P, nous devons prouver que a est irréductible dans A.

(1a) a **n'est pas inversible** Si a était inversible dans A, alors nous pourrions considérer le polynôme $Q \in \mathcal{P}_0(A)$ dont le coefficient est a^{-1}. Nous aurions alors $PQ = U$ où $U \in \mathcal{P}(A)$ est le polynôme dont le coefficient est $1 \in A$.

Ce U étant le neutre pour la multiplication dans $\mathcal{P}(A)$, le polynôme P est inversible, ce qui est contraire à l'hypothèse.

(1b) a **n'est pas produit de deux non inversibles** Même jeu : si $a = xy$ avec x et y non inversibles, alors en prenant les polynômes correspondants, P est produit de deux non inversibles, le polynôme P serait produit de deux non inversibles, et donc pas irréductible dans $\mathcal{P}(A)$.

[15] Définition 3.14.
[16] Cette notation $\mathcal{P}$ de (3.383) devrait être utilisée plus souvent ; dans le meilleur des mondes, on n'utiliserait jamais $A[X]$.

(2) **Degré zéro, $\Leftarrow$**

Si a est irréductible dans A, le polynôme P de coefficient a est irréductible dans $\mathcal{P}(A)$. Même principe de preuve que le point précédent.

(3) **Degré $n \geqslant 1$, $\Rightarrow$**

Soit $P \in \mathcal{P}_n(A)$ irréductible dans $\mathcal{P}(A)$. Nous devons démontrer que P est dans le cas (2). Nous écrivons $P = c(P)P_1$ avec P_1 primitif. Vu que P n'est pas produit de deux non inversibles et que P_1 n'est pas inversible, le polynôme $c(P) \in \mathcal{P}_0(A)$ est inversible[17], et donc $c(P)$ est inversible dans A. Cela démontre déjà que P est primitif.

Pour voir que P est irréductible dans $\mathcal{P}(\mathbb{K})$, nous supposons avoir une égalité $P = QR$ avec $Q, R \in \mathcal{P}(\mathbb{K})$. Par le lemme 8.33, il existe $q, r \in \mathbb{K}$ tels que

$$P = (qQ)(rR) \tag{8.87}$$

avec $qQ, rR \in \mathcal{P}(A)$. Vu que P est irréductible dans $\mathcal{P}(A)$, soit qQ soit rR doit être inversible dans $\mathcal{P}(A)$. Supposons que ce soit qQ. Nous avons donc $qQ \in A^\times$ (qui serait mieux écrit $qQ \in \mathcal{P}_0(A^\times)$), et donc $Q \in \mathcal{P}(\mathbb{K})^\times$.

En résumé nous avons prouvé que si $P = QR$ (dans $\mathcal{P}(\mathbb{K})$), alors soit Q soit R était dans $\mathcal{P}(\mathbb{K})^\times$.

(4) **Degré $n \geqslant 1$, $\Leftarrow$**

Nous supposons que $P \in \mathcal{P}_n(A)$ vérifie la condition (2), et nous montrons qu'il est irréductible dans $\mathcal{P}(A)$. Les polynômes non constants ne sont jamais inversibles, donc pour cette partie-là de la définition d'irréductibilité on est bon.

Supposons que $P = QR$ avec $Q, R \in \mathcal{P}(A) \subset \mathcal{P}(\mathbb{K})$. Comme P est irréductible dans $\mathcal{P}(\mathbb{K})$, un des deux Q ou R est inversible dans $\mathcal{P}(\mathbb{K})$. Disons que Q le soit. Donc $Q \in \mathcal{P}(\mathbb{K})^\times$, et nous notons $q \in \mathbb{K}^\times$ l'unique coefficient de Q. Nous avons donc

$$P = qR. \tag{8.88}$$ EQooQUMSooFGIGxE

Comme, dès le début, on avait dit $Q \in \mathcal{P}(A)$, nous avons en réalité $q \in A$. Nous pouvons donc prendre le contenu de (8.88) en appliquant le lemme 3.27 : $c(P) = q\,c(R)$. Nous savons que $c(P)$ est inversible dans A ; nous multiplions par $c(P)^{-1}$:

$$1 = qc(R)c(P)^{-1}. \tag{8.89}$$

Nous voyons que $c(R)c(P)^{-1}$ est un inverse de q dans A. Donc P est irréductible dans $\mathcal{P}(A)$.

□ THOooVZUBooNSvcBr

Théorème 8.35 ([72]).
Si A est un anneau factoriel, l'anneau des polynômes $\mathcal{P}(A)$ est factoriel.

Démonstration. Si $P \in \mathcal{P}(A)$, nous devons prouver l'existence et l'unicité d'un décomposition de P en irréductibles.

Existence

Nous y allons par récurrence sur le degré de P.

(1) **Si $\deg(P) = 0$** L'unique coefficient de P est un élément de A, et se décompose en irréductibles parce que A est factoriel.

(2) **Si $\deg(P) = n + 1$** Nous supposons que l'existence est prouvée pour tout $k \leqslant n$. Nous écrivons $P = c(P)P_1^{(0)}$ avec P primitif dans $\mathcal{P}(A)$. Il y a deux possibilités : soit $c(P)$ est inversible, soit non. Si $c(P)$ est inversible, alors P est primitif et nous posons $P_1 = P$ et $c_1 = 1$. Si $c(P)$ n'est pas inversible, alors nous posons $c_1 = c(P)$ et $P_1 = P_1^{(0)}$. Dans les deux cas nous avons

$$P = c_1 P_1 \tag{8.90}$$

où P_1 est primitif et c_1 est soit 1 soit non inversible. Si $c_1 = 1$, il n'y a rien à faire avec lui. Sinon, il est non inversible et non nul dans A qui est factoriel. Nous avons donc une décomposition en irréductibles $c_1 = p_1 \dots p_k$. Dans le cas $c_1 = 1$, nous avons $p_1 = 1$ et c'est tout.

[17] On note de la même manière le polynôme constant $c(P)$ et l'élément $c(P)$ dans A, parce qu'on a beau détester les abus de notations, il y a des limites.

En ce qui concerne P_1, il y a deux possibilités : soit il est irréductible dans $\mathcal{P}(\mathbb{K})$ soit pas. Si il est irréductible dans $\mathcal{P}(\mathbb{K})$ alors il est à fortiori irréductible dans $\mathcal{P}(A)$ et

$$P = p_1 \dots p_k P_1 \tag{8.91}$$

est une décomposition de P en irréductibles dans $\mathcal{P}(A)$.

Et si P_1 n'est pas irréductible ? C'est qu'il existe deux non inversibles $Q, R \in \mathcal{P}(\mathbb{K})$ tels que $P = QR$. Le lemme 8.33 permet d'écrire alors

$$P_1 = QR = Q_1 R_1 \tag{8.92}$$

avec $Q_1, R_1 \in \mathcal{P}(A)$. Notons que ni P_1 ni R_1 ne sont des constantes : les constantes sont inversibles dans $\mathcal{P}(\mathbb{K})$. Et comme la construction du lemme montre que $\deg(Q_1) = \deg(Q)$ et $\deg(R_1) = \deg(R)$, les polynômes Q_1 et R_1 sont non constants dans $\mathcal{P}(A)$. Nous avons donc $\deg(Q_1) < n+1$ et $\deg(R_1) < n+1$.

L'hypothèse de récurrence fonctionne pour les polynômes Q_1 et R_1 dans $\mathcal{P}(A)$. Nous avons donc des polynômes irréductibles $S_1, \dots S_l$ tels que

$$P_1 = Q_1 R_1 = S_1 \dots S_l. \tag{8.93}$$

Au final, nous avons la décomposition[18]

$$P = p_1 \dots p_k S_1 \dots S_l. \tag{8.94}$$

Unicité

Soient $P = p_1 \dots p_k S_1 \dots S_m = q_1 \dots q_l T_1 \dots T_n$ deux décompositions de P en irréductibles de A. Les p_i et les q_i sont les polynômes de degré zéro (donc dans A) et les S_i, T_j sont ceux de degré strictement positifs.

(1) **Pour les p_i et q_j**

Comme les polynômes S_i et T_j sont irréductibles leurs contenus sont inversibles, et en utilisant les lemmes 3.275 et 3.27, l'égalité

$$c(p_1 \dots p_k S_1 \dots S_m) = c(q_1 \dots q_l T_1 \dots T_n) \tag{8.95}$$

devient

$$p_1 \dots p_k c(S_1 \dots S_m) = q_1 \dots q_l c(T_1 \dots T_n). \tag{8.96}$$

Il existe donc un inversible $u \in A$ tel que $p_1 \dots p_k = u q_1 \dots q_l$. L'élément (uq_1) est irréductible (lemme 3.17) et donc

$$p_1 \dots p_k = (uq_1) q_2 \dots q_l \tag{8.97}$$

sont deux décompositions en irréductibles du même élément dans A. Donc, parce que A est factoriel, nous avons $k = l$ et il existe une permutation σ qui fait que p_i est associé à $q_{\sigma(i)}$.

(2) **Pour les polynômes**

Nous avons $S_1 \dots S_m = T_1 \dots T_m$. Le polynôme S_1 divise le produit $T_1 \dots T_m$. Comme S_1 est irréductible dans $\mathcal{P}(A)$, il est irréductible dans $\mathcal{P}(\mathbb{K})$ par le théorème 8.34.

L'anneau $\mathcal{P}(\mathbb{K})$ est euclidien par 3.266 et donc principal par 3.38. Or dans un anneau principal, les irréductibles sont premiers par 3.93. Tout ça pour dire que S_1 est premier dans $\mathcal{P}(\mathbb{K})$. Donc, comme il divise un produit, il doit diviser un des facteurs. Disons que $S_1 \mid T_i$ dans $\mathcal{P}(\mathbb{K})$.

Il existe $R \in \mathcal{P}(\mathbb{K})$ tel que $S_1 R = T_i$. Comme S_1 est non inversible (irréductible), et T_i est irréductible, R doit être inversible dans $\mathcal{P}(\mathbb{K})$. Il existe $q \in \mathbb{K}^\times$ tel que $T_i = qS_1$.

Comme T_i et S_1 sont irréductibles, ils sont primitifs dans $\mathcal{P}(A)$ (théorème 8.34). Supposons que q s'écrive sous forme irréductible $q = s/t$ avec $s, t \in A$. On note $T_i = \sum_j a_j X^j$ et $S_1 = \sum_j b_j X^j$. Pour tout i nous avons

$$\frac{sb_j}{t} = a_j, \tag{8.98}$$

ou encore $sb_j = ta_j$. Donc t divise sb_j pour tout j. Mais comme t est premier avec s, l'élément t divise b_j pour tout j. Il divise dont le pgcd des a_j qui est inversible parce que T_i est primitif. Bref, t est inversible dans A. Nous avons donc

$$q = \frac{s}{t} = \frac{st^{-1}}{tt^{-1}} = st^{-1} \in A. \tag{8.99}$$

[18] Ici [129] utilise le théorème 8.34. Certes, il présente sa récurrence de façon un peu différente, mais j'espère n'avoir pas loupé une étape. Soyez prudent et écrivez-moi si vous voyez une erreur.

Nous avons donc $T_i = qS_1$ avec $q \in A$. Comme T_i et S_1 sont irréductibles dans $\mathcal{P}(A)$, l'élément q est inversible dans A.

Nous avons fini de montrer que S_1 était associé à un des T_i. L'égalité

$$S_1 \dots S_m = T_1 \dots T_n \tag{8.100}$$

peut être alors récrite

$$S_1 \dots S_m = qT_1 \dots T_{i-1} S_1 T_{i+1} \dots T_n \tag{8.101}$$

Comme A est factoriel, il est intègre, et donc $\mathcal{P}(A)$ est intègre (théorème 3.260). Nous pouvons donc simplifier par S_1 et il reste

$$S_2 \dots S_m = uT_1 \dots T_{i-1} T_{i+1} \dots T_n. \tag{8.102}$$

Par récurrence, nous avons que chacun des S_i est associé à un des T_j.

□

PropqGZXvr

Proposition 8.36 ([129, 195])**.**
Si $\mathbb{K}$ est un corps commutatif, alors l'anneau des polynômes $\mathcal{P}(\mathbb{K})$ est est factoriel[19]*.*

Démonstration. Un corps est un anneau factoriel (proposition 3.210), donc le théorème 8.35 conclut que l'anneau des polynômes sur un corps est factoriel. □

8.3.1 Irréductibilité

Pour rappel, un élément irréductible dans un anneau est la définition 3.14 : non inversible et pas les produits de deux non inversibles.

LEMooTMSUooCWoVHG

Lemme 8.37.
Soit un corps $\mathbb{K}$. Les éléments inversibles dans $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Exemple 8.38.
Si un polynôme $P \in \mathbb{Z}[X]$ n'a que des racines complexes, ça ne l'empêche pas d'être réductible sur $\mathbb{Z}$. La réductibilité ne signifie pas qu'on peut mettre des racines en évidence. Par exemple le polynôme $P = X^4 + 3X^2 + 2$ est réductible sur $\mathbb{Z}$ en

$$P = (X^2 + 1)(X^2 + 2), \tag{8.103}$$

mais n'a pas de racines dans $\mathbb{Z}$. Si on veut réduire plus, il faut sortir de $\mathbb{Z}$.

△

DefCPLSooQaHJKQ

Définition 8.39 (Polynôme scindé)**.**
*Nous disons que $P \in \mathbb{K}[X]$ est **scindé** sur $\mathbb{K}$ si il est produit dans $\mathbb{K}[X]$ de polynômes de degré 1.*

Note : les constantes ne sont donc pas des polynômes scindés.

Proposition 8.40 (Critère d'Eisenstein)**.**
Soit le polynôme $P = \sum_{k=0}^{n} a_n X^n$ dans $\mathbb{Z}[X]$. Nous supposons avoir un nombre premier p tel que

(1) p divise tous les $a_0, \dots, a_{n-1}$,

(2) p ne divise pas a_n,

(3) p^2 ne divise pas a_0.

Alors P est irréductible dans $\mathbb{Q}[X]$.

Si de plus P est primitif au sens du pgcd *(définition 3.271) alors P est irréductible dans $\mathbb{Z}[X]$.*

Démonstration. Nous considérons $\bar{P}$ le polynôme réduit modulo p, c'est-à-dire $\bar{P} \in \mathbb{F}_p[X]$. Étant donné que par hypothèse tous les coefficients sont multiples de p sauf a_n, nous avons $\bar{P} = cX^n$. Supposons par l'absurde que $P = QR$ avec $Q, R \in \mathbb{Q}[X]$. Alors le lemme de Gauss (3.201) impose $P, Q \in \mathbb{Z}[X]$.

Nous avons aussi, au niveau des réductions modulo p que $\bar{Q}\bar{R} = \bar{P}$. Or $\bar{P}$ est un monôme, donc $\bar{Q}$ et $\bar{R}$ doivent également l'être. Donc $\bar{Q} = dX^k$ et $\bar{R} = eX^{n-k}$ et en particulier $\bar{Q}(0) = \bar{R}(0) = 0$, c'est-à-dire que $Q(0)$ et $R(0)$ sont divisibles par p. Cela impliquerait que $a_0 = Q(0)R(0)$ soit divisible par p^2, ce qui est exclu par les hypothèses. Donc P est irréductible.

Supposons de surcroît que P soit primitif au sens du pgcd. Il est donc irréductible et primitif sur $\mathbb{Q}[X]$ et le corolaire 3.290 nous dit alors que P est irréductible sur $\mathbb{Z}[X]$. □

[19] Définition 3.194.

Exemple 8.41.
Soit le polynôme $P = 3X^4 + 15X^2 + 10$. Pour appliquer le critère d'Eisenstein il nous faut un nombre premier p divisant 15 et 10, mais pas 3, et dont le carré ne divise pas 10. On aura vite vu que $p = 5$ fait l'affaire. Le polynôme P est donc irréductible sur $\mathbb{Q}[X]$. △

8.3.2 Idéaux

Soit $P \in \mathbb{K}[X]$ un polynôme. Nous notons (P) l'idéal engendré par P :

$$(P) = \{PR \text{ tel que } R \in \mathbb{K}[X]\}. \tag{8.104}$$ EqDefxMkDtW

Lemme 8.42.
Nous avons

(1) $(P) \subset (Q)$ *si et seulement si* Q *divise* P,

(2) $(P) = (Q)$ *si et seulement si* P *et* Q *sont multiples (non nuls) l'un de l'autre.*

Démonstration. Si $(P) \subset (Q)$, en particulier $P \in (Q)$ et il existe $R \in \mathbb{K}[X]$ tel que $P = QR$, ce qui signifie que Q divise P.

Si les idéaux de P et de Q sont identiques, l'un divise l'autre et l'autre divise l'un. Ils sont donc multiples l'un de l'autre. □

ThoCCHkoU

Théorème 8.43.
Soit $\mathbb{K}$ *un corps commutatif.*

ITEMooLZWMooDRsRwW

(1) L'anneau $\mathbb{K}[X]$ *est euclidien et principal.*

(2) Si I *est un idéal dans* $\mathbb{K}[X]$ *et si* $P \in I$ *est de degré minimal, alors* $(P) = I$.

ITEMooASHKooZqkiCH

(3) De plus si $I \neq \{0\}$, *il existe un unique polynôme unitaire* μ *tel que* $I = (\mu)$.

Démonstration. Le point (1) a déjà été démontré dans le lemme 3.266 via le fait que $\mathbb{K}[X]$ est euclidien. Nous allons cependant donner ici une preuve directe que tous les idéaux de $\mathbb{K}[X]$ sont principaux. Si $I = \{0\}$, le résultat est évident. Nous supposons donc I non nul. Soit P de degré minimum parmi les éléments de I. Évidemment $(P) \subset I$. Nous allons démontrer qu'en réalité $(P) = I$.

Soit $P' \in I$. Par le théorème 3.263 de la division euclidienne[20], il existe Q et R dans $\mathbb{K}[X]$ tels que $P' = PQ + R$ avec $\deg(R) < \deg(P)$. Étant donné que $R = P' - PQ$ nous avons $R \in I$ et par conséquent $R = 0$ parce que P a été choisi de degré minimum dans I. Nous avons donc $P' = PQ$ et $I \subset (P)$.

L'existence d'un polynôme unitaire qui génère I est obtenu en choisissant $\mu = P/a_n$ où a_n est le coefficient du terme de plus haut degré. L'unicité d'un tel polynôme est obtenu par le fait que si μ et μ' génèrent le même idéal, alors ils sont multiples l'un de l'autre, or puisqu'ils sont unitaires, ils sont égaux. □

Nous voyons que n'importe quel polynôme de degré minimum dans un idéal génère l'idéal. Une importante conséquence du théorème 8.43 que nous verrons plus bas est que tout polynôme annulateur d'un endomorphisme est divisé par le polynôme minimal (proposition 10.98).

CorsLGiEN

Corolaire 8.44.
Si $\mathbb{K}$ *est un corps et si* P *est un polynôme irréductible, alors l'ensemble* $\mathbb{L} = \mathbb{K}[X]/(P)$ *est un corps. De plus* $\mathbb{L}$ *est un espace vectoriel de dimension* $\deg(P)$.

Démonstration. En effet $\mathbb{K}[X]$ est un anneau principal par le théorème 8.43, par conséquent la proposition 3.128(2) déduit que $\mathbb{K}[X]/(P)$ est un corps.

Une base de $\mathbb{L}$ est donnée par les projections de $1, X, X^2, \dots, X^{n-1}$. En effet ces éléments forment une famille libre parce que si $\sum_{k=0}^{n-1} a_k \bar{X}^n = 0$ alors un représentant de cette classe doit être de la forme SP dans $\mathbb{K}[X]$, c'est-à-dire

$$\sum_{k=0}^{n-1} a_k X^k = SP, \tag{8.105}$$

ce qui n'est possible que si $S = 0$ et $a_k = 0$. D'autre part c'est un système générateur. En effet si $P = X^n + Q$ avec $\deg(Q) = n - 1$ alors

$$\bar{X}^{n+l} = \bar{X}^n \bar{X}^l = (\bar{P} - \bar{Q})\bar{X}^l = \bar{Q}\bar{X}^l. \tag{8.106}$$

Nous avons donc exprimé $\bar{X}^{n+l}$ comme une somme de termes de degré $n+l-1$. Par récurrence nous pouvons exprimer tout $\bar{X}^{n+l}$ comme combinaison d'éléments de degré plus petit que n. □

[20] Ici $\mathbb{K}$ est un corps et donc l'hypothèse d'inversibilité est automatiquement vérifiée.

8.45.
Ce corolaire prendra une nouvelle jeunesse lorsque nous parlerons de polynômes d'endomorphismes, en particulier la proposition 10.108 va donner des précisions.

LEMooGRIMooPxCXAZ

Lemme 8.46 ([196]).
Soit un isomorphisme de corps $\tau\colon \mathbb{K} \to \mathbb{K}'$. Alors

(1) L'application étendue

$$\begin{aligned}\tau\colon \mathbb{K}[X] &\to \mathbb{K}'[X]\\ \sum_i a_i X^i &\mapsto \sum_i \tau(a_i)X^i\end{aligned} \tag{8.107}$$

est un isomorphisme d'anneaux ;

(2) pour tout $P \in \mathbb{K}[X]$, le passage au quotient

$$\begin{aligned}\phi_\tau\colon \mathbb{K}[X]/(P) &\to \mathbb{K}'[X]/\big(\tau(P)\big)\\ \bar{Q} &\mapsto \overline{\tau(Q)}\end{aligned} \tag{8.108}$$

est un isomorphisme d'anneaux (et d'abord est bien définie).

Démonstration. Nous n'allons pas faire explicitement toutes les vérifications, mais tout de même les principales. Montrons que τ respecte le produit entre $\mathbb{K}[X]$ et $\mathbb{K}'[X]$. Nous rappelons que ce produit est défini par la formule (3.386). En notant P_i les coefficients de P et Q_i ceux de Q et en remarquant que la définition de τ est essentiellement que $\tau(P)_i = \tau(P_i)$, nous avons :

$$\tau(PQ) = \tau\Big(\sum_k \big(\sum_{l=0}^{k} P_l Q_{k-l}\big)X^k\Big) \tag{8.109a}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P_l Q_{k-l}) \tag{8.109b}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P_l)\tau(Q_{k-l}) \tag{8.109c}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P)_l \tau(Q)_{k-l} \tag{8.109d}$$
$$= \sum_i \big(\tau(P)_i X^i\big) \sum_j \big(\tau(Q)_j X^j\big) \tag{8.109e}$$
$$= \tau(P)\tau(Q). \tag{8.109f}$$

Passons à l'isomorphisme d'anneaux donné par ϕ_τ.

(1) **Bien définie**
Si $\bar{Q}_1 = \bar{Q}_2$ alors $Q_2 = Q_1 + RP$ pour un certain $R \in \mathbb{K}[X]$. Dans ce cas,

$$\phi_\tau(Q_2) = \overline{\tau(Q_2)} = \overline{\tau(Q_1) + \tau(RP)} \tag{8.110a}$$
$$= \overline{\tau(Q_1) + \tau(R)\tau(P)} \tag{8.110b}$$
$$= \overline{\tau(Q_1)}. \tag{8.110c}$$

L'application ϕ_τ est donc bien définie.

(2) **Injection**
Si $\phi_\tau(\bar{Q}_1) = \phi_\tau(\bar{Q}_2)$ alors $\overline{\tau(Q_1)} = \overline{\tau(Q_2)}$, ce qui signifie que

$$\tau(Q_1) = \tau(Q_2) + R\,\tau(P) \tag{8.111}$$

pour un certain $R \in \mathbb{K}'[X]$. Puisque $\tau\colon \mathbb{K}[X] \to \mathbb{K}'[X]$ est un isomorphisme, nous pouvons y appliquer τ^{-1} pour trouver :

$$Q_1 = Q_2 + \tau^{-1}(R)P, \tag{8.112}$$

ce qui signifie que $\bar{Q}_1 = \bar{Q}_2$.

(3) **Surjection**

Un élément de $\mathbb{K}'[X]/\big(\tau(P)\big)$ est de la forme $\bar{Q}$ avec $Q \in \mathbb{K}'[X]$. C'est l'image par ϕ_τ de l'élément $\overline{\tau^{-1}(Q)} \in \mathbb{K}[X]/(P)$.

(4) **Morphisme**

Nous vous laissons vérifier que l'application ϕ_τ est un morphisme d'anneaux.

□

8.3.3 Identité de Bézout

ThoBezoutOuGmLB

Théorème 8.47 (Bézout)**.**
Les polynômes $P_1, \dots, P_n$ dans $\mathbb{K}[X]$ sont premiers dans leur ensemble si et seulement si il existe des polynômes $Q_1, \dots, Q_n \in \mathbb{K}[X]$ tels que

$$P_1Q_1 + \cdots + P_nQ_n = 1. \tag{8.113}$$

Démonstration. L'anneau $\mathbb{K}[X]$ est principal (lemme 3.266). La proposition 3.200 s'applique donc. □

Deux polynômes P et Q ne sont donc pas premiers entre eux si il existe des polynômes x et y tels que l'identité de Bézout soit vérifiée :

EqkbbzAj
$$xP + yQ = 0; \tag{8.114}$$

cette dernière pourra être écrite en termes de la matrice de Sylvester, voir sous-section 10.2.6.

LemuALZHn

Lemme 8.48.
Soient $(P_i)_{i=1,\dots,n} \in \mathbb{K}[X]$ des polynômes étrangers deux à deux. Alors les polynômes

$$Q_i = \prod_{j \neq i} P_j \tag{8.115}$$

sont étrangers entre eux[21]*.*

LemzwkYdn

Lemme 8.49 ([197])**.**
Soit $\mathbb{K}$ un corps commutatif et $\mathbb{A} \subset \mathbb{K}$ un sous anneau de $\mathbb{K}$. Alors $\mathbb{A}[X]$, vu comme idéal de $\mathbb{K}[X]$, est un idéal premier.

En d'autres termes, si $\phi \in \mathbb{K}[X]$, et si il existe $Q \in \mathbb{K}[X]$ unitaire tel que $\phi Q \in \mathbb{A}[X]$, alors $\phi \in \mathbb{A}[X]$.

8.3.4 Lemme et théorème de Gauss

ThoLLgIsig

Théorème 8.50 (Théorème de Gauss)**.**
Soient $P, Q, R \in \mathbb{K}[X]$ tels que P soit premier avec Q et divise QR. Alors P divise R.

Démonstration. Étant donné que P est premier avec Q, le théorème de Bézout[22] nous donne $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$. De plus il existe un polynôme S tel que $PS = QR$. En multipliant l'identité de Bézout par R, nous obtenons

$$R = PUR + QVR = PUR + VPS = P(UR + VS), \tag{8.116}$$

ce qui signifie que P divise R. □

Le lemme suivant est une généralisation du lemme de Gauss dans $\mathbb{Z}$ (lemme 3.201).

LemEfdkZw

Lemme 8.51 (Lemme de Gauss[121])**.**
Soient les polynômes unitaires $P, Q \in \mathbb{Q}[X]$. Si $PQ \in \mathbb{Z}[X]$, alors P et Q sont tous deux dans $\mathbb{Z}[X]$.

[21] Et non seulement deux à deux.
[22] théorème 8.47.

Démonstration. Soit $a > 0$ le plus petit entier tel que $aP \in \mathbb{Z}[X]$ (c'est le PPCM des dénominateurs) et de la même façon $b > 0$ le plus petit entier tel que $bQ \in \mathbb{Z}[X]$. On pose $P_1 = aP$ et $Q_1 = bQ$.

Si $ab = 1$, alors $a = b = 1$ et nous avons tout de suite $P, Q \in \mathbb{Z}[X]$. Nous supposons donc $ab > 1$ et nous considérons p, un diviseur premier de ab. Ensuite nous considérons la projection

$$\pi_p \colon \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]. \tag{8.117}$$

Par définition $abPQ = P_1Q_1 \in \mathbb{Z}[X]$; en prenant la projection,

$$\pi_p(P_1)\pi_p(Q_1) = \pi_p(P_1Q_1) = \pi_P(ab)\pi_p(PQ) = 0 \tag{8.118}$$

parce que $\pi_p(ab) = 0$. Étant donné que $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre (théorème 3.260), nous avons soit $\pi_p(P_1) = 0$ soit $\pi_p(Q_1) = 0$. Supposons pour fixer les idées que $\pi_p(P_1) = 0$. Alors $P_1 = pP_2$ pour un certain $P_2 \in \mathbb{Z}[X]$. Par ailleurs P est unitaire et $P_1 = aP$, donc le coefficient de plus haut degré de P_1 est a, et nous concluons que p divise a.

Mettons $a = pa'$. Dans ce cas, $pa'P = P_1 = pP_2$, et donc $a'P = P_2 \in \mathbb{Z}[X]$. Cela contredit la minimalité de a. □

8.3.5 Polynômes sur un corps et pgcd

Nous savons qu'un corps est un anneau intègre (lemme 3.23). De plus l'ensemble des polynômes sur un anneau intègre est lui-même un anneau intègre (théorème 3.260). Donc la notion de pgcd à utiliser dans le cas de $\mathbb{K}[X]$ est celle de la définition 1.113.

LEMooXISOooNAMeVX

Lemme 8.52 (Unicité du pgcd à inversibles près)**.**
Soit un corps commutatif $\mathbb{K}$ et $S \subset \mathbb{K}[X]$.

(1) Si δ_1 et δ_2 sont des pgcd[23] de S, alors $\delta_1 = k\delta_2$ avec $k \in \mathbb{K}$.

ITEMooARLJooOQvBcw

(2) Il existe un unique polynôme unitaire dans $\operatorname{pgcd}(S)$.

Démonstration. Nous savons que δ_1 est un pgcd de S, mais que δ_2 divise S. Donc $\delta_2 \mid \delta_1$. De la même manière, $\delta_1 \mid \delta_2$. Il existe donc $A, B \in \mathbb{K}[X]$ tels que $\delta_1 = A\delta_2$ et $\delta_2 = B\delta_1$. En substituant,

$$\delta_1 = AB\delta_1. \tag{8.119}$$

Mais $\mathbb{K}[X]$ possède la propriété de simplification par la proposition 3.22(3). Donc $AB = 1$. Cela signifie entre autres que A et B sont des inversibles de $\mathbb{K}[X]$.

Or les seuls inversibles dans $\mathbb{K}[X]$ sont les éléments de $\mathbb{K}$; si vous en doutez, pensez que le degré de AB est supérieur ou égal à celui de A.

En ce qui concerne l'existence et l'unicité d'un polynôme unitaire dans $\operatorname{pgcd}(S)$. Existence : si $P = \sum_{k=0}^{n} a_k X^k \in \operatorname{pgcd}(S)$, alors le polynôme P/a_n est unitaire et également dans $\operatorname{pgcd}(S)$. Unicité : supposons que P est unitaire dans $\operatorname{pgcd}(S)$ et que Q est dans $\operatorname{pgcd}(S)$. Il existe $k \in \mathbb{K}$ tel que $Q = kP$. Vu que P est unitaire, Q ne l'est pas. □

NORMooUJDJooWfijxT

8.53.
En général, lorsque nous dirons « le » pgcd d'un ensemble de polynômes, nous parlerons du pgcd unitaire, qui existe et est bien défini par le lemme 8.52. En particulier, si P et Q sont des polynômes, nous notons $\operatorname{pgcd}(P, Q)$ l'unique polynôme unitaire parmi les PGCD de P et Q.

LEMooIAGMooHUQtUs

Lemme 8.54 ([198])**.**
Soit un corps commutatif $\mathbb{K}$, deux polynômes quelconques $A, B \in \mathbb{K}[X]$ et un polynôme unitaire G.

Nous avons $G = \operatorname{pgcd}(A, B)$ si et seulement si les deux conditions suivantes sont satisfaites :

(1) Il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = G$,

(2) G divise A et B.

Démonstration. Une implication dans chaque sens.

(1) $\Rightarrow$

Si G est le pgcd de A et B, il est clair que $G|A$ et $G|B$. Il reste donc à montrer l'existence des polynômes U et V vérifiant $AU + BV = G$. Puisque G divise A et B, il existe des polynômes A_1, B_1 tels que $A = GA_1$ et $B = GB_1$.

[23] Définition 1.113.

Nous montrons que les polynômes A_1 et B_1 sont premiers entre eux. S'ils ont un diviseur commun D, alors GD est un diviseur commun à A et B. Or, G est le pgcd de A et B donc $GD|G$; D ne peut être qu'un polynôme constant (c'est-à-dire un élément de $\mathbb{K}$). Mais comme G est unitaire, le coefficient du terme de plus haut degré de GD doit être 1. Donc $D = 1$. L'élément 1 est l'unique diviseur commun de A_1 et B_1 ; donc A_1 et B_1 sont bien premiers entre eux.

D'après le théorème de Bézout 8.47, il existe donc U et V tels que $A_1U + B_1V = 1$. En multipliant par G, nous obtenons l'égalité voulue : $AU + BV = G$.

(2) $\Leftarrow$

Si G vérifie les deux conditions, montrons que G est le pgcd de A et B. Nous savons déjà (par hypothèse) que G divise A et B, il reste à montrer que tous les diviseurs commun à A et B divisent aussi G. Soit donc D un diviseur commun à A et B : il existe A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$. Nous savons que $G = AU + BV$ donc $G = D(A_1U + B_1V)$, et $D|G$.

Par définition, G est bien le pgcd de A et B.

□

Notons qu'en supprimant la condition d'unitarité de G, le résultat tient presque : il suffit de remplacer partout « le pgcd » par « un pgcd ».

LEMooVFBUooLoaOGr

Lemme 8.55 ([199])**.**
Soit un corps $\mathbb{K}$. Soient des polynôme P et Q dans $\mathbb{K}[X]$. Si S est un diviseur commun de P et Q, alors

ITEMooZTCCooPBqzNE

(1) S divise $\operatorname{pgcd}(P, Q)$

ITEMooIIINooUZVtAb

(2) $\deg(S) \leqslant \deg\big(\operatorname{pgcd}(P, Q)\big)$.

Démonstration. Il faut bien relire la définition 1.113 du pgcd ; en particulier le point (2) dit exactement notre point (1).

Étant donné que S divise $\operatorname{pgcd}(P, Q)$ nous avons automatiquement que le degré de S est plus petit que celui de $\operatorname{pgcd}(P, Q)$. □

LEMooGNAMooXRpgBn

Lemme 8.56 ([198])**.**
Soient deux polynômes A, B premiers entre eux. Si le polynôme P est divisible par A et par B alors P est divisible par AB.

Démonstration. Comme $A \mid P$, il existe $Q_1 \in \mathbb{K}[X]$ tel que $P = AQ_1$. Mais B divise $P = AQ_1$ alors que B est premier avec A ; donc d'après le théorème de Gauss 8.50 : $B|Q_1$.

Il existe donc $Q_2 \in \mathbb{K}[X]$ tel que $Q_1 = BQ_2$. On a donc $P = ABQ_2$: P est bien divisible par AB. □

LemUELTuwK

Lemme 8.57 ([198])**.**
Quelques propriétés du PGCD[24] dans les polynômes. Soient des polynômes $P, Q, R \in \mathbb{K}[X]$.

ITEMooBPOZooYeFGjl

(1) Nous avons l'égalité[25]

$$\operatorname{pgcd}(P, PQ + R) = \operatorname{pgcd}(P, R). \tag{8.120}$$

ITEMooUVGRooNSGDZn

(2) Si Q et R sont premiers entre eux,

$$\operatorname{pgcd}(P, QR) = \operatorname{pgcd}(P, Q)\operatorname{pgcd}(P, R) \tag{8.121}$$

ITEMooYXAHooXibkgV

(3) Si P et Q sont premiers entre eux,

$$\operatorname{pgcd}(P, QR) = \operatorname{pgcd}(P, R) \tag{8.122}$$

Démonstration. Dans la suite si A et B sont des polynômes, nous dirons « les diviseurs de $\{A, B\}$ » pour parler des diviseurs communs de A et B.

[24] Définition 1.113.
[25] Notez l'analogie avec le lemme 3.149.

(1) **Pour (1)**

Nous montrons que $\{P, PQ+R\}$ a les mêmes diviseurs que $\{P, R\}$.

D'une part, si $A \mid \{P, PQ+R\}$, alors il existe des polynômes B_1 et B_2 tels que $P = AB_1$ et $PQ+R = AB_2$. Donc

$$R = AB_2 - PQ = AB_2 - AB_1Q = A(B_2 - B_1Q), \tag{8.123}$$

et nous concluons que A divise R.

D'autre part, si $A \mid \{P, R\}$ alors il existe des polynômes B_1 et B_2 tels que $P = AB_1$ et $R = AB_2$. Donc

$$PQ + R = AB_1Q + AB_2 = A(B_1Q + B_2), \tag{8.124}$$

et A divise $PQ + R$.

Conclusion : les paires $\{P, PQ+R\}$ et $\{P, R\}$ ont même ensemble de diviseurs, et donc même pgcd.

(2) **Pour (2)**

Nous avons trois polynômes P, Q, R et nous savons que Q et R sont premiers entre eux. Nous notons : $G_1 = \text{pgcd}(P, Q)$ et $G_2 = \text{pgcd}(P, R)$. Il faut montrer que G_1G_2 est le pgcd de P et QR ; pour cela nous allons utiliser le lemme 8.54.

(2a) **$\exists U, V$ tels que $G_1G_2 = PU + QRV$**

Puisque $G_1 = \text{pgcd}(P, Q)$, il existe U_1 et V_1 tels que $G_1 = PU_1 + QV_1$ (lemme 8.54). On a de même : $G_2 = PU_2 + RV_2$. En prenant le produit :

$$G_1G_2 = (PU_1 + QV_1)(PU_2 + RV_2) = P(PU_1U_2 + RU_1V_2 + QV_1V_2) + QR(V_1V_2). \tag{8.125}$$

Donc c'est bon pour ce point.

(2b) **G_1 et G_2 sont premiers entre eux**

Si D est un diviseur commun à G_1 et G_2, alors D divise Q et R qui sont premiers entre eux ; D ne peut être qu'un polynôme constant. Tous les diviseurs communs de G_1 et G_2 sont dans $\mathbb{K}$. Mais le pgcd est par définition un diviseur commun unitaire, donc $\text{pgcd}(G_1, G_2) = 1$. Cela signifie que G_1 et G_2 sont premiers entre eux (définition 3.52).

(2c) $G_1G_2 \mid QR$ En effet : $G_1|Q$ et $G_2|R$ donc $G_1G_2|QR$.

(2d) $G_1G_2 \mid P$ Le polynôme P est divisible par G_1 et par G_2, et de plus G_1 et G_2 sont premiers entre eux. Donc le lemme 8.56 conclut que P est divisible par G_1G_2.

(3) **(3)**

Supposons d'abord que $A \in \mathbb{K}[X]$ divise P et QR. Le théorème de Bézout 8.47 assure l'existence de polynômes U et V tels que $PU + QV = 1$. Ensuite l'hypothèse de division nous donne des polynômes B_1 et B_2 tels que $P = AB_1$ et $QR = AB_2$. Nous avons :

$$1 = PU + QV = AB_1U + QV. \tag{8.126}$$

Cela prouve que A est premier avec Q grâce encore à Bézout, mais dans l'autre sens. Donc A est premier avec Q et $A \mid QR$. Donc $A|R$ par le théorème de Gauss 8.50.

Dans l'autre sens, si $A|R$ alors on a évidemment : $A|QR$.

Les diviseurs de $\{P, QR\}$ sont exactement les diviseurs de $\{P, R\}$. En conséquence, nous concluons que les paires $\{P, QR\}$ et $\{P, R\}$ ont le même pgcd.

□

8.4 Extension de corps

SECooLQVLemmeCaFR

Lemme 8.58.
Soit $\mathbb{L}$ un corps[26] *fini et $\mathbb{K}$ un sous-corps de $\mathbb{L}$. Alors il existe $s \in \mathbb{N}$ tel que*

EqUgqlJQ

$$\text{Card}(\mathbb{L}) = \text{Card}(\mathbb{K})^s. \tag{8.127}$$

Démonstration. Le corps $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie. Si s est la dimension alors nous avons la formule (8.127) parce que chaque élément de $\mathbb{L}$ est un s-uple d'éléments de $\mathbb{K}$. □

[26] Définition 1.213.

DEFooFLJJooGJYDOe

Définition 8.59 ([200]).
Soit $\mathbb{K}$ un corps commutatif. Une ***extension*** *de $\mathbb{K}$ est un couple $(\mathbb{L}, j)$ où $\mathbb{L}$ est un corps et $j\colon \mathbb{K} \to \mathbb{L}$ est un morphisme de corps.*

Nous identifions le plus souvent $\mathbb{K}$ avec $j(\mathbb{K}) \subset \mathbb{L}$, mais il faut savoir que le corps $\mathbb{L}$ étendant $\mathbb{K}$ n'est pas toujours un sur-corps de $\mathbb{K}$. En particulier, l'ensemble $\mathbb{L}$ peut ne pas être une extension de l'ensemble $\mathbb{K}$.

LemooOLIIooXzdppM

Lemme-Définition 8.60.
Si $(\mathbb{L}, i)$ est une extension de $\mathbb{K}$, alors $\mathbb{L}$ devient un espace vectoriel sur $\mathbb{K}$ si nous posons

$$\lambda \cdot x = i(\lambda)x \tag{8.128}$$

pour tout $\lambda \in \mathbb{K}$ et $x \in \mathbb{L}$. La multiplication du membre de droite est celle du corps $\mathbb{L}$.

DefUYiyieu

Définition 8.61.
Le ***degré*** *de $\mathbb{L}$ est la dimension de cet espace vectoriel. Il est noté $[\mathbb{L} : \mathbb{K}]$; notons qu'il peut être infini.*

PROPooCFGUooCQqWZd

Proposition 8.62.
Le corps $\mathbb{C}$ est une extension de $\mathbb{R}$ et son degré[27] *est $[\mathbb{C} : \mathbb{R}] = 2$.*

PROPooEGSGWBSMpTF

Proposition 8.63 (Composition des degrés[201]).
Si $\mathbb{L}_2$ est une extension de $\mathbb{L}_1$ qui est elle-même une extension de $\mathbb{K}$, alors $\mathbb{L}_2$ est une extension de $\mathbb{K}$ et on a :

EQooOLLQooFdYtnb

$$[\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_2 : \mathbb{L}_1][\mathbb{L}_1 : \mathbb{K}]. \tag{8.129}$$

Dans ce cas, si $\{v_i\}_{i\in I}$ est une $\mathbb{K}$-base de $\mathbb{L}_1$ et si $\{w_\alpha\}_{\alpha\in A}$ est une $\mathbb{L}_1$-base de $\mathbb{L}_2$ alors $\{v_i w_\alpha\}_{\substack{i\in I\\ \alpha\in A}}$ est une $\mathbb{K}$-base de $\mathbb{L}_2$.

Notons que la formule (8.129) n'est pas très instructive dans le cas des extensions non finies. La seconde partie, sur les bases, est en réalité nettement plus intéressante.

Démonstration. Soit $a \in \mathbb{L}_2$. Puisque les w_α forment une $\mathbb{L}_1$-base de $\mathbb{L}_2$, il existe des $a_\alpha \in \mathbb{L}_1$ tels que

$$a = \sum_\alpha a_\alpha w_\alpha. \tag{8.130}$$

Mais les v_i forment une $\mathbb{K}$-base de $\mathbb{L}_1$, donc chacun des a_α peut être décomposé comme $a_\alpha = \sum_i a_{\alpha i} v_i w_\alpha$. Donc :

$$a = \sum_{\alpha i} a_{\alpha i} v_i w_\alpha, \tag{8.131}$$

qui donne une décomposition de a en éléments de $\{v_i w_\alpha\}$ à coefficients dans $\mathbb{K}$. La partie proposée est donc génératrice.

Pour prouver qu'elle est également libre, nous supposons avoir des éléments $a_{\alpha i} \in \mathbb{K}$ tels que

$$\sum_{\alpha i} a_{\alpha i} v_i w_\alpha = 0. \tag{8.132}$$

En récrivant sous la forme

$$\sum_\alpha \Big(\sum_i a_{\alpha i} v_i\Big) w_\alpha = 0, \tag{8.133}$$

nous reconnaissons une combinaison linéaire nulle des w_α à coefficients dans $\mathbb{L}_1$. Les coefficients sont donc nuls : $\sum_i a_{\alpha i} v_i = 0$. C'est une combinaison linéaire nulle des v_i à coefficients dans $\mathbb{K}$. Comme les v_i forment une base, les coefficients sont nuls : $a_{\alpha i} = 0$. □

8.4.1 Extension et polynôme minimal

DefCVMooFGSAgL

Lemme-Définition 8.64 (Polynôme minimal).
Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $a \in \mathbb{L}$. Nous considérons la partie

$$I_a = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\} \tag{8.134}$$

que nous supposons non réduite à $\{0\}$[28]

[27] Définition 8.61.

[28] La non trivialité de I_a est une vraie hypothèse. En effet si nous prenons $\mathbb{K} = \mathbb{Q}$ et l'extension $\mathbb{L} = \mathbb{R}$, alors il suffit de prendre un réel a non algébrique sur $\mathbb{Q}$ pour que I_a soit réduit au seul polynôme identiquement nul.

ITEMooUNLCooIfYZry
(1) *La partie I_a est un idéal dans $\mathbb{K}[X]$,*

ITEMooDCDRooPDnnbu
(2) *la partie I_a est un idéal principal dans $\mathbb{K}[X]$,*

ITEMooXFYQooTuMzIu
(3) *l'idéal I_a possède un unique générateur unitaire.*

*Cet unique générateur unitaire est le **polynôme minimal** de a sur $\mathbb{K}$.*

Démonstration. En plusieurs parties.

(1) **Pour (1)** Soit $P \in I_a$: $P(a) = 0$. Si $Q \in \mathbb{K}[X]$ alors la proposition 3.232 nous indique que

$$(PQ)(a) = P(a)Q(a) = 0. \tag{8.135}$$

Donc $PQ \in I_a$. Comme de plus I_a est clairement vectoriel, I_a est un idéal.

(2) **Pour (2)** Nous savons par le théorème 8.43 que $\mathbb{K}[X]$ est un anneau principal. En particulier, tous ses idéaux sont principaux, c'est dans la définition 3.37 d'un anneau principal.

(3) **Pour (3)** Le théorème 8.43(3) nous informe alors que I_a possède un unique générateur unitaire.

□

Si nous avons un corps et un élément dans une extension du corps, il n'est pas autorisé de dire « soit le polynôme minimal de cet élément dans le premier corps » parce qu'il n'existe peut-être pas de polynôme annulateur.

8.65.
Dans le cas des opérateurs sur un espace de dimension finie (par exemple les matrices), il existe toujours un polynôme minimal, comme nous le verrons dans le lemme 10.94.

Exemple 8.66.
Le polynôme minimal dépend du corps sur lequel on le considère. Par exemple le nombre imaginaire pur i accepte $X - i$ comme polynôme minimal sur $\mathbb{C}$ et $X^2 + 1$ sur $\mathbb{Q}[X]$. △

PropRARooKavaIT
Proposition 8.67 ([1]).
Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $a \in \mathbb{L}$ dont le polynôme minimal sur $\mathbb{K}$ est $\mu_a \in \mathbb{K}[X]$. Alors

ItemDOQooYpLvXri
(1) *le polynôme μ_a est irréductible*[29] *sur $\mathbb{K}$;*

(2) *Le polynôme μ_a est premier*[30] *avec tout polynôme de $\mathbb{K}[X]$ non annulateur de a.*

Démonstration. Une chose à la fois.

(1) D'abord le polynôme μ_a n'est pas inversible parce que seuls les éléments de $\mathbb{K}$ (ceux de degré zéro) peuvent être inversibles[31]. Mais ces polynômes sont constants et ne peuvent donc pas être des polynômes annulateurs de quoi que ce soit.

Ensuite, supposons la décomposition $\mu_a = PQ$ avec $P, Q \in \mathbb{K}[X]$. En évaluant cette égalité en a nous avons

$$0 = P(a)Q(a). \tag{8.136}$$

Puisque nous sommes sur un corps, nous avons la règle du produit nul[32] et nous déduisons que soit $P(a)$ soit $Q(a)$ est nul, ou les deux. Pour fixer les idées, nous supposons $P(a) = 0$.

Dans ce cas, P fait partie de l'idéal annulateur de a, lequel idéal est engendré par μ_a. Donc il existe $S \in \mathbb{K}[X]$ tel que $P = S\mu_a$. En récrivant $\mu_a = PQ$ avec cela nous avons :

$$\mu_a = S\mu_a Q \tag{8.137}$$

ou encore : $SQ = 1$, ce qui signifie que S et Q sont dans $\mathbb{K}$ et inversibles.

Nous concluons que μ_a ne peut pas être écrit sous forme de produit de deux non inversibles.

[29] Définition 3.14.
[30] Définition 3.267.
[31] Et d'ailleurs, le sont, mais ce n'est pas important ici.
[32] Parce qu'un corps est un anneau intègre par le lemme 3.23 et qu'un anneau intègre est justement un anneau sur lequel nous avons la règle du produit nul, voir la définition 3.22.

(2) Soit Q un polynôme non annulateur de a. Soit aussi un diviseur commun P de Q et μ_a dans $\mathbb{K}[X]$. Nous devons prouver que P est un inversible, c'est-à-dire un élément de $\mathbb{K}$ (le fait que P ne soit pas le polynôme nul est évident). Nous avons $\mu_a = PR_1$ et $Q = PR_2$ pour certains polynômes $R_1, R_2 \in \mathbb{K}[X]$. Puisque μ_a est irréductible par (1), il n'est pas produit de deux non inversibles. En d'autres termes, soit P soit R_1 est inversible. Si P n'est pas inversible, alors R_1 est inversible ; disons $R_1 = k \in \mathbb{K}$. Alors

$$0 = \mu_a(a) = P(a)k, \tag{8.138}$$

donc $P(a) = 0$. Mais alors

$$Q(a) = P(a)R_2(a) = 0, \tag{8.139}$$

ce qui est contraire à l'hypothèse selon laquelle Q n'était pas annulateur de a.

Nous retenons donc que P est inversible, ce qu'il fallait montrer.

□

DEFooJQQYooMKqWov

Définition 8.68.
*Deux éléments α et β dans $\mathbb{L}$ sont dit **conjugués** s'ils ont même polynôme minimal*[33]*. Par exemple i et $-i$ sont conjugués dans $\mathbb{C}$ vu comme extension de $\mathbb{Q}$.*

8.4.2 Extensions algébriques et éléments transcendants

8.4.2.1 Éléments algébriques et transcendants

8.69.
Mise en garde pour les gens qui aiment avoir des notations précises. Dans les lemmes 8.71 et 8.73 ainsi que dans la définition 8.75 il faut garder en tête qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est une application $\iota\colon \mathbb{K} \to \mathbb{L}$. Il n'est pas spécialement vrai que $\mathbb{K}$ est un sous-sensemble de $\mathbb{L}$.

Pour être rigoureux, beaucoup d'énoncés devraient contenir plus d'applications ι un peu partout.

DEFooBBYGooWoOloR

Définition 8.70.
L'ensemble $A[X]$ devient un $\mathbb{K}$-espace vectoriel avec la définition

$$(\lambda P)_k = \lambda P_k. \tag{8.140}$$

Voici une définition d'un élément algébrique sur un corps. Une caractérisation plus « pratique » sera donnée dans le lemme 8.73.

LEMooLVPLooEkWYDN

Lemme-Définition 8.71 (Élément algébrique et transcendant[202])**.**
Soit une extension $\mathbb{L}$ de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned} \varphi\colon \mathbb{K}[X] &\to \mathbb{L} \\ P &\mapsto P(\alpha). \end{aligned} \tag{8.141}$$

Alors

(1) L'application φ est un morphisme d'anneaux[34]*.*

(2) L'application φ est un morphisme de $\mathbb{K}$-espace vectoriel.

*Si φ est injective, nous disons que α est **transcendant**. Sinon, nous disons qu'il est **algébrique**.*

Démonstration. Le fait que φ soit un morphisme d'anneaux est le lemme 3.232 déjà prouvé.

Pour le morphisme de $\mathbb{K}$-espace vectoriel, il faut seulement ajouter le calcul

$$\varphi(\lambda P) = (\lambda P)(\alpha) = \lambda P(\alpha) = \lambda\varphi(P). \tag{8.142}$$

Notons la justification suivante qui n'est pas tout à fait triviale :

$$(\lambda P)(\alpha) = \sum_k (\lambda P)_k \alpha^k = \sum_k \lambda P_k \alpha^k = \lambda P(\alpha) \tag{8.143}$$

qui utilise la définition 8.70. □

[33] Définition 8.64.
[34] Définition 1.106.

Exemple 8.72.
L'injectivité de φ n'est pas automatique. Prenons par exemple $\mathbb{L} = \mathbb{Q}[\sqrt{2}]$ dans $\mathbb{R}$. Les polynômes dans $\mathbb{Q}[X]$ ont des degrés arbitrairement élevés en X, tandis que les éléments de $\mathbb{L}$ n'ont pas de degré très élevés en $\sqrt{2}$ parce que $\sqrt{2}\sqrt{2} = 2$. L'ensemble $\mathbb{Q}[\sqrt{2}]$ ne contient donc que des éléments de la forme $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$.

Si par contre $x_0 \in \mathbb{R}$ n'est racine d'aucun polynôme (cela existe parce que $\mathbb{R}$ n'est pas dénombrable), alors $\mathbb{Q}[x_0]$ contient tous les $\sum_{k=0}^{N} a_k x_0^k$ avec N arbitrairement grand. Et tous ces nombres sont différents. △

Le lemme suivant donne une caractérisation d'élément algébrique moins abstraite que la définition 8.71.

LEMooTZSSooZmwYji

Lemme 8.73.
Soit $\mathbb{K}$, un corps et $\mathbb{L}$, une extension de $\mathbb{K}$. Un élément $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ si et seulement si existe un polynôme non nul $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$.

Démonstration. Nous considérons l'application φ de la définition 8.71. Si φ n'est pas injective, c'est qu'il existe un polynôme P dans $\mathbb{K}[X]$ tel que $\varphi(P) = 0$. Dans ce cas, $P(\alpha) = 0$.

À l'inverse si il existe P non nul dans $\mathbb{K}[X]$ tel que $P(\alpha) = 0$, alors $\varphi(P) = 0$ et φ n'est pas injective. □

DEFooYZOYooAesmnP

Définition 8.74.
*Un corps $\mathbb{K}$ est **algébriquement clos** si tout polynôme non constant à coefficients dans $\mathbb{K}$ contient au moins une racine dans $\mathbb{K}$.*

Nous verrons dans le théorème de d'Alembert 14.92 que $\mathbb{C}$ est un corps algébriquement clos.

DEFooREUHooLVwRuw

Définition 8.75 (Extension algébrique, clôture algébrique)**.**
Soient un corps $\mathbb{K}$ et une extension $\alpha\colon \mathbb{K} \to \mathbb{L}$.

*(1) L'extension $\mathbb{L}$ est une extension **algébrique** de $\mathbb{K}$ si tous ses éléments sont algébriques[35] sur $\mathbb{K}$, c'est-à-dire sont racines de polynômes à coefficients dans $\alpha(\mathbb{K})$, voir le lemme 8.73.*

ITEMooEIWVooVjJRoR

*(2) L'extension $\mathbb{L}$ est **algébriquement close** si le corps $\mathbb{L}$ est algébriquement clos (définition 8.74).*

*(3) L'extension $\mathbb{L}$ est une **clôture algébrique** du corps $\mathbb{K}$ si elle est une extension algébrique qui est algébriquement close.*

8.76.
Donc une extension est algébrique si elle contient seulement des racines de polynômes ; elle est close si elle contient au moins une racine de chaque polynôme. L'extension est une clôture algébrique si elle est les deux en même temps.

8.77 (Unicité)**.**
Le théorème de Steinitz 8.134 donnera une unicité de la clôture algébrique.

Exemple 8.78.
Le corps $\mathbb{R}$ n'est pas une extension algébrique de $\mathbb{Q}$. En effet il existe seulement une infinité *dénombrable* de polynômes dans $\mathbb{Q}[X]$ et donc une infinité dénombrable de racines de tels polynômes. Toute extension algébrique de $\mathbb{Q}$ est donc dénombrable. Voir aussi la proposition 8.130. △

LEMooEYRSooUREeDl

Lemme 8.79.
Un corps est algébriquement clos si et seulement si tous ses polynômes sont scindés[36].

Démonstration. Si tout polynôme est scindé, tout polynôme possède des racines ; c'est l'autre sens qui est plus consistant.

Soit un corps algébriquement clos $\mathbb{K}$. Nous allons effectuer une récurrence sur le degré des polynômes. Si P est un polynôme de degré 1, alors il est scindé.

Nous supposons que tous les polynômes de degré $n-1$ sont scindés. Soit un polynôme P de degré n. Le corps étant algébriquement clos, le polynôme P a une racine que nous notons $a_n \in \mathbb{K}$. La proposition 3.283 nous explique qu'il existe un polynôme Q de degré $n-1$ tel que $P = (X - a_n)Q$.

Par hypothèse de récurrence, le polynôme Q est scindé : il existe $\{a_i\}_{i=1,\dots,n-1}$ dans $\mathbb{K}$ tels que $Q = \prod_{i=1}^{n-1}(X - a_i)$. Au final,

$$P = (X - a_n)Q = \prod_{k=1}^{n}(X - a_k) \tag{8.144}$$

[35] Définition 8.71.
[36] Définition 8.39

et P est scindé. □

LEMooYVHKooWhewKp

Lemme 8.80.
Soient un corps $\mathbb{K}$ et un polynôme $P \in \mathbb{K}[X]$. Nous supposons que P est scindé :

$$P = \prod_{k=1}^{n} (X - a_k). \tag{8.145}$$

Si α est une racine de P, alors α est l'un des a_k.

Démonstration. Dire que α est une racine de P revient à dire que

$$\prod_{k=1}^{n} (\alpha - a_k) = 0 \tag{8.146}$$

EQooXHSCooVdMixa

Un corps est toujours un anneau intègre (lemme 3.23), c'est-à-dire que la règle du produit nul est utilisable. Dans notre cas, le produit nul (8.146) nous indique que $\alpha - a_k = 0$ pour (au moins) un des k. Donc effectivement α est l'un des a_k. □

Lemme 8.81.
Soient un corps algébriquement clos $\mathbb{K}$ ainsi qu'une extension algébrique $\alpha\colon \mathbb{K} \to \mathbb{L}$. Alors $\alpha(\mathbb{K}) = \mathbb{L}$.

Démonstration. Nous allons montrer que tous les éléments de $\mathbb{L}$ sont dans l'image de α. Soit donc $l \in \mathbb{L}$. Puisque l'extension $\alpha\colon \mathbb{K} \to \mathbb{L}$ est une extension algébrique, il existe un polynôme $P \in \alpha(\mathbb{K})[X]$ tel que $P(l) = 0$.

Étant donné que α est injective, il est possible de considérer le polynôme $Q = \alpha^{-1}(P)$, c'est-à-dire que, si $P = \sum_k a_k X^k$, nous posons $Q = \sum_k \alpha^{-1}(a_k) X^k$.

Le corps $\mathbb{K}$ étant algébriquement clos, le polynôme Q est scindé (proposition 8.79) :

$$Q = \prod_{k=1}^{n} (X - b_k) \tag{8.147}$$

avec $b_k \in \mathbb{K}$. Nous avons alors aussi la factorisation

$$P = \prod_{k=1}^{n} (X - \alpha(b_k)) \tag{8.148}$$

dans $\mathbb{L}[X]$. Nous avons vu que l était une racine de P. Donc l est un des $\alpha(b_k)$ (lemme 8.80). Cela prouve que $l \in \alpha(\mathbb{K})$. □

8.4.3 Extension algébrique et polynôme minimal

PROPooALFJooDjmIcb

Proposition 8.82 ([103]).
Soit une extension algébrique[37] $\mathbb{L}$ du corps $\mathbb{K}$.

(1) Pour tout $a \in \mathbb{L}$, il existe un polynôme $P \in \mathbb{K}[X]$ tel que $P(a) = 0$.

ITEMooEFNFooKYqXDk

(2) Le polynôme minimal de a dans $\mathbb{K}[X]$ est l'unique polynôme unitaire irréductible annulant a.

Démonstration. Le premier point est seulement la définition 8.75 d'une extension algébrique.

L'idéal annulateur $I_a = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\}$ n'est pas réduit à $\{0\}$ parce que $\mathbb{L}$ est une extension algébrique. L'existence du polynôme minimal est le lemme 8.64 et le fait qu'il soit irréductible est la proposition 8.67(1).

Ce qui nous intéresse ici est l'unicité. Soit $\mu_1 \in \mathbb{K}[X]$, un polynôme annulateur de a irréductible et unitaire. Puisque $\mu_1 \in I_a$ et que par définition, $I_a = (\mu)$, il existe $P \in \mathbb{K}[X]$ tel que $\mu_1 = P\mu$. Comme μ n'est pas inversible et que μ_1 est irréductible, P doit être inversible : $\mu_1 = k\mu$ pour un certain $k \in \mathbb{K}$.

Puisque μ et μ_1 sont unitaires, $k = 1$. Donc $\mu_1 = \mu$. □

[37] Définition 8.75.

LEMooHKTMooKEoOuK

Lemme 8.83.
Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ et $\alpha \in \mathbb{L}$, un élément algébrique[38] *sur $\mathbb{K}$. Si μ est le polynôme minimal de α sur $\mathbb{K}$ alors*

$$\begin{aligned} \varphi\colon \mathbb{K}[\alpha] &\to \mathbb{K}[X]/(\mu) \\ Q(\alpha) &\mapsto \bar{Q} \end{aligned} \tag{8.149}$$

avec $Q \in \mathbb{K}[X]$ est un isomorphisme de corps et de $\mathbb{K}$-espaces vectoriels.

Démonstration. D'abord, α est algébrique, donc l'idéal annulateur I_α n'est pas réduit à $\{0\}$, et l'existence d'un polynôme minimal est assurée par le lemme 8.64.

Ensuite, le fait que $\mathbb{K}[X]/(\mu)$ soit un corps est le corolaire 8.44. Nous montrons à présent que φ est un isomorphisme (d'anneaux) ; cela suffit pour en déduire que $\mathbb{K}[\alpha]$ est également un corps.

Ces préliminaires étant dits, nous commençons.

(1) **Bien définie** Nous devons prouver que φ est bien définie, c'est-à-dire que tout élément de $\mathbb{K}[\alpha]$ peut être écrit sous la forme $Q(\alpha)$ pour un $Q \in \mathbb{K}[X]$, et que si $Q_1(\alpha) = Q_2(\alpha)$ alors $\bar{Q}_1 = \bar{Q}_2$.

Le fait que tous les éléments de $\mathbb{K}[\alpha]$ peuvent être écrits sous la forme $Q(\alpha)$ est la proposition 3.259. Supposons que $Q_1(\alpha) = Q_2(\alpha)$. Alors nous définissons $R \in \mathbb{K}[X]$ par $Q_1 = Q_2 + R$, et en évaluant cette égalité en α nous avons

$$Q_1(\alpha) = Q_2(\alpha) + R(\alpha), \tag{8.150}$$

autrement dit $R(\alpha) = 0$. Donc R est dans l'idéal annulateur de α et est donc dans (μ), c'est-à-dire que dans le quotient $\mathbb{K}[X]/(\mu)$ nous avons $\bar{R} = 0$ et donc $\bar{Q}_1 = \bar{Q}_2$.

(2) **Surjective**

Tout élément de $\mathbb{K}[X]/(\mu)$ est de la forme $\bar{Q}$ pour un $Q \in \mathbb{K}[X]$. Or ces éléments sont ceux de l'ensemble d'arrivée de φ.

(3) **Injective**

Si $\bar{Q}_1 = \bar{Q}_2$, alors $Q_1 = Q_2 + R$ avec R dans l'idéal engendré par μ, c'est-à-dire entre autres $R(\alpha) = 0$. Donc $Q_1(\alpha) = Q_2(\alpha)$.

Nous devons encore montrer que nous avons là un morphisme de $\mathbb{K}$-espaces vectoriels.

(1) Si $k \in \mathbb{K}$ alors $\varphi\big(kQ(\alpha)\big) = \overline{kQ}$. Mais par définition de la structure d'espace vectoriel sur $\mathbb{K}[X]/(\mu)$, $\overline{kQ} = k\bar{Q}$ (vérifier que cette définition de la multiplication par un scalaire sur $\mathbb{K}[X]/(\mu)$ est correcte).

(2) Nous avons aussi $\varphi\big(Q_1(\alpha) + Q_2(\alpha)\big) = \varphi\big((Q_1 + Q_2)(\alpha)\big) = \overline{Q_1 + Q_2} = \bar{Q}_1 + \bar{Q}_2$.

□

8.4.4 Extensions et polynômes

Nous savons déjà depuis la définition 3.228 ce qu'est $A[X]$ pour tout anneau A et donc, à fortiori, pour un corps.

DEFooQPZIooQYiNVh

Définition 8.84.
Soit un corps commutatif[39]*. Nous notons $\mathbb{K}(X)$ le corps des fractions*[40] *de $\mathbb{K}[X]$.*

DEFooZHBZooKlNfGZ

Lemme-Définition 8.85.
Si $R \in \mathbb{K}(X)$, avec $R = P/Q$ et si $\mathbb{L}$ est une extension[41] *de $\mathbb{K}$ contenant l'élément α, alors nous définissons*

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \tag{8.151}$$

Cela est une bonne définition au sens où elle ne dépend pas du choix du représentant (P, Q) pris dans la classe P/Q.

[38] Définition 8.71.
[39] Sauf mention du contraire, tous les corps du Frido sont commutatifs.
[40] Définition 3.239.
[41] Définition 8.59.

Démonstration. Supposons $R = P_1/Q_1 = P_2/Q_2$. Par définition des classes (définition 3.239) nous avons

$$P_1Q_2 = Q_1P_2. \tag{8.152}$$

EQooKHVNooABuHaQ

Puisque l'évaluation est un morphisme $\mathbb{K}[X] \to \mathbb{K}$ [42] nous pouvons évaluer l'équation (8.152) en α :

$$P_1(\alpha)Q_2(\alpha) = Q_1(\alpha)P_2(\alpha). \tag{8.153}$$

EQooJAIGooRADgiD

Cette dernière est une égalité dans le corps $\mathbb{K}$. Nous pouvons donc la multiplier par $Q_2(\alpha)^{-1}Q_1(\alpha)^{-1}$ (et utiliser toutes les hypothèses de commutativité des anneaux et corps) pour obtenir

$$P_1(\alpha)Q_1(\alpha)^{-1} = P_2(\alpha)Q_2(\alpha)^{-1}, \tag{8.154}$$

c'est-à-dire

$$(P_1/Q_1)(\alpha) = (P_2/Q_2)(\alpha). \tag{8.155}$$

□

DEFooVSKGooMyeGel

Proposition-Définition 8.86 ([1]).
Soient un corps $\mathbb{K}$, une extension $(\mathbb{L}, j_{\mathbb{L}})$ de $\mathbb{K}$ et un élément $\alpha \in \mathbb{L}$. Nous définissons $\mathbb{K}(\alpha)_{\mathbb{L}}$ comme étant l'intersection de tous les sous-corps de $\mathbb{L}$ contenant $j_{\mathbb{L}}(\mathbb{K})$ et α.

Alors

(1) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est un sous-corps de $\mathbb{L}$,

(2) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est une extension[43] de $\mathbb{K}$.

Démonstration. Nous commençons par prouver que $\mathbb{K}(\alpha)_{\mathbb{L}}$ est bien un corps. Si $a, b \in \mathbb{K}(\alpha)_{\mathbb{L}}$ alors il suffit de calculer ab, $a+b$ et a^{-1} dans n'importe quel sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α ; nous avons une garantie que a, b, ab, $a+b$ et a^{-1} sont dans tous les tels sous-corps.

Pour prouver que $\mathbb{K}(\alpha)_{\mathbb{L}}$ est bien une extension, nous devons trouver un morphisme de corps $j\colon \mathbb{K} \to \mathbb{K}(\alpha)_{\mathbb{L}}$. On constate que prendre $j = j_{\mathbb{L}}$ fonctionne parce que par définition, $\mathbb{K}(\alpha)_{\mathbb{L}}$ est une partie de $\mathbb{L}$ contenant l'image de $j_{\mathbb{L}}$. □

LEMooHZLCooPLHkLS

Lemme 8.87.
Soit n tel que $\sqrt{n}$ ne soit pas un rationnel. Si $\alpha \in \{a+b\sqrt{n}\}_{a,b\in\mathbb{Q}}$, alors il existe un unique choix $(x, y) \in \mathbb{Q}^2$ tel que

$$\alpha = x + y\sqrt{n}. \tag{8.156}$$

Démonstration. L'existence est dans la définition de α. Il s'agit de voir l'unicité. Supposons $x + y\sqrt{n} = a + b\sqrt{n}$ avec $x, y, a, b \in \mathbb{Q}$. Si $b \neq y$ nous pouvons écrire

$$\sqrt{n} = \frac{x-a}{b-y}. \tag{8.157}$$

Comme $\sqrt{n}$ n'est pas un rationnel, une telle écriture est impossible. Donc $b = y$. Nous avons alors $x+y\sqrt{n} = a + y\sqrt{n}$ et du coup aussi $x = a$. □

Exemple 8.88.
Nous avons

$$\mathbb{Q}(\sqrt{2})_{\mathbb{R}} = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}} \tag{8.158}$$

où à droite nous calculons les sommes et les produits dans $\mathbb{R}$. Le tout est un sous-ensemble de $\mathbb{R}$ qui se révèle être un corps contenant $\mathbb{Q}$ et $\sqrt{2}$.

En particulier, dans $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ nous avons $\sqrt{2}\sqrt{2} = 2$. △

LEMooKVPZooPqPrce

Lemme 8.89.
Les corps $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ et $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ ne sont pas isomorphes.

Démonstration. Supposons l'existence d'un morphisme de corps[44]

$$\psi\colon \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \to \mathbb{Q}(\sqrt{3})_{\mathbb{R}}. \tag{8.159}$$

[42] Lemme 3.232. Certes ce lemme ne parle que d'anneaux, mais à y bien penser, dans le passage de (8.152) à (8.153), nous ne considérons que les structures d'anneaux sur $\mathbb{K}[X]$ et $\mathbb{K}$.
[43] Définition 8.59.
[44] Définition 1.106. Oui, c'est un bête morphisme d'anneaux. Il n'y a pas plus de structure dans un corps que dans un anneau.

Nous notons « 1 » à la fois le neutre de la multiplication dans $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ et $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ (qui s'avèrent être les mêmes en tant qu'élément de $\mathbb{R}$, mais ça n'a pas d'importance ici).

Soit $\alpha \in \mathbb{Q}(\sqrt{2})_{\mathbb{R}}$ tel que $\alpha^2 - 2 = 0$. Alors nous avons aussi

$$\psi(\alpha)^2 - 2 = \psi(\alpha^2) - \psi(2) = \psi(\alpha^2 - 2) = \psi(0) = 0. \tag{8.160}$$

Donc $\psi(\alpha)$ est un élément de $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ qui est une racine de $X^2 - 1$.

Or un tel élément n'existe pas dans $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$ parce que nous savons que dans $\mathbb{R}$ entier, il n'y a que deux racines : $\pm\sqrt{2}$, et aucune des deux n'est dans $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$. □

EXooJRSUooYhAZkR

Exemple 8.90.
Est-ce que $\mathbb{K}(\alpha)_{\mathbb{L}}$ dépend réellement de $\mathbb{L}$? Si $\mathbb{L}_2$ est une extension de $\mathbb{L}$ alors nous avons évidemment[45] $\mathbb{K}(\alpha)_{\mathbb{L}_2} = \mathbb{K}(\alpha)_{\mathbb{L}}$.

Nous commençons par construire un corps $\mathbb{K}$ un peu idiot qui, comme ensemble, est comme $\mathbb{Q}(\sqrt{2})_{\mathbb{R}}$, c'est-à-dire la partie

$$\{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}, \tag{8.161}$$

de $\mathbb{R}$.

Mais cette fois nous définissons la multiplication suivante :

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 3bd + (ad + bc)\sqrt{2}. \tag{8.162}$$

C'est un corps parce que tout élément non nul est inversible. En effet, l'équation

$$(a + b\sqrt{2})(x + y\sqrt{2}) = 1 \tag{8.163}$$

EQooIZLEooLPOBcC

donne

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{8.164}$$

Ce système a une unique solution si et seulement si $\det \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} = 0$. Cela survient si et seulement si

$$a^2 - 3b^2 = 0. \tag{8.165}$$

Les solutions de cette équation dans $\mathbb{R}$ sont $a = \pm\sqrt{3}|b|$. Dès que a ou b est non nul, cela ne peut pas satisfaire $a, b \in \mathbb{Q}$. Donc le déterminant est toujours non nul et il existe $x, y \in \mathbb{Q}$ tels que (8.163) soit satisfaite.

Tout cela nous a donné un corps $\mathbb{K}$ dont $\mathbb{Q}$ est un sous-corps et qui contient l'élément $\sqrt{2}$ de $\mathbb{R}$. Il n'est cependant pas un sous-corps de $\mathbb{R}$.

Ce corps est isomorphe à $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$. En effet, nous montrons que

$$\begin{aligned} \psi\colon \mathbb{K} &\to \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \\ a + b\sqrt{2} &\mapsto a + b\sqrt{3} \end{aligned} \tag{8.166}$$

est un isomorphisme de corps. Pour le produit, nous avons

$$\begin{aligned} \psi\big((a + b\sqrt{2})(c + d\sqrt{2})\big) &= \psi\big(ac + 3bd + (ad + bc)\sqrt{2}\big) && \text{(8.167a)} \\ &= ac + 3bd + (ad + bc)\sqrt{3} && \text{(8.167b)} \\ &= (a + b\sqrt{3})(c + d\sqrt{3}) && \text{(8.167c)} \\ &= \psi(a + b\sqrt{2})\psi(c + d\sqrt{2}). && \text{(8.167d)} \end{aligned}$$

SUBEQooQSZBooHZDTKo
SUBEQooPEKHooNPcUiE
SUBEQooIGBZooMwrmFe

Remarques :

- L'application ψ est bien définie grâce au lemme 8.87 couplé au théorème 4.26 appliqué à $n = 2$ et $n = 3$.
- Dans le membre de gauche de (8.167a), $b\sqrt{2}$ est un produit dans $\mathbb{R}$ (d'où l'importance du lemme 8.87 qui permet de re-séparer les éléments de $\mathbb{R}$ partie rationnelle et partie multiple de $\sqrt{2}$), et le produit entre $(a + b\sqrt{2})$ et $(c + d\sqrt{2})$ est un produit dans $\mathbb{K}$.
- Dans (8.167b) et (8.167c), tous les produits sont dans $\mathbb{R}$.

[45] Vérifiez-le tout de même.

En comparant avec le lemme 8.89, nous avons alors

$$\mathbb{Q}(\sqrt{2})_{\mathbb{K}} = \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \neq \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \tag{8.168}$$

△

8.91.
Nous allons encore enfoncer le clou sur le fait que $\mathbb{K}(\alpha)_{\mathbb{L}}$ dépend de $\mathbb{L}$.

Le fait est que si on y pense, l'objet $\sqrt{2}$ n'a aucun rapport avec $\mathbb{Q}$. En effet les objets de $\mathbb{Q}$ sont des classes d'équivalence de couples d'éléments de $\mathbb{Z}$, alors que l'élément $\sqrt{2}$ est une classe d'équivalence de suites de Cauchy dans $\mathbb{Q}$.

Lorsque nous écrivons $\mathbb{Q}(\sqrt{2})$, nous associons des objets de nature complètement différentes, et il n'y a aucune raison à priori de définir la multiplication entre eux d'une façon plutôt qu'une autre.

Plus généralement, dans ZF (nous faisons semblant de suivre ZF tout en sachant que nous ne savons pas ce que c'est réellement[46]), tout est ensemble. Peut-on dire ce que serait $\mathbb{Q}(I)$ si I est un ensemble quelconque ? Attention : en écrivant $\mathbb{Q}(I)$, nous entendons un corps dont I est un élément, pas un corps qui contiendrait comme éléments tous les éléments de I.

Si I est juste un ensemble, quelle définition donner de I^2 ? Il y a plein de choix et rien ne se dégage clairement comme étant pertinent. Si par contre, en guise de I nous considérons l'ensemble $\sqrt{2}$ (oui, c'est un ensemble : un ensemble de suites de Cauchy dans $\mathbb{Q}$), alors tout de suite nous nous disons que la bonne façon de faire est $\sqrt{2}^2 = 2$. Ce réflexe est juste conditionné par le fait que nous connaissons déjà par ailleurs le corps $\mathbb{R}$. Rien de plus.

Donc oui, $\mathbb{K}(\alpha)_{\mathbb{L}}$ dépend de $\mathbb{L}$, mais dans les cas particuliers où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, il y a une égalité implicite $\mathbb{L} = \mathbb{C}$. Cela étant dit, il n'y a plus d'ambiguïté en écrivant $\mathbb{Q}(\sqrt{2})$.

EXooKLRBooUswzpV

Exemple 8.92.
Soit $\mathbb{K} = \mathbb{Q}$ et $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Afin de montrer que $\mathbb{L} = \mathbb{Q}(\alpha)$ avec $\alpha = \sqrt{2} + \sqrt{3}$ nous devons montrer que $\sqrt{2}$ et $\sqrt{3}$ sont des polynômes en α. △

DefZCYIbve

Définition 8.93.
Soit une extension[47] *de corps $j : \mathbb{K} \to \mathbb{L}$. Soit $A \subset \mathbb{L}$.*

ITEMooJEGUooMsDBhF

(1) Nous notons $\mathbb{K}(A)_{\mathbb{L}}$ le plus petit sous-corps de $\mathbb{L}$ contenant $j(\mathbb{K})$ et A. C'est l'intersection de tous les sous-corps de $\mathbb{L}$ contenant A et $j(\mathbb{K})$.

(2) Nous notons $\mathbb{K}[A]_{\mathbb{L}}$ le plus petit sous-anneau de $\mathbb{L}$ contenant $j(\mathbb{K})$ et A. C'est l'intersection de tous les sous-anneaux de $\mathbb{L}$ contenant A et $j(\mathbb{K})$.

*Nous disons que l'extension $\mathbb{L}$ de $\mathbb{K}$ est **monogène** ou **simple** si il existe $\theta \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\theta)$. Un tel élément θ est dit **élément primitif** de $\mathbb{L}$. Il n'est pas nécessairement unique.*

Le plus souvent, l'indice $\mathbb{L}$ dans $\mathbb{K}(A)_{\mathbb{L}}$ et $\mathbb{K}[A]_{\mathbb{L}}$ est omis parce que le contexte est clair[48], et nous avons même très souvent $\mathbb{K} \subset \mathbb{L}$ en tant qu'ensembles. Dans ce cas, l'application j est l'identité et elle sera omise.

Remarque 8.94.
Les ensembles $\mathbb{K}(A)$ et $\mathbb{K}[A]$ sont aussi appelés respectivement corps **engendré** et anneau engendré par A. Cependant il faut bien remarquer que ce sont les parties de $\mathbb{L}$ engendrées par A. Il n'est pas question à priori de parler de corps engendré par A sans dire dans quel corps plus grand nous nous plaçons.

Exemple 8.95.
Nous savons que $\mathbb{R}$ est une extension de $\mathbb{Q}$. Si $a \in \mathbb{R}$ alors $\mathbb{Q}(a)$ est le plus petit corps contenant $\mathbb{Q}$ et a. △

Exemple 8.96.
Nous avons déjà vu à l'occasion de la définition 3.228 que $A[X]$ est l'anneau de tous les polynômes de degré fini en X. Cela rentre dans le cadre de la définition 8.93 parce qu'un anneau contenant X doit contenir tous les X^n.

Notons que même si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ reste un anneau parce qu'un éventuel inverse de X n'est pas dedans[49]. Par contre, $\mathbb{K}(X)$ est un corps parce qu'il contient également les fractions rationnelles. △

[46] En lisant quelques pages de Wikipédia, vous pourrez briller en société, mais ne tentez pas le coup à l'agrégation.
[47] Définition 8.59.
[48] Et je me demande si il est possible de trouver un cas tordu où $\mathbb{K}(A)_{\mathbb{L}} \neq \mathbb{K}(A)_{\mathbb{M}}$. Par exemple lorsque A est dans $\mathbb{L}$ et $\mathbb{M}$, mais que $\mathbb{L}$ n'est pas inclus dans $\mathbb{M}$, ni $\mathbb{M}$ dans $\mathbb{L}$.
[49] Lorsqu'on multiplie, les degrés montent toujours.

ExLQhLhJ

Exemple 8.97.
Si nous prenons $\mathbb{F}_5$ et que nous l'étendons par i, nous obtenons le corps $\mathbb{K} = \mathbb{F}_5(i)$. Nous savons que tous les éléments $a \in \mathbb{F}_5$ sont racines de $X^5 - X$. Mais étant donné que $i^5 = i$, nous avons aussi $x^5 = x$ pour tout $x \in \mathbb{F}_5(i)$. Pour le prouver, utiliser le morphisme de Frobenius. Le polynôme $X^5 - X$ est donc le polynôme nul dans $\mathbb{K}$.

Ceci est un cas très particulier parce que nous avons étendu $\mathbb{F}_p$ par un élément α tel que $\alpha^p = \alpha$. En général sur $\mathbb{F}_p(\alpha)$, le polynôme $X^p - X$ n'est pas identiquement nul, et possède donc au maximum p racines. Pour $x \in \mathbb{F}_p(\alpha)$, nous avons $x^p = x$ si et seulement si $x \in \mathbb{F}_p$. △

Dans l'énoncé suivant, la notation $R(\alpha)_{\mathbb{L}}$ signifie que l'évaluation de R sur α se fait en calculant dans le sur-corps $\mathbb{L}$ de $\mathbb{K}$. Cette proposition semble indiquer que $\mathbb{K}(\alpha)$ est donné en termes de $\mathbb{K}(X)$, lequel est défini de façon très intrinsèque sans faire appel implicitement à un sur-corps de $\mathbb{K}$.

PROPooYSFNooFGbbCi

Proposition 8.98 ([1])**.**
Soit une extension $\mathbb{L}$ du corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Alors nous avons les isomorphismes de corps suivants :

(1) $\mathbb{K}(\alpha)_{\mathbb{L}} = \text{Frac}\big(\mathbb{K}[\alpha]_{\mathbb{L}}\big)$,

ITEMooATPTooVXKdlK

(2) $\mathbb{K}(\alpha)_{\mathbb{L}} = \{P(\alpha)_{\mathbb{L}}/Q(\alpha)_{\mathbb{L}}$ *tel que* $P, Q \in \mathbb{K}[X], Q(\alpha) \neq 0\ \}$.

Le point (2) pourrait être écrit $\mathbb{K}(\alpha)_{\mathbb{L}} = \{R(\alpha)_{\mathbb{L}}$ *tel que* $R \in \mathbb{K}(X)\}$*, avec sous-entendu que seuls les* $R \in \mathbb{K}(X)$ *tels que* $R(\alpha)$ *est bien défini sont pris en compte*[50].

Démonstration. Le corps $\mathbb{K}(\alpha)$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}[\alpha]$ comme sous-anneau. La proposition 3.246 nous dit alors que l'application suivante est un morphisme injectif de corps :

$$\begin{aligned}\epsilon\colon \text{Frac}\big(\mathbb{K}[\alpha]\big) &\to \mathbb{K}(\alpha)\\ P/Q &\mapsto PQ^{-1}.\end{aligned} \tag{8.169}$$

Pour rappel, la notation P/Q est bien une notation pour la classe d'équivalence du couple (P, Q) pour la relation définie en 3.239.

Par ailleurs, la partie $\epsilon\Big(\text{Frac}\big(\mathbb{K}[\alpha]\big)\Big)$ de $\mathbb{L}$ et est un corps contenant $\mathbb{K}$ et α. Donc ce corps fait partie des corps sur lesquels on prend l'intersection pour définir $\mathbb{K}(\alpha)$[51]. Cela prouve que

$$\mathbb{K}(\alpha) \subset \epsilon\Big(\text{Frac}\big(\mathbb{K}[\alpha]\big)\Big). \tag{8.170}$$

L'application ϵ est donc surjective sur $\mathbb{K}(\alpha)$. Comme elle était déjà injective, elle est bijective.

Pour la seconde partie, veuillez lire la définition 3.248 de l'évaluation d'une fraction rationnelle sur un élément de l'anneau. Si $R = P/Q \in \mathbb{K}(X)$ et si $\alpha \in \mathbb{L}$, nous avons

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \tag{8.171}$$

Tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α doit contenir en particulier $\{P(\alpha)$ tel que $P \in \mathbb{K}[X]\}$, les inverses $\{P(\alpha)^{-1}$ tel que $P \in \mathbb{K}[X]$, $P(\alpha) \neq 0\}$ et les produits de ceux-ci. Donc tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α contient $\{R(\alpha)$ tel que $R \in \mathbb{K}(X)\}$.

Nous avons donc

$$\{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\} \subset \mathbb{K}(\alpha). \tag{8.172}$$

Mais puisque $\mathbb{K}(\alpha)$ est lui-même un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α, il est contenu dans $\{R(\alpha)$ tel que $R \in \mathbb{K}(X)\}$. D'où l'égalité. □

Pourquoi cela ne contredit pas l'exemple 8.90 ? Lorsque nous écrivons

$$\mathbb{K}(\alpha) = \{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\}, \tag{8.173}$$

certes $\mathbb{K}(X)$ est défini sans faire appel à un corps contenant $\mathbb{K}$. Mais l'évaluation $R(\alpha)$, oui. Pour calculer $R(\alpha)$, il faut écrire $R = P/Q$ et calculer $P(\alpha)Q(\alpha)^{-1}$. Tous les calculs de cette dernière expression doivent se faire dans un sur-corps de $\mathbb{K}$. Il suffit que le sur-corps en question soit un monceau de mauvaise foi comme celui de l'exemple 8.90, et en réalité $\mathbb{K}(\alpha)$ peut ne pas être ce que l'on croit.

Le corolaire suivant montre que les choses s'arrangent.

[50] Merci à jeanas pour m'avoir fait remarquer le danger[203].
[51] Pour rappel, la définition 8.93(1) donne $\mathbb{K}(\alpha)$ comme une intersection.

Corolaire 8.99.
Soient un corps $\mathbb{K}$, une extension $\mathbb{L}_1$ de $\mathbb{K}$, un élément $\alpha \in \mathbb{L}_1$ et une extension $\mathbb{L}_2$ de $\mathbb{L}_1$. Alors

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \mathbb{K}(\alpha)_{\mathbb{L}_2}. \tag{8.174}$$

Démonstration. La proposition 8.98 nous dit que

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \{R(\alpha)_{\mathbb{L}_1} \text{ tel que } R \in \mathbb{K}(X)\} \tag{8.175a}$$
$$\mathbb{K}(\alpha)_{\mathbb{L}_2} = \{R(\alpha)_{\mathbb{L}_2} \text{ tel que } R \in \mathbb{K}(X)\}. \tag{8.175b}$$

Mais lorsque $R \in \mathbb{K}(X)$, le calcul de $R(\alpha)$ est exactement le même dans $\mathbb{L}_1$ et dans $\mathbb{L}_2$ parce que $\mathbb{L}_2$ est un sur-corps de $\mathbb{L}_1$ et que les calculs effectifs de $R(\alpha) = P(\alpha)Q(\alpha)^{-1}$ ne font intervenir que des quantités de $\mathbb{K}$ et des puissances de α. □

Ce que ce corolaire nous dit est que si le contexte fixe une extension de $\mathbb{K}$, nous pouvons faire tous les calculs dans cette extension, même si il y a des piles d'extensions à côté.

Typiquement, à chaque fois que nous considérons des sous-corps de $\mathbb{C}$, les extensions se feront dans $\mathbb{C}$: pour tout $\alpha \in \mathbb{C}$, les corps $\mathbb{Q}(\alpha)$, $\mathbb{R}(\alpha)$ se calculent dans $\mathbb{C}$.

PROPooSYQWooFbfQtm

Proposition 8.100.
Soit un corps $\mathbb{K}$, une extension $\mathbb{L}$ et un élément $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned} \varphi\colon \mathbb{K}[X] &\to \mathbb{L} \\ P &\mapsto P(\alpha). \end{aligned} \tag{8.176}$$

ITEMooUZDQooOasiRQ

(1) Si α est transcendant, alors $\mathbb{K}[\alpha] = \mathbb{K}[X]$ (isomorphisme d'anneaux).

(2) Si α est transcendant, alors $\mathbb{K}(\alpha)_{\mathbb{L}} = \mathbb{K}(X)$ (isomorphisme de corps),

(3) Si α est algébrique, alors $\ker(\varphi)$ est un idéal possédant un unique générateur unitaire, lequel est le polynôme minimal[52] de α sur $\mathbb{K}$.

Démonstration. Point par point.

(1) Nous savons que $\mathbb{K}[\alpha] = \{Q(\alpha) \text{ tel que } Q \in \mathbb{K}[X]\}$ (c'est la proposition 3.259). Donc φ est surjective sur $\mathbb{K}[\alpha]$, et est donc bijective. Elle est un isomorphisme[53] parce que le lemme 8.71 dit déjà que c'est un morphisme.

(2) Nous supposons encore que α est transcendant et nous considérons l'application

$$\begin{aligned} \psi\colon \mathbb{K}(X) &\to \mathbb{K}(\alpha) \\ P &\mapsto R(\alpha). \end{aligned} \tag{8.177}$$

Note : cette application n'est pas φ. En effet φ n'est définie que sur $\mathbb{K}[X]$; le corps des fractions $\mathbb{K}(X)$ est nettement plus grand (classes d'équivalence de couples).

Le fait que cette application soit surjective est la proposition 8.98(2). Pour l'injectivité nous supposons que $\psi(R) = 0$, c'est-à-dire que $R(\alpha) = 0$. Nous considérons un représentant (P, Q) de R ; c'est-à-dire $R = P/Q$. L'égalité $R(\alpha) = 0$ signifie $P(\alpha)Q(\alpha)^{-1} = 0$ (égalité dans $\mathbb{L}$). Puisque $\mathbb{L}$ est un corps, c'est un anneau intègre et nous avons la règle du produit nul ; soit $P(\alpha) = 0$, soit $Q(\alpha)^{-1} = 0$. La seconde possibilité est impossible parce que zéro n'est pas inversible. Donc $P(\alpha) = 0$. Donc $\varphi(P) = 0$ et φ étant injective, $P = 0$.

Lorsque $P = 0$, la classe P/Q est nulle dans $\mathbb{K}(X) = \text{Frac}\big(\mathbb{K}[X]\big)$.

(3) C'est le lemme-définition 8.64.

□

PropXULooPCusvE

Proposition 8.101.
Soit un corps $\mathbb{K}$ et une extension $\mathbb{L}$. Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{L}$, une racine de P. Alors le polynôme minimal d'une racine divise[54] tout polynôme annulateur.

Autrement dit, l'idéal engendré par le polynôme minimal est l'idéal des polynômes annulateurs.

[52] Définition 8.64.
[53] Les amateurs d'écriture inclusive ne seront, je l'espère, pas choqué par « *elle* est *un* isomorphisme » ; c'est une tournure que je propose ici sur le modèle de l'immonde « *elle* est *un* ministre » ou, à peine moins grave, « *il* est *une* sommité ».
[54] Définition 3.264.

Démonstration. Nous considérons l'idéal

$$I = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}. \tag{8.178}$$

Le fait que cela soit un idéal est simplement dû à la définition du produit : $(PQ)(a) = P(a)Q(a)$. Par le théorème 8.43, le polynôme minimal μ_a de a est dans I et, qui plus est, le génère : $I = (\mu_a)$. Par conséquent tout polynôme annulateur de a est divisé par μ_a. □

8.4.4.1 Extension algébrique, degré

Proposition 8.102.
Toute extension finie est algébrique.

Démonstration. Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de degré[55] n de $\mathbb{K}$ et $a \in \mathbb{L}$. Nous devons montrer qu'il existe un polynôme annulateur de a à coefficients dans $\mathbb{K}$.

Soit la partie $S = \{1, a, a^2, \dots, a^n\}$ de $\mathbb{L}$. Si cette partie contient des éléments non distincts, alors c'est plié. En effet, si $a^k = a^l$, alors le polynôme X^{k-l} est un polynôme annulateur de a.

Nous supposons donc que S contienne exactement $n+1$ éléments distincts. Le lemme 6.13 nous assure que S est une partie liée : il existe des éléments $k_i \in \mathbb{K}$ tels que $\sum_{i=0}^{n} k_i a^i = 0$.

Donc le polynôme $\sum_i a_i X^i$ est un polynôme annulateur de a. □

PropURZooVtwNXE

Proposition 8.103 (Propriétés d'extensions algébriques[1])**.**
Soit $\mathbb{K}$ un corps commutatif[56] *et a un élément algébrique*[57] *sur $\mathbb{K}$, de polynôme minimal μ_a de degré n. Alors*

ItemJCMooDgEHajmi

(1) En considérant l'application d'évaluation

$$\begin{aligned} \varphi_a \colon \mathbb{K}[X] &\to \mathbb{L} \\ Q &\mapsto Q(a), \end{aligned} \tag{8.179}$$

nous avons $\mathbb{K}[a] = \text{Image}(\varphi_a)$.

ItemJCMooDgEHajiv

(2) Une base de $\mathbb{K}[a]$ comme espace vectoriel sur $\mathbb{K}$ est donnée par $\{1, a, a^2, \dots, a^{n-1}\}$.

ItemJCMooDgEHajiii

(3) Le degré de l'extension $\mathbb{K}[a]$ est égal au degré du polynôme minimal :

$$\big[\mathbb{K}[a] : \mathbb{K}\big] = n. \tag{8.180}$$

(4) L'anneau $\mathbb{K}[a]$ est l'ensemble des polynômes en a de degré jusqu'à $n-1$ à coefficient dans $\mathbb{K}$.

ItemJCMooDgEHaji

(5) $\mathbb{K}(a) = \mathbb{K}[a]$.

ItemJCMooDgEHajii

(6) Il existe un isomorphisme d'anneaux $\varphi \colon \mathbb{K}[a] \to \mathbb{K}[X]/(\mu_a)$ tel que $\varphi(k) = \bar{k}$ pour tout $k \in \mathbb{K}$. $\mathbb{K}[a] \simeq \mathbb{K}[X]/(\mu_a)$ (isomorphisme d'anneau).

L'intérêt de (6) est qu'il permet de caractériser $\mathbb{K}[a]$ sans avoir recours à un sur-corps de $\mathbb{K}$. Le point (3) indique que le degré d'une extension algébrique est égal au degré du polynôme minimal.

Démonstration. (1) Nous avons $\mathbb{K}[a] \subset \text{Image}(\varphi_a)$ parce que $\text{Image}(\varphi_a)$ est lui-même un sous-anneau de $\mathbb{L}$ contenant $\mathbb{K}$ et a. Pour rappel, $\mathbb{K}[a]$ est l'intersection de tous les tels sous-anneaux.

L'inclusion inverse est le fait que si $Q \in \mathbb{K}[X]$ alors $Q(a) \in \mathbb{K}[a]$ parce que $\mathbb{K}[a]$ est un anneau et contient donc tous les a^n.

(2) La partie $\{1, a, a^2, \dots, a^{n-1}\}$ est libre parce qu'une combinaison linéaire de ces éléments est un polynôme de degré au plus $n-1$ en a. Un tel polynôme ne peut pas être nul parce que nous avons mis comme hypothèse que le polynôme minimal de a est de degré n.

Rappelons qu'en vertu de la définition 8.64, le polynôme minimal μ_a est unitaire ; donc $\deg\big(\mu_a(X) - X^n\big) \leqslant n-1$. Par conséquent en posant $S(X) = X^n - \mu_a(X)$, nous avons $\deg(S) \leqslant n-1$ et $S(a) = a^n$.

En vertu du point (1), un élément de $\mathbb{K}[a]$ s'écrit $Q(a)$ pour un certain $Q \in \mathbb{K}[X]$. Supposons que Q soit de degré $p > n-1$; alors nous le décomposons en une partie contenant les termes de degré jusqu'à $n-1$ et une partie contenant les autres :

$$Q(X) = Q_1(X) + X^n Q_2(X) \tag{8.181}$$

[55] Définition 8.61.
[56] Juste en passant nous rappelons que tous les corps considérés ici sont commutatifs
[57] Définition 8.71.

où $\deg(Q_1) \leqslant n-1$ et $\deg(Q_2) = p-n$. Nous évaluons cette égalité en a :

$$Q(a) = Q_1(a) + S(a)Q_2(a). \tag{8.182}$$

Donc $Q(a)$ est l'image de a par le polynôme $Q_1 + SQ_2$ qui est de degré $p-1$. Par récurrence, $Q(a)$ est l'image de a par un polynôme de degré $n-1$.

Notons que l'idée est très simple : il s'agit de remplacer récursivement tous les a^n par $S(a)$.

(3) Conséquence immédiate de (2).

(4) Conséquence immédiate de (2).

(5) Un élément général non nul de $\mathbb{K}[a]$ est de la forme $Q(a)$ avec $Q \in \mathbb{K}[X]$; il s'agit de lui trouver un inverse. Pour cela nous remarquons que les polynômes $\mu_a(X)$ et $Q(x)$ sont premiers entre eux, sinon μ_a ne serait pas un polynôme minimal (voir la proposition 8.67). Donc le théorème de Bézout 8.47 affirme l'existence d'éléments $U, V \in \mathbb{K}[X]$ tels que

$$U\mu_a + VQ = 1 \tag{8.183}$$

dans $\mathbb{K}[X]$. Nous évaluons cette égalité en a en tenant compte de $\mu_a(a) = 0$ dans $\mathbb{K}[a]$:

$$U(a)\mu_a(a) + V(a)Q(a) = 1 \tag{8.184}$$

dans $\mathbb{K}[a]$. Par conséquent $V(a)Q(a) = 1$, ce qui signifie que $V(a)$ est l'inverse de $Q(a)$.

(6) Nous considérons l'application

$$\begin{aligned} \psi\colon \mathbb{K}[X]/(\mu_a) &\to \mathbb{K}[a] \\ \bar{R} &\mapsto R(a) \end{aligned} \tag{8.185}$$

et nous montrons qu'elle convient. Pour cela, nous nous souvenons que la proposition 8.101 nous enseigne que (μ_a), l'idéal engendré par μ_a, est égal à l'idéal des polynômes annulateurs de a dans $\mathbb{K}[X]$. Le polynôme μ_a divise tous les éléments de cet idéal ; voir aussi la définition 3.6 de l'idéal (μ_a). Cela étant mis au point, nous passons à la preuve.

(6a) **ψ est bien définie**
Si $\bar{R} = \bar{S}$ alors $R = S + Q$ avec $Q \in (\mu_a)$, et par conséquent $R(a) = S(a) + Q(a)$ avec $Q(a) = 0$.

(6b) **Surjective**
Nous savons que $\mathbb{K}[a] = \text{Image}(\varphi_a)$. Si $x \in \mathbb{K}[a]$ alors il existe $Q \in \mathbb{K}[X]$ tel que $x = Q(a)$. Dans ce cas nous avons aussi $x = \psi(\bar{Q})$.

(6c) **Injective**
Si $\psi(\bar{R}) = 0$ alors $R(a) = 0$, mais comme mentionné plus haut, μ_a engendre l'idéal des polynômes annulateurs de a. Donc $R \in (\mu_a)$ et nous avons $\bar{R} = 0$ dans $\mathbb{K}[X]/(\mu_a)$.

□

Exemple 8.104.
Un fait connu est que $\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$. Donc l'inverse de $\sqrt{2}$ s'exprime bien comme un polynôme en $\sqrt{2}$ à coefficients dans $\mathbb{Q}$, ce qui confirme le point (5) de la proposition 8.103. Du point de vue de Bézout, $\mu_{\sqrt{2}}(X) = X^2 - 2$, et nous cherchons des polynômes U et V tels que

$$U(X^2 - 2) + VX = 1. \tag{8.186}$$

cette égalité est réalisée par $U = -\frac{1}{2}$ et $V = \frac{1}{2}X$. Et effectivement $V(\sqrt{2})$ est bien l'inverse de $\sqrt{2}$:

$$V(\sqrt{(2)}) = \frac{1}{2}\sqrt{2}. \tag{8.187}$$

△

PROPooNGJWooYSpwVn

Proposition 8.105 ([202]).
Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de $\mathbb{K}$ et un élément α de $\mathbb{L}$. Il y a équivalence entre les trois points suivants :

ITEMooYTEBooUuEfBz

(1) α est algébrique sur $\mathbb{K}$,

ITEMooWMQTooLnepQl

(2) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$,

ITEMooAQIUooMVZojp

(3) $\mathbb{K}[\alpha]$ *est un* $\mathbb{K}$*-espace vectoriel de dimension finie.*

Si ces affirmations sont vraies, alors $[\mathbb{K}(\alpha) : \mathbb{K}]$ *est le degré du polynôme minimal de* α *sur* $\mathbb{K}$.

Démonstration. Démonstration décomposée en plusieurs implications.

(1) **(1) implique (2)**

Soit α algébrique sur $\mathbb{K}$. Nous considérons le polynôme minimal de α sur $\mathbb{K}$ (définition 8.64). Nous savons par le lemme 8.83 (qui fonctionne parce que α est algébrique) que $\mathbb{K}[\alpha] = \mathbb{K}[X]/(\mu)$ en tant qu'anneaux.

Mais $\mathbb{K}[X]$ est un anneau principal et μ en est un élément irréductible. Donc la proposition 3.126 dit que (μ) est un idéal maximum ; la proposition 3.128 avance encore un peu en disant que $\mathbb{K}[X]/(\mu)$ est un corps.

Donc $\mathbb{K}[X]/(\mu)$ est un corps isomorphe à $\mathbb{K}[\alpha]$ en tant qu'anneaux. En conséquence de quoi $\mathbb{K}[\alpha]$ est un corps.

Le corps $\mathbb{K}[\alpha]$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α ; par définition nous avons donc $\mathbb{K}(\alpha) \subset \mathbb{K}[\alpha]$.

Mais d'autre part, $\mathbb{K}[\alpha]$ est contenu dans tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α, donc il est inclus dans l'intersection de tout ces corps, donc $\mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$.

Nous avons donc l'égalité $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

(2) **(2) implique (1)**

Nous montrons que non-(1) implique non-(2). Nous disons donc que α est transcendant sur $\mathbb{K}$; cela implique par la proposition 8.100(1) que $\mathbb{K}[\alpha] = \mathbb{K}[X]$ en tant qu'anneaux. Donc $\mathbb{K}[\alpha]$ n'est pas un corps parce que $\mathbb{K}[X]$ ne l'est pas.

N'étant pas un corps, $\mathbb{K}[\alpha]$ ne peut pas être égal à $\mathbb{K}(\alpha)$ qui, lui, est un corps.

(3) **(1) implique (3)**

L'élément α est maintenant algébrique et nous considérons son polynôme minimal μ. Nous savons par le lemme 8.83 que $\mathbb{K}[\alpha] = \mathbb{K}[X]/(\mu)$ en tant qu'espaces vectoriels. Or $\mathbb{K}[X]/(\mu)$ est de dimension finie $\deg(\mu)$. Donc $\mathbb{K}[\alpha]$ est également de dimension finie.

(4) **(3) implique (1)**

Nous démontrons la contraposée. En supposant que α est transcendant nous avons $\mathbb{K}[\alpha] = \mathbb{K}[X]$ par la proposition 8.100. Or $\mathbb{K}[X]$ n'est pas de dimension finie sur $\mathbb{K}$, donc $\mathbb{K}[\alpha]$ non plus.

□

Lemme 8.106.
Soit $P \in \mathbb{K}[X]$ *un polynôme unitaire irréductible de degré* n*. Il existe une extension* $\mathbb{L}$ *de* $\mathbb{K}$ *et* $a \in \mathbb{L}$ *telle que* $\mathbb{L} = \mathbb{K}(a)$ *et* P *est le polynôme minimal de* a *dans* $\mathbb{L}$.

Démonstration. Nous prenons $\mathbb{L} = \mathbb{K}[X]/(P)$ où (P) est l'idéal dans $\mathbb{K}[X]$ généré par P. C'est un corps par le corolaire 8.44. Nous identifions $\mathbb{K}$ avec $\phi(\mathbb{K})$ où

$$\phi\colon \mathbb{K}[X] \to \mathbb{L} \tag{8.188}$$

est la projection canonique. Nous considérons également $a = \phi(X)$.

Nous avons alors $P(a) = 0$ dans $\mathbb{L}$. En effet $P(a) = P\big(\phi(X)\big)$ est à voir comme l'application du polynôme P au polynôme X, le résultat étant encore un élément de $\mathbb{L}$. En l'occurrence le résultat est P qui vaut 0 dans $\mathbb{L}$.

Le polynôme P étant unitaire et irréductible, il est minimum dans $\mathbb{L}$.

Nous devons encore montrer que $\mathbb{L} = \mathbb{K}(a)$. Le fait que $\mathbb{K}(a) \subset \mathbb{L}$ est une tautologie parce qu'on calcule $\mathbb{K}(a)$ dans $\mathbb{L}$. Pour l'inclusion inverse soit $Q(X) = \sum_i Q_i X^i$ dans $\mathbb{K}[X]$. Dans $\mathbb{L}$ nous avons évidemment $Q = \sum_i Q_i a^i$. □

PropyMTEbH

Proposition 8.107 ([103])**.**
Soit $\mathbb{K}$*, un corps et* $P \in \mathbb{K}[X]$ *un polynôme. Soient* a *et* b*, deux racines de* P *dans (éventuellement) une extension* $\mathbb{L}$ *de* $\mathbb{K}$*. Si* μ_a *et* μ_b *sont les polynômes minimaux de* a *et* b *(dans* $\mathbb{K}[X]$*) et si* $\mu_a \neq \mu_b$*, alors* $\mu_a\mu_b$ *divise* P *dans* $\mathbb{K}[X]$.

Démonstration. Nous considérons les idéaux

$$I_a = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}; \tag{8.189a}$$
$$I_b = \{Q \in \mathbb{K}[X] \text{ tel que } Q(b) = 0\}. \tag{8.189b}$$

Même si $Q(a)$ et $Q(b)$ sont calculés dans $\mathbb{L}$, I_a, I_b sont des idéaux de $\mathbb{K}[X]$. Le polynôme μ_a est par définition le générateur unitaire de I_a, et comme a est une racine de P, nous avons $P \in I_a$ et il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = \mu_a Q. \tag{8.190}$$

Montrons que $\mu_a(b) \neq 0$. Pour cela, nous supposons que $\mu_a(b) = 0$, c'est-à-dire que $\mu_a \in I_b$. Il existe alors $R \in \mathbb{K}[X]$ tel que $\mu_a = \mu_b R$. Mais par la proposition 8.67, le polynôme μ_a est irréductible, donc soit μ_b, soit R, est inversible. Comme les inversibles sont les éléments de $\mathbb{K}$ (polynômes de degré zéro), μ_b n'est pas inversible (sinon il serait constant et ne pourait pas être annulateur de b). Donc R est inversible. Disons $R = k$.

Donc $\mu_a = k\mu_b$. Mais puisque μ_a et μ_b sont unitaires, nous avons obligatoirement $k = 1$. Cela donnerait $\mu_a = \mu_b$, ce qui est contraire aux hypothèses. Nous en déduisons que $\mu_a(b) \neq 0$.

Étant donné que $\mu_a(b) \neq 0$, l'évaluation de (8.190) en b montre que $Q(b) = 0$, de telle sorte que $Q \in I_b$ et il existe un polynôme S tel que $Q = \mu_b S$, c'est-à-dire tel que $P = \mu_a \mu_b S$, ce qui signifie que $\mu_a\mu_b$ divise P. □

Exemple 8.108.
Soit $P = (X^2 + 1)(X^2 + 2)$ dans $\mathbb{R}[X]$. Dans $\mathbb{C}$ nous avons les racines $a = i$ et $b = \sqrt{2}i$ dont les polynômes minimaux sont $\mu_a = X^2 + 1$ et $\mu_b = X^2 + 2$. Nous avons effectivement $\mu_a\mu_b$ divise P dans $\mathbb{R}[X]$.

Si par contre nous considérions les racines $a = i$ et $b = -i$, nous aurions $\mu_a = \mu_b = X^2 + 1$, tandis que le polynôme μ_a^2 ne divise pas P. △

8.4.5 Racines de polynômes

CorDIYooEtmztc

Corolaire 8.109 (Factorisation d'une racine)**.**
Soit $P \in \mathbb{K}[X]$, un polynôme de degré n et $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$. Alors il existe un polynôme Q de degré $n - 1$ tel que $P(x) = (X - \alpha)Q$.

Démonstration. Il s'agit d'un cas particulier de la proposition 8.101 : si $\alpha \in \mathbb{K}$ alors son polynôme minimal dans $\mathbb{K}$ est $X - \alpha$; donc $X - \alpha$ divise P. Il existe un polynôme Q tel que $P = (X - \alpha)Q$. Le degré est alors immédiat. □

Nous sommes sur le point de prouver le théorème 8.110 qui dit qu'un polynôme avec trop de racines est nul.

(1) Relisez d'abord la définition 3.257 pour savoir ce qu'est un polynôme nul.

(2) Si vous être seulement intéressé par le cas de polynôme réels, peut-être que le déterminant de Vandermonde 6.135 sera une façon plus facile de prouver.

ThoLXTooNaUAKR

Théorème 8.110 (Polynôme qui a tellement de racines qu'il s'annule)**.**
Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme de degré n possédant $n + 1$ racines distinctes α_1,..., α_{n+1}, alors $P = 0$.

Démonstration. Si P est de degré 1, il s'écrit $P = aX + b$; si il a comme racines α et β, nous avons le système

$$\begin{cases} a\alpha + b = 0 & (8.191a) \\ a\beta + b = 0. & (8.191b) \end{cases}$$

La différence entre les deux donne $a(\alpha - \beta) = 0$. Puisque $\alpha \neq \beta$, la règle du produit nul (lemme 3.23) nous donne $a = 0$. Maintenant que $a = 0$, l'annulation de b est alors immédiate.

Nous faisons maintenant la récurrence en supposant le théorème vrai pour le degré n et en considérant un polynôme P de degré $n + 1$ possédant $n + 2$ racines distinctes. Puisque $P(\alpha_1) = 0$, le corolaire 8.109 nous donne un polynôme Q de degré n tel que

$$P = (X - \alpha_1)Q. \tag{8.192}$$

EqQGSooNdTWfx

Étant donne que pour tout $i \neq 1$ nous avons $\alpha_i \neq \alpha_1$,

$$0 = P(\alpha_i) = \underbrace{(\alpha_i - \alpha_1)}_{\neq 0} Q(\alpha_i), \tag{8.193}$$

et la règle du produit nul donne $Q(\alpha_i) = 0$. Par conséquent le polynôme Q est de degré n et possède $n+1$ racines distinctes ; tous ses coefficients sont alors nuls par hypothèse de récurrence. Tous les coefficients du produit (8.192) sont alors également nuls. □

ExGRHooBNpjSP

Exemple 8.111.
Un polynôme à plusieurs variables peut s'annuler en une infinité de points sans être nul. Par exemple le polynôme $X^2 + Y^2 - 1 \in \mathbb{R}[X, Y]$ s'annule sur tout un cercle de $\mathbb{R}^2$ mais n'est pas nul, loin s'en faut.

Nous verrons dans la proposition 8.185 une condition pour qu'un polynôme à plusieurs variables s'annule du fait qu'il ait « trop » de racines. △

Remarque 8.112.
L'intérêt du théorème 8.110 est que si l'on prouve qu'un polynôme s'annule sur un corps infini, alors il s'annulera sur n'importe quel autre corps. Nous aurons un exemple d'utilisation de cela dans le théorème de Cayley-Hamilton 15.31.

8.4.6 Corps de rupture

DEFooVALTooDJJmJv

Définition 8.113 (Corps de rupture)**.**
Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Une extension $\mathbb{L}$ de $\mathbb{K}$ est un ***corps de rupture*** *pour P si il existe $a \in \mathbb{L}$ tel que $P(a) = 0$ et $\mathbb{L} = \mathbb{K}(a)$.*

NORMALooTPOIooVZAfUo

8.114.
Nous insistons sur le fait que nous ne définissons le concept de corps de rupture que pour un polynôme irréductible à coefficients dans un corps. Les deux points sont importants : irréductible et à coefficient dans un corps.

Nous discuterons brièvement le pourquoi de cela dans la section 8.4.11.

ExemGVxJUC

Exemple 8.115.
Soit $\mathbb{K} = \mathbb{Q}$ et $P = X^2 - 2$. On pose $a = \sqrt{2}$ et $\mathbb{L} = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. De cette façon P est scindé dans $\mathbb{L}$:

$$P = (X - \sqrt{2})(X + \sqrt{2}). \tag{8.194}$$

Le corps $\mathbb{Q}(\sqrt{2})$ est donc un corps de rupture pour P. △

Exemple 8.116.
Dans l'exemple 8.115, nous avions un corps de rupture dans lequel le polynôme P était scindé. Il n'en est pas toujours ainsi. Prenons

$$P = X^3 - 2 \tag{8.195}$$

et $a = \sqrt[3]{2}$. Nous avons, certes, $P(a) = 0$ dans $\mathbb{Q}(\sqrt[3]{2})$, mais P n'est pas scindé parce qu'il y a deux racines complexes. △

Exemple 8.117.
Nous considérons le corps $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier. Si $s \in \mathbb{Z}/p\mathbb{Z}$ n'est pas un carré, alors le polynôme $P = X^2 + s$ est irréductible et un corps de rupture de P sur $\mathbb{Z}/p\mathbb{Z}$ est donné par $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + s)$, c'est-à-dire l'ensemble des polynômes de degré 1 en $\sqrt{s}$. Le cardinal en est p^2. △

Comme nous allons abondamment parler du quotient $\mathbb{K}[X]/(P)$, nous nous permettons un petit lemme.

LEMooWYYFooXYacdF

Lemme 8.118.
Soit un corps $\mathbb{K}$ et $P \in \mathbb{K}[X]$ non constant. Alors $\mathbb{K}[X]/(P)$ est un corps si et seulement si P est irréductible.

Démonstration. Nous utilisons le trio d'enfer dont il est question dans le thème 18. D'abord $\mathbb{K}[X]$ est un anneau principal par le lemme 3.266. Donc $\mathbb{K}[X]/(P)$ sera un corps si et seulement si (P) est un idéal maximum (proposition 3.86), et cela sera le cas si et seulement si (P) est engendré par un polynôme irréductible (proposition 3.126).

Il ne nous reste qu'à montrer que (P) est engendré par un irréductible si et seulement si P est irréductible. Il y a un sens dans lequel c'est évident.

Soit un irréductible μ tel que $(P) = (\mu)$. En particulier $\mu \in (P)$, c'est-à-dire qu'il existe Q tel que $\mu = PQ$. Puisque μ est irréductible, soit P, soit Q, est inversible. Si P est inversible, c'est-à-dire constant,

c'est ce que nous avons exclu par hypothèse. Si par contre Q est inversible, alors $P = k\mu$ pour un certain $k \in \mathbb{K}$, ce qui montre que P est irréductible autant que μ. □

PROPooUBIIooGZQyeE

Proposition 8.119 (Existence d'un corps de rupture)**.**
Soit un corps $\mathbb{K}$ et un polynôme irréductible non constant P. Alors

(1) Le corps $\mathbb{L} = \mathbb{K}[X]/(P)$ est un corps de rupture pour P.

(2) L'élément $\bar{X}$ de $\mathbb{L}$ est une racine de P.

(3) $\mathbb{L} = \mathbb{K}(\bar{X})_{\mathbb{L}}$

Démonstration. Commençons par nous convaincre que $\mathbb{K}[X]/(P)$ est une extension de $\mathbb{K}$ (définition 8.59). Le fait que ce soit un corps est le lemme 8.118. Le morphisme $j\colon \mathbb{K} \to \mathbb{K}[X]/(P)$ est simplement $k \mapsto \bar{k}$ où à droite, $\bar{k}$ voit k dans $\mathbb{K}[X]$ comme étant le polynôme constant. Notez qu'il est automatiquement injectif (lemme 2.6).

Il faut maintenant voir que $\mathbb{K}[X]/(P) = \mathbb{K}(\alpha)$ pour un certain $\alpha \in \mathbb{K}[X]/(P)$. Grâce à notre compréhension des notations acquise dans 3.15.2.2, nous savons que $X \in \mathbb{K}[X]$ et qu'il est donc parfaitement légitime de poser $\alpha = \bar{X}$ dans $\mathbb{K}[X]/(P)$. Il s'agit simplement de l'ensemble $\bar{X} = \{X + QP \text{ tel que } Q \in \mathbb{K}[X]\}$ où X est une notation pour la suite $(0, 1, 0, 0, \ldots)$.

Bref, nous notons $\alpha = \bar{X}$ et nous démontrons que $P(\alpha) = 0$ et que $\mathbb{K}[X]/(P) = \mathbb{K}(\alpha)$ (isomorphisme de corps).

(1) $P(\bar{X}) = 0$

C'est le moment de nous souvenir comment la notation des X fonctionne, et en particulier la pirouette autour de (3.395). D'abord la définition du produit sur $\mathbb{K}[X]/(P)$ est $\bar{P}\bar{Q} = \overline{PQ}$; en particulier si $P = \sum_k a_k X^k$, alors $P(\bar{X}) = \sum_k a_k \bar{X}^k = \sum_k a_k \overline{X^k}$, et

$$P(\bar{X}) = \overline{P(X)} = \bar{P} = 0. \tag{8.196}$$

(2) **L'égalité**

Nous montrons à présent que $\mathbb{K}(\bar{X})_{\mathbb{L}} = \mathbb{L}$. C'est-à-dire que $\mathbb{L}$ est bien engendrée par $\mathbb{K}$ et un seul élément. D'abord, $\mathbb{L} = \mathbb{K}[X]/(P)$ contient bien évidemment $\mathbb{K}$ et $\bar{X}$. Ensuite nous devons prouver que tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et $\bar{X}$ est en réalité $\mathbb{L}$ entier.

Soit $Q \in \mathbb{K}[X]$, et montrons que $\bar{Q}$ est dans tout sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et $\bar{X}$.

Par le lemme 3.255 nous avons $\bar{Q} = Q(\bar{X})$. Et si un corps contient $\mathbb{K}$ et $\bar{X}$, il doit contenir tous les polynômes en $\bar{X}$ à coefficients dans $\mathbb{K}$. Donc un tel corps doit contenir $Q(\bar{X})$ et donc $\bar{Q}$.

□

Exemple 8.120.
Soit le polynôme $P = X^2 + 1 \in \mathbb{Z}[X]$. Dans le quotient $\mathbb{Z}[X]/(P)$ nous avons $\bar{X}^2 + 1 = 0$ et donc $\bar{X}^2 = -1$. C'est-à-dire que $\mathbb{Z}[X]/(P)$ contient un élément dont le carré est -1. Avouez que c'est bien ce à quoi nous nous attendions.

Notons que $-\bar{X}$ est également une racine de P dans $\mathbb{Z}[X]/(P)$.

En calculant dans les polynômes à coefficients dans $\mathbb{Z}(\bar{X})$ nous avons :

$$(X + \bar{X})(X - \bar{X}) = X^2 - \bar{X}^2 = X^2 + 1, \tag{8.197}$$

c'est-à-dire que P est bien factorisé, et que nous avons retrouvé la multiplication $x^2 + 1 = (x + i)(x - i)$. △

8.121.
Il n'y a évidemment pas unicité d'un corps de rupture pour un polynôme donné. Une raison est qu'un polynôme peut accepter plusieurs racines complètement indépendantes. Le corps étendu par l'une ou l'autre racine donne deux corps de rupture différents. Par exemple dans $\mathbb{Q}[X]$, le polynôme

$$P = X^4 - X^2 - 2 \tag{8.198}$$

a pour racines (dans $\mathbb{C}$) les nombres $\sqrt{2}$ et i. Donc on a deux corps de rupture complètement différents : $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i)$.

NORMooIQIRooEoDjwm

8.122.
Un polynôme sur $\mathbb{Q}$ peut avoir de nombreuses racines sur $\mathbb{C}$. Par exemple $X^4 - 5X^2 + 6$ a pour racines $\pm\sqrt{2}$ et $\pm\sqrt{3}$. Il existe donc à priori quatre corps de rupture différents : $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[-\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ et $\mathbb{Q}[-\sqrt{3}]$. Ensuite vous pouvez réfléchir pour savoir si l'un ou l'autre de ces quatre sont identiques ou isomorphes ; ce n'est pas la question ici.

La proposition suivante met un tout petit peu d'ordre dans les corps de ruptures en disant que le corps $\mathbb{K}[X]/(P)$ est quand même plus pertinent que les autres.

PROPooVJACooNDmlfb

Proposition 8.123 ([196]).
Soient un corps $\mathbb{K}$ et un polynôme irréductible $P \in \mathbb{K}[X]$. Alors toute extension $\mathbb{L}$ contenant une racine α de P admet un unique morphisme de corps

$$\psi\colon \mathbb{K}[X]/(P) \to \mathbb{L} \tag{8.199}$$

tel que $\psi(\bar{X}) = \alpha$.

Dans un tel cas,

ITEMooHRFHooWLIdWU

(1) l'image de ψ est $\mathbb{K}(\alpha)_{\mathbb{L}}$,

(2) si $\mathbb{L} = \mathbb{K}(\alpha)_{\mathbb{L}}$ alors ψ est un isomorphisme.

Démonstration. L'idéal annulateur de α parmi les polynômes de $\mathbb{K}[X]$ n'est pas réduit à $\{0\}$ parce qu'il contient P. Le lemme 8.64 s'applique donc et nous avons μ, le polynôme minimal de α dans $\mathbb{K}[X]$. Il divise P qui est irréductible, donc

$$P = \lambda\mu \tag{8.200}$$

pour un certain $\lambda \in \mathbb{K}$.

Nous posons

$$\begin{aligned}\psi\colon \mathbb{K}[X]/(P) &\to \mathbb{L}\\ \bar{Q} &\mapsto Q(\alpha).\end{aligned} \tag{8.201}$$

(1) **Bien définie** Si $\bar{Q}_1 = \bar{Q}_2$ alors il existe un $R \in \mathbb{K}[X]$ tel que $Q_1 = Q_2 + RP$. Mais alors $\psi(\bar{Q}_1) = Q_1(\alpha) = Q_2(\alpha) + R(\alpha)P(\alpha) = Q_2(\alpha)$.

(2) **Injective**

Si $\psi(\bar{Q}_1) = \psi(\bar{Q}_2)$ alors $Q_1 - Q_2 = R$ pour un certain $R \in \mathbb{K}[X]$ vérifiant $R(\alpha) = 0$. Nous avons alors un polynôme S tel que $R = S\mu = \lambda^{-1}SP$. Donc $\bar{R} = 0$ et donc $\bar{Q}_1 = \bar{Q}_2$.

(3) **Morphisme**

Laissé comme exercice ; la paresse de l'auteur de ces lignes attend vos contributions.

(4) **La condition**

Le morphisme ψ respecte de plus la condition

$$\psi(\bar{X}) = X(\alpha) = \alpha. \tag{8.202}$$

En ce qui concerne l'unicité, fixer $\psi(\bar{X})$ est suffisant pour fixer un morphisme. En effet si $\psi(\bar{X}) = \alpha$, alors

$$\psi(\bar{Q}) = \psi\Big(\sum_k a_k \bar{X}^k\Big) = \sum_k a_k \psi(\bar{X})^k = \sum_k a_k \alpha^k. \tag{8.203}$$

Pour le second point de l'énoncé, il faut remarquer que α est algébrique et non transcendant. Donc en utilisant les propositions 3.259 et 8.103(5) nous trouvons

$$\text{Image}(\psi) = \{Q(\alpha) \text{ tel que } Q \in \mathbb{K}[X]\} = \mathbb{K}[\alpha] = \mathbb{K}(\alpha). \tag{8.204}$$

Et finalement pour le dernier point, un morphisme de corps est toujours injectif. Si il est également surjectif, il sera bijectif. □

8.4.7 Pile d'extensions

LEMooTURZooXnjmjT

Lemme 8.124 ([1]).
Soient un corps $\mathbb{K}$, des extensions $\mathbb{L}_1$,..., $\mathbb{L}_n$ et des éléments $\alpha_i \in \mathbb{L}_i$ tels que

$$\mathbb{L}_1 = \mathbb{K}(\alpha_1)_{\mathbb{L}_1} \tag{8.205}$$

EQooOCQSooFMkzTc

et

$$\mathbb{L}_k = \mathbb{L}_{k-1}(\alpha_k)_{\mathbb{L}_k}. \tag{8.206}$$

Alors

$$\mathbb{L}_n = \mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}. \tag{8.207}$$

Démonstration. Nous démontrons par récurrence sur n. Le cas $n = 1$ est simplement l'hypothèse (8.205).

Supposons donc que le lemme soit correct pour n, et étudions le cas $n+1$. Nous avons, par définition et par hypothèse de récurrence :

$$\mathbb{L}_{n+1} = \mathbb{L}_n(\alpha_{n+1})_{\mathbb{L}_{n+1}} = \Big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\Big)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \tag{8.208}$$

Notre tâche sera donc de montrer que

$$\Big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\Big)(\alpha_{n+1}) = \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \tag{8.209}$$

EQooIHMGooTlPcsd

où nous n'écrivons plus les indices $\mathbb{L}_{n+1}$ partout.

Le membre de gauche est un sous-corps de $\mathbb{L}_{n+1}$ contenant à la fois $\mathbb{K}$ et tous les α_i, si bien que

$$\mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \subset \big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \tag{8.210}$$

EQooLLRHooHQiLfk

Il faut donc prouver l'inclusion inverse ; c'est-à-dire montrer que tout élément x du corps $\big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})$ est forcément dans tout sous-corps de $\mathbb{L}_{n+1}$ contenant $\mathbb{K}$ et les α_i. Un tel élément x est, par la proposition 8.98(2), de la forme $r(\alpha_{n+1})$ avec $r \in \mathbb{K}(\alpha_1, \dots, \alpha_n)(X)$, c'est-à-dire

$$P(\alpha_{n+1})Q(\alpha_{n+1})^{-1} \tag{8.211}$$

avec $P, Q \in \mathbb{K}(\alpha_1, \dots, \alpha_n)[X]$.

Prouvons d'abord que si $P \in \mathbb{K}(\alpha_1, \dots, \alpha_n)[X]$, alors $P(\alpha_{n+1})$ est dans tout sous-corps de $\mathbb{L}_{n+1}$ contenant $\mathbb{K}$ et les α_i. Nous pouvons écrire $P = \sum_i a_i X^i$ avec $a_i \in \mathbb{K}(\alpha_1, \dots, \alpha_n)$, et donc

$$P(\alpha_{n+1}) = \sum_i a_i \alpha_{n+1}^i. \tag{8.212}$$

Tout corps contenant $\mathbb{K}$ et les α_1,..., α_n contient les a_i. Par produit, tout corps contenant $\mathbb{K}$, α_1,..., α_{n+1} contient les termes $a_i\alpha_{n+1}^i$, et donc $P(\alpha_{n+1})$ par somme.

De la même façon, si un corps contient $\mathbb{K}$ et les α_i, $(i = 1, \dots, n+1)$, alors il contient $Q(\alpha_{n+1})$. Comme c'est un corps, il contient aussi son inverse $Q(\alpha_{n+1})^{-1}$, et il contient aussi le produit

$$r(\alpha_{n+1}) = P(\alpha_{n+1})Q(\alpha_{n+1})^{-1}. \tag{8.213}$$

On vient ainsi de montrer que tout élément $x \in \big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})$ était dans tout sous-corps de $\mathbb{L}_{n+1}$ qui contient $\mathbb{K}$ et les α_i, $(i = 1, \dots, n+1)$; en d'autres termes :

$$\big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})_{\mathbb{L}_{n+1}} \subset \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}). \tag{8.214}$$

EQooUFSMooJzzpqL

Les inclusions (8.210) et (8.214) prouvent l'égalité d'ensembles (8.209) que nous voulions montrer. □

8.4.8 Clôture algébrique

Le concept de clôture algébrique a été défini dans 8.75. Voici un lemme qui dit qu'une clôture algébrique est en quelque sorte une extension algébrique maximale.

LEMooQSCGooMyCktA

Lemme 8.125 ([1]).
Soient un corps $\mathbb{K}$ et une extension algébrique $\mathbb{F}$ de $\mathbb{K}$. Nous supposons que pour toute extension algébrique de $\mathbb{L}$ nous avons $\mathbb{L} = \mathbb{F}$

Alors $\mathbb{F}$ est algébriquement clos[58].

[58] Définition 8.75(2).

Démonstration. Soit un polynôme $P \in \mathbb{K}[X]$. Nous voudrions prouver que P a des racines dans $\mathbb{F}$. Pour cela, nous voyons P comme un polynôme sur $\mathbb{F}[X]$ et, grace à la proposition 8.119 nous considérons un corps de rupture $\mathbb{L}$ pour P. Puisque $\mathbb{L}$ est une extension de $\mathbb{F}$, nous avons $\mathbb{L} = \mathbb{F}$. Donc $\mathbb{F}$ contient des racines de P. □

8.126.
Nous avons défini le concept d'extension algébrique en 8.75. Nous allons en construire un petit exemple très piéton.

Souvenez-vous que la proposition 4.99 nous donne l'existence et l'unicité d'un réel $\sqrt{2}$ strictement positif dont le carré est 2. Ce réel est irrationnel par la proposition 4.25.

Proposition 8.127 ([204]).
Soit $\mathbb{L} = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}$.

(1) *C'est un sous-corps de* $\mathbb{R}$.
ITEMooUSOAooZoBhla

(2) *Tout sous-corps de* $\mathbb{R}$ *contenant* $\mathbb{Q}$ *et* $\sqrt{2}$ *contient* $\mathbb{L}$.

Démonstration. Nous devons d'abord prouver que $\mathbb{L}$ est un corps en vérifiant d'une part que c'est un anneau (définition 1.100) et d'autre part le fait que tous les éléments non nuls sont inversibles.

- La partie $\mathbb{L}$ de $\mathbb{R}$ est stable pour l'addition : dès que $a, b, a', b' \in \mathbb{Q}$,
$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2} \in \mathbb{L}. \tag{8.215}$$
- Les neutres 0 et 1 sont dans $\mathbb{L}$.
- Si $\alpha \in \mathbb{L}$, alors $-\alpha \in \mathbb{L}$:
$$-(a + b\sqrt{2}) = -a - b\sqrt{2}. \tag{8.216}$$
- La partie $\mathbb{L}$ est stable pour le produit parce que
$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + ba')\sqrt{2}. \tag{8.217}$$
- L'inverse d'un élément de $\mathbb{L}$ est dans $\mathbb{L}$. C'est le seul point pas tout à fait évident. D'abord, l'ensemble $\mathbb{R}$ est un corps par le théorème 4.36. Donc pour tout $a, b \in \mathbb{R}$, le nombre
$$\frac{1}{a + b\sqrt{2}} \tag{8.218}$$
existe dans $\mathbb{R}$.

  D'abord $a - b\sqrt{2}$ n'est pas nul, parce que si il l'était, nous aurions $\sqrt{2} = a/b \in \mathbb{Q}$ alors que $\sqrt{2}$ n'est pas rationnel par la proposition 4.25. Nous pouvons donc faire le coup de multiplier le numérateur et le dénominateur par le binôme conjugué :
$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}. \tag{8.219}$$
  Cela est un rationnel. Donc le éléments non nuls de $\mathbb{L}$ ont un inverse qui appartient également à $\mathbb{L}$.

Nous passons à la preuve du point (2). Si $\mathbb{L}'$ est un corps qui contient $\mathbb{Q}$ et $\sqrt{2}$, il doit contenir $b\sqrt{2}$ pour tout $b \in \mathbb{Q}$ et donc aussi tous les $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$. Par conséquent, $\mathbb{L}'$ doit contenir au moins tout $\mathbb{L}$. □

Proposition 8.128.
Soit $\mathbb{L} = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}$.
ITEMooOMDMooLNhlyh

(1) *C'est un espace vectoriel de dimension* 2 *sur* $\mathbb{Q}$.
ITEMooWGGDooSbsesf

(2) *Si* $\alpha \in \mathbb{L}$, *alors il existe un polynôme* $P \in \mathbb{L}[X]$ *de degré* 2 *ou moins tel que* $P(\alpha) = 0$.
ITEMooPNNYooPtKYwQ

(3) *Le corps* $\mathbb{L}$ *est une extension algébrique de* $\mathbb{Q}$.

Démonstration. En plusieurs parties.

(1) **(1)** Pour la dimension, notez que $\{1, \sqrt{2}\}$ est une partie libre et génératrice de $\mathbb{L}$.

(2) **(2)**

Soit $\alpha \in \mathbb{L}$. La partie $\{1, \alpha, \alpha^2\}$ est de cardinal 1, 2 ou 3. Si c'est 1 ou 2, c'est que $1 = \alpha$ ou $1 = \alpha^2$ ou $\alpha = \alpha^2$. Si par exemple $1 = \alpha$ alors avec $P = X - 1$ nous avons $P(\alpha) = 0$.

Si au contraire $\{1, \alpha, \alpha^2\}$ est de cardinal 3, alors c'est une partie liée par la proposition 6.8. Il existe donc des rationnels a, b, c tels que $a + b\alpha + c\alpha^2 = 0$, c'est-à-dire $P(\alpha) = 0$ avec $P = cX^2 + bX + a$.

(3) **(3)** Nous venons de voir que tous les éléments de $\mathbb{L}$ sont des racines de polynômes de $\mathbb{Q}[X]$.

□

LEMooHWPHooZeWqns

Lemme 8.129.
Si $\mathbb{K}$ est un corps infini, alors $\mathbb{K}[X]$ est équipotent[59] *à $\mathbb{K}$.*

Démonstration. Notons provisoirement $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré n. Nous avons une surjection

$$\begin{aligned} \varphi\colon \mathbb{K}^{n+1} &\to \mathbb{K}_n[X] \\ (k_0, \dots, k_n) &\mapsto \sum_{i=0}^{n} k_i X^i. \end{aligned} \tag{8.220}$$

EQooFGZVooKIMKRA

Par récurrence sur le théorème[60] 2.66, nous avons $\mathbb{K}^{n+1} \approx \mathbb{K}$. La surjection (8.220) dit alors que

$$\mathbb{K}_n[X] \preceq \mathbb{K}^{n+1} \approx \mathbb{K}. \tag{8.221}$$

Mais puisqu'il y a une surjection $\mathbb{K} \to \mathbb{K}_n[X]$, nous avons aussi $\mathbb{K}_n[X] \succeq \mathbb{K}$. Le théorème 1.84 dit alors que $\mathbb{K}_n[X] \approx \mathbb{K}$.

Le lemme 2.67 nous permet alors de conclure que

$$\mathbb{K}[X] = \bigcup_{n=0}^{\infty} \mathbb{K}_n[X] \approx \mathbb{K}. \tag{8.222}$$

□

PROPooVPQFooScWvkS

Proposition 8.130 ([1])**.**
Soit un corps $\mathbb{K}$. Une extension algébrique de $\mathbb{K}$ est

(1) au plus dénombrable si $\mathbb{K}$ est fini,

(2) équipotente à $\mathbb{K}$ si $\mathbb{K}$ est infini.

Démonstration. En deux parties.

(1) **Si $\mathbb{K}$ est fini** Un polynôme non nul possède toujours au maximum un nombre fini de racines (éventuellement zéro) par la proposition 8.110. Par ailleurs, chaque degré de polynôme ayant seulement un nombre fini de possibilités, l'ensemble $\mathbb{K}[X]$ est au plus dénombrable (proposition 2.42).

Pour $P \in \mathbb{K}[X]$ nous avons une surjection de $\mathbb{N}$ vers l'ensemble des racines de P. Nous la notons $\varphi_P\colon \mathbb{N} \to \mathbb{L}$, en posant par exemple $\varphi_P(n) = 1$ si P n'a pas de racines. Enfin nous posons

$$\begin{aligned} \varphi\colon \mathbb{K}[X] \times \mathbb{N} &\to \mathbb{L} \\ (P, n) &\mapsto \varphi_P(n). \end{aligned} \tag{8.223}$$

C'est la fonction qui à un polynôme P et un nombre n fait correspondre la n^{e} racine de P.

Comme $\mathbb{L}$ est une extension algébrique, φ est surjective.

En termes de cardinalité, que $\mathbb{K}[X]$ soit fini ou dénombrable, dans les deux cas, $\mathbb{K}[X] \times \mathbb{N}$ est dénombrable (proposition 2.38). Il existe donc une surjection d'un ensemble dénombrable vers $\mathbb{L}$. Le lemme 2.41 conclut que $\mathbb{L}$ est fini ou dénombrable.

(2) **Si $\mathbb{K}$ est infini** Nous procédons de la même manière, mais nous devons faire appel à des résultats plus technologiques pour maitriser la cardinalité. Nous considérons à nouveau l'application

$$\begin{aligned} \varphi\colon \mathbb{K}[X] \times \mathbb{N} &\to \mathbb{L} \\ (P, n) &\mapsto \varphi_P(n). \end{aligned} \tag{8.224}$$

[59] Définition 1.71.

[60] J'ai quand même du mal à croire qu'il faille vraiment le lemme de Zorn pour prouver que $\mathbb{K}[X]$ est équipotent à $\mathbb{K}$. Si vous connaissez un moyen plus direct, écrivez-moi.

Cette application est encore surjective : $\mathbb{L} \preceq \mathbb{K}[X] \times \mathbb{N}$. Le lemme 8.129 nous assure que $\mathbb{K}[X] \approx \mathbb{K}$ parce que $\mathbb{K}$ est infini. Ensuite la proposition 2.59 nous dit que $\mathbb{K}[X] \times \mathbb{N} \approx \mathbb{K}[X]$. Donc

$$\mathbb{K} \approx \mathbb{K}[X] \approx \mathbb{K}[X] \times \mathbb{N} \succeq \mathbb{F}. \tag{8.225}$$

Mais $\mathbb{F}$ est une extension de $\mathbb{K}$. Donc il existe une injection $\mathbb{K} \to \mathbb{F}$, c'est-à-dire $\mathbb{K} \preceq \mathbb{F}$.

Ayant $\mathbb{K} \preceq \mathbb{F} \preceq \mathbb{K}$, le théorème 1.84 implique que $\mathbb{K} \approx \mathbb{F}$.

□

Lemme 8.131 ([1]).
Soient des corps $\mathbb{K}$ et $\mathbb{L}$ ainsi qu'un morphisme de corps $\rho\colon \mathbb{K} \to \mathbb{L}$. Si $P \in \mathbb{K}[X]$ a une racine dans $\mathbb{K}$, alors le polynôme $\rho(P)$ a une racine dans $\mathbb{L}$.

Démonstration. Nous notons $P = \sum_k P_k X^k$. Si $a \in \mathbb{K}$ est une racine de P, alors $\sum_k P_k a^k = 0$. Nous appliquons ρ à cette égalité : $\sum_k \rho(P_k)\rho(a)^k = 0$, c'est-à-dire $\rho(P)\big(\rho(a)\big) = 0$. Donc $\rho(a) \in \mathbb{L}$ est une racine de $\rho(P)$. □

Note à propos du lemme suivant (8.132) : en pratique, les corps $\mathbb{L}$ et $\mathbb{F}$ sont le plus souvent des sur-corps de $\mathbb{K}$, de telle sorte que les applications α et β sont l'identité. En particulier, la conclusion de ce lemme s'écrit le plus souvent $\sigma|_{\mathbb{K}} = \mathrm{Id}$. Il faut juste savoir que le Frido est un névrosé des notations précises.

LEMooIIKYooHMNqYn

Lemme 8.132 ([205]).
Nous considérons un triplet $(\mathbb{K}, \mathbb{L}, \mathbb{F})$ où

(1) $\mathbb{K}$, $\mathbb{L}$ et $\mathbb{F}$ sont des corps

(2) il existe $a \in \mathbb{L}$ algébrique sur $\mathbb{K}$ tel que $\mathbb{L} = \mathbb{K}(a)$ et un morphisme de corps $\alpha\colon \mathbb{K} \to \mathbb{L}$.

(3) $\mathbb{F}$ est une extension algébriquement close de $\mathbb{K}$: il existe un morphisme $\beta\colon \mathbb{K} \to \mathbb{F}$.

Alors il existe un morphisme de corps $\sigma\colon \mathbb{L} \to \mathbb{F}$ tel que $\sigma|_{\alpha(\mathbb{K})} = \beta$.

Démonstration. Comme $\mathbb{L}$ est monogène, si $\mu_a \in \mathbb{K}[X]$ est le polynôme minimal de $a \in \mathbb{L}$, alors les points (5) et (6) de la proposition 8.103 disent que $\mathbb{L} \simeq \mathbb{K}[a] \simeq \mathbb{K}[X]/(\mu_a)$. Pour référence ultérieure, nous considérons un isomorphisme

$$\varphi\colon \mathbb{L} \to \mathbb{K}[X]/(\mu_a). \tag{8.226}$$

Les coefficients de μ_a sont dans $\mathbb{K}$, donc nous pouvons voir $\mu_a \in \mathbb{F}[X]$. Plus précisément, si $\mu_a = \sum_k a_k X^k$, nous définissons

$$\mu'_a = \sum_k \beta(a_k) X^k \in \mathbb{F}[X]. \tag{8.227}$$

Comme $\mathbb{F}$ est algébriquement clos, le polynôme μ'_a possède une racine (au moins) $b \in \mathbb{F}$: $\mu'_a(b) = 0$.

Nous posons

$$\begin{aligned} \sigma'\colon \mathbb{K}[X]/(\mu_a) &\to \mathbb{F} \\ \overline{\sum_k s_k X^k} &\mapsto \sum_k \beta(s_k) b^k. \end{aligned} \tag{8.228}$$

(1) **σ' est bien définie** La réalité est que nous utilisons la proposition 1.58. Si $P = \sum_k s_k X^k$ et $\mu_a = \sum_k a_k X^k$ $(a_k, s_k \in \mathbb{K})$, alors

$$\sigma'(\overline{P + \mu_a}) = \sigma'\big(\overline{\sum_k (a_k + s_k) X^k}\big) = \sum_k \beta(a_k) b^k + \sum_k s_k b^k = \mu'_a(b) + \sigma'(\overline{P}) = \sigma'(\overline{P}). \tag{8.229}$$

(2) **σ' est un morphisme de corps** Il s'agit de vérifier les conditions de la définition 1.106. Soient deux

polynômes $P = \sum_k P_k X^k$ et $Q = \sum_l Q_l X^l$. Nous avons

$$\begin{aligned}
\sigma'(\bar{P}) + \sigma'(\bar{Q}) &= \sum_k \beta(P_k)b^k + \sum_l \beta(Q_l)X^l && (8.230a)\\
&= \sum_k \big(\beta(P_k) + \beta(Q_k)\big) && (8.230b)\\
&= \sum_k \beta(P_k + Q_k)b^k && \beta \text{ est morphisme} \quad (8.230c)\\
&= \sigma'\Big(\overline{\sum_k (P_k + Q_k)}X^k\Big) && (8.230d)\\
&= \sigma'(\overline{P+Q}) && (8.230e)\\
&= \sigma'(\overline{P} + \overline{Q}). && (8.230f)
\end{aligned}$$

Pour prouver que $\sigma'(PQ) = \sigma'(P)\sigma'(Q)$, c'est le même type de calcul[61]. Il suffit d'écrire $PQ = \sum_k S_k X^k$ et remarquer que S_k s'exprime en fonction des P_i et Q_j rien qu'avec des sommes et produits.

Enfin le polynôme 1 est donné par $s_0 = 1$ et $s_k = 0$ pour $k \geqslant 1$. Donc $\sigma'(\bar{1}) = 1$ parce que $\beta(s_0)b^0 = \beta(1) = 1$. Toujours parce que β est un morphisme de corps.

(3) $\varphi\big(\alpha(k)\big) = \bar{k}$ Quand nous parlons de $\bar{k}$, nous parlons de la classe du polynôme de degré zéro donné par $k \in \mathbb{K}$.

(4) **La réponse** Nous posons

$$\sigma = \sigma' \circ \varphi. \tag{8.231}$$

Pour tout $k \in \mathbb{K}$,

$$(\sigma'\varphi\alpha)(k) = \sigma'(\bar{k}) = \beta(k), \tag{8.232}$$

c'est ce qu'il fallait.

□

LEMooUULTooYcytat

Lemme 8.133 ([205]).
Soit un corps $\mathbb{K}$ muni de deux extensions $\alpha\colon \mathbb{K} \to \mathbb{L}$ et $\beta\colon \mathbb{K} \to \mathbb{F}$. Nous supposons que

(1) $\mathbb{L}$ est algébrique sur $\mathbb{K}$;

(2) $\mathbb{F}$ est algébriquement clos.

Alors il existe un morphisme de corps $\sigma\colon \mathbb{L} \to \mathbb{F}$ tel que $\sigma \circ \alpha = \beta$.

Démonstration. Nous allons utiliser le lemme de Zorn 1.42 sur l'ensemble

$$\mathcal{A} = \Big\{(\mathbb{M}, \varphi) \text{ tel que } \begin{cases} \mathbb{M} \text{ est un sous-corps de } \mathbb{L} \\ \alpha(\mathbb{K}) \subset \mathbb{M} \\ \varphi\colon \mathbb{M} \to \mathbb{F} \text{ est une extension de corps} \\ \varphi \circ \alpha = \beta \end{cases}\Big\}. \tag{8.233}$$

Nous ordonnons (partiellement) cet ensemble en disant que $(\mathbb{M}_1, \varphi_1) < (\mathbb{M}_2, \varphi_2)$ si $\mathbb{M}_1 \subset \mathbb{M}_2$ et $\varphi_2|_{\mathbb{M}_1} = \varphi_1$. Il se fait que $\mathcal{A}$ est un ensemble inductif et que nous pouvons donc lui appliquer le lemme de Zorn.

Soit un élément maximal $(\mathbb{M}, \varphi)$. Nous allons montrer que $\mathbb{M} = \mathbb{L}$.

Soit $l \in \mathbb{L}$. Puisque $\mathbb{L}$ est une extension algébrique de $\mathbb{K}$, il existe un polynôme P à coefficients dans $\alpha(\mathbb{K})$ tel que $P(l) = 0$. Mais comme $\alpha(\mathbb{K}) \subset \mathbb{M}$, ce polynôme est également à coefficients dans $\mathbb{M}$. Donc l est un élément algébrique sur $\mathbb{M}$.

Nous pouvons donc considérer le triplet $\big(\mathbb{M}, \mathbb{M}(l), \mathbb{F}\big)$ qui vérifie les hypothèses du lemme 8.132. Il existe donc un morphisme de corps $\sigma\colon \mathbb{M}(l) \to \mathbb{F}$ tel que $\sigma|_{\mathbb{M}} = \varphi$.

Nous avons

$$\sigma \circ \alpha = \sigma|_{\sigma(\mathbb{K})} \circ \alpha = \sigma|_{\mathbb{M}} \circ \alpha = \varphi \circ \alpha = \beta. \tag{8.234}$$

Donc l'élément $\big(\mathbb{M}(l), \sigma\big)$ majore $(\mathbb{M}, \varphi)$ dans $\mathcal{A}$.

Par maximalité, nous déduisons que $\mathbb{M} = \mathbb{L}$. Donc le morphisme $\varphi\colon \mathbb{L} \to \mathbb{F}$ vérifie $\varphi \circ \alpha = \beta$, ce qu'il nous fallait. □

[61] J'ai pas vérifié ; écrivez-moi si ça pose un problème.

THOooEDQKooLEGlDv

Théorème 8.134 (Steinitz[206, 207]).
À propos de clôture algébrique.

(1) Tout corps possède une clôture algébrique[62].

(2) Si $\alpha_1 : \mathbb{K} \to \mathbb{F}_1$ et $\alpha_2 : \mathbb{K} \to \mathbb{F}_2$ sont deux clôtures algébriques du même corps $\mathbb{K}$, alors il existe un isomorphisme de corps $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$ tel que $\varphi \circ \alpha_1 = \alpha_2$.

Démonstration. Nous commençons par l'existence, en plusieurs points.

(1) **Un ensemble** Nous considérons un ensemble Ω qui contient $\mathbb{K}$, qui est strictement surpotent[63] à $\mathbb{K}$ et qui est infini non dénombrable si $\mathbb{K}$ est fini. Par exemple $\mathcal{P}(\mathbb{K}) \cup \mathbb{K}$ si $\mathbb{K}$ est infini et $\mathbb{R} \cup \mathbb{K}$ si $\mathbb{K}$ est fini (voir le théorème de Cantor 1.88).

(2) **L'ensemble pour Zorn** Nous considérons l'ensemble des extensions algébriques de $\mathbb{K}$ contenues dans Ω, c'est-à-dire

$$\mathcal{A} = \left\{ (\mathbb{L}, +_{\mathbb{L}}, \times_{\mathbb{L}}) \text{ tel que } \begin{cases} \mathbb{K} \subset \mathbb{L} \subset \Omega \\ (\mathbb{L}, +_{\mathbb{L}}, \times_{\mathbb{L}}) \text{ est une extension algébrique de } (\mathbb{K}, +, \times). \end{cases} \right\} \tag{8.235}$$

Nous ordonnons $\mathcal{A}$ par l'inclusion : nous disons que

$$(\mathbb{L}_1, +_1, \times_1) < (\mathbb{L}_2, +_2, \times_2) \tag{8.236}$$

lorsque $(\mathbb{L}_2, +_2, \times_2)$ est un sur-corps de $(\mathbb{L}_1, +_1, \times_1)$ (en particulier $\mathbb{L}_1 \subset \mathbb{L}_2$).

(3) **$\mathcal{A}$ est inductif** Soit une partie $\mathcal{F} = \{(\mathbb{L}_i, +_i, \times_i)\}_{i \in I}$ de $\mathcal{A}$ que nous supposons être totalement ordonnée. Nous allons lui trouver un majorant dans $\mathcal{A}$. Nous posons $\mathbb{L} = \bigcup_{i \in I} \mathbb{L}_i$, et si $a \in \mathbb{L}_i$, $b \in \mathbb{L}_j$, alors nous définissons

$$\begin{cases} a +_{\mathbb{L}} b = a +_k b & \text{(8.237a)} \\ a \times_{\mathbb{L}} b = a \times_k b & \text{(8.237b)} \end{cases}$$

où $k \in I$ est sélectionné de telle façon à avoir $(\mathbb{L}_i, +_i, \times_i) < (\mathbb{L}_k, +_k, \times_k)$ et $(\mathbb{L}_j, +_j, \times_j) < (\mathbb{L}_k, +_k, \times_k)$. Comme tous les corps L_i sont des sous-corps les uns des autres, c'est une bonne définition.

(4) **Lemme de Zorn** Nous utilisons le lemme de Zorn 1.42. Nous notons $(\mathbb{F}, +, \times)$ un élément maximal de $\mathcal{A}$. Puisque $\mathbb{K}$ en est un sous-corps, il n'y a pas d'ambiguïté de noter $+$ et $\times$ ses opérations.

(5) **Stratégie pour la suite** Nous allons montrer que si $\mathbb{E}$ est une extension algébrique de $\mathbb{F}$, alors $\mathbb{E} = \mathbb{F}$ (le but est d'utiliser le lemme 8.125).

(6) **Un peu de cardinalité** D'abord, comme $\mathbb{F}$ est algébrique sur $\mathbb{K}$, l'ensemble $\mathbb{F}$ est équipotent à $\mathbb{K}$ si $\mathbb{K}$ est infini, et au plus dénombrable, si $\mathbb{K}$ est fini ; c'est la proposition 8.130. En bref :

- Si $\mathbb{K}$ est infini, $\mathbb{K} \approx \mathbb{F} \approx \mathbb{E} \prec \Omega$.
- Si $\mathbb{K}$ est fini, $\mathbb{K} \preceq \mathbb{F} \preceq \mathbb{E} \prec \Omega$ où $\mathbb{E}$ est au maximum dénombrable et Ω est indénombrable.

Dans tous les cas, Ω est strictement surpotent à $\mathbb{F}$, et le lemme 2.61 permet de dire

$$\mathbb{E} \setminus \mathbb{F} \preceq \mathbb{E} \prec \Omega \approx \Omega \setminus \mathbb{F}. \tag{8.238}$$

(7) **Quelques injections** Il existe donc une injection $\varphi : \mathbb{E} \setminus \mathbb{F} \to \Omega \setminus \mathbb{F}$. Nous posons

$$\begin{aligned} f : \mathbb{E} &\to \Omega \\ x &\mapsto \begin{cases} x & \text{si } x \in \mathbb{F} \\ \varphi(x) & \text{si } x \notin \mathbb{F}. \end{cases} \end{aligned} \tag{8.239}$$

Nous montrons que f est injective. Soient $x, y \in \mathbb{E}$ tels que $f(x) = f(y)$. Si $x, y \in \mathbb{F}$, alors $x = f(x) = f(y) = y$. Si $x \in \mathbb{F}$ et $y \notin \mathbb{F}$, alors $x = \varphi(y)$ alors que $x \in \mathbb{F}$ et $\varphi(y) \in \Omega \setminus F$; ce cas est impossible. Enfin si x et y sont hors de $\mathbb{F}$, alors $f(x) = \varphi(x)$ et $f(y) = \varphi(y)$; donc $\varphi(x) = \varphi(y)$ et $x = y$ par injectivité de φ.

Nous avons donc bien une injection $f : \mathbb{E} \to \Omega$.

[62] Définition 8.75.
[63] Définition 1.71.

(8) **La maximalité**

Nous pouvons mettre sur $f(\mathbb{E}) \subset \Omega$ la structure de corps venant de $\mathbb{E}$. Comme $f(\mathbb{F}) = \mathbb{F}$, le corps $f(\mathbb{E})$ est une extension algébrique de $\mathbb{F}$. Par maximalité, $f(\mathbb{E}) = \mathbb{F}$.

Mais si $x \in \mathbb{E} \setminus \mathbb{F}$, alors $f(x) \in \Omega \setminus \mathbb{F}$. Donc en réalité nous avons aussi $\mathbb{E} \subset \mathbb{F}$.

(9) **Conclusion** En conclusion $\mathbb{E} = \mathbb{F}$ et le lemme 8.125 termine en disant que $\mathbb{F}$ est une clôture algébrique de $\mathbb{K}$.

Nous passons à la partie « unicité » de la clôture algébrique. Étant donné que $\mathbb{F}_1$ est une extension algébrique de $\mathbb{K}$ et que $\mathbb{F}_2$ est algébriquement clos, le lemme 8.133 nous donne un morphisme de corps $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ tel que $\sigma \circ \alpha_1 = \alpha_2$.

Nous sommes donc dans la situation où $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ est une extension de corps où $\mathbb{F}_1$ est algébriquement clos et $\mathbb{F}_2$ est algébrique. Le lemme 8.80 conclut que $\sigma(\mathbb{F}_1) = \mathbb{F}_2$, c'est-à-dire que σ est surjectif. En tant que morphisme de corps, σ était déjà injective ; elle est donc bijective.

Donc $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ est un isomorphisme de corps vérifiant $\sigma \circ \alpha_1 = \alpha_2$. □

8.135.
Bien que $\mathbb{C}$ soit une extension algébriquement close de $\mathbb{Q}$, l'ensemble $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$. C'est ce que nous montrons maintenant.

LEMooRDIZooRjWNMa

Lemme 8.136.
Le corps $\mathbb{C}$ n'est pas une clôture algébrique[64] *de $\mathbb{Q}$.*

Démonstration. Nous montrons qu'il existe des éléments de $\mathbb{C}$ qui ne sont pas des racines de polynômes à coefficients rationnels. L'ensemble $\mathbb{Q}$ est dénombrable par la proposition 4.17. L'ensemble des polynômes de degré n à coefficients dans $\mathbb{Q}$ est en bijection avec les n-uples de rationnels, c'est-à-dire avec $\mathbb{Q}^n$ qui est également dénombrable par la proposition 2.47. Enfin l'ensemble des polynômes à coefficients sur $\mathbb{Q}$ est l'union des polynômes de degré fixés, donc dénombrable par la proposition 2.42.

Jusqu'ici nous avons prouvé que l'ensemble des polynômes à coefficients rationnels était dénombrable. Or chaque polynôme possède une quantité finie de racines par le corolaire 3.287. Donc la partie de $\mathbb{C}$ constituée des nombres qui sont des racines de polynômes à coefficients dans $\mathbb{Q}$ est dénombrable. Mais $\mathbb{C}$ n'est pas dénombrable, donc possède des éléments qui ne sont pas des racines de polynômes. □

La proposition suivante est une conséquence de Steinitz 8.134, de 8.62.

PROPooZWVPooStuTAO

Proposition 8.137 (Clôture algébrique de $\mathbb{R}$[208])**.**
Le corps $\mathbb{C}$ est l'unique (à isomorphisme près) clôture algébrique de $\mathbb{R}$. Son degré est 2.

8.4.9 Polynômes à plusieurs variables

Nous avons déjà vu $A[X, Y]$ lorsque A est un anneau en la définition 3.180.

DEFooRHRKooPqLNOp

Définition 8.138.
Soit un corps $\mathbb{K}$. Le corps $\mathbb{K}(X_1, \dots, X_n)$ est le corps des fractions de l'anneau $\mathbb{K}[X_1, \dots, X_n]$.

DEFooOCPHooXneutp

Définition 8.139.
Soient un corps $\mathbb{K}$ et une extension $\mathbb{L}$ de $\mathbb{K}$ contenant les éléments α_1,..., α_n de $\mathbb{L}$. Nous définissons $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ comme étant l'intersection de tous les sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et les α_i.

La proposition suivante est analogue à 8.98(2).

LEMooQEJHooAmSNxU

Lemme 8.140 ([1])**.**
Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ et des éléments $\alpha_1, \dots, \alpha_n$ dans $\mathbb{L}$. Alors[65]

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \{r(\alpha_1, \dots, \alpha_n) \text{ tel que } r \in \mathbb{K}(X_1, \dots, X_n)\}. \tag{8.240}$$

EQooDYLXooYtZtwC

Démonstration. Ce que nous avons à droite est un corps : par exemple pour l'inverse, si $r = P/Q$ alors $r(\alpha_1, \dots, \alpha_n) = P(\alpha_1, \dots, \alpha_n)Q(\alpha_1, \dots, \alpha_n)^{-1}$. Cet élément a un inverse en la fraction $(Q/P)(\alpha_1, \dots, \alpha_n)$.

Donc à droite nous avons un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ ainsi que les α_i. Donc

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) \subset \big\{r(\alpha_1, \dots, \alpha_n) \text{ tel que } r \in \mathbb{K}(X_1, \dots, X_n)\big\}. \tag{8.241}$$

[64] Clôture algébrique, définition 8.75.

[65] Dans l'expression (8.240), seuls les r tels que $r(\alpha_1, \dots, \alpha_n)$ est bien défini sont pris en compte. Il faut exclure les r sont le dénominateur s'annule en $(\alpha_1, \dots, \alpha_n)$. Voir [203].

D'autre part, tout corps contenant $\mathbb{K}$ et les α_i doit contenir tous les $P(\alpha_1,\dots,\alpha_n)$ ($P\in\mathbb{K}[X_1,\dots,X_n]$), leurs inverses ainsi que leurs produits ; bref doit contenir tous les $r(\alpha_1,\dots,\alpha_n)$ avec $r\in\mathbb{K}[X_1,\dots,X_n]$. □

8.4.10 Corps de décomposition

DEFooEKGZooSkvbum

Définition 8.141 (Corps de décomposition)**.**
*Soit $\mathbb{K}$ un corps commutatif et $F=(P_i)_{i\in I}$ une famille d'éléments non constants de $\mathbb{K}[X]$. Un **corps de décomposition** de F est une extension $\mathbb{L}$ de $\mathbb{K}$ telle que*

(1) les P_i sont scindés sur $\mathbb{L}$,

(2) $\mathbb{L}=\mathbb{K}(R)$ où $R=\bigcup_{i\in I}\{x\in\mathbb{L}$ tel que $P_i(x)=0\}$.

C'est-à-dire que $\mathbb{L}$ étend $\mathbb{K}$ par toutes les racines de tous les polynômes de F.

PROPooDPOYooFHcqkU

Proposition 8.142 ([209])**.**
Tout polynôme admet un corps de décomposition. Plus précisément, soit un corps $\mathbb{K}$ et un polynôme $P\in\mathbb{K}[X]$ de degré n. Il existe un corps de décomposition $\mathbb{D}$ de la forme $\mathbb{D}=\mathbb{K}(\alpha_1,\dots,\alpha_n)$ où les α_i sont des racines de P dans $\mathbb{D}$.

Notons que rien dans l'énoncé ne prétend que les α_i soient tous distincts, ni même que certains (voire tous) ne seraient pas dans $\mathbb{K}$.

Démonstration. Soient un corps $\mathbb{K}$ et un polynôme $P\in\mathbb{K}[X]$. Si le degré de P est 0 ou 1, alors $\mathbb{K}$ est un corps de décomposition pour P. Pour le reste nous faisons une récurrence sur le degré de P.

Il y a deux possibilités, soit il existe $\alpha\in\mathbb{K}$ tel que $P(\alpha)=0$, soit non.

(1) **Si racine dans $\mathbb{K}$** Alors le corolaire 8.109 nous permet de factoriser $X-\alpha$:

$$P=(X-\alpha)Q \tag{8.242}$$

avec $\deg(Q)=\deg(P)-1$. Dans ce cas, $\mathbb{K}$ est un corps de rupture de P.

(2) **Si pas de racines dans $\mathbb{K}$**
Nous prenons alors un corps de rupture $\mathbb{L}=\mathbb{K}(\alpha)$ avec $P(\alpha)=0$ (c'est la proposition 8.119 qui donne l'existence d'un corps de rupture). Dans $\mathbb{L}_1$ nous avons

$$P=(X-\alpha)Q \tag{8.243}$$

avec $Q\in\mathbb{L}_1[X]$ et $\deg(Q)=\deg(P)-1$.

(3) **Dans les deux cas**
Dans les deux cas, par hypothèse de récurrence nous avons un corps de décomposition pour Q qui se présente sous la forme

$$\mathbb{L}=\mathbb{K}(\alpha_1,\dots,\alpha_{n-1}). \tag{8.244}$$

De plus, $\mathbb{L}$ est une extension de $\mathbb{L}_1$ parce que c'est une extension du corps sur lequel est Q.

Pour terminer la preuve nous prouvons que

$$\mathbb{D}=\mathbb{K}(\alpha_1,\dots,\alpha_{n-1},\alpha) \tag{8.245}$$

est un corps de décomposition de P. Vu que $\mathbb{D}$ contient $\mathbb{K}(\alpha)$ (comme cas particulier du lemme 8.140), dans $\mathbb{D}$ nous avons l'égalité $P=(X-\alpha)Q$. Et vu que $\mathbb{D}$ contient également $\mathbb{K}(\alpha_1,\dots,\alpha_{n-1})$, toujours dans $\mathbb{D}$ nous avons aussi

$$Q=(X-\alpha_1)\dots(X-\alpha_{n-1}). \tag{8.246}$$

Donc nous avons dans $\mathbb{D}$ l'égalité

$$P=(X-\alpha)(X-\alpha_1)\dots(X-\alpha_{n-1}). \tag{8.247}$$

□

LEMooJNGWooTXdGre

Lemme 8.143 ([1])**.**
Soit un polynôme $P\in\mathbb{K}[X]$, et un corps $\mathbb{L}$ dans lequel P est scindé. Si $P=P_1\dots P_r$ est la décomposition de P en irréductibles dans $\mathbb{K}$, alors chacun des P_i est scindé dans $\mathbb{L}$.

Démonstration. Juste pour le mentionner, le fait que P ait une décomposition en irréductibles est le fait que $\mathbb{K}[X]$ soit factoriel, c'est-à-dire la proposition 8.36.

Le polynôme P est scindé dans $\mathbb{L}$, c'est-à-dire que, en notant n le degré de P,

$$P = \prod_{i=1}^{n}(X - \lambda_i) \tag{8.248}$$

EQooNFXSooUkWsQu

avec $\lambda_i \in \mathbb{L}$.

Soit $\mathbb{L}_1$, une extension de $\mathbb{L}$ dans laquelle P_1 est scindé. Ensuite, $\mathbb{L}_2$ une extension de $\mathbb{L}_1$ dans laquelle P_2 est scindé et ainsi de suite. Nous avons construit $\mathbb{L}_r$, une extension de $\mathbb{L}$ dans laquelle tous les P_i sont scindés ainsi que P lui-même. Dans ce corps nous avons l'égalité

$$P = \prod_{k=1}^{n}(X - \mu_k) \tag{8.249}$$

EQooBEFUooBnqSUS

où les μ_k sont des éléments des diverses extensions $\mathbb{L}_i$, et sont les racines des P_i. En tout cas, tous sont dans $\mathbb{L}_r$.

Les deux décompositions (8.248) et (8.249) sont des décompositions dans $\mathbb{L}_r[X]$ du polynôme P. Vu que ce dernier est factoriel, en réalité les deux décompositions sont identiques (se souvenir de la définition 3.194), et nous avons $\mu_k \in \mathbb{L}$ pour tout k. Toutes les extensions $\mathbb{L}_i$ sont en réalité triviales, et nous avons $\mathbb{L}_r = \mathbb{L}$.

Bref, tout cela pour dire que les P_i ont toutes leurs racines dans $\mathbb{L}$. □

THOooQVKWooZAAYxK

Théorème 8.144 ([196]).
Soient :

(1) *un isomorphisme de corps $\tau\colon \mathbb{K} \to \mathbb{K}'$;*

(2) *un polynôme non constant $P \in \mathbb{K}[X]$ de degré n ;*

(3) *un corps de décomposition $\mathbb{L}$ de P sur $\mathbb{K}$;*

(4) *un corps de décomposition $\mathbb{L}'$ de $\tau(P)$ sur $\mathbb{K}'$;*

Alors τ se prolonge en un isomorphisme $\sigma\colon \mathbb{L} \to \mathbb{L}'$.

Démonstration. Soit m le nombre de racines de P dans $\mathbb{L} \setminus \mathbb{K}$. Nous faisons une récurrence sur m.

Si $m = 0$ alors $\mathbb{K}$ est un corps de rupture de P ; nous avons

$$P = (X - \lambda_1)\dots(X - \lambda_n) \tag{8.250}$$

avec $\lambda_i \in \mathbb{K}$. Dans ce cas nous avons aussi

$$\tau(P) = \big(X - \tau(\lambda_1)\big)\dots\big(X - \tau(\lambda_n)\big) \tag{8.251}$$

avec $\tau(\lambda_i) \in \mathbb{K}'$. Nous avons donc $\mathbb{L}' = \mathbb{K}'$ et prendre $\sigma = \tau$ fonctionne.

Nous supposons à présent que $m > 0$. Plus précisément nous considérons un polynôme possédant exactement m racines dans $\mathbb{L} \setminus \mathbb{K}$. Soit

$$P = P_1 \dots P_r \tag{8.252}$$

sa décomposition en irréductibles dans $\mathbb{K}[X]$ (notons que $r \leqslant n$ parce que chacun des facteurs est de degré au moins 1). Au moins un des P_i est de degré plus grand ou égal à 2. Nous savons de la proposition 8.36 que $\mathbb{K}[X]$ est un anneau factoriel. Le lemme 8.143 nous assure que les polynômes P_i sont également scindés dans $\mathbb{L}$. Et l'unicité de la décomposition fait en sorte que les racines des P_i sont celles de P.

Soit $\alpha \in \mathbb{L}$, une racine de P_1. Vu que P_1 est irréductible sur $\mathbb{K}$, l'application suivante est un isomorphisme de corps par le lemme 8.83 :

$$\begin{aligned}\psi\colon \mathbb{K}[X]/(P_1) &\to \mathbb{K}[\alpha]\\ \bar{Q} &\mapsto Q(\alpha).\end{aligned} \tag{8.253}$$

Notons que le lemme parle du quotient par le polynôme minimal, mais ici nous avons un irréductible. Un polynôme annulateur irréductible est multiple du polynôme minimal, et l'idéal engendré est le même.

Nous avons aussi la décomposition

$$\tau(P) = \tau(P_1)\dots\tau(P_r), \tag{8.254}$$

et chacun des $\tau(P_i)$ a ses racines dans $\mathbb{L}'$. Soit β, une racine de $\tau(P_1)$ dans $\mathbb{L}'$. Alors nous avons l'isomorphisme

$$\psi'\colon \mathbb{K}'[X]/\big(\tau(P_1)\big) \to \mathbb{K}'[\beta]. \tag{8.255}$$

De plus, par le lemme 8.46, nous savons que τ passe aux classes :

$$\phi_\tau\colon \mathbb{K}[X]/(P_1) \to \mathbb{K}'[X]/\big(\tau(P_1)\big) \tag{8.256}$$

est un isomorphisme d'anneaux. Et enfin, dernier résultat externe à invoquer, la proposition 8.103 nous assure que $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$ et $\mathbb{K}'[\beta] = \mathbb{K}'(\beta)$. Posons pour l'occasion $\mathbb{K}_1 = \mathbb{K}(\alpha)$ et $\mathbb{K}'_1 = \mathbb{K}'(\beta)$.

Nous avons l'enchainement suivant d'isomorphismes de corps[66] :

$$\tau_1 = \psi' \circ \phi_\tau \circ \psi^{-1}\colon \mathbb{K}_1 \to \mathbb{K}[X]/(P_1) \to \mathbb{K}'[X]/\big(\tau(P_1)\big) \to \mathbb{K}'_1. \tag{8.257}$$

Cet isomorphisme $\tau_1\colon \mathbb{K}_1 \to \mathbb{K}'_1$ prolonge τ. Si vous aimez les diagrammes, en voici un sur lequel les i représentent des inclusions et où τ et τ_1 sont des isomorphismes

$$\begin{array}{ccccc} \mathbb{K} & \xrightarrow{i} & \mathbb{K}_1 & \xrightarrow{i} & \mathbb{L} \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau_1} & & \\ \mathbb{K}' & \xrightarrow[i]{} & \mathbb{K}'_1 & \xrightarrow{i} & \mathbb{L}' \end{array} \tag{8.258}$$

Le corps $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}_1$, et le nombre de racines de P dans $\mathbb{L} \setminus \mathbb{K}_1$ est strictement plus petit que m parce qu'il y en a exactement m dans $\mathbb{L} \setminus \mathbb{K}$ et que $\mathbb{K}_1$ en a au moins une de plus que $\mathbb{K}$. Même raisonnement pour $\mathbb{K}'$, $\mathbb{K}'_1$ et $\mathbb{L}'$.

Résumons la situation :

- $\tau_1\colon \mathbb{K}_1 \to \mathbb{K}'_1$ est un isomorphisme de corps ;
- $P \in \mathbb{K}_1[X]$ est un polynôme non constant ;
- $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}_1$;
- $\mathbb{L}'$ est un corps de décomposition de P sur $\mathbb{K}'_1$;
- le nombre de racines de P dans $\mathbb{L} \setminus \mathbb{K}_1$ est strictement inférieur à m.

Donc, par hypothèse de récurrence sur m, il existe un isomorphisme $\sigma\colon \mathbb{L} \to \mathbb{L}'$ qui prolonge τ_1. Vu que τ_1 prolonge τ, nous avons également σ qui prolonge τ. □

L'énoncé le plus compact pour l'unicité du corps de décomposition (à isomorphisme près) est le suivant :

PropTMkfyM

Proposition 8.145.
Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. Soient $\mathbb{L}$ et $\mathbb{F}$ deux corps de décomposition de P. Alors il existe un isomorphisme $f\colon \mathbb{L} \to \mathbb{F}$ tel que $f|_{\mathbb{K}} = \mathrm{Id}$.

Démonstration. C'est un cas particulier du théorème 8.144, où nous considérons $\mathbb{K} = \mathbb{K}'$ muni de l'isomorphisme identité. □

Cependant le passage par l'énoncé plus compliqué 8.144 est nécessaire pour les besoins de la récurrence.

8.146.
À propos de terminologie. Lorsque nous disons « *un* corps de décomposition » nous référons à la définition 8.141 et il n'y a pas vraiment unicité. Si nous disons « *le* corps de décomposition » nous référons en général à celui construit dans la proposition 8.142 qui n'est en réalité même pas très explicite.

Quoi qu'il en soit, nous nous permettons de dire « le » corps de décomposition lorsque nous parlons de propriétés invariantes par isomorphisme.

8.147.
La construction du corps de décomposition d'un polynôme fonctionne en prenant successivement le corps de rupture des facteurs irréductibles. Nous insistons sur le fait que cette opération se fait sur chaque facteur irréductible séparément.

L'exemple suivant montre dans quel ordre se passent les choses.

[66] En réalité il est plus exact de dire « isomorphisme d'anneaux », parce que la structure de corps n'est en réalité aucune nouvelle structure par rapport à l'anneau.

Exemple 8.148.
Soit le polynôme $P = X^4 - 5X^2 + 6$. Sa factorisation en irréductibles est :

$$P = (X^2 - 2)(X^2 - 3). \tag{8.259}$$

Ce polynôme n'est pas irréductible sur $\mathbb{Q}$ et il ne s'agit donc pas de prendre brutalement un corps de rupture pour P. Il s'agit de poser $P = P_1P_2$ avec

$$P_1 = X^2 - 2 \tag{8.260a}$$
$$P_2 = X^2 - 3, \tag{8.260b}$$

de remarquer que P_1 et P_2 sont irréductibles sur $\mathbb{Q}$ et de chercher des corps de rupture pour eux. On commence par P_1. Nous avons le corps de rupture $\mathbb{L}_1 = \mathbb{Q}(\sqrt{2})$ et la factorisation

$$P_1 = (X + \sqrt{2})(X - \sqrt{2}). \tag{8.261}$$

Ensuite nous considérons P_2 dans $\mathbb{L}_1[X]$. Ce P_2 est encore irréductible. Nous lui cherchons un corps de rupture, et c'est $\mathbb{L}_2 = \mathbb{L}_1(\sqrt{3})$ dans lequel nous avons

$$P_2 = (X - \sqrt{3})(X + \sqrt{3}). \tag{8.262}$$

Nous savons (par le lemme 8.124) que

$$\mathbb{L}_2 = \mathbb{L}_1(\sqrt{3}) = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}). \tag{8.263}$$

Nous pouvons donc écrire en toute confiance, dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ la factorisation

$$P = (X + \sqrt{2})(X - \sqrt{2})(X + \sqrt{3})(X - \sqrt{3}). \tag{8.264}$$

Et nous notons que si nous avions commencé par P_2 au lieu de P_1, nous aurions eu le même résultat final. △

CORooELAUooPQGLkR

Corolaire 8.149 ([1]).
Le corps de décomposition d'un polynôme est une extension finie.

Démonstration. Soient un corps $\mathbb{K}$, un polynôme $P \in \mathbb{K}[X]$ et un corps de décomposition $\mathbb{D}$ de P de la forme $\mathbb{D} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ où les α_i sont les racines de P dans $\mathbb{D}$. Cela existe par la proposition 8.142.

Vu que le lemme 8.124 donne

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \big(\mathbb{K}(\alpha_1, \dots, \alpha_{n-1})\big)(\alpha_n), \tag{8.265}$$

le corps $\mathbb{D}$ se construit comme une pile d'extensions finies. Les degrés se composant par le lemme 8.63, au final ce corps de décomposition est une extension finie.

Soit maintenant un corps de décomposition quelconque $\mathbb{L}$. La proposition 8.145 donne un isomorphisme de corps[67] $f : \mathbb{L} \to \mathbb{D}$ tel que f soit l'identité sur $\mathbb{K}$.

Si $\{v_i\}_{i\in I}$ est une base de $\mathbb{D}$ comme espace vectoriel sur $\mathbb{K}$, êtes-vous prêts à parier que $\{f(v_i)\}_{i\in I}$ est une base de $\mathbb{L}$ comme espace vectoriel sur $\mathbb{K}$[68] ? □

8.4.11 Non irréductible ou pas corps ?

SUBSECooEDMJooTXBfOu

Nous avons déjà mentionné que nous ne définissons le corps de rupture d'un polynôme que dans le cas de polynôme irréductible à coefficients dans un corps.

D'abord si P n'est pas irréductible, la question de chercher un corps de rupture n'a pas beaucoup de sens.

Si A est un anneau intègre et si P est un polynôme irréductible sur A, nous pouvons considérer le corps des fractions de A, dire $P \in \text{Frac}(A)[X]$ et continuer. Étendre la définition de corps de rupture de cette façon aux polynômes à coefficients dans un anneau intègre n'est pas une grande révolution.

Au lieu de cela, nous pouvons nous demander dans quel cas nous aurions que $A[X]/(P)$ est directement un corps.

Exemple 8.150.
Soit le polynôme constant $P = 2$ dans $\mathbb{Z}[X]$. Il y est irréductible parce qu'il ne peut pas être écrit comme produit de deux non inversibles. Ce polynôme a deux propriétés ennuyeuses :

- Il n'est plus irréductible sur $\mathbb{Q}$,
- Il n'existe aucun corps contenant une racine de P tout en contenant $\mathbb{Z}$ comme sous-anneau.

△

[67] Un isomorphisme de corps est juste un isomorphisme d'anneaux.
[68] Personnellement, je n'ai pas vérifié. Vérifiez vous-même et écrivez-moi pour dire si c'est bon ou non.

8.4.12 Clôture algébrique

THOooQFWWooMWXEhT

Théorème 8.151.
Tout corps $\mathbb{K}$ possède une clôture algébrique[69] *Ω. De plus si $\mathbb{L}$ est une extension de $\mathbb{K}$, alors $\mathbb{L}$ est $\mathbb{K}$-isomorphe à un sous corps de Ω.*

Les deux parties de ce théorème utilisent l'axiome du choix.

Notons en particulier que si Ω' est une autre clôture algébrique de $\mathbb{K}$, alors Ω et Ω' sont des sous corps l'un de l'autre et sont donc $\mathbb{K}$-isomorphes.

Lemme 8.152.
Les polynômes $P, Q \in \mathbb{K}[X]$ ne sont pas premiers entre eux si et seulement s'ils ont une racine commune dans la clôture algébrique Ω de $\mathbb{K}$.

Démonstration. Soit A un polynôme non inversible divisant P et Q. Par définition de Ω, ce polynôme A a une racine dans Ω qui est alors une racine commune à P et Q dans Ω.

Pour le sens inverse, si α est une racine commune de P et Q, alors le polynôme $X - \alpha$ divise P et Q et donc P et Q ne sont pas premiers entre eux. □

ExfUqQXQ

Exemple 8.153.
Soit p un nombre premier. Montrons que le polynôme

$$Q(X) = X^p - X + 1 \tag{8.266}$$

est irréductible dans $\mathbb{F}_p$.

Nous supposons qu'il n'est pas irréductible, c'est-à-dire que

$$Q(X) = R(X)S(X) \tag{8.267}$$

avec R et S, des polynômes de degrés $\geqslant 1$ dans $\mathbb{F}_p[X]$

Soit $\bar{\mathbb{F}}_p$ une clôture algébrique[70] de $\mathbb{F}_p$ et $\alpha \in \bar{\mathbb{F}}_p$ tel que $R(\alpha) = 0$. Pour tout $a \in \mathbb{F}_p$, nous avons

$$\begin{aligned} Q(\alpha + a) &= (\alpha + a)^p - (\alpha + a) + 1 && \text{(8.268a)}\\ &= \alpha^p + a^p - \alpha - a + 1 && \text{(8.268b)}\\ &= \alpha^p - \alpha + 1 && \text{(8.268c)}\\ &= Q(\alpha) && \text{(8.268d)}\\ &= 0 && \text{(8.268e)} \end{aligned}$$

où nous avons utilisé le fait que $a^p = a$ et que α était une racine de Q. Ce que nous venons de prouver est que l'ensemble des racines de Q dans $\bar{\mathbb{F}}_p$ est donné par $\{\alpha + a \text{ tel que } a \in \mathbb{F}_p\}$.

Les polynômes R et S sont donc formés de produits de termes $X - (\alpha + a)$ avec $a \in \mathbb{F}_p$. L'un des deux –disons R pour fixer les idées– doit bien en avoir plus que 1. Nous avons alors

$$R(X) = \prod_{i=1}^{k} \big(X - (\alpha + a_i)\big) \tag{8.269}$$

où les a_i sont les éléments de $\mathbb{F}_p$. En développant un peu,

$$R(X) = X^k - \sum_{i=1}^{k} (\alpha + a_i) X^{k-1} + \text{termes de degré plus bas en } X. \tag{8.270}$$

Le coefficient devant X^{k-1} n'est autre que $k\alpha + \sum_i a_i$. Étant donné que $k \neq 0$ et que $R \in \mathbb{F}_p[X]$, nous devons avoir $\alpha \in \mathbb{F}_p$. Par conséquent nous avons $\alpha^p = \alpha$ et une contradiction :

$$Q(\alpha) = \alpha^p - \alpha + 1 = 1 \neq 0. \tag{8.271}$$

Le polynôme $X^p - X + 1$ est donc irréductible sur $\mathbb{F}_p$. △

[69] Définition 8.75.
[70] Définition 8.75. Pour l'existence c'est le théorème 8.151.

8.4.13 Dérivée de polynômes

DEFooICHTooAggARW

Définition 8.154 ([210]).
Soit un anneau A ainsi que $a_i \in A$. Pour le polynôme $P = \sum_{k=0}^{n} a_k X^k$, nous définissons le ***polynôme dérivé***

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}. \tag{8.272}$$

LEMooEFQQooTzDanH

Lemme 8.155 (Règle de Leibniz[210]).
Soit un anneau A. Nous considérons l'application dérivée[71]

$$\begin{aligned} D\colon A[X] &\to A[X] \\ P &\mapsto P'. \end{aligned} \tag{8.273}$$

(1) L'application D est A-linéaire.

(2) Elle vérifie $(PQ)' = PQ' + P'Q$.

LEMooFNFYooAfIPRT

Lemme 8.156 ([210]).
Soit un corps $\mathbb{K}$. Nous considérons l'application de dérivation[72] *$D\colon \mathbb{K}[X] \to \mathbb{K}[X]$.*

(1) Si $\mathbb{K}$ est de caractéristique nulle, alors $\ker(D) = \mathbb{K}$.

(2) Si $\mathbb{K}$ est de caractéristique $p \neq 0$, alors $\ker(D) = \mathbb{K}[X^p]$.

Ici, $\mathbb{K}[X^p]$ est un gros abus de notations pour dire

$$\mathbb{K}[X^p] = \{Q(X^p) \text{ tel que } Q \in \mathbb{K}[X]\}. \tag{8.274}$$

8.4.14 Extensions séparables

Notons que dans ce qui va suivre nous allons parler de $\mathbb{K}[X]$, l'ensemble des polynômes sur un corps. Cela ne s'applique donc pas à $\mathbb{Z}[X]$ par exemple.

Une des choses intéressantes avec les extensions séparables c'est qu'elles vérifient le théorème de l'élément primitif 8.171.

LEMooGUUJooDSrQFU

Lemme 8.157 ([210]).
Soit un corps $\mathbb{K}$. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Nous avons équivalence entre :

ITEMooHMMMooWKzSLA

(1) a est une racine multiple[73] *de P.*

ITEMooZXCTooPctrMm

(2) $(X-a) \mid P$ et $(X-a) \mid P'$.

ITEMooBMSSooNOYfKn

(3) $P(a) = P'(a) = 0$

Démonstration. Soit n la multiplicité de la racine a de P. Éventuellement $n = 0$ si a n'est en réalité pas une racine. Nous avons

EQooRGYSooSkATBv

$$P = (X-a)^n Q \tag{8.275}$$

avec $Q(a) \neq 0$.

En ce qui concerne la dérivée, si $n = 0$ nous avons $P' = Q'$, et si $n \geqslant 1$ nous avons

EQooQLINooPKUENl

$$P' = n(X-a)^{n-1}Q + (X-a)^n Q'. \tag{8.276}$$

Nous faisons maintenant la preuve.

(1) **(1) implique (2)** Nous supposons que a est une racine multiple, c'est-à-dire $n \geqslant 2$. Les relations (8.275) et (8.276) nous montrent que $(X-a)$ divise aussi bien P que P'.

(2) **(2) implique (3)** Celle-ci est facile. Les hypothèses sont qu'il existe des polynômes A et B tels que $P = (X-a)A$ et $P' = (X-a)B$. Nous avons alors bien $P(a) = P'(a) = 0$.

[71] Définition 8.154.
[72] Voir lemme 8.155.
[73] Racine multiple, définition 3.280.

(3) **(3) implique (1)** Nous avons $P = (X-a)^n Q$ avec $Q(a) \neq 0$. Par hypothèse $P(a) = 0$. Donc $n \geqslant 1$. Nous pouvons alors utiliser la formule (8.276) pour la dérivée :

$$P' = n(X-a)^{n-1}Q(a) + (X-a)^n Q'. \tag{8.277}$$

Nous avons donc $P'(a) = n0^{n-1}Q(a)$ avec $Q(a) \neq 0$. Par hypothèse $P'(a) = 0$ et donc $n - 1 \geqslant 0$, ce qui signifie $n \geqslant 2$ et donc que a est une racine multiple de P.

□

Proposition 8.158.
Soit P irréductible dans $\mathbb{K}[X]$ ayant des racines distinctes dans le corps de décomposition $\mathbb{L}$. Si $\mathbb{L}'$ est un autre corps de décomposition pour P, alors P a aussi ses racines distinctes dans $\mathbb{L}'$.

Démonstration. L'ingrédient est la proposition 8.145 qui donne l'unicité du corps de décomposition à $\mathbb{K}$-isomorphisme près. Soit donc $\psi\colon \mathbb{L} \to \mathbb{L}'$ un isomorphisme laissant invariant les éléments de $\mathbb{K}$. D'une part, étant donné que P est à coefficients dans $\mathbb{K}$, nous avons $\psi(P) = P$. D'autre part dans $\mathbb{L}$ le polynôme P s'écrit

$$P = a(X-\alpha_1)\dots(X-\alpha_n) \tag{8.278}$$

avec $a \in \mathbb{K}$ et $\alpha_i \in \mathbb{L}$. Nous avons donc

$$P = \psi(P) = a(X-\psi(\alpha_1))\dots(X-\psi(\alpha_n)). \tag{8.279}$$

Donc les racines de P dans $\mathbb{L}'$ sont les éléments $\psi(\alpha_i)$ qui sont distincts. □

Exemple 8.159.
Un polynôme peut être séparable sur un corps, mais non séparable sur un autre. Soit $\mathbb{L} = \mathbb{F}_p(T)$ et $\mathbb{K} = \mathbb{F}_p(T^p)$. Nous considérons le polynôme

$$P = X^p - T^p \tag{8.280}$$

dans $\mathbb{K}[X]$. Par le morphisme de Frobenius nous avons

$$P = (X-T)^p \tag{8.281}$$

dans $\mathbb{L}[X]$. Le polynôme P est irréductible sur $\mathbb{K}[X]$ parce que ses diviseurs sont de la forme $(X-T)^k$ qui contiennent T^k qui n'est pas dans $\mathbb{K}$ (sauf si $k = n$ ou $k = 0$).

Ce polynôme n'est pas séparable sur $\mathbb{K}$ parce que dans le corps de décomposition $\mathbb{L}$, la racine T est multiple. Notons bien le raisonnement : P étant irréductible, pour savoir si il est séparable, on le regarde dans un corps de décomposition.

Par contre si nous regardons P dans $\mathbb{L}[X]$ alors P n'est plus irréductible parce que ses facteurs irréductibles sont $(X-T)$. N'étant pas irréductible, nous regardons les racines de *ses facteurs irréductibles*. Or chacun des facteurs irréductibles étant $X - T$, les racines sont simples. △

Exemple 8.160.
Le polynôme $X^3 - 1$ est séparable sur $\mathbb{Q}$ parce que ses facteurs irréductibles dans $\mathbb{Q}[X]$ sont $X - 1$ et $X^2 + X + 1$, et ces deux polynômes ont des racines simples (dans $\mathbb{Q}(i)$). △

Exemple 8.161.
Le polynôme $(X^2+1)^2$ est séparable dans $\mathbb{Q}[X]$. En effet, il a pour facteurs irréductibles le polynôme X^2+1 (en deux exemplaires), et ce polynôme a pour racines $\pm i$ dans l'extension $\mathbb{Q}(i)$, racines qui sont simples pour ce polynôme. △

PropolyeZff

Proposition 8.162 ([211])**.**
Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Les propriétés suivantes sont équivalentes.

ItemdqPFUi

(1) Il existe une extension de $\mathbb{K}$ dans laquelle P a une racine multiple.

ItemdqPFUib

(2) P a une racine multiple dans tout corps de décomposition .

ItemdqPFUii

(3) P et P' ont une racine commune dans une extension de $\mathbb{K}$.

ItemdqPFUiii

(4) le degré de $\operatorname{pgcd}(P, P')$ *est* $\geqslant 1$.

Démonstration. En plusieurs parties.

(1) **(1)⇒(2)** Soit a, une racine multiple de P dans une extension $\mathbb{L}$ de $\mathbb{K}$, et $\mathbb{E}$, un corps de décomposition de P. Alors nous voulons prouver que P ait une racine multiple dans $\mathbb{E}$.

Nous pouvons voir $P \in \mathbb{L}[X]$, et construire un corps de décomposition $\mathbb{E}'$ qui est une extension de $\mathbb{L}$. Vu que $\mathbb{E}$ et $\mathbb{E}'$ sont deux corps de décomposition de P nous avons un isomorphisme $\psi\colon \mathbb{E}' \to \mathbb{E}$. Si $a \in \mathbb{E}$ est une racine multiple de P, alors $\psi(a)$ est une racine multiple de P dans $\mathbb{E}'$ parce que

$$P\big(\psi(a)\big) = \psi\big(P(a)\big). \tag{8.282}$$

(2) **(2)⇒(3)** Soit $\mathbb{L}$ un corps de décomposition de P sur $\mathbb{K}$ et $a \in \mathbb{L}$, une racine multiple de P. On a alors $P = (X-a)^2Q$ avec $Q \in \mathbb{L}[X]$. En dérivant,

$$P' = 2(X-a)Q + (X-a)^2Q', \tag{8.283}$$

et donc a est également une racine de P'.

(3) **(3)⇒(4)** Soit D un pgcd de P et P'. D'après le théorème de Bézout il existe $A, B \in \mathbb{K}[X]$ tels que

$$AP + BP' = D. \tag{8.284}$$

Si a est une racine commune de P et P' dans une extension $\mathbb{L}$, alors c'est aussi une racine de D et donc $\deg(D) \geqslant 1$.

(4) **(4)⇒(1)** Si le degré de D est plus grand ou égal à 1, alors nous considérons une racine a de D dans $\mathbb{L}$ (une extension de $\mathbb{K}$). Étant donné que D divise P et P', l'élément a est une racine commune de P et P'. Nous montrons maintenant que a est alors une racine multiple de P. Vu que $P(a) = 0$ nous avons

$$P = (X-a)Q, \tag{8.285}$$

et $P' = Q + (X-a)Q'$. Mais alors $P'(a) = Q(a)$ et donc $Q(a) = 0$ et donc a est une racine double de P. Par conséquent a est une racine multiple de P dans $\mathbb{K}$.

□

Notons que si P est irréductible, cette proposition donne des conditions pour que P ne soit pas séparable.

LEMooVWBPooQITlUL

Lemme 8.163 ([199]).
Soient un corps $\mathbb{K}$ ainsi qu'un polynôme irréductible non nul $P \in \mathbb{K}[X]$. Soit un polynôme $Q \in \mathbb{K}[X]$. Alors P divise Q si et seulement si $\operatorname{pgcd}(P,Q) \neq 1$.

Démonstration. Nous notons $D = \operatorname{pgcd}(P,Q)$. C'est un polynôme qui divise P. De plus P est irréductible, donc non inversible. Vu que P est non nul, nous avons $\deg(P) \geqslant 1$.

(1) $\Rightarrow$ Nous supposons que P divise Q. Alors P est un diviseur commun de P et Q. Le lemme 8.55 (qui n'est en fait qu'une répétition de la définition du pgcd) nous dit alors que P divise $\operatorname{pgcd}(P,Q)$. Nous avons donc

$$0 < \deg(P) \leqslant \deg\big(\operatorname{pgcd}(P,Q)\big). \tag{8.286}$$

Donc le polynôme $\operatorname{pgcd}(P,Q)$ est un polynôme non constant et n'est en particulier pas 1.

(2) $\Leftarrow$ Le polynôme D est un diviseur commun de P et Q. En particulier $P = SD$ pour un certain polynôme S. Étant donné que P est irréductible, soit S soit D (ou les deux) est inversible. Par hypothèse $D \neq 1$, et comme D est unitaire, nous savons que D n'est pas un inversible. Bref, S est un inversible, c'est-à-dire que $S = k \in \mathbb{K}$. Nous notons que

$$P = kD. \tag{8.287}$$

EQooQESZooDHgkWn

Le polynôme D divise également Q. Il existe $T \in \mathbb{K}[X]$ tel que $Q = TD$. En remplaçant D par sa valeur déduite de (8.287) nous avons

$$Q = TD = k^{-1}TP, \tag{8.288}$$

ce qui signifie que P divise Q.

□

Nous rappelons à le très aimable lecteur que $\operatorname{pgcd}(P,Q)$ est l'unique polynôme unitaire parmi les PGCD de P et Q. La définition des PGCD est 1.113 et l'unicité de l'unitaire est dans le lemme 8.52(2).

PROPooPRGQooOkEmag

Proposition-Définition 8.164 ([210, 212]).
Soient un corps $\mathbb{K}$, un polynôme non constant $P \in \mathbb{K}[X]$ ainsi qu'une extension algébriquement close Ω et un corps de décomposition[74] *$\mathbb{M}$ pour P. Alors les propriétés suivantes sont équivalentes*[75] *:*

ITEMooVMJLooUdZLQR

(1) $\operatorname{pgcd}(P, P') = 1$.

(2) *P et P' n'ont de racines communes dans aucune extension de $\mathbb{K}$.*

(3) *P et P' n'ont pas de racines communes dans $\mathbb{M}$.*

(4) *P et P' n'ont pas de racines communes dans Ω.*

ITEMooARPLooBoUrxX

(5) *P n'a de racines multiples dans aucune extension de $\mathbb{K}$.*

(6) *P n'a que des racines simples dans $\mathbb{M}$.*

(7) *P n'a que des racines simples dans Ω.*

(8) *Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ ainsi que $\beta, \alpha_i \in \mathbb{L}$ tels que*

$$P = \beta \prod_{i=1}^{n} (X - \alpha_i) \tag{8.289}$$

où les α_i sont distincts.

(9) *Il existe $\beta, \alpha_i \in \mathbb{M}$ tels que $P = \beta \prod_{i=1}^{n} (X - \alpha_i)$ où les α_i sont distincts.*

(10) *Il existe $\beta, \alpha_i \in \Omega$ tels que $P = \beta \prod_{i=1}^{n} (X - \alpha_i)$ où les α_i sont distincts.*

*Un polynôme irréductible qui vérifie ces conditions est dit **séparable**.*

*Si P est un polynôme non constant dont la décomposition en irréductibles est $P = P_1 \dots P_r$, nous disons qu'il est **séparable** si tous les P_i le sont.*

PROPooMOZFooDGemBJ

Proposition 8.165 ([210, 212]).
Soit un corps $\mathbb{K}$ et un polynôme irréductible non nul $P \in \mathbb{K}[X]$. Les conditions suivantes sont équivalentes :

ITEMooDOTTooTZGhSq

(1) *P est séparable*[76]

ITEMooRTDCooJGEtum

(2) $P' \neq 0$

ITEMooZOMZooDPrNaC

(3) *Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P a une racine simple.*

Démonstration. En plusieurs parties.

(1) **(3) implique (2)** Soient une extension $\mathbb{L}$ de $\mathbb{K}$ ainsi qu'une racine simple $a \in \mathbb{L}$. Nous utilisons la proposition 3.284 : il existe un polynôme $Q \in \mathbb{L}[X]$ tel que $P = (X - a)Q(X)$ avec $\mathbb{L} \neq 0$.

Nous utilisons la règle de Leibniz (lemme 8.155) : $P' = (X-a)'Q(X) + (X-a)Q'(X) = Q(X) + (X-a)Q'(X)$. En évaluant en a,

$$P'(a) = Q(a) \neq 0. \tag{8.290}$$

(2) **(2) implique** $\operatorname{pgcd}(P, P') = 1$ Notons $D = \operatorname{pgcd}(P, P')$. Vu que D divise P, il existe un polynôme Q tel que $P = QD$. Le polynôme P étant irréductible, soit Q soit D est inversible. Supposons que Q est inversible. Alors $P = kD$ avec $k \in \mathbb{K}$. En particulier $\deg(P) = \deg(D)$. Mais comme D est un diviseur de P', nous avons

$$\deg(D) \leqslant \deg(P') < \deg(P). \tag{8.291}$$

Nous avons une contradiction.

Nous en déduisons que dans l'égalité $P = DQ$, c'est D qui est inversible. Donc $D \in \mathbb{K}$. Vu que D est unitaire[77], nous avons $D = 1$.

(3) **(2) implique (1)** Nous avons déjà vu que dans le cas (2) nous avons $\operatorname{pgcd}(P, P') = 1$. La proposition-définition 8.164(1) nous indique qu'alors P est séparable.

[74] Tout polynôme admet un corps de décomposition, proposition 8.142.
[75] Pour lee polynôme dérivé P', définition 8.154.
[76] Polynôme séparable, définition 8.164.
[77] Le pgcd de deux polynômes est l'unitaire parmi tous les pgcd, voir 8.53.

(4) **(1) implique (3)** La proposition 8.142 nous permet de considérer un corps de décomposition de P. Dans ce corps, P admet des racines (autant que son degré, mais c'est une autre histoire), et ces racines sont simples par la définition 8.164(5).

□

CorUjfJSE

Corolaire 8.166.
Si $\mathbb{K}$ est de caractéristique nulle, alors tout polynôme de $\mathbb{K}[X]$ est séparable.

Démonstration. Il suffit de montrer que les irréductibles sont séparables. Soit P un polynôme irréductible et unitaire de degré d. Le terme de plus haut degré de P' est alors dX^{d-1} qui est non nul parce que $d \neq 0$ en caractéristique nulle. Donc $P' \neq 0$ et donc P est séparable par la proposition 8.162. □

DEFooKTVHooTydOTM

Définition 8.167.
Soit $\mathbb{L}$ une extension algébrique de $\mathbb{K}$.

ITEMooOFYPooLYkIPr

*(1) On dit que l'élément $a \in \mathbb{L}$ est **séparable** sur $\mathbb{K}$ si son polynôme minimal dans $\mathbb{K}[X]$ est séparable sur $\mathbb{K}$ (définition 8.164).*

*(2) L'extension $\mathbb{L}$ est **séparable** si tous ses éléments sont séparables.*

PropUmxJVw

Proposition 8.168.
Soit $\mathbb{K}$ un corps. Les conditions suivantes sont équivalentes :

ITEMooUSKRooDmsGmw

(1) toutes les extensions algébriques de $\mathbb{K}$ sont séparables ;

ITEMooJGWLooKInxSG

(2) tout polynôme irréductible de $\mathbb{K}[X]$ est séparable.

En particulier les extensions algébriques des corps de caractéristique nulle sont toutes séparables.

Démonstration. En plusieurs parties.

(1) **(1) implique (2)**
Soit un polynôme irréductible P de $\mathbb{K}[X]$, et un corps de décomposition $\mathbb{L}$ de P. Cela est une extension algébrique par le corolaire 8.149. Elle est donc séparable par hypothèse.

Voilà une première chose de dite.

Maintenant, nous voudrions montrer que P est un polynôme séparable. Dans $\mathbb{L}$ nous avons

$$P = \prod_{i=1}^{n}(X - a_i), \tag{8.292}$$

et tout le défi est de prouver que les a_i sont tous distincts.

Soient deux racines $a, b \in \mathbb{L}$ de P. Nous considérons les polynômes minimaux μ_a et μ_b dans $\mathbb{K}[X]$. Ces deux polynômes divisent P parce que P est à la fois dans l'idéal annulateur de a et de b. Mais comme P est irréductible, il existe $k_a, k_n \in \mathbb{K}$ tels que $P = k_a\mu_a$ et $P = k_b\mu_b$. Donc les polynômes μ_a, μ_b et P sont multiples les uns des autres. Vu que μ_a et μ_n sont unitaires, $\mu_a = \mu_b$.

Nous avons :

$$P = k\mu = \prod_{i=1}^{n}(X - a_i). \tag{8.293}$$

Or le polynôme μ est irréductible par la proposition 8.67(1), et l'extension $\mathbb{L}$ est séparable, donc μ n'a que des racines simples, Donc tous les a_i sont distincts.

(2) **(2) implique (1)**
Soit une extension algébrique $\mathbb{L}$ de $\mathbb{K}$. Soit $a \in \mathbb{L}$. Nous devons prouver que le polynôme minimal de a dans $\mathbb{K}$ est séparable, c'est-à-dire qu'il n'a que des racines simples.

Le polynôme minimal $\mu_a \in \mathbb{K}[X]$ de a est irréductible et donc séparable. Donc $\mathbb{L}$ est séparable.

La dernière phrase est une conséquence du corolaire 8.166. □

CORooNZZMooIoBYXY

Corolaire 8.169.
Toute les extensions algébriques de $\mathbb{Q}$ sont séparables.

Démonstration. Le corps $\mathbb{Q}$ est de caractéristique nulle (définition 3.114). Le corolaire 8.166 dit alors que tout polynôme sur $\mathbb{Q}$ est séparable. La proposition 8.168 conclut en disant que toutes les extensions algébriques de $\mathbb{Q}$ sont séparables. □

ThobkwCMm

Théorème 8.170 ([108]).
Soit $\mathbb{K}$ un corps (pas spécialement fini). Tout sous-groupe fini de $\mathbb{K}^*$ est cyclique.

Démonstration. Soit G un sous-groupe fini de $\mathbb{K}^*$ et ω son exposant (qui est le PPCM des ordres des éléments de G). Étant donné que $|G|$ est divisé par tous les ordres, il est divisé par le PPCM des ordres. Bref, nous avons

$$x^\omega = 1 \tag{8.294}$$

pour tout $x \in G$. Mais ce polynôme possède au plus ω racines dans $\mathbb{K}$. Du coup $|G| \leqslant \omega$. Et comme on avait déjà vu que $\omega \mid |G|$, on a $\omega = |G|$. Il suffit plus que trouver un élément d'ordre effectivement ω. Cela est fait par le lemme 3.170. □

ThoORxgBC

Théorème 8.171 (Théorème de l'élément primitif[108]).
Toute extension de corps séparable finie admet un élément primitif[78].

Autrement dit, soient des éléments algébriques $\alpha_1, \dots, \alpha_n$ séparables[79] *sur $\mathbb{K}$, et soit l'extension engendrée $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Alors $\mathbb{L}$ admet un élément primitif, c'est-à-dire un élément θ tel que $\mathbb{L} = \mathbb{K}(\theta)$.*

Démonstration. Si le corps $\mathbb{K}$ est fini, alors $\mathbb{L}$ est également fini. Donc $\mathbb{L}^*$ est cyclique par le théorème 8.170. Si θ est un générateur de $\mathbb{L}^*$, alors $\mathbb{L} = \mathbb{K}(\theta)$.

Passons au cas où $\mathbb{K}$ est infini. Il suffit d'examiner le cas $n = 2$; en effet pour $n = 1$ c'est trivial et si $n > 2$, alors

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n), \tag{8.295}$$

et donc si $\mathbb{K}(\alpha_1, \dots, \alpha_{n-1}) = \mathbb{K}(\theta)$, nous avons

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\theta, \alpha_n) \tag{8.296}$$

et nous sommes réduit au cas $n = 2$ par récurrence.

Soit donc $\mathbb{L} = \mathbb{K}(\alpha, \beta)$; soit P le polynôme minimal de α sur $\mathbb{K}$ et Q celui de β. Nous nommons $\mathbb{E}$, un corps de décomposition de PQ. Nous avons $\mathbb{L} \subset \mathbb{E}$. Vu que P et Q sont polynômes minimaux d'éléments qui sont par hypothèse séparables, les polynômes P et Q sont séparables. Donc dans $\mathbb{E}$ les racines de P sont distinctes parce que P est irréductible (et idem pour Q). Soient les racines

$$\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r \tag{8.297}$$

de P dans $\mathbb{E}$ et les racines

$$\beta_1 = \beta, \beta_2, \dots, \beta_s \tag{8.298}$$

de Q dans $\mathbb{E}$. Ici r et s sont les degrés de P et Q.

Si $s = 1$ alors $Q = X - \beta$ et donc $\beta \in \mathbb{K}$ (parce que $Q \in \mathbb{K}[X]$). Du coup nous avons $\mathbb{L} = \mathbb{K}(\alpha)$ et le théorème est démontré. Nous supposons donc maintenant que $s \geqslant 2$.

Pour chaque $(i, j) \in [\![1, r]\!] \times [\![2, s]\!]$, l'équation $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ pour $x \in \mathbb{K}$ a au plus[80] une solution donnée le cas échéant par

$$x = (\alpha_i - \alpha_1)(\beta_1 - \beta_k)^{-1} \tag{8.299}$$

EqWzUFHe

Notons que cela est de toutes façons dans $\mathbb{L}$ et qu'étant donné que $\beta_1 \neq \beta_k$, cette solution a un sens (ici on utilise l'hypothèse de séparabilité). Étant donné que $\mathbb{K}$ est infini nous pouvons donc trouver un $c \in \mathbb{K}$ qui ne résout aucune des équations (8.299) :

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1. \tag{8.300}$$

EQooIIMVooSmyriP

Nous posons $\theta = \alpha_1 + c\beta_1$ et nous prétendons que $\mathbb{L} = \mathbb{K}(\theta)$.

Pour cela, commençons par montrer que $\beta_1 \in \mathbb{K}(\theta)$. On considère, dans $\mathbb{K}(\theta)[T]$, les polynômes $Q(T)$ et $S(T) = P(\theta - cT)$, et on nomme R le PGCD de ces deux polynômes. Alors, une racine de R doit être une racine de Q, et est donc un des β_i. Or, d'une part, le choix de θ fait que β_1 est une racine de R parce que

$$S(\beta_1) = P(\theta - c\beta_1) = P(\alpha_1 + c\beta_1 - c\beta_1) = P(\alpha_1) = 0. \tag{8.301}$$

[78] Définition 8.93.
[79] Définition 8.167(1).
[80] La solution (8.299) peut être dans $\mathbb{L}$ et non dans $\mathbb{K}$. L'équation peut donc très bien ne pas avoir de solutions $x \in \mathbb{K}$.

D'autre part, si $k \geqslant 2$, alors

$$S(\beta_k) = P(\alpha_1 + c\beta_1 - c\beta_k) = P\big(\alpha_1 + c(\beta_1 - \beta_k)\big) \neq 0 \tag{8.302}$$

parce que $\alpha_1 + c(\beta_1 - \beta_k)$ ne vaut ni α_1 (le second terme est non-nul), ni un autre α_i (à cause de (8.300)).

Il s'ensuit que Q et S n'ont qu'une racine commune $\beta_1 = \beta$, qui est donc l'unique racine de R. Ainsi,

$$R = X - \beta \in \mathbb{K}(\theta)[T], \tag{8.303}$$

et donc $\beta \in \mathbb{K}(\theta)$.

Dès lors $\alpha = \alpha_1 = \theta - c\beta$ est alors immédiatement dans $\mathbb{K}(\theta)$; puisque les deux éléments α et β sont dans $\mathbb{K}(\theta)$, nous avons obtenu $\mathbb{L} = \mathbb{K}(\alpha, \beta) = \mathbb{K}(\theta)$.

□

Exemple 8.172.
Le théorème de l'élément primitif 8.171 ne tient pas pour les corps non commutatifs. Considérons par exemple le corps $\mathbb{K}$ des quaternions et le groupe à 8 éléments $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Ce dernier groupe n'est pas cyclique alors qu'il est un groupe fini dans $\mathbb{K}^*$. △

Exemple 8.173.
Il est aussi possible pour un groupe fini d'avoir $\omega(G) = |G|$ sans pour autant que G soit cyclique. Par exemple pour $G = S_3$, nous avons $|S_3| = 6$ alors que les éléments de S_3 sont soit d'ordre 2 soit d'ordre 3 et $\omega(G) = \text{ppcm}(2, 3) = 6$. Pourtant S_3 n'est pas cyclique. △

8.5 Idéal maximum

8.5.1 Idéal maximum

DefWHDdTrC

Définition 8.174.
*Une $\mathbb{K}$-algèbre est de **type fini** si elle est le quotient de $\mathbb{K}[X_1, \dots, X_n]$ par un idéal (pour un certain n).*

ThonoZyKa

Théorème 8.175 ([213]).
Soit $\mathbb{K}$ un corps et B, une $\mathbb{K}$-algèbre de type fini. Si B est un corps, alors c'est une extension algébrique finie de $\mathbb{K}$.

ThowgZYqx

Théorème 8.176 ([213]).
Si $\mathbb{K}$ est un corps algébriquement clos, les idéaux maximaux[81] *de $\mathbb{K}[X_1, \dots, X_n]$ sont de la forme*

$$(X_1 - a_1, \dots, X_n - a_n) \tag{8.304}$$

où les a_i sont des éléments de $\mathbb{K}$.

Démonstration. Nous commençons par montrer que

$$J = (X_1 - a_1, \dots, X_n - a_n) \tag{8.305}$$

est un idéal maximum. Pour cela nous considérons le morphisme surjectif d'anneaux

$$\begin{aligned} \phi\colon \mathbb{K}[X_1, \dots, X_n] &\to \mathbb{K} \\ P &\mapsto P(a_1, \dots, a_n). \end{aligned} \tag{8.306}$$

Soit $P \in \ker(\phi)$; nous écrivons la division euclidienne de P par $X - a_1$ puis celle du reste par $X - a_2$ et ainsi de suite :

$$P = (X - a_1)Q_1 + \cdots + (X_n - a_n)Q_n + R \tag{8.307}$$

FqDAkiiH

où R doit être une constante parce que le premier reste est de degré zéro en X_1, le second est de degré zéro en X_1 et X_2, etc. Afin d'identifier cette constante, nous appliquons l'égalité (8.307) à $(a_1, \dots, a_n)$ et en nous rappelant que $P \in \ker(\phi)$ nous obtenons

$$0 = P(a_1, \dots, a_n) = R, \tag{8.308}$$

donc $R = 0$ et $P = (X_1 - a_1)Q_1 + \cdots + (X_n - a_n)Q_n$, c'est-à-dire $P \in J$. Nous avons donc $\ker(\phi) \subset J$. Par ailleurs $J \subset \ker(\phi)$ est évident, donc $J = \ker(\phi)$.

[81] Définition 3.85.

Vu que J est le noyau de l'application $\mathbb{K}[X_1,\dots,X_n]\to\mathbb{K}$, nous avons

$$\frac{\mathbb{K}[X_1,\dots,X_n]}{J}=\mathbb{K}. \tag{8.309}$$

Donc J est un idéal maximal parce que tout polynôme n'étant pas dans J doit avoir un terme indépendant non nul et donc être dans $\mathbb{K}$ vis-à-vis du quotient $\mathbb{K}[X_1,\dots,X_n]/J$.

Nous montrons maintenant l'implication inverse. Nous supposons que I est un idéal maximum et nous montrons qu'il doit être égal à J (pour un certain choix de $a_1,\dots,a_n$).

Le quotient

$$\frac{\mathbb{K}[X_1,\dots,X_n]}{I} \tag{8.310}$$

est une $\mathbb{K}$-algèbre de type fini (définition 8.174). De plus c'est un corps par la proposition 3.86. C'est donc une extension algébrique finie de $\mathbb{K}$ par le théorème 8.175. Mais $\mathbb{K}$ étant algébriquement clos, il est sa propre et unique extension algébrique ; nous en déduisons que

$$\frac{\mathbb{K}[X_1,\dots,X_n]}{I}=\mathbb{K}. \tag{8.311}$$

Donc pour tout $1\leqslant i\leqslant n$, il existe $a_i\in\mathbb{K}$ tel que $X_i-a_i\in I$, sinon le monôme X_i ne se projetterait pas sur un élément dans $\mathbb{K}$ dans le quotient. Cela prouve que J est contenu dans I ; par maximalité nous avons donc $I=J$. □

Corolaire 8.177.
Soit $\mathbb{K}$ un corps algébriquement clos et I, un idéal de $\mathbb{K}[X_1,\dots,X_n]$. Si nous notons

$$V(I)=\{x\in\mathbb{K}^n \text{ tel que } P(x_1,\dots,x_n)=0,\forall P\in I\} \tag{8.312}$$

l'ensemble des racines communes à tous les éléments de I, on a $V(I)=\varnothing$ si et seulement si $I=\mathbb{K}[X_1,\dots,X_n]$.

Démonstration. Si $I=\mathbb{K}[X_1,\dots,X_n]$ en particulier $1\in I$ et nous avons évidemment $V(I)=\varnothing$. Le sens difficile est l'autre sens.

Supposons que $I\neq\mathbb{K}[X_1,\dots,X_n]$ et que K est un idéal maximum contenant I (ça existe par le théorème de Krull 3.87). Nous savons déjà par le théorème 8.176 que K est de la forme $K=(X_1-a_1,\dots,X_n-a_n)$. Un élément de I est dans K, donc si $P\in I$ nous avons

$$P(a_1,\dots,a_n)=0, \tag{8.313}$$

c'est-à-dire que $(a_1,\dots,a_n)\in V(I)$ et donc que $V(I)\neq\varnothing$. □

8.6 Polynômes symétriques et alternés

8.6.1 Polynômes symétriques, alternés ou semi-symétriques

Nous rappelons que le groupe symétrique S_n agit sur l'anneau des polynômes de n variables sur l'anneau A par le lemme 3.237.

Définition 8.178.
Un polynôme Q en n indéterminées est

(1) ***symétrique*** *si $Q=\sigma\cdot Q$ pour tout $\sigma\in S_n$;*

(2) ***alterné*** *si $\sigma\cdot Q=\epsilon(\sigma)Q$ pour tout $\sigma\in S_n$;*

(3) ***semi-symétrique*** *si $\sigma\cdot Q=Q$ pour tout $\sigma\in A_n$*

Le polynôme T_1+T_2 est symétrique ; le polynôme $T_1+T_2^2$ ne l'est pas.

8.6.2 Polynôme symétrique élémentaire

DEFooTREUooZKoXeg

Définition 8.179.
*Le k-ième **polynôme symétrique élémentaire** à n inconnues est le polynôme*

$$\sigma_k(T_1,\dots,T_n)=\sum_{s\in F_k}\prod_{i=1}^{k}T_{s(i)}=\sum_{1\leqslant i_1<\dots<i_k\leqslant n}X_{i_1}\dots X_{i_k}. \tag{8.314}$$

où F_k est l'ensemble des fonctions strictement croissantes $\{1,2,\dots,k\}\to\{1,2,\dots,n\}$.

$$\sigma_1(T_1,\dots,T_n) = T_1 + T_2 + \cdots + T_n \tag{8.315a}$$
$$\sigma_2(T_1,\dots,T_n) = T_1T_2 + \cdots + T_1T_n + T_2T_3 + \cdots + T_2T_n + \cdots + T_{n-1}T_n \tag{8.315b}$$
$$\sigma_n(T_1,\dots,T_n) = T_1\dots T_n. \tag{8.315c}$$

En particulier, $\sigma_2(x,y,z) = xy + yz + xz$.

ThoReBiw

Théorème 8.180 ([214, 215]).
Soit un anneau commutatif A. Soit un polynôme symétrique à n indéterminées P à coefficients dans A. Alors il existe un unique polynôme Q à coefficients dans A tel que

$$P = Q(\sigma_1,\dots,\sigma_n) \tag{8.316}$$

où les σ_i sont les polynômes symétriques élémentaires[82].

Exemple 8.181.
Nous voulons décomposer $P(x,y,z) = x^3 + y^3 + z^3$ en polynômes symétriques élémentaires, c'est-à-dire en

$$\begin{cases} \sigma_1 = x + y + z & (8.317a)\\ \sigma_2 = xy + xz + yz & (8.317b)\\ \sigma_3 = xyz. & (8.317c) \end{cases}$$

Étant donné que P est de degré 3, les seules combinaisons des σ_i qui peuvent intervenir sont σ_1^3, $\sigma_1\sigma_2$ et σ_3. Étant donné que dans P le coefficient de x^3 est un, il est obligatoire d'avoir un coefficient 1 devant σ_1^3. Nous le calculons :

```
--------------------------------------------------------------------------
| Sage Version 4.8, Release Date: 2012-01-20                             |
| Type notebook() for the GUI, and license() for information.            |
--------------------------------------------------------------------------
sage: var('x,y,z')
(x, y, z)
sage: P=x**3+y**3+z**3
sage: S1=x+y+z
sage: S2=x*y+x*z+y*z
sage: S3=x*y*z
sage: (S1**3).expand()
x^3 + 3*x^2*y + 3*x^2*z + 3*x*y^2 + 6*x*y*z + 3*x*z^2 + y^3
                + 3*y^2*z + 3*y*z^2 + z^3
sage: (S1**3-P).expand()
3*x^2*y + 3*x^2*z + 3*x*y^2 + 6*x*y*z + 3*x*z^2 + 3*y^2*z + 3*y*z^2
x^3 + 3*x^2*y + 3*x^2*z + 3*x*y^2 + 6*x*y*z + 3*x*z^2
            + y^3 + 3*y^2*z + 3*y*z^2 + z^3
```

Dans la différence $\sigma_1^3 - P$ nous voyons que le terme en xyz est $6xyz$; par conséquent nous savons que le coefficient de σ_3 sera -6. Il nous reste :

```
sage: (S1**3+6*S3-P).expand()
3*x^2*y + 3*x^2*z + 3*x*y^2 + 12*x*y*z + 3*x*z^2 + 3*y^2*z + 3*y*z^2
```

que nous identifions facilement avec $3\sigma_1\sigma_2$. Nous avons donc

$$P = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \tag{8.318}$$

△

LemSoXCQH

Lemme 8.182 ([121]).
Soit $\mathbb{K}$ une extension de degré δ de $\mathbb{Q}$ et $P \in \mathbb{K}[T_1,\dots,T_m]$. Alors il existe $\bar{P} \in \mathbb{Q}[T_1,\dots,T_m]$ tel que

(1) $\deg \bar{P} = \delta \deg(P)$

[82] Définition 8.179.

(2) pour tout $(z_1,\dots,z_m)\in\mathbb{C}^m$ *tel que* $P(z_1,\dots,z_m)=0$*, on a* $\bar{P}(z_1,\dots,z_m)=0$.

Démonstration. En vertu de la proposition 8.168 et du corolaire 8.169, $\mathbb{K}$ est une extension séparable de $\mathbb{Q}$, et donc vérifie le théorème de l'élément primitif (8.171). Il existe $\theta\in\mathbb{K}$ tel que $\mathbb{K}=\mathbb{Q}(\theta)$. Soit $P_\theta\in\mathbb{Q}[X]$ le polynôme minimal de θ. L'extension $\mathbb{K}$ étant de degré δ, et θ étant un générateur, une base de $\mathbb{K}$ comme espace vectoriel sur $\mathbb{Q}$ est

$$\{1,\theta,\dots,\theta^{\delta-1}\}. \tag{8.319}$$

Mais par ailleurs la proposition 8.103(2) nous indique qu'une base de $\mathbb{Q}(\theta)$ sur $\mathbb{Q}$ est donnée par

$$\{1,\theta,\dots,\theta^{n-1}\} \tag{8.320}$$

où n est le degré de P_θ. Donc P_θ est de degré δ. Nous nommons $\theta_1,\dots,\theta_\delta$ les racines de P_θ dans un corps de décomposition. Ici nous notons $\theta=\theta_1$ et nous ne prétendons pas que $\theta_k\in\mathbb{K}$. Notons que ces θ_i sont toutes des racines simples de P_θ, sinon nous aurions un facteur irréductible $(X-\theta_k)^2$, et P_θ ne serait pas irréductible sur $\mathbb{Q}$.

Soit σ_k le morphisme canonique

$$\begin{aligned}\sigma_k\colon\mathbb{Q}(\theta)&\to\mathbb{Q}(\theta_k)\\ \sum_i q_i\theta^i&\mapsto\sum_i q_i\theta_k^i\end{aligned} \tag{8.321}$$

Nous avons $\sigma_1\colon\mathbb{K}\to\mathbb{K}$ qui est l'identité.

Notons N le degré du polynôme $P\in\mathbb{K}[T_1,\dots,T_m]$ dont il est question dans l'énoncé. Nous le décomposons alors en

$$P=\sum_{l=0}^{N}\sum_{i=1}^{m}c_{il}T_i^l \tag{8.322}$$

avec $c_{il}\in\mathbb{K}$. Nous voyons $c_{i,.}$ comme un élément de $\mathbb{K}^m$ et donc nous écrivons[83]

$$P=\sum_{l=0}^{N}\sum_{i=1}^{m}c_l(\theta)_iT_i^l \tag{8.323}$$

où $c_l\in\mathbb{Q}[X]^m$. Nous pouvons choisir $\deg(c_l)<\delta$ parce que les puissances plus grandes de θ ne génèrent rien de nouveau.

Nous posons aussi

$$P^{\sigma_k}=\sum_{l,i}c_l(\theta_k)_iT_i^l\in\mathbb{Q}(\theta_k)[T_1,\dots,T_m], \tag{8.324}$$

et $\bar{P}=PP^{\sigma_2}\dots P^{\sigma_k}$. Le coefficient de T_i^l dans $\bar{P}$ est

$$\bar{c}_l(\theta_1,\dots,\theta_\delta)_i=\sum_{l_1+\dots+l_\delta=l}c_{l_1}(\theta_1)_i\dots c_{l_\delta}(\theta_\delta)_i. \tag{8.325}$$

Ce dernier est un polynôme en les θ_k à coefficients dans $\mathbb{Q}$. Qui plus est, c'est un polynôme symétrique. En effet un terme contenant $\theta_k^a\theta_l^b$ provenant de $c_{l_i}(\theta_k)c_{l_j}(\theta_l)$ a un terme correspondant $\theta_k^b\theta_l^a$ provenant de $c_{l_j}(\theta_k)c_{l_i}(\theta_l)$.

C'est donc le moment d'utiliser le théorème 8.180 à propos des polynômes symétriques élémentaires qui nous dit que les coefficients de $\bar{P}$ sont en réalité des polynômes en ceux de P_θ qui sont dans $\mathbb{Q}$. Donc $\bar{P}\in\mathbb{Q}[T_1,\dots,T_m]$. Par ailleurs nous avons que

$$\deg(\bar{P})=\delta\deg(P) \tag{8.326}$$

parce que $\bar{P}$ est le produit de δ « copies » de P. De plus $P=P^{\sigma_1}$ divise $\bar{P}$ donc on a bien que si $P(z)=0$ alors $\bar{P}(z)=0$. Le polynôme $\bar{P}$ est celui que nous cherchions. □

8.6.3 Relations coefficients racines

ThoOQRgjpl

Théorème 8.183 (Relations coeffitients-racines)**.**
Soit le polynôme $P=a_nX^n+\dots+a_1X+a_0$ *et* r_i *ses* n *racines. Alors nous avons pour chaque* $1\leqslant k\leqslant n$ *la relation*

$$\sigma_k(r_1,\dots,r_n)=(-1)^k\frac{a_{n-k}}{a_n} \tag{8.327}$$

où σ_k *est le* k^e *polynôme symétrique défini en 8.179.*

[83] Il me semble qu'il manque la somme sur i dans [121].

ExHIfHhBr

Exemple 8.184.
Soit le polynôme

$$P(x) = x^3 + 2x^2 + 3x + 4 \tag{8.328}$$

et ses racines que nous nommons a, b, c. Nous voudrions calculer $a^2 + b^2 + c^2$. D'abord nous décomposons $Q(a, b, c) = a^2 + b^2 + c^2$ en polynômes symétriques élémentaires : $Q(a, b, c) = \sigma_1(a, b, c)^2 - 2\sigma_2(a, b, c)$.

Mais les relations coefficients-racines[84] nous donnent $\sigma_1(a, b, c) = -2$ et $\sigma_2(a, b, c) = 3$, donc

$$a^2 + b^2 + c^2 = (-2)^2 - 2 \cdot 3 = -2. \tag{8.329}$$

Cela nous assure déjà qu'au moins une des solutions n'est pas réelle.

Nous pouvons en avoir une vérification directe en calculant explicitement les racines (ce qui est possible pour le degré 3) :

```
sage: P(x)=x**3+2*x**2+3*x+4
sage: S=solve(  P(x)==0,x  )
sage: sols=[ s.rhs() for s in S  ]
sage: Q=[  s**2 for s in sols ]
sage: s=sum(Q)
sage: s.simplify_full()
-2
```

tex/frido/VAYVmNRpolynomeSym.py

Notez qu'il faut un peu chipoter pour isoler les solutions depuis la réponse de la fonction `solve`. △

En suivant le même cheminement que dans l'exemple, si P est un polynôme de degré n et si r_i sont ses racines, il est facile de calculer $Q(r_1, \dots, r_n)$ pour n'importe quel polynôme symétrique Q

PropTETooGuBYQf

Proposition 8.185 (Annulation de fonctions polynomiales[216])**.**
Soit $\mathbb{K}$ un corps et P un polynôme à n indéterminées. Nous supposons que P s'annule sur un ensemble de la forme $A_1 \times \cdots \times A_n$ avec $\text{Card}(A_j) > \deg_{X_j}(P)$ pour tout j. Alors $P = 0$.

De plus si $P = 0$ alors tous ses coefficients sont nuls[85]*.*

Démonstration. Nous prouvons le résultat par récurrence sur le nombre n d'indéterminées. Si $n = 1$, cela est le théorème 8.110. Nous classons les monômes du polynôme P par ordre de puissance de X_n et nous le factorisons :

$$P = \sum_{i=1}^{m} P_i X_n^i \tag{8.330}$$

avec $P_i \in \mathbb{K}[X_1, \dots, X_{n-1}]$. Soit $(a_1, \dots, a_{n-1}) \in A_1 \times \dots \times A_{n-1}$ et posons

$$Q(T) = P(a_1, \dots, a_{n-1}, T) = \sum_{i=1}^{m} P_i(a_1, \dots, a_{n-1}) T^i. \tag{8.331}$$

Le polynôme Q s'annule sur A_n avec $\deg(Q) = \deg_{X_n}(P) < \text{Card}(A_n)$ et le théorème 8.110 nous donne $Q = 0$. Or les coefficients des différentes puissances de T dans $Q(T)$ sont les $P_i(a_1, \dots, a_{n-1})$; ils sont donc nuls.

Nous avons montré que le polynôme P_i s'annule pour tout élément de $A_1 \times \dots \times A_{n-1}$, mais nous avons

$$\deg_{X_j}(P_i) \leqslant \deg_{X_j} P < \text{Card}(A_j), \tag{8.332}$$

donc l'hypothèse de récurrence donne $P_i = 0$. Par suite, $P = 0$ également. □

8.7 Minuscule morceau sur la théorie de Galois

Vous trouverez des détails et des preuves à propos de la théorie de Galois dans [217, 108].

[84] Théorème 8.183

[85] L'intérêt de cela est qu'un polynôme de $\mathbb{Z}[X_1, \dots, X_n]$ peut s'évaluer sur un élément de n'importe quel corps ; il restera le polynôme nul.

Définition 8.186.
Soit $\mathbb{K}$, un corps.

*Le **groupe de Galois** d'une extension $\mathbb{L}$ de $\mathbb{K}$ est le groupe des automorphismes de $\mathbb{L}$ laissant $\mathbb{K}$ invariant.*

Le groupe de Galois d'un polynôme sur $\mathbb{K}$ est le groupe de Galois de son corps de décomposition sur $\mathbb{K}$.

Définition 8.187.
*Des éléments $b_1, \dots, b_n$ d'une extension de $\mathbb{K}$ sont **algébriquement indépendants** si ils ne satisfont à aucune relation du type*

$$\sum \alpha_{i_1 \dots i_n} b_1^{i_1} \dots b_n^{i_n} = 0 \tag{8.333}$$

avec $\alpha_{i_1 \dots i_n} \in \mathbb{K}$.

Nous disons que l'équation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{8.334}$$

est l'**équation générale** de degré n si les coefficients a_i sont algébriquement indépendants sur $\mathbb{K}$.

THOooDTCXooTIOSZe

Théorème 8.188.
Le groupe de Galois d'un polynôme de degré n est isomorphe au groupe symétrique S_n.

CORooBRKTooBWldRC

Corolaire 8.189 ([218])**.**
L'équation générale de degré n est résoluble par radicaux si et seulement si $n \leq 5$.

Chapitre 9

Topologie générale

9.1 Éléments généraux de topologie

9.1.1 Définitions et propriétés de base

DefTopologieGene

Définition 9.1 ([219]).
Soient X, un ensemble et $\mathcal{T}$, une partie de l'ensemble de ses parties qui vérifie les propriétés suivantes.

(1) Les ensembles $\varnothing$ et X sont dans $\mathcal{T}$,

(2) Une union quelconque[1] *d'éléments de $\mathcal{T}$ est dans $\mathcal{T}$.*

ITEMooGJAPooOWIOzv

(3) Une intersection finie *d'éléments de $\mathcal{T}$ est dans $\mathcal{T}$.*

*Un tel choix $\mathcal{T}$ de sous-ensembles de X est une **topologie** sur X, et les éléments de $\mathcal{T}$ sont appelés des **ouverts**. On dit aussi que $(X, \mathcal{T})$ (voire simplement X lorsqu'il n'y a pas d'ambiguïté) est un **espace topologique**.*

Deux espaces topologiques sont isomorphes quand il existe une bijection continue d'inverse continue. Nous verrons ça en la définition 9.54.

9.1.2 Base de topologie

DEFooLEHPooIlNmpi

Proposition-Définition 9.2 (Base de topologie[220, 221]).
Soit un espace topologique $(X, \mathcal{T})$. Soit une partie $\mathcal{B}$ de $\mathcal{T}$. Les propriétés suivantes sont équivalentes :

ITEMooCTPEooRCaxvx

(1) Tout élément de $\mathcal{T}$ est une réunion d'éléments de $\mathcal{B}$.

ITEMooWOVWooRozYmM

(2) Pour tout $x \in X$ et pour tout ouvert $\mathcal{O}$ contenant x, il existe $B \in \mathcal{B}$ tel que

$$x \in B \subset \mathcal{O}. \tag{9.1}$$

*Une partie $\mathcal{B}$ de $\mathcal{T}$ qui vérifie ces propriétés est une **base de topologie** pour X.*

Démonstration. En deux parties.

(1) **(1) implique (2)** Soient $x \in X$ et $\mathcal{O}$ un ouvert contenant x. Étant donné que $\mathcal{O}$ est une réunion d'éléments de $\mathcal{B}$, il y a au moins un $B \in \mathcal{B}$ contenant x. Ce B vérifie $x \in B \subset \mathcal{O}$.

(2) **(2) implique (1)** Soit $\mathcal{O}$ un ouvert de X ; pour chaque $x \in \mathcal{O}$ nous considérons un ouvert $B(x) \in \mathcal{B}$ tel que $x \in B(x) \subset \mathcal{O}$. Nous avons alors $\mathcal{O} = \bigcup_{x \in \mathcal{O}} B(x)$.

□

[1] Par « quelconque » nous entendons vraiment quelconque : c'est-à-dire indicée par un ensemble qui peut autant être $\mathbb{N}$ que $\mathbb{R}$ qu'un ensemble encore considérablement plus grand.

9.1.3 Fermés

DEFFermeooNSAAooHxZbAo

Définition 9.3.
*Si X est un espace topologique, un sous-ensemble F de X est dit **fermé** si son complémentaire, $X \setminus F$, est ouvert.*

DEFVoisinageooGHZCooLRcpXY

Définition 9.4.
*Si $a \in X$, on dit que $V \subset X$ est un **voisinage** de a si il existe un ouvert $\mathcal{O} \in \mathcal{T}$ tel que $a \in \mathcal{O}$ et $\mathcal{O} \subset V$.*

DEFooBWZIooXotZLA

Définition 9.5 (Base de voisinage[222])**.**
*Soient un espace topologique X ainsi que $a \in X$. Un ensemble $\{U_i\}_{i\in I}$ de voisinages de a est une **base de voisinages** de a si pour tout voisinage V de a, il existe $k \in I$ tel que $U_k \subset V$.*

LemQYUJwPC

Lemme 9.6.
Union et intersection de fermés.

ITEMooBHIGooMvkUtX

(1) Une intersection quelconque de fermés est fermée.

ItemKJYVooMBmMbG

(2) Une union finie de fermés est fermée.

Démonstration. Soit $\{F_i\}_{i\in I}$ un ensemble de fermés ; nous avons

$$\left(\bigcap_{i\in I} F_i\right)^c = \bigcup_{i\in I} F_i^c. \tag{9.2}$$

Le membre de droite est une union d'ouverts, c'est donc un ouvert ; donc l'intersection qui apparaît dans le membre de gauche est le complémentaire d'un ouvert : c'est donc un fermé.

De la même manière, le complémentaire d'une union finie de fermés est une intersection finie de complémentaires de fermés, et est donc ouvert[2]. □

LEMooSFMZooBguLdf

Lemme 9.7.
Ouverts et fermés.

ITEMooFPGVooUZHzkA

(1) Si F est fermé et si $\mathcal{O}$ est ouvert, alors $F \setminus \mathcal{O}$ est fermé.

ITEMooULNTooKQyrJb

(2) Si F est fermé dans l'ouvert $\mathcal{O}$, alors $\mathcal{O} \setminus F$ est ouvert.

Démonstration. Nous savons par le lemme 1.49 que $(F \setminus \mathcal{O})^c = F^c \cup \mathcal{O}$. Vu que F^c et $\mathcal{O}$ sont ouverts, l'union est ouverte. Le complémentaire de $F \setminus \mathcal{O}$ étant ouvert, il est fermé.

Pour le second point, nous considérons le complémentaire. Si nous nommons X l'espace topologique, nous avons

$$X \setminus (\mathcal{O} \setminus F) = (X \setminus \mathcal{O}) \cup F. \tag{9.3}$$

Étant une union de fermés, cela est fermé (lemme 9.6). Donc $\mathcal{O} \setminus F$ est ouvert. □

Dans un espace topologique, nous avons une caractérisation très importante des ouverts.

ThoPartieOUvpartouv

Théorème 9.8.
Une partie d'un espace topologique est ouverte si et seulement si elle contient un ouvert autour de chacun de ses éléments.

Démonstration. Soit X un espace topologique et $A \subset X$. Le sens direct est évident : A lui-même est un ouvert autour de $x \in A$, qui est inclus dans X.

Pour le sens inverse, nous supposons que A contienne un ouvert autour de chacun de ses points. Pour chaque $x \in A$, choisissons $\mathcal{O}_x \subset A$ un ouvert autour de x. Alors,

$$A = \bigcup_{x\in A} \mathcal{O}_x \tag{9.4}$$

EqAUniondesOx

en effet, d'une part, $A \subset \bigcup_{x\in A} \mathcal{O}_x$ parce que chaque élément x de A est dans le $\mathcal{O}_x$ correspondant, par construction ; et d'autre part, $\bigcup_{x\in A} \mathcal{O}_x \subset A$ parce que chacun des $\mathcal{O}_x$ est inclus dans A.

Ainsi, A est égal à une union d'ouverts, cela prouve que A est un ouvert. □

Le lemme 9.315 est une version particulière de celui-ci, pour l'espace topologique $\mathbb{R}$. Une autre application typique est la proposition 9.2 et le théorème 9.286.

[2] Un bon exercice est d'écrire ces unions et intersections, pour se convaincre que ça fonctionne.

9.1.4 Quelques exemples

9.1.4.1 Une première vague

DefTopologieGrossiere

Exemple 9.9.
Soit un ensemble quelconque X. L'ensemble de parties $\mathcal{T} = \{\varnothing, X\}$ est une topologie sur X.

La topologie ainsi définie sur X est appelée **topologie grossière**. △

DefTopologieDiscrete

Exemple 9.10.
Pour un ensemble X quelconque, on considère l'ensemble $\mathcal{T}$ constitué de toutes les parties de X. Avec cet ensemble, on confère à nouveau une structure d'espace topologique à X ; toutes les parties sont des ouverts, et aussi des fermés. La topologie ainsi posée sur X est appelée **topologie discrète**. △

EXooLAOSooJtjJnu

Exemple 9.11 (Toutes les topologies d'un ensemble à 3 éléments)**.**
On pose $X = \{1, 2, 3\}$. Alors on peut munir X de 29 topologies différentes[223] ; saurez-vous les retrouver toutes ? △

¡¡ Avertissement/question au lecteur !! 9.12
Je n'ai pas réfléchi à faire 9.11. Ou au moins pas comment le faire autrement qu'en passant en revue les 2^8 possibilités. Si vous savez comment faire, écrivez-moi.

9.1.4.2 Topologie engendrée

DefTopologieEngendree

Proposition-Définition 9.13 (Topologie engendrée, prébase[224])**.**
Soient un ensemble X, et $\mathcal{T}_0$ un ensemble de parties de X. Nous définissons $\tau(\mathcal{T}_0)$ comme étant l'union quelconque d'intersections finies d'éléments de $\mathcal{T}_0$.

Plus précisément, nous faisons les constructions suivantes :

(1) Nous notons $\{\mathcal{O}_i\}_{i\in I}$ les éléments de $\mathcal{T}_0$ indexés par l'ensemble I.

(2) Soit $B(\mathcal{T}_0)$ l'ensemble des intersections finies d'éléments de $\mathcal{T}_0$:

$$B(\mathcal{T}_0) = \Big\{ \bigcap_{j\in J} \mathcal{O}_j \Big\}_{J \text{ fini dans } I} \tag{9.5}$$

où nous convenons que $\bigcap_{j\in\varnothing} \mathcal{O}_j = X$[3].

(3) Soit A un ensemble qui indexe $B(\mathcal{T}_0)$:

$$B(\mathcal{T}_0) = \{B_\alpha\}_{\alpha\in A}. \tag{9.6}$$

(4) Nous posons

$$\tau(\mathcal{T}_0) = \Big\{ \bigcup_{\alpha\in S} B_\alpha \Big\}_{S\subset A}. \tag{9.7}$$

Alors :

ITEMooTCGTooJwfpel

(1) $\tau(\mathcal{T}_0)$ est une topologie sur X.

ITEMooBJVVooEVRgdq

(2) Toute topologie sur X contenant $\mathcal{T}_0$ contient $\tau(\mathcal{T}_0)$.

*La topologie $\tau(\mathcal{T}_0)$ est appelée la **topologie engendrée** par $\mathcal{T}_0$. La partie $\mathcal{T}_0$ est appelée **prébase** de la topologie $\tau(\mathcal{T}_0)$.*

Démonstration. Pour (1), nous devons montrer les différents points de la définition 9.1 d'une topologie.

(1) L'ensemble vide est dans $\tau(\mathcal{T}_0)$ parce que $\varnothing = \bigcup_{\alpha\in\varnothing} B_\alpha$. L'ensemble X est également dans $\tau(\mathcal{T}_0)$ parce que $X \in B(\mathcal{T}_0)$.

(2) Soient $\{D_l\}_{l\in L}$ des éléments de $\tau(\mathcal{T}_0)$ indexés par un ensemble L. Pour chaque l nous avons un ensemble $S \subset A$ tel que $D_l = \bigcup_{\alpha\in S_l} B_\alpha$. En posant $S = \bigcup_{l\in L} S_l$ nous avons

$$\bigcup_{l\in L} D_l = \bigcup_{\alpha\in S} B_\alpha \in \tau(\mathcal{T}_0). \tag{9.8}$$

Donc $\tau(\mathcal{T}_0)$ est stable par union quelconque.

[3] Bref, nous mettons X dans $B(\mathcal{T}_0)$.

(3) Soient D_1 et D_2 des éléments de $\tau(\mathcal{T}_0)$. Nous posons $D_i = \bigcup_{\alpha\in S_i} B_\alpha$. Alors nous avons

$$\bigcup_{\alpha\in S_1} B_\alpha \cap \bigcup_{\beta\in S_2} B_\beta = \bigcup_{\alpha,\beta\in S_1\times S_2} (B_\alpha \cap B_\beta). \tag{9.9}$$

EQooUCJOooCbKVqw

Mais B_α et B_β sont dans $B(\mathcal{T}_0)$. Donc $B_\alpha \cap B_\beta \in B(\mathcal{T}_0)$. Donc (9.9) est une union d'éléments de $B(\mathcal{T}_0)$.

Au final nous avons prouvé que $\tau(\mathcal{T}_0)$ est une topologie sur X.

Nous démontrons à présent le point (2). Soit une topologie μ sur X contenant $\tau(\mathcal{T}_0)$. Puisque μ est une topologie, les intersections finies d'éléments de μ sont dans μ, donc, en suivant les notations de 9.13, $B(\mathcal{T}_0) \subset \mu$.

Comme toutes les unions d'éléments de μ sont dans μ, l'inclusion de $B(\mathcal{T}_0)$ dans μ implique celle de $\tau(\mathcal{T}_0)$. □

Dès que nous avons une topologie, nous avons une notion de convergence de suite.

DefXSnbhZX

Définition 9.14 (Convergence de suite)**.**
*Une suite (x_n) d'éléments de X **converge** vers un élément x de X si pour tout ouvert $\mathcal{O}$ contenant x , il existe un $K \in \mathbb{N}$ tel que $k \geqslant K$ implique $x_k \in \mathcal{O}$.*

*Nous disons alors que x est une **limite** de (x_k).*

La proposition suivante montre que vérifier la convergence d'une suite sur une prébase suffit pour vérifier la convergence.

PROPooJTJBooNtczsO

Proposition 9.15.
Soit $\mathcal{T}_0$ un ensemble de parties de l'ensemble X. Soient une suite (x_n) dans X ainsi que $x \in X$. Nous supposons que la suite (x_n) satisfait la propriété suivante : pour tout $A \in \mathcal{T}_0$ tel que $x \in A$, il existe $K \in \mathbb{N}$ tel que $k \geqslant K$ implique $x_k \in A$.

Alors nous avons la convergence de suite[4]

$$x_n \xrightarrow{(X,\tau(\mathcal{T}_0))} x. \tag{9.10}$$

Démonstration. Nous considérons la topologie $\tau(\mathcal{T}_0)$ sur X. Soit un ouvert $\mathcal{O}$ contenant x. Nous le décomposons en suivant (à l'envers) la construction de la définition 9.13 :

$$\mathcal{O} = \bigcup_{\alpha\in S} B_\alpha \tag{9.11}$$

avec $B_\alpha \in B(\mathcal{T}_0)$. Donc pour chaque α, il existe un ensemble fini J_α tel que

$$B_\alpha = \bigcap_{j\in J_\alpha} A_j \tag{9.12}$$

avec $A_j \in \mathcal{T}_0$. Puisque $x \in \mathcal{O}$, nous avons un α_0 tel que $x \in B_{\alpha_0}$. Donc $x \in A_j$ pour tous les $j \in J_{\alpha_0}$.

Pour chaque $j \in J_{\alpha_0}$, il existe $K_j \in \mathbb{N}$ tel que $k \geqslant K_j$ implique $x_k \in A_j$. Comme J_{α_0} est un ensemble fini, nous pouvons poser $K = \max_{j\in J_{\alpha_0}} K_j$.

Maintenant, si $k \geqslant K$, nous avons $x_k \in A_j$ pour tout j, et donc $x_k \in B_{\alpha_0}$. Par conséquent, $x_k \in \mathcal{O}$. □

9.1.5 Adhérence, fermeture, intérieur, point d'accumulation et point isolé

DEFooSVWMooLpAVZRInt

Définition 9.16.
Soient un espace topologique X et une partie A de X.

*(1) Un point $x \in X$ est **intérieur** à A si il existe un ouvert $\mathcal{O}$ tel que$x \in \mathcal{O} \subset A$.*

*(2) L'**intérieur** de A, notée $\mathrm{Int}(A)$, est l'union de tous les ouverts de X contenus dans A.*

Lemme 9.17.
Quelques propriétés en vrac.

ITEMooHLIMooJEacKt

(1) L'intérieur de A est l'ensemble de tous les points intérieurs de A.

[4] Définition 9.14.

ITEMooYTXSooMyiBpMgzK

(2) *Pour tout $A \subset X$, l'ensemble* $\mathrm{Int}(A)$ *est un ouvert.*

ITEMooYYFDooHgsRfV

(3) *On a* $\mathrm{Int}(A) \subset A$

ITEMooTDXFooFdyLeO

(4) *Nous avons* $\mathrm{Int}(A) = A$ *si et seulement si A est un ouvert.*

Démonstration. En plusieurs morceaux.

(1) (1) Si $a \in \mathrm{Int}(A)$, alors a est dans un ouvert contenu dans A, et donc a est un point intérieur à A. Dans l'autre sens, si a est un point intérieur à A, alors il existe un ouvert $\mathcal{O} \subset A$ contenant a. Puisque $\mathcal{O}$ est un ouvert dans A, nous avons $\mathcal{O} \subset \mathrm{Int}(A)$, et en particulier $a \in \mathrm{Int}(A)$.

(2) (2) L'ensemble $\mathrm{Int}(A)$ est une union d'ouverts.

(3) (3) L'ensemble $\mathrm{Int}(A)$ est une union d'ensembles contenus dans A.

(4) (4) Supposons que $\mathrm{Int}(A) = A$. Puisque $\mathrm{Int}(A)$ est ouvert (point (3)), A est ouvert aussi.

Dans l'autre sens, nous supposons que A est ouvert. Puisque A est un ouvert contenu dans A, nous avons $A \subset \mathrm{Int}(A)$. Mais comme $\mathrm{Int}(A) \subset A$, nous avons l'égalité.

□

9.1.5.1 Adhérence et fermeture

9.18.
Les mots « adhérence » et « fermeture » sont synonymes. Dans le Frido, nous allons utiliser les notations $\mathrm{Adh}(A)$ et $\bar{A}$ de façon opportuniste. La notation $\bar{z}$ définissant le complexe conjugué de z, si A est une partie de $\mathbb{C}$, il est plus sûr d'écrire $\mathrm{Adh}(A)$ pour la fermeture, plutôt que $\bar{A}$.

Au contraire, pour éviter une quantité excessive de parenthèses, nous écrirons $\overline{B(a,r)}$ pour la boule fermée.

DEFooSVWMooLpAVZR

Définition 9.19.
Soient un espace topologique X et une partie A de X. Un point $x \in X$ est ***adhérent*** *à A si tout ouvert de X contenant x a une intersection non vide avec A. L'ensemble des points d'adhérence de A est noté* $\mathrm{Adh}(A)$ *ou* $\bar{A}$.

LEMooILNCooOFZaTe

Lemme 9.20.
À propos d'adhérence.

ITEMooEGDXooQVHyNBZ

(1) *L'adhérence de A est l'intersection de tous les fermés de X contenant A.*

(2) *Nous avons l'égalité*

$$\mathrm{Int}(A)^c = \mathrm{Adh}(A^c). \tag{9.13}$$

Démonstration. Commençons par prouver la dernière égalité d'ensembles. On a les équivalences entre les affirmations suivantes, pour tout $x \in X$:

- x n'est pas dans $\mathrm{Int}(A)$;
- il n'y a aucun ouvert contenant x et inclus dans A ;
- tout ouvert contenant x a une intersection non-vide avec A^c ;
- x est dans $\mathrm{Adh}(A^c)$.

Nous allons à présent montrer l'égalité d'ensembles $\mathrm{Int}(A)^c = \mathrm{Adh}(A^c)$ en prouvant la double inclusion.

(1) **Si** $\mathrm{Int}(A)^c \subset \mathrm{Adh}(A^c)$ Soit $x \in \mathrm{Int}(A)^c$. Nous devons prouver que $x \in \mathrm{Adh}(A^c)$. Soit un ouvert $\mathcal{O}$ contenant x. Vu que x n'est pas dans l'intérieur de A, l'ouvert $\mathcal{O}$ est pas inclus dans A, et donc $\mathcal{O} \cap A^c$ est non vide.

Nous avons montré que tout ouvert contenant x intersecte A^c. Autrement dit : $x \in \mathrm{Adh}(A^c)$.

(2) $\mathrm{Adh}(A^c) \subset \mathrm{Int}(A)^c$

Soit $x \in \mathrm{Adh}(A^c)$. Tout ouvert contenant x intersecte A^c, et ne peut donc pas être inclus dans A. Si aucun ouvert contenant x n'est inclus dans A, alors x n'est pas dans $\mathrm{Int}(A)$.

□

PROPooTTWBooOyxWzr

Proposition 9.21 ([1]).
Soient un espace topologique X, et une partie $A \subset X$. Nous avons

$$X = \text{Int}(A) \cup \overline{X \setminus A}, \tag{9.14}$$

et cette union est disjointe.

Démonstration. En deux parties.

(1) **Disjoint** Si $x \in \text{Int}(A)$, alors il existe un ouvert U vérifiant $x \in U \subset A$. Autrement dit, $U \cap (X \setminus A) = \varnothing$. Donc x n'est pas dans $\overline{X \setminus A}$

(2) **Union** Soit $x \in X$. Il y a deux possibilités : soit il existe un ouvert U vérifiant $x \in U \subset A$, soit ça n'existe pas. Si ça existe, alors $x \in \text{Int}(A)$. Sinon, ça veut dire que tout ouvert contenant x intersecte $X \setminus A$, et donc $x \in \overline{X \setminus A}$.

□

RemAdhFerme

Remarque 9.22.
Comme corolaire du lemme 9.20, et grâce aux remarques faites pour les intérieurs, on obtient que pour $A \subset X$:

(1) l'ensemble $\bar{A}$ est fermé : c'est en effet le complémentaire d'un ouvert, précisément l'intérieur de A^c ;

(2) A est fermé si et seulement si $\bar{A} = A$: en effet, A est fermé si et seulement si A^c est ouvert, si et seulement si l'intérieur de A^c est A^c lui-même ; or, l'intérieur de A^c est le complémentaire de $\bar{A}$ par le lemme 9.20, si bien que A est fermé si et seulement si $(\bar{A})^c = A^c$, ou encore… ce qu'on affirmait au début.

PROPooMDQDooBYjvXO

Proposition 9.23 ([1]).
Si V et W sont des ouverts tels que $V \cap W = \varnothing$, alors $\bar{V} \cap W = \varnothing$.

Démonstration. Pour l'absurde nous considérons $a \in \bar{V} \cap W$. Étant donné que W est ouvert, il existe un ouvert A tel que $a \in A \subset W$. Mais comme A est un voisinage de $a \in \bar{V}$, nous avons $A \cap V \neq \varnothing$. Un élément de $A \cap V$ serait dans $W \cap V$, impossible. □

PROPooEQYEooZHXKnL

Proposition 9.24 ([225]).
Une réunion finie de fermeture sest la fermeture de l'union :

$$\bar{A} \cup \bar{B} = \overline{A \cup B}. \tag{9.15}$$

EQooSBGTooGPPbCl

La fermeture de l'intersection est inclue à l'intersection des fermetures :

$$\overline{A \cap B} \subset \bar{A} \cap \bar{B} \tag{9.16}$$

Démonstration. Soient des parties A, B de l'espace topologique X.

(1) $\bar{A} \cup \bar{B} \subset \overline{A \cup B}$ Soit $x \in \bar{A} \cup \bar{B}$. Disons $x \in \bar{A}$. Alors tout ouvert autour de x intersecte A et donc intersecte A^{b}. Même raisonnement si $x \in B$. Donc $x \in \overline{A \cup B}$.

(2) $\overline{A \cup B} \subset \bar{A} \cup \bar{B}$ La partie $\bar{A} \cup \bar{B}$ est un fermé (lemme 9.6(2)) qui contient $A \cup B$. Donc $\overline{A \cup B} \subset \bar{A} \cup \bar{B}$ (lemme 9.20(1)).

(3) **Pour l'intersection** Si $x \in \overline{A \cap B}$ alors tout voisinage de x contient un élément de $A \cap B$. Cet élément est un élément de A. Donc $x \in \bar{A}$. Et l'élément de $A \cap B$ est également dans B, donc $x \in \bar{B}$.

□

PROPooLPYFooOfIzxB

Proposition 9.25 ([226]).
Soient des parties $\{A_i\}_{i \in I}$ d'un espace topologique. Alors

$$\bigcup_{i \in I} \bar{A}_i \subset \overline{\bigcup_{i \in I} A_i}. \tag{9.17}$$

Note : nous verrons dans la proposition 9.107 que dans le cas d'une famille localement finie, il y a égalité.

Démonstration. Pour chaque $j \in I$ nous avons

$$A_j \subset \bigcup_{i\in I} A_i. \tag{9.18}$$

En prenant la fermeture des deux côtés : $\bar{A}_j \subset \overline{\bigcup_{i\in I} A_i}$. Cela étant valable pour tout j, en prenant l'union sur j nous avons encore l'inclusion :

$$\bigcup_{j\in I} \bar{A}_j \subset \overline{\bigcup_{i\in I} A_i}. \tag{9.19}$$

□

9.1.5.2 Densité

DefEnsembleDense

Définition 9.26.
*Soit X un espace topologique. Un sous-ensemble A de X est **dense** dans X si $\bar{A} = X$.*

LEMooITBVooBUYpve

Lemme 9.27 ([1])**.**
Soit un espace topologique X. Soient $A \subset X$ et un ouvert non vide $U \in \tau_X$. Si $U \subset \mathrm{Adh}(A)$ alors $U \cap A = \varnothing$.

Démonstration. Soit $x \in U$. Vu que $x \in \mathrm{Adh}(A)$, tout ouvert contenant x intersecte A. La partie U est un de ces ouverts. Donc $U \cap A \neq \varnothing$. □

PROPooTKHVooMderxm

Proposition 9.28 ([1])**.**
Soient un espace topologique X, une partie A et $Q \subset A$. Si Q est fermé dans X et dense dans A, alors $Q = A$.

Démonstration. Soit $a \in A$. Nous supposons que a n'est pas dans Q, c'est-à-dire que $a \in Q^c$. Vu que Q est fermé, le complémentaire est ouvert, et il existe un ouvert $U \in \tau_X$ tel que $a \in U \subset Q^c$. Cela contredit la densité de Q dans A parce que tout ouvert contenant un élément de A devrait intersecter Q. □

DEFooQUNJooWZasqV

Définition 9.29.
*Une partie A d'un espace topologique X est **discrète** si pour tout $a \in A$, il existe un ouvert $\mathcal{O}$ de X tel que $\mathcal{O} \cap A \neq \{a\}$.*

9.1.5.3 Topologie induite

DefVLrgWDB

Proposition-Définition 9.30 (Topologie induite[227])**.**
Soit un espace topologique (X, τ_X), et soit $Y \subset X$. Nous définissons

$$\tau_Y = \{Y \cap \mathcal{O} \text{ tel que } \mathcal{O} \in \tau_X\}. \tag{9.20}$$

L'ensemble τ_Y est une topologie sur Y.
*Elle est la **topologie induite**.*

Démonstration. Il s'agit de vérifier les conditions de la définition 9.1.

(1) $\underline{Y \in \tau_Y}$ Parce que $Y = X \cap Y$ et que X est un ouvert de X.

(2) $\underline{\varnothing \in \tau_Y}$ Parce que $\varnothing = Y \cap \varnothing$ et que $\varnothing$ est un ouvert de X.

(3) **Union quelconque** Soient des ouverts A_i de X. Nous avons

$$\bigcup_{i\in I} Y \cap A_i = Y \cap \big(\bigcup_{i\in I} A_i\big). \tag{9.21}$$

EQooJUYHooIugQXG

Comme les A_i sont des ouverts de X, leur union est encore un ouvert de X. Donc (9.21) est encore dans τ_Y.

(4) **Intersection finie** Nous avons

$$\bigcap_{i\in I} Y \cap A_i = Y \cap \left(\bigcap_{i\in I} A_i\right). \tag{9.22}$$

□

LemBWSUooCCGvax

Lemme 9.31 ([1]).
Soit (X, τ_X) un espace topologique et $S \subset X$, un fermé de X sur lequel nous considérons la topologie induite τ_S. Si F est un fermé de (S, τ_S) alors F est fermé de (X, τ_X).

Démonstration. Nous savons que $F \subset S$ et que le complémentaire de F dans S est un ouvert de (S, τ_S) : il existe un ouvert $\Omega \in \tau_X$ tel que $S \setminus F = S \cap \Omega$. Si maintenant nous considérons le complémentaire de F dans X nous avons

$$F^c = (S \setminus F) \cup (X \setminus S) = (S \cap \Omega) \cup S^c = (S \cap \Omega) \cup (S^c \cap \Omega) \cup S^c = \Omega \cup S^c. \tag{9.23}$$

Puisque Ω et S^c sont des ouverts de X, l'union est un ouvert. Donc $F^c \in \tau_X$ et F est un fermé de X. □

DEFooEXHFooKlKcQD

Définition 9.32 ([228]).
*Si X est un espace topologique, un **sous-espace topologique** de X est une partie de X munie de la topologie induite*[5].

PROPooQFIMooYmgjhA

Proposition 9.33 ([1]).
Soit une partie $\mathcal{O}$ de l'espace topologique X. Les fermés de $\mathcal{O}$ sont les parties de la forme $F \cap \mathcal{O}$ où F est fermé de X.

Démonstration. En deux parties.

(1) **Dans un sens** Soit un fermé A de $\mathcal{O}$. La partie $\mathcal{O} \setminus A$ est ouverte dans $\mathcal{O}$, de telle sorte qu'il existe un ouvert S de X satisfaisant $\mathcal{O} \setminus A = S \cap \mathcal{O}$. La partie $F = X \setminus S$ est fermée dans X, et nous allons prouver que $A = (X \setminus S) \cap \mathcal{O}$. D'abord nous avons

$$(X \setminus S) \cap \mathcal{O} = \mathcal{O} \setminus S. \tag{9.24}$$

EQooORVBooCxgCgw

Nous avons l'union disjointe $\mathcal{O} = (\mathcal{O} \setminus S) \cup (\mathcal{O} \cap S)$. Tenant compte du fait que $\mathcal{O} \cap S = \mathcal{O} \setminus A$, nous avons l'union disjointe

$$\mathcal{O} = (\mathcal{O} \setminus S) \cup (\mathcal{O} \setminus A). \tag{9.25}$$

EQooXKPVooMoYECB

Par ailleurs, vu que $A \setminus \mathcal{O}$, nous avons également l'union disjointe

$$\mathcal{O} = A \cup (\mathcal{O} \setminus A) \tag{9.26}$$

EQooQEMTooLFZwuv

En comparant (9.25) avec (9.26), nous trouvons $A = \mathcal{O} \cap S$.

En repartant de (9.24), nous avons maintenant

$$F \cap \mathcal{O} = (X \setminus S) \cap \mathcal{O} = \mathcal{O} \setminus S = A. \tag{9.27}$$

(2) **Dans l'autre sens** Soit un fermé F de X. Montrons que $F \cap \mathcal{O}$ est fermé dans $\mathcal{O}$. Pour cela nous prouvons que le complémentaire (dans $\mathcal{O}$) est ouvert dans $\mathcal{O}$. Nous avons :

$$\mathcal{O} \setminus (F \cap \mathcal{O}) = \mathcal{O} \cap (X \setminus F). \tag{9.28}$$

Comme F est fermé, $X \setminus F$ est ouvert.

□

PROPooNZTTooTrKoVF

Proposition 9.34 ([1]).
Soient un espace topologique X et une partie $A \subset X$. Nous notons τ_X la topologie de X et τ_A la topologie induite de X vers A. Si (A, τ_A) est un espace topologique compact, alors A est compact dans X.

Démonstration. Soit un recouvrement $\{U_i\}_{i \in I}$ de A par des ouverts de X. La famille $\{U_i \cap A\}_{i \in I}$ sont des ouverts de τ_A recouvrant A. Donc il existe une partie finie $I_0 \subset I$ telle que $\{U_i \cap A\}_{i \in I_0}$ recouvre A. Dans ce cas, la famille $\{U_i\}_{i \in I_0}$ recouvre également A. □

PROPooBKPEooQupIUx

Proposition 9.35 ([1]).
Soient un espace topologique X, et une partie $M \subset X$. Nous notons τ_X la topologie de X et τ_M la topologie induite de X vers M. Soit un τ_X-compact $K \subset M$. Alors K est τ_M-compact.

[5] Définition 9.30.

Démonstration. Soient des τ_M-ouverts $\{A_i\}_{i\in I}$ recouvrant K. Par définition de la topologie induite nous avons $A_i = M \cap U_i$ avec $U_i \in \tau_X$. Les parties $\{U_i\}_{i\in I}$ recouvrent K et il existe donc une partie finie $I_0 \subset I$ telle que $\{U_i\}_{i\in I_0}$ recouvre K.

Donc $\{U_i \cap M\}_{i\in I_0}$ recouvre également K. Donc $\{A_i\}_{i\in I_0}$ recouvre K qui est donc bien τ_M-compact. □

PROPooHQHWooFHHAXP

Proposition 9.36 ([1]).
Soient un espace topologique (X, τ_X), une partie A ainsi que $x \in A$. Si $\mathcal{B}$ est une base de topologie τ_X autour de x, alors

$$\mathcal{S} = \{B \cap A \text{ tel que } B \in \mathcal{B}\} \tag{9.29}$$

est une base de la topologie induite τ_A autour de x.

Démonstration. Soient $a \in A$ et un ouvert $\mathcal{O}$ de τ_A. Nous devons trouver un élément $S \in \mathcal{S}$ tel que

$$a \in S \subset \mathcal{O}. \tag{9.30}$$

Étant donné que $\mathcal{O} \in \tau_A$, il existe un ouvert U de X tel que $\mathcal{O} = A \cap U$. Étant donné que $\mathcal{B}$ est une base de topologie de X, il existe $B \in \mathcal{B}$ tel que $a \in B \subset U$. En posant $S = B \cap A$ nous avons $S \in \mathcal{S}$ et

$$a \in B \cap A \subset U \cap A = \mathcal{O}. \tag{9.31}$$

□

LEMooCXHEooKNmLma

Lemme 9.37 ([1]).
Soient un espace topologique X ainsi que $U \subset X$ (pas spécialement ouvert). Soit $A \subset U$. Nous avons

$$\mathrm{Adh}_U(A) = \mathrm{Adh}_X(A) \cap U \tag{9.32}$$

Si F est fermé dans U, alors

$$F = \mathrm{Adh}_X(F) \cap U. \tag{9.33}$$

EQooMZOOooKHfZTk

Démonstration. En deux inclusions.

(1) **Sens direct** Soit $x \in \mathrm{Adh}_U(A)$. Par définition nous avons $x \in U$. Nous devons prouver que $x \in \mathrm{Adh}_X(A)$. Pour cela nous considérons un ouvert $\mathcal{O} \in \tau_X$ contenant x. La partie $\mathcal{O} \cap U$ est un ouvert de U contenant x. Vu que $x \in \mathrm{Adh}_U(A)$, nous avons $(\mathcal{O} \cap U) \cap A \neq \varnothing$. À fortiori nous avons $\mathcal{O} \cap A \neq \varnothing$.

(2) **L'autre sens** Soit $x \in \mathrm{Adh}_X(A) \cap U$. Pour prouver que $x \in \mathrm{Adh}_U(A)$ nous considérons $\mathcal{O} \in \tau_U$ contenant x, et nous prouvons que $\mathcal{O} \cap A \neq \varnothing$. Comme $\mathcal{O}$ est un ouvert de U, il existe un ouvert $\mathcal{O}' \in \tau_X$ tel que $\mathcal{O} = \mathcal{O}' \cap U$.

Donc $\mathcal{O}'$ est un ouvert de X vérifiant $x \in \mathcal{O}'$. Vu que $x \in \mathrm{Adh}_X(A)$ nous avons aussi $\mathcal{O}' \cap A \neq \varnothing$. Il existe donc un y vérifiant

$$y \in \mathcal{O}' \cap A \subset \mathcal{O}' \cap U = \mathcal{O}. \tag{9.34}$$

Nous avons donc aussi $y \in \mathcal{O} \cap A$, comme il le fallait.

La formule (9.33) est la même, en tenant compte du fait que $\mathrm{Adh}_U(F) = F$ lorsque F est fermé dans U. □

LEMooXCNDooDkbaip

Lemme 9.38 ([1, 229]).
Soient un espace topologique X un un ouvert $U \in \tau_X$. Nous considérons $A \in \bar{\tau}_U$[6] tel que $\mathrm{Int}_U(A) = \varnothing$. Alors

$$\mathrm{Int}_X\big(\mathrm{Adh}_X(A)\big) = \varnothing. \tag{9.35}$$

Démonstration. Nous considérons $U_1 \in \tau_X$ tel que $U_1 \subset \mathrm{Adh}_X(A)$. Le but est de prouver que $U_1 = \varnothing$. Nous avons

(1) $U_1 \cap U \in \tau_X$ en tant qu'intersection d'ouverts.

(2) $U_1 \cap U \in \tau_U$ par définition de la topologie induite.

De plus en utilisant le lemme 9.37,

$$U_1 \cap U \subset \mathrm{Adh}_X(A) \cap U = \mathrm{Adh}_U(A) = A. \tag{9.36}$$

Donc $U_1 \cap U$ est un ouvert de U contenu dans A dont l'intérieur dans U est vide. Bref : $U_1 \cap U = \varnothing$.

Nous supposons par l'absurde que $U_1 \neq \varnothing$. Alors le lemme 9.27 dit que $U_1 \cap A \neq \varnothing$. Soit $x \in U_1 \cap A$. Nous avons :

$$x \in U_1 \cap A \subset U_1 \cap U. \tag{9.37}$$

Et comme nous avons déjà prouvé que $U_1 \cap U = \varnothing$, nous avons une contradiction. □

[6] $\bar{\tau}_U$ est l'ensemble des fermés de U.

LEMooLKHEooRqrqkA

Lemme 9.39 ([1]).
Soit un espace topologique X. Soient A ouvert dans X et $S \subset X$. Si $A \cap S = \varnothing$, alors $A \cap \bar{S} \neq \varnothing$

Démonstration. Supposons par l'absurde que $x \in A \cap \bar{S}$. Vu que A est ouvert, il existe un voisinage V de x contenu dans A (théorème 9.8). Étant donné que $x \in \bar{S}$, l'intersection $V \cap S$ est non vide. Tout élément de $V \cap S$ est dans $A \cap S$. □

PROPooRRWQooASUUIr

Proposition 9.40 ([1]).
Soit une bijection continue $f : X \to Y$. Soient $A \subset X$ et $B = f(A) \subset Y$ sur lesquels nous considérons les topologies induites. Alors la restriction $f : A \to B$ est continue.

Démonstration. Soit un ouvert $\mathcal{O}$ dans B. Il existe un ouvert $\mathcal{O}'$ de Y tel que $\mathcal{O} = \mathcal{O}' \cap B$. Vu que f est continue, la partie $f^{-1}(\mathcal{O}')$ est ouverte dans X. Vu que f est une bijection nous avons de plus

$$\begin{aligned} f^{-1}(\mathcal{O}) &= f^{-1}(\mathcal{O}' \cap B) && \text{(9.38a)}\\ &= f^{-1}(\mathcal{O}') \cap f^{-1}(B) && \text{(9.38b)}\\ &= f^{-1}(\mathcal{O}') \cap A. && \text{(9.38c)} \end{aligned}$$

Donc $f^{-1}(\mathcal{O})$ est un ouvert de A. □

LEMooPONCooJbuBMl

Lemme 9.41 ([1]).
Soient deux espaces topologiques X et Y. Soit $Q \subset X$ sur lequel nous considérons la topologie induite depuis X. Soient encore $a \in X$ et une base $\mathcal{B}$ de voisinages[7] de X autour de a.

Nous considérons une application $f : Y \to Q$ telle que $f^{-1}(Q \cap B)$ est ouvert pour tout $B \in \mathcal{B}$. Alors f est continue en a.

Démonstration. Soit un voisinage ouvert W de $f(a)$ dans Q. Nous devons trouver un voisinage ouvert V de a tel que $f(V) \subset W$.

Vu que W est ouvert autour de $f(a)$ pour Q, il existe un ouvert W' de X tel que $W = W' \cap Q$. Et comme W' est un ouvert contenant $f(a)$, il existe un élément $B \in \mathcal{B}$ tel que $f(a) \in B \subset W'$. Par hypothèse la partie $f^{-1}(B \cap Q)$ est ouverte. Donc en posant $V = f^{-1}(B \cap Q)$ on est bon. □

LEMooGANPooUJZmnM

Lemme 9.42 ([1]).
Soient deux espaces topologiques U et V. Nous supposons avoir :

(1) Une bijection continue d'inverse continue[8] *$f : U \to V$*

(2) Un fermé $H \subset V$ sur lequel nous considérons la topologie induite de V,

(3) Un ferme $\mathcal{H} \subset U$ sur lequel nous considérons la topologie induite de U,

(4) $f(\mathcal{H}) \subset H$

(5) Une partie $A \subset \mathcal{H}$ telle que $f(A)$ est ouverte dans H.

Alors

ITEMooIYGLooTrxugS

(1) A est ouvert dans $\mathcal{H}$.

ITEMooDZHUooFJRRfi

(2) L'application $f : A \to f(A)$ est un homéomorphisme.

Démonstration. Vu que $f(A)$ est ouvert dans H, il existe un ouvert W de V tel que $f(A) = H \cap W$. À partir de là, nous prouvons plusieurs choses.

(1) $\underline{A \subset \mathcal{H} \cap f^{-1}(W)}$ Nous avons $A \subset \mathcal{H}$ par définition. De plus $f(A) = H \cap W$, donc $f(A) \subset W$ et donc

$$A = f^{-1}\big(f(A)\big) \subset f^{-1}(W). \tag{9.39}$$

(2) $\underline{\mathcal{H} \cap f^{-1}(W) \subset A}$ Soit $x \in \mathcal{H} \cap f^{-1}(W)$. Vu que $f(\mathcal{H}) \subset H$, nous avons $f(x) \in H$. Mais évidemment $f(x) \in f\big(f^{-1}(W)\big) = W$. Donc $f(x) \in W$. Donc

$$f(x) \in H \cap W = f(A). \tag{9.40}$$

Vu que f est une bijection, nous en déduisons que $x \in A$.

[7] définition 9.5.
[8] C'est-à-dire un homéomorphisme.

(3) **Conclusion** Nous avons prouvé que

$$A = \mathcal{H} \cap f^{-1}(W) \tag{9.41}$$

Étant donné que W est ouvert dans U et que f est continue, $f^{-1}(W)$ est ouvert de U. Donc A est ouvert de $\mathcal{H}$.

Cela conclu la preuve de notre point (1).

En ce qui concerne le point (2), c'est la proposition 9.40 qui fait le boulot. □

9.1.6 Topologie sur $\mathbb{Q}$

Si A est un ouvert de X, on pourrait croire que la topologie induite n'a rien de spécial. Il est vrai que B sera ouvert dans A si et seulement si il est ouvert dans X, mais certaines choses surprenantes se produisent tout de même.

LEMooIGQCooOrroHT

Lemme 9.43.
La partie $\mathbb{Q}$ dans $\mathbb{R}$ est d'intérieur vide, et sa fermeture est $\mathbb{R}$.

Démonstration. Prouvons que $\mathbb{Q}$ est d'intérieur vide dans $\mathbb{R}$. Si $q \in \mathbb{Q}$, alors par le lemme 4.60(1), toute boule $B(q, \epsilon)$ contient un élément de $\mathbb{R} \setminus \mathbb{Q}$. Pour cela, il suffit de prendre un élément $r < \epsilon$ dans $\mathbb{R} \setminus \mathbb{Q}$ et ensuite $q + r \in B(q, \epsilon)$ qui marche par le lemme 4.73(4)(3).

Prouvons maintenant que tout élément de $\mathbb{R}$ est dans la fermeture de $\mathbb{Q}$. Soient $r \in \mathbb{R}$, et $\epsilon > 0$. En prenant un $s \in \mathbb{Q}$ vérifiant $r < s < r + \epsilon$ (lemme 4.60(1)), nous avons bien $s \in \mathbb{Q}$ et $s \in B(r, \epsilon)$. Donc toute boule centrée en r contient un élément de $\mathbb{Q}$. Tous les éléments de $\mathbb{R}$ sont dans la fermeture de $\mathbb{Q}$. □

ExloeyoR

Exemple 9.44.
Prenons $X = \mathbb{R}$ et $A =]0, 1[$. Si $B =]\frac{1}{2}, 1[$, alors la fermeture de B dans A sera $\tilde{B} = [\frac{1}{2}, 1[$ et non $[\frac{1}{2}, 1]$ comme on l'aurait dans $\mathbb{R}$. △

Prendre la topologie induite de $\mathbb{R}$ vers un fermé de $\mathbb{R}$ donne des boules un peu spéciales comme le montre l'exemple suivant.

ExKYZwYxn

Exemple 9.45.
Quid de la boule ouverte $B(1, \epsilon)$ dans le fermé $[0, 1]$? Par définition c'est

$$B(1, \epsilon) = \{x \in [0, 1] \text{ tel que } |x - 1| < \epsilon\} =]1 - \epsilon, 1]. \tag{9.42}$$

Oui, c'est *ouvert* dans $[0, 1]$. C'est d'ailleurs un des ouverts de la topologie induite de $\mathbb{R}$ sur $[0, 1]$.

Donc pour la topologie de $[0, 1]$, toutes les boules ouvertes $B(x, \delta)$ avec $x \in [0, 1]$ sont incluses dans $[0, 1]$. Bref, vous pouvez écrire

$$B(\frac{1}{2}, 10) \subset [0, 1], \tag{9.43}$$

mais vous avez intérêt à être très clair sur la topologie sous-entendue. △

9.1.6.1 Points d'accumulation et isolés

DEFooGHUUooZKTJRi

Définition 9.46.
*Soient un espace topologique X et une partie A de X. Un point $s \in X$ est un **point d'accumulation** de A si tout ouvert de X contenant s contient au moins un élément de $A \setminus \{s\}$.*

Quelle est la différence entre un point d'accumulation et un point d'adhérence ? La différence est que tous les points de A sont des points d'adhérence de A, parce que tout voisinage de $a \in A$ contient au moins a lui-même, alors que certains points de A peuvent ne pas être des points d'accumulation de A. Voir l'exemple 9.320.

Notons qu'un point d'accumulation de A dans X n'est pas spécialement dans A.

DEFooXIOWooWUKJhN

Définition 9.47.
*Soient un espace topologique X et une partie A de X. Un point $s \in A$ est un **point isolé** de A si il existe un voisinage ouvert $\mathcal{O}$ de s dans X tel que $A \cap \mathcal{O} = \{s\}$.*

9.1.7 Applications continues

La définition suivante est *la* définition de la continuité dans tous les cas.

DefOLNtrxB

Définition 9.48 (Application continue[230])**.**
Deux définitions :

ITEMooXARPooNzsWLr

(1) *Soient une application $f\colon X\to Y$ entre les espaces topologiques X et Y et un point $a\in X$. Nous disons que f est **continue en** a si pour tout ouvert W contenant $f(a)$, il existe un voisinage V de a dans X tel que $f(V)\subset W$.*

ITEMooEHGWooDdITRV

(2) *Une fonction $f\colon X\to Y$ est **continue** sur X si pour tout ouvert $\mathcal{O}$ de Y, l'ensemble*

$$f^{-1}(\mathcal{O})=\{x\in X \text{ tel que } f(x)\in\mathcal{O}\} \tag{9.44}$$

defFminuslofaset

est ouvert dans X.

PROPooOVKEooCkJmmO

Proposition 9.49 ([1])**.**
Une application $f\colon X\to Y$ entre deux espaces topologiques est continue sur X si et seulement si elle est continue en chacun des points de X.

Démonstration. Dans les deux sens.

(1) $\Rightarrow$ Nous supposons que $f\colon X\to Y$ est continue. Soit $a\in X$. Si W est un ouvert contenant $f(a)$, alors $V=f^{-1}(W)$ est un ouvert contenant a et vérifiant $f(V)\subset W$.

(2) $\Leftarrow$ Nous supposons que $f\colon X\to Y$ est continue en chaque point de X. Soit un ouvert $\mathcal{O}$ de Y. Pour $a\in f^{-1}(\mathcal{O})$, la partie $\mathcal{O}$ est un ouvert contenant $f(a)$. Donc il existe un ouvert V_a contenant a et tel que $f(V_a)\subset\mathcal{O}$.

Nous posons à présent $V=\bigcup_{a\in f^{-1}(\mathcal{O})}V_a$. C'est un ouvert comme union d'ouverts. Ensuite nous avons $V=f^{-1}(\mathcal{O})$. En effet d'une part nous avons $f(V_a)\subset\mathcal{O}$, donc $V_a\subset f^{-1}(\mathcal{O})$ pour tout $a\in X$. Donc $V\subset f^{-1}(\mathcal{O})$.

D'autre part, pour chaque $a\in f^{-1}(\mathcal{O})$ nous avons $a\in V_a$, et donc $f^{-1}(\mathcal{O})\subset V$.

□

LEMooYTLSooKhetml

Lemme 9.50.
Soient deux espaces topologiques X et Y et une application $f\colon X\to Y$. Soit une base de topologie $\{A_i\}_{i\in I}$ de Y. Si $f^{-1}(A_i)$ est ouvert dans X pour tout $i\in I$ alors f est continue.

Exemple 9.51 ([1])**.**
Un truc bien avec la définition 9.48(1) est que la continuité de f en un point est définie pour tout point du domaine ; pas seulement les points d'accumulation. Soit par exemple une fonction simple

$$\begin{aligned} f\colon\{a\}&\to\mathbb{R}\\ a&\mapsto 4. \end{aligned} \tag{9.45}$$

Si W est un ouvert de $\mathbb{R}$ contenant 4, nous avons l'ouvert $V=\{a\}$ tel que $f(V)\subset W$. Donc f est continue au point 4.

Mais f est également continue sur $\{4\}$ en tant qu'espace topologique. En effet, si W est un ouvert de $\mathbb{R}$, l'ensemble $f^{-1}(W)$ est soit $\varnothing$ soit $\{a\}$. Dans les deux cas c'est un ouvert. △

LEMooATLRooEKnlro

Lemme 9.52.
Une application $f\colon X\to Y$ est continue si et seulement si pour tout fermés F de Y, la partie $f^{-1}(F)$ est fermée dans X.

Démonstration. Supposons que f est continue. Si F est fermé dans Y, alors F^c est ouvert et donc $f^{-1}(F^c)=f^{-1}(F)^c$ est ouvert. Donc $f^{-1}(F)$ est fermé.

Dans l'autre sens, si $\mathcal{O}$ est ouvert dans Y, alors $f^{-1}(\mathcal{O})^c=f^{-1}(\mathcal{O}^c)$ est fermé, de telle sorte que $f^{-1}(\mathcal{O})$ est ouvert. L'application f est alors continue. □

PROPooXGBEooZRVkSc

Proposition 9.53 ([231])**.**
Une application $f\colon X\to Y$ entre espaces topologiques est continue si et seulement si $f(\bar{A})\subset\overline{f(A)}$ pour toute partie $A\subset X$.

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que f est continue. Nous considérons un élément de $f(\bar{A})$, c'est-à-dire $f(a)$ avec $a \in \bar{A}$. Nous considérons un ouvert $\mathcal{O}$ autour de $f(a)$. La partie $f^{-1}(\mathcal{O})$ est ouverte dans X et contient $a \in \bar{A}$. Donc $f^{-1}(\mathcal{O})$ intersecte A. Nous en concluons que $\mathcal{O}$ intersecte A. Nous avons montré que tout ouvert autour de $f(a)$ intersecte $f(A)$. Donc $f(a) \in \overline{f(A)}$.

(2) $\Leftarrow$ Nous supposons que $f(\bar{A}) \subset \overline{f(A)}$ pour toute partie $A \subset X$. Pour prouver la continuité de f, nous utilisons le critère du lemme 9.52 qui dit que f est continue si et seulement si $f^{-1}(F)$ est fermé pour tout fermé F.

Soit donc un fermé $F \subset Y$. Nous posons $D = f^{-1}(F)$. Nous avons

$$f(\bar{D}) \subset \overline{f(D)} = \overline{f\big(f^{-1}(F)\big)} = \bar{F} = F. \tag{9.46}$$

Nous prenons ensuite f^{-1} des deux côtés : $\bar{D} \subset f^{-1}(F) = D$. Donc $\bar{D} \subset D$; donc $\bar{D} = D$ et D est fermé.

□

9.1.7.1 Isomorphismes

DEFooYPGQooMAObTO

Définition 9.54 (Isomorphisme d'espaces topologiques)**.**
*Un **isomorphisme** d'espaces topologiques est une application bijective continue*[9] *entre deux espaces topologiques dont la réciproque est continue. On dit également **homéomorphisme**.*

*Un isomorphisme d'un espace avec lui-même est un **automorphisme**.*

LEMooMJSHooOszteq

Lemme 9.55 ([1])**.**
Si $f : X \to Y$ est un homéomorphisme[10] *et si F est fermé dans X, alors $f(F)$ est fermé dans Y.*

Démonstration. Le complémentaire F^c est ouverte. Vu que f^{-1} est continue, la partie $f(F^c)$ est ouverte. Comme f est une bijection, nous avons $f(F^c) = f(F)^c$. D'où le fait que $f(F)^c$ est ouvert, et donc que $f(F)$ est fermé. □

LEMooNMPGooRlgppQ

Lemme 9.56.
Soient un isomorphisme d'espaces topologiques $\varphi : X \to Y$ ainsi qu'une partie $S \subset X$. Alors

$$\varphi(\bar{S}) = \overline{\varphi(S)}. \tag{9.47}$$

Démonstration. Nous prouvons que $\overline{\varphi(S)} \subset \varphi(\bar{S})$; pour l'inclusion inverse, le lecteur fera lui-même.

Soit $x \in \overline{\varphi(S)}$. Nous allons prouver que $x \in \varphi(\bar{S})$, c'est-à-dire que $\varphi^{-1}(x) \in \bar{S}$. Pour cela nous considérons un ouvert $\mathcal{O}$ autour de $\varphi^{-1}(x)$. La partie $\varphi(\mathcal{O})$ est un ouvert contenant x. Donc $\varphi(\mathcal{O}) \cap \varphi(S) \neq \varnothing$, et donc $\mathcal{O} \cap S \neq \varnothing$, ce qui prouve que $\varphi^{-1}(x) \in \bar{S}$. □

9.57.
Note qu'en général, il n'est pas vrai que $f(\bar{S}) = \overline{f(S)}$ lorsque f est seulement continue. Nous avons par exemple[231] ceci :

$$\begin{aligned} f : \mathbb{R}^2 &\to \mathbb{R} \\ (x, y) &\mapsto x \end{aligned} \tag{9.48}$$

et $S = \{(x, 1/x) \text{ tel que } x \neq 0\}$. Nous avons $S = \bar{S}$ et donc $f(S) = f(\bar{S}) = \mathbb{R} \setminus \{0\}$. Mais $\overline{f(S)} = \mathbb{R}$.

La réalité est la proposition 9.53 qui dit que f est continue si et seulement si $f(\bar{S}) \subset \overline{f(S)}$ pour toute partie S.

9.2 Topologies rendant continue

9.2.1 Topologie initiale

PROPooGOEVooZBAOQh

Proposition-Définition 9.58 (Topologie initiale[232, 1])**.**
Soient un ensemble X, des espaces topologiques $(Y_i, \tau_i)_{i \in I}$, et des applications $\varphi_i : X \to Y_i$. Nous notons

$$\Lambda = \{(i, \omega_i) \text{ tel que } i \in I, \omega_i \in \tau_i\}, \tag{9.49}$$

[9] Application continue, définition 9.48.
[10] Définition 9.54.

et $P(\Lambda)$ l'ensemble des parties finies de Λ. Pour chaque $\lambda \in P(\Lambda)$, nous posons

$$\Phi_\lambda = \bigcap_{(i,\omega_i)\in\lambda} \varphi_i^{-1}(\omega_i). \tag{9.50}$$

Enfin nous posons[11]

$$\tau_I = \Big\{ \bigcup_{\lambda\in\Gamma} \Phi_\lambda \Big\}_{\Gamma\subset P(\Lambda)}. \tag{9.51}$$

EQooUAZMooImvinM

Nous avons :

(1) τ_I est une topologie sur X.

(2) Toutes les applications φ_i sont continues[12] *pour cette topologie.*

ITEMooJLXPooMokQuP

(3) La topologie τ_I est la plus faible topologie sur X pour laquelle toutes les φ_i sont continues. Autrement dit, si τ_X est une topologie pour laquelle toutes les φ_i sont continues, alors $\tau_I \subset \tau_X$.

La topologie ainsi définie est souvent référée comme la plus petite topologie qui rend les applications φ_i continues. Elle est aussi appelée ***topologie initiale*** *des φ_i.*

Démonstration. En plein de parties.

(1) **τ_I est une topologie** Vérification des conditions de la définition 9.1.

(1a) **$\varnothing$ et X sont dans τ_I** Pour $\varnothing$, il suffit de prendre $\Gamma = \varnothing$. Pour X, nous prenons un i quelconque et nous choisissons $\omega_i = Y_i$. Alors $\varphi_i^{-1}(\omega_i) = X$ et en prenant $\Gamma = \{(i,\omega_i)\}$ on est bon.

(1b) **Union quelconques** Nous avons $\bigcup_{\lambda\in\Gamma_1}\Phi_\lambda \cup \bigcup_{\lambda\in\Gamma_2}\Phi_\lambda = \bigcup_{\lambda\in\Gamma_1\cup\Gamma_2}\Phi_\lambda$. Les éléments de $\Gamma_1\cup\Gamma_2$ sont des parties finies de Λ.

(1c) **Intersection finie** D'abord, de la définition $\Phi_\alpha = \bigcap_{(i,\omega_i)\in\alpha}\varphi_i^{-1}(\omega_i)$, nous voyons que

$$\Phi_\alpha \cap \Phi_\beta = \bigcap_{(i,\omega_i)\in\alpha\cup\beta} \varphi_i^{-1}(\omega_i) = \Phi_{\alpha\cup\beta}. \tag{9.52}$$

En utilisant le lemme 1.51, nous avons alors

$$\Big(\bigcup_{\alpha\in\Gamma_\alpha}\Phi_\alpha\Big)\cap\Big(\bigcup_{\nu\in\Gamma_2}\Phi_\beta\Big) = \bigcup_{(\alpha,\beta)\in\Gamma_1\times\Gamma_2}(\Phi_\alpha\cap\Phi_\beta) = \bigcup_{(\alpha,\beta)\in\Gamma_1\times\Gamma_2}\Phi_{\alpha\cup\beta} = \bigcup_{\sigma\in\Gamma}\Phi_\sigma \tag{9.53}$$

où $\Gamma = \{\alpha\cup\beta \text{ tel que } (\alpha,\beta)\in\Gamma_1\times\Gamma_2\}$. Notez l'utilisation de la proposition 2.139(5) : chacun des $\alpha\cup\beta$ est fini.

(2) **Les φ_i sont continues** Soit un ouvert $\omega \subset Y_i$. Nous avons $\varphi_i^{-1}(\omega) = \Phi_\lambda$ avec $\lambda = \{(i,\omega)\}$. Mais $\Phi_\lambda \in \tau_I$. Donc $\varphi_i^{-1}(\omega)$ est ouvert dans (X,τ_I).

(3) **Topologie minimale** Une topologie τ_X sur X telle que tous les φ_i soient continues. Elle doit contenir tous les $\varphi_i^{-1}(\omega)$ avec $\omega\in\tau_i$. Comme une topologie doit contenir toutes les intersections finies, tous les Φ_λ sont dans τ_X. Comme τ_X doit contenir toutes les unions d'éléments de τ_X, elle doit contenir en particulier toutes les unions de parties de la forme Φ_λ. Donc $\tau_I\subset\tau_X$.

□

La topologie quotient d'un espace topologique par une relation d'équivalence est définie comme la plus petite topologie rendant continue la projection. Voir la définition 9.72.

LEMooVRGFooNgbwKu

Lemme 9.59 ([232, 233, 1])**.**
Soient des espaces topologiques $\{(Y_i,\tau_i)\}_{i\in I}$, et X, un ensemble. Pour chaque i nous considérons une base de topologie $\mathcal{B}_i$ de τ_i. Nous considérons des applications $\varphi_i\colon X\to Y_i$.

L'ensemble

$$\mathcal{B} = \left\{ \bigcap_{j=1}^{n} \varphi_{\alpha_j}^{-1}(U_j) \text{ tel que } n\in\mathbb{N}, \alpha_1,\dots,\alpha_n\in I, U_k\in\mathcal{B}_k \right\} \tag{9.54}$$

est une base de la topologie initiale[13] *des φ_i.*

[11] Juste pour être explicite : dans (9.51), Γ est un ensemble de parties finies de Λ. Donc chaque λ est une partie finie de Λ.
[12] Application continue, définition 9.48.
[13] Proposition 9.58.

Démonstration. En suivant les notations de la définition 9.58, nous considérons

$$\Phi_\lambda = \bigcap_{(i,\omega_i)\in\lambda} \varphi_i^{-1}(\omega_i). \tag{9.55}$$

Soit $x \in \Phi_\lambda$. Nous allons construire un $A \in \mathcal{B}$ tel que $x \in A \subset \Phi_\lambda$, et ce sera suffisant parce que les éléments de la topologie initiale sont des unions d'éléments de la forme Φ_λ.

Étant donné que $x \in \varphi_i^{-1}(\omega_i)$ pour tout $i \in \lambda$, nous pouvons poser $y_i = \varphi_i(x)$. Vu que $\mathcal{B}_i$ est une base de topologie de τ_i, nous pouvons prendre $U_i \in \mathcal{B}_i$ tel que

$$y_i \in U_i \subset \omega_i. \tag{9.56}$$

Enfin nous posons

$$A = \bigcap_{j\in\lambda} \varphi_j^{-1}(U_j). \tag{9.57}$$

Nous avons $x \in A \in \mathcal{B}$. De plus, étant donné que $U_i \subset \omega_i$, nous avons $\varphi_i^{-1}(U_j) \subset \varphi_j^{-1}(\omega_i)$ et donc $A \subset \Phi_\lambda$. □

PROPooOPJCooAIUXCW

Proposition 9.60 ([1]).
Soient un espace topologique (Y, τ_Y) et une application $f\colon X \to Y$. Soient $x_0 \in X$ et $y_0 = f(y_0)$. Si $\{B_i\}_{i\in I}$ est une base de voisinages de y_0, alors $\{f^{-1}(B_i)\}_{i\in I}$ est une base de voisinages de x_0 pour la topologie initiale[14] de f.

Démonstration. Soit un ouvert $\mathcal{O}$ autour de x_0 pour la topologie initiale de f. En adaptant le lemme 9.59 au cas d'une seule application,

$$\mathcal{B} = \{f^{-1}(U) \text{ tel que } U \in \tau_Y\} \tag{9.58}$$

est une base de topologie sur X. Donc $\mathcal{O}$ est une union de la forme[15]

$$\mathcal{O} = \bigcup_{\alpha\in A} f^{-1}(U_\alpha) \tag{9.59}$$

avec $U_\alpha \in \tau_Y$. Soit $\alpha \in A$ tel que $x_0 \in f^{-1}(U_\alpha)$. Nous avons $y_0 = f(x_0) \in U_\alpha$. Vu que U_α est un ouvert contenant y_0, et vu que $\{B_i\}_{i\in I}$ est une base de voisinages de y_0, nous avons un $i \in I$ tel que

$$y_0 \in B_i \subset U_\alpha. \tag{9.60}$$

Donc nous avons aussi

$$f^{-1}(B_i) \subset f^{-1}(U_\alpha) \subset \mathcal{O}. \tag{9.61}$$

Donc tout voisinage de x_0 contient un élément de $\{f^{-1}(B_i)\}_{i\in I}$. Cela prouve que ce dernier est une base des voisinages de x_0. □

PROPooSEQRooZoQPbZ

Proposition 9.61 ([234]).
Soient des applications $\{f_i\colon X \to Y_i\}_{i\in I}$ où les Y_i sont des espaces topologiques séparés. La topologie initiale τ_I sur X est séparée si et seulement si les f_i séparent les points de X.

Démonstration. En deux parties.

(1) $\Rightarrow$ Par contraposée, nous supposons avoir $x \neq y$ dans X tels que $f_i(x) = f_i(y)$ pour tout $i \in I$. Nous posons

$$\tau_0 = \{U \subset X \text{ tel que } x, y \in U \text{ ou } x, y \notin U\}. \tag{9.62}$$

C'est-à-dire que τ_0 contient les parties de X qui contiennent soit x et y soit aucun des deux.

Ce τ_0 est une topologie sur X. Voyons que les f_i sont continues. Si $A \subset Y_i$, alors soit $f_i(x) \in A$ et alors $x, y \in f_i^{-1}(A)$). Dans ce cas $f_i^{-1}(A) \in \tau_0$. Soit $f_i(x) \notin A$ et alors ni x ni y ne sont dans $f_i^{-1}(A)$. Dans ce cas $f_i^{-1}(A) \in \tau_0$. Bref, pour tout $i \in I$ et pour tout partie A de Y_i nous avons $f_i^{-1}(A) \in \tau_0$. Donc f_i est continue.

Donc τ_0 est une topologie rendant continue toutes les f_I. Elle est donc au moins aussi grande que le topologie initiale τ_I. Étant donne que τ_0 ne sépare pas les points x et y, la topologie τ_I ne les sépare pas non plus. Nous avons donc démontré que τ_i n'est pas séparé.

[14] Définition 9.58.
[15] Définition 9.2(1).

(2) $\Leftarrow$ Nous supposons maintenant que les f_i séparent les points de X, et nous devons en déduire que (X, τ_I) est séparé. Soient $x, y \in X$. Nous considérons $i \in I$ tel que $f_i(x) \neq f_i(y)$. Étant donné que Y_i est séparé, nous pouvons considérer des voisinages ouverts disjoints W_1 de $f_i(x)$ et W_2 de $f_i(y)$ dans Y_i.

Vu que f_i est continue, les parties $f_i^{-1}(W_1)$ et $f_i^{-1}(W_2)$ sont ouvertes. Elles sont de plus disjointes parce que si $z \in f_i^{-1}(W_1) \cap f_i^{-1}(W_2)$, alors $f_i(z) \in W_1 \cap W_2 = \varnothing$.

Donc τ_I sépare x et y.

□

LEMooZLZKooHElBOs

Lemme 9.62 ([1]).
Soient un ensemble A et un espace topologique séparé S. Nous considérons $\mathrm{Fun}(A, S)$ *l'ensemble de toutes les applications $A \to S$. Pour chaque $x \in A$ nous posons*

$$\begin{aligned} \pi_x \colon \mathrm{Fun}(A, S) &\to S \\ f &\mapsto f(x). \end{aligned} \tag{9.63}$$

Si τ_I est la topologie initiale de A pour les $\{\pi_x\}_{x\in A}$, alors (A, τ_I) est séparé.

Démonstration. En vertu de la proposition 9.61, il suffit de vérifier que les π_x séparent les points dans $\mathrm{Fun}(A, S)$. Pour cela nous considérons $f \neq g$ dans $\mathrm{Fun}(A, \mathbb{R})$. Il existe donc $x \in A$ tel que $f(x) \neq g(x)$. Dans ce cas nous avons $\pi_x(f) \neq \pi_x(g)$. Donc f et g sont bien séparés. □

LEMooADPLooYylNsj

Lemme 9.63 ([232]).
Soient des espaces topologiques $\{(Y_i, \tau_i)\}_{i\in I}$, et X, un ensemble. Nous considérons des applications $\varphi_i \colon X \to Y_i$ ainsi que τ, la topologie minimale sur X telle que les applications φ_i soient continues.

Soit une suite (x_n) dans X. Nous avons $x_n \xrightarrow{\tau} x$ si et seulement si $\varphi_i(x_n) \xrightarrow{\tau_i} \varphi_i(x)$ pour tout $i \in I$.

Démonstration. Dans le sens direct, c'est seulement le fait que les φ_i sont continues.

Dans le sens réciproque, nous supposons que $\varphi_i(x_n) \xrightarrow{\tau_i} \varphi_i(x)$ pour tout i et nous devons prouver que $x_n \xrightarrow{\tau} x$.

Soit un voisinage U de x. Vue la base de topologie donnée dans le lemme 9.59, il existe un J fini dans I ainsi que des ouverts $\{V_j\}_{j\in J}$ tels que

$$x \in W = \bigcap_{j\in J} \varphi_j^{-1}(V_j) \subset U \tag{9.64}$$

Par hypothèse, $\varphi_i(x_n) \to \varphi_i(x)$. Mais V_j est un ouvert qui contient $\varphi_j(x)$. Donc il existe $N_j \in \mathbb{N}$ tel que $\varphi_j(x_n) \in V_j$ pour tout $n \geqslant N_j$. En posant[16] $N = \max\{N_j\}_{j\in J}$, nous avons que $\varphi_j(x_n) \in V_j$ pour tout $n \geqslant N$ et pour tout $j \in J$.

Dans ce cas nous avons aussi $x_n \in W \subset U$. La convergence est prouvée. □

PROPooCBPEooCuaLUk

Proposition 9.64 ([232]).
Soient des espaces topologiques (Y_i, τ_i), un ensemble X, et des applications $\varphi_i \colon X \to Y_i$. Nous considérons sur X la plus petite topologie rendant continues[17] *les φ_i.*

Soit un espace topologique Z. Une application $\psi \colon Z \to (X, \tau_I)$ est continue si et seulement si les applications $\varphi_i \circ \psi \colon Z \to Y_i$ sont continues pour tout $i \in I$.

Démonstration. Le sens direct est une simple composée de fonctions continues. Pour l'autre sens, nous supposons que les $\phi_i \circ \psi$ sont continues, nous considérons $U \in \tau_I$ et nous devons montrer que $\psi^{-1}(U)$ est un ouvert de Z.

En posant

$$\Lambda = \{(i, \omega) \text{ tel que } i \in I, \omega \in \tau_i\}, \tag{9.65}$$

il existe un ensemble Γ de parties finies de Λ tel que

$$U = \bigcup_{\lambda\in\Gamma} \bigcap_{(i,\omega)\in\lambda} \varphi_i^{-1}(\omega). \tag{9.66}$$

Nous avons donc

$$\psi^{-1}(U) = \bigcup_{\lambda\in\Gamma} \bigcap_{(i,\omega_i)\in\lambda} (\psi \circ \varphi_i^{-1})(\omega_i). \tag{9.67}$$

Vu que $\psi \circ \varphi^{-1}$ est continue, chacun des $(\psi \circ \varphi_i^{-1})(\omega)$ est ouvert. Donc $\psi^{-1}(U)$ est ouvert comme intersection finie et union arbitraire d'ouverts. □

[16] Notez l'utilisation du lemme 2.33 pour justifier que le maximum existe.
[17] Proposition 9.58.

9.2.2 Topologie produit

DEFooJHXKooQApPtQ

Définition 9.65 (Topologie produit[235]).
*Soit une famille d'espaces topologiques $\{(X_i, \tau_i)\}_{i\in I}$. La **topologie produit** sur*[18]

$$\prod_{i\in I} A_i = \{f \in \mathrm{Fun}(I, \bigcup_{i\in I} A_i) \text{ tel que } \forall i \in I, f(i) \in A_i\} \tag{9.68}$$

est la topologie initiale[19] *des projections*

$$\begin{aligned} p_i\colon \mathrm{Fun}(I, \bigcup_{i\in I} A_i) &\to A_i \\ f &\mapsto f(i). \end{aligned} \tag{9.69}$$

DefIINHooAAjTdY

Proposition 9.66 (Produit d'espaces topologiques, thème 27).
Soient $\{(X_i, \tau_i)\}_{i=1,\dots,n}$ des espaces topologiques. La topologie produit[20] *sur $X = \prod_{i=1}^n X_i$ est donnée par*

EQooVECGooKLUkTy

$$\mathcal{T} = \{\mathcal{O} \subset X \text{ tel que } \forall x \in U, \exists U_i \in \tau_i \text{ tel que } x \in U_1 \times \dots \times U_n \subset \mathcal{O}\}. \tag{9.70}$$

Démonstration. Nous devons montrer que lesp_i sont continues pour $\mathcal{T}$ et que toute topologie rendant les p_i continues doit contenir $\mathcal{T}$.

(1) **Les p_i sont continues pour $\mathcal{T}$** Soit un ouvert $\mathcal{O}$ de $\mathcal{T}$. Nous devons montrer que $p_i^{-1}(\mathcal{O}) \in \tau_i$. Soit $a \in p_i^{-1}(\mathcal{O})$. Soit $x \in \mathcal{O}$ tel que $p_i(a) = x$. Il existe des ouverts $U_j \in \tau_j$ tels que

$$x \in U_1 \times \dots \times U_n \subset \mathcal{O}. \tag{9.71}$$

Nous avons alors $p_i^{-1}(U_1 \times \dots \times U_n) = U_i$. Et donc $a \in U_i \subset p_i^{-1}(\mathcal{O})$.

(2) **Si les p_i sont continues pour $\mathcal{T}_0$** Soit une topologie $\mathcal{T}_0$ pour laquelle toutes les projections sont continue. Soient des ouverts $U_i \in \tau_i$. Nous devons prouver que $U_1 \times \dots \times U_n \in \mathcal{T}_0$. Vu que p_i est continue et que U_i est un ouvert, nous devons avoir $p_i^{-1}(U_i) \in \tau_0$. Et par stabilité d'une topologie pour les intersections,

$$\bigcap_{i=1}^n p_i^{-1}(U_i) = U_1 \times \dots \times U_n \tag{9.72}$$

doit encore être dans $\mathcal{T}_0$. Donc $\mathcal{T} \subset \mathcal{T}_0$.

□

Dans le cas d'espaces normés, nous verrons dans le lemme 9.306 que la topologie produit est la même que celle obtenue par la norme produit.

Proposition 9.67 (Convergence composante par composante).
Soient des espaces topologiques X_i $(i = 1, \dots, n)$ et une suite $(a_k^{(1)}, \dots, a_k^{(n)})$ dans $X_1 \times \dots \times X_n$. Nous avons la convergence

$$(a_k^{(1)}, \dots, a_k^{(n)}) \xrightarrow{X_1\times\dots\times X_n} (a^{(1)}, \dots, a^{(n)}) \tag{9.73}$$

si et seulement si $a_k^{(i)} \to a^{(i)}$ pour chaque i.

Démonstration. En deux parties.

(1) **Sens direct** Soient des ouverts $\mathcal{O}_i$ autour de $a^{(i)}$ dans X_i. Puisque $\mathcal{O}_1 \times \dots \times \mathcal{O}_n$ est un ouvert autour de $(a^{(1)}, \dots, a^{(n)})$, il existe $K \in \mathbb{N}$ tel que si $k \geqslant K$ nous avons $(a_k^{(1)}, \dots, a_k^{(n)}) \in \mathcal{O}_1 \times \dots \times \mathcal{O}_n$. Pour ce K nous avons séparément $a_k^{(i)} \in \mathcal{O}_i$ pour chaque i.

(2) **Sens inverse** Une prébase de la topologie sur $X_1 \times \dots \times X_n$ est donnée par les $\mathcal{O}_1 \times \dots \times \mathcal{O}_n$ où $\mathcal{O}_i$ est un ouvert de X_i. Voir la définition 9.66 de la topologie produit et la définition 9.13 de ce qu'est une prébase.

La proposition 9.15 nous permet de ne vérifier la convergence de $(a_k^{(1)}, \dots, a_k^{(n)})$ que sur la prébase. Soit donc $\mathcal{O} = \mathcal{O}_1 \times \dots \times \mathcal{O}_n$ avec $(a^{(1)}, \dots, a^{(n)}) \in \mathcal{O}$. Puisque $(a_k^{(i)})_{k\in\mathbb{N}} \to a^{(i)}$, pour chaque i, il existe $K_i \in \mathbb{N}$ tel que si $k \geqslant K_i$ alors $a_k^{(i)} \in \mathcal{O}_i$.

En posant $K = \max_i(K_i)$, nous avons $(a_k^{(1)}, \dots, a_k^{(n)}) \in \mathcal{O}_1 \times \dots \mathcal{O}_n$ pour tout $k \geqslant K$.

La proposition 9.15 permet de conclure.

[18] Produit cartésien infini, définition 1.22.
[19] Définition 9.58.
[20] Définition 9.65.

□

LEMooRTWNooMZTWgS

Lemme 9.68 ([1]).
Soient des espaces topologiques $X_1, \dots, X_n$ et Y. Si une application $f\colon X_1 \times \dots \times X_n \to Y$ est continue, alors pour tout $(a_1, \dots, a_{n-1}) \in X_1 \times \dots X_{n_1}$, l'application partielle

$$\begin{aligned} f_{a_1,\dots,a_{n-1}}\colon X_n &\to Y \\ x &\mapsto f(a_1, \dots, a_{n-1}, x) \end{aligned} \tag{9.74}$$

est continue.

9.2.3 Topologie de la convergence simple

DEFooOKYYooBbowQC

Définition 9.69.
Soient un ensemble X et un espace topologique Y. Pour $x \in X$ et $V \in \tau_Y$, nous posons

$$W(x, V) = \{f\colon X \to Y \text{ tel que } f(x) \in V\}. \tag{9.75}$$

*La **topologie de la convergence simple** sur $\mathrm{Fun}(X, Y)$ est la topologie engendrée*[21] *par les parties $\{W(x, V)\}_{\substack{x\in X \\ V\in\tau_Y}}$.*

PROPooWLWYooBWCajp

Proposition 9.70.
Soient un ensemble X et un espace topologique Y. La topologie de la convergence simple[22] *et la topologie produit*[23] *sur $\mathrm{Fun}(X, Y) = \prod_{x\in X} Y$ sont identiques.*

Démonstration. Nous notons τ_P la topologie produit, et τ_C celle de la convergence simple.

(1) <u>Une bonne formule</u>

La topologie produit est la topologie initiale des projections

$$\begin{aligned} p_x\colon \prod_{s\in X} Y = \mathrm{Fun}(X, Y) &\to Y \\ f &\mapsto f(x) \end{aligned} \tag{9.76}$$

Si V est ouvert dans Y et si $x \in X$, alors

$$p_x^{-1}(V) = W(x, V). \tag{9.77}$$

(2) <u>$\tau_P \subset \tau_C$</u> Nous prouvons que les $p_x\colon X \to Y$ sont continues pour τ_C. En effet si U est un ouvert de Y, alors $p_x^{-1}(U) = W(x, U)$ qui est ouvert dans τ_C. La proposition 9.58(3) dit qu'alors $\tau_P \subset \tau_C$.

(3) <u>$\tau_C \subset \tau_P$</u> Toutes les parties de la forme $p_x^{-1}(U)$ sont ouvertes pour τ_P. Donc τ_P contient une base de la topologie τ_C. Donc $\tau_C \subset \tau_P$.

□

9.2.4 Topologie finale

PROPooZRQTooOtqjLn

Proposition-Définition 9.71 ([236]).
Soient un ensemble X, des espaces topologiques $\{(Y_i, \tau_i)\}_{i\in I}$ et une application $f_i\colon Y_i \to X$ pour chaque i. Nous posons

$$\tau_F = \{U \subset X \text{ tel que } \forall i \in I, f_i^{-1}(U) \in \tau_i\}. \tag{9.78}$$

Alors

(1) τ_F est une topologie sur X.

(2) τ_F est la plus fine topologie sur X pour lesquelles toutes les applications f_i sont continues. C'est-à-dire que si τ_X est une topologie sur X telle que toutes les f_i sont continues, alors $\tau_X \subset \tau_F$.

*Cette topologie est nommée **topologie finale** sur X.*

[21] Définition 9.13.
[22] Définition 9.69.
[23] Produit en tant que ensemble des application, définition 1.22, et topologie produit 9.66.

Démonstration. Nous commençons par prouver que τ_F est une topologie.

(1) $\varnothing \in\in \tau_F$ Pour chaque i nous avons $f_i^{-1}(\varnothing) = \varnothing \in \tau_i$.

(2) $X \in\in \tau_F$ Pour chaque i nous avons $f_i^{-1}(X) = Y_i \in \tau_i$.

(3) **Union** Soient des éléments $\{A_s\}_{s\in S}$ de τ_F. Nous avons

$$f_i^{-1}\Big(\bigcup_{s\in S} A_s\Big) = \bigcup_{s\in S} f_i^{-1}(A_s). \tag{9.79}$$

Étant donné que $f_i^{-1}(A_s) \in \tau_i$ et que τ_i est une topologie, la dernière union est une union d'éléments de τ_i et est donc un élément de τ_i.

(4) **Intersection** Soient $A, B \in \tau_F$. Nous avons

$$f_i^{-1}(A \cap B) = f_i^{-1}(A) \cap f_i^{-1}(B) \in \tau_i. \tag{9.80}$$

Nous montrons maintenant que τ_F est la plus fine topologie sur X pour lesquelles toutes les applications f_i sont continues. Soient une topologie τ_X et une partie $A \subset X$ telle que $A \in \tau_X$ mais $A \notin \tau_F$. Il existe donc un $i \in I$ tel que $f_i^{-1}(A) \notin \tau_i$. Donc $f_i\colon (Y_i, \tau_i) \to (X, \tau_X)$ n'est pas continue. □

9.2.5 Topologie quotient

DEFooHWSYooZZLXQU

Définition 9.72 ([237]).
*Soit un espace topologique X ainsi qu'une relation d'équivalence $\sim$ sur X. La **topologie quotient** sur l'ensemble $X/\sim$ est la topologie finale[24] de la projection canonique $p\colon X \to X/\sim$.*

PROPooDRPLooONCwYs

Proposition 9.73.
Soit un espace topologique X muni d'une relation d'équivalence $\sim$. Une partie $\mathcal{O} \in X/\sim$ est ouverte[25] si et seulement si $p^{-1}(\mathcal{O})$ est ouverte dans X.

Démonstration. C'est la définition d'une topologie finale. □

DEFooBXGJooOBQaNw

Définition 9.74 (Passage d'une application aux classes).
*Soient deux ensembles X et E ainsi qu'une relation d'équivalence $\sim$ sur X. Nous disons qu'une application $f\colon X \to E$ **passe aux classes** si f est constante sur chaque classe d'équivalence de X. Dans ce cas nous considérons l'**application quotient***

$$\begin{aligned} \tilde{f}\colon X/\sim &\to E \\ [x] &\mapsto f(x). \end{aligned} \tag{9.81}$$

LEMooKTINooKDjNeX

Lemme 9.75 ([238]).
Soient deux espaces topologiques X et Y. Soit une relation d'équivalence $\sim$ sur X. Nous considérons une application continue[26] $f\colon X \to Y$ capable de descendre aux classes[27]. Alors l'application quotient $\tilde{f}\colon X/\sim \to Y$ est continue.

Démonstration. Nous considérons la projection canonique $p\colon X \to X/\sim$. Soit un ouvert $\mathcal{O}$ dans Y. La partie $\tilde{f}^{-1}(\mathcal{O})$ sera ouverte si $p^{-1}\big(\tilde{f}^{-1}(\mathcal{O})\big)$ est ouverte (proposition 9.73). Nous avons

$$p^{-1}\big(\tilde{f}^{-1}(\mathcal{O})\big) = (\tilde{f} \circ p)^{-1}(\mathcal{O}). \tag{9.82}$$

Mais $\tilde{f} \circ p = f$ parce que $(\tilde{f} \circ p)(x) = \tilde{f}([x]) = f(x)$. Donc

$$p^{-1}\big(\tilde{f}^{-1}(\mathcal{O})\big) = (\tilde{f} \circ p)^{-1}(\mathcal{O}) = f^{-1}(\mathcal{O}) \tag{9.83}$$

qui est ouvert parce que f est continue. □

LEMooIGLQooIMSWYg

Lemme 9.76 ([238]).
Soient deux espaces topologiques X et Y ainsi qu'une relation d'équivalence $\sim$ sur X. Nous considérons une application continue $g\colon X/\sim \to Y$. Alors

[24] C'est la plus grande topologie rendant continue. Définition 9.71.
[25] La topologie est définie en 9.72.
[26] Définition 9.48.
[27] Voir la définition 9.74.

(1) L'application $g \circ p$ est continue.

(2) Si nous posons $f = g \circ p$, alors f descend aux classes et $\tilde{f} = g$.

Démonstration. La projection p est toujours continue par définition de la topologie quotient. Donc $g \circ p$ est continue par composition d'applications continues.

Voyons que f descend aux classes. Si $x \sim y$, alors $p(x) = p(y)$ et donc $f(x) = f(y)$. En ce qui concerne l'application $\tilde{f}$, nous avons

$$\tilde{f}\big([x]\big) = (g \circ p)(x) = g\big([x]\big), \tag{9.84}$$

donc $\tilde{f} = g$ et le lemme est démontré. □

PROPooYKLBooQuqnfA

Proposition 9.77 ([237])**.**
Soient des espaces topologiques X et Y ainsi qu'une relation d'équivalence $\sim$ sur X. Soit la projection canonique $p\colon X \to X/\sim$. Une application $f\colon X/\sim \to Y$ est continue si et seulement si l'application composée $f \circ p\colon X \to Y$ est continue.

9.3 Espace séparable

Notons que l'on a parlé d'*une* limite de suite jusqu'à présent : en effet, si il existe deux éléments distincts x et y tels que tout ouvert contenant x contient y, alors la définition 9.14 dit que toute suite convergeant vers y converge aussi vers x…

EXooSHKAooZQEVLB

Exemple 9.78.
Oui, il y a moyen de converger vers plusieurs points distincts si l'espace n'est pas super cool. Nous pouvons par exemple [239] considérer la droite réelle munie de sa topologie usuelle et y ajouter un point $0'$ (qui clone le réel 0) dont les voisinages sont les voisinages de 0 dans lesquels nous remplaçons 0 par $0'$. Dans cet espace, la suite $(1/n)$ converge à la fois vers 0 et $0'$.

En fait, on « voit » le problème : on ne peut pas distinguer d'un point de vue topologique le 0 et le $0'$. △

Nous posons la définition suivante, qui nous permettra de donner une assez grande classe d'espaces topologiques dans lesquels nous avons unicité de la limite[28].

DefYFmfjjm

Définition 9.79 (Espace topologique séparé ou Hausdorff)**.**
Si deux points distincts admettent toujours deux voisinages disjoints[29], nous disons que l'espace est ***séparé*** *ou* ***de Hausdorff****.*

Attention, cette notion est à ne pas confondre avec :

DefUADooqilFK

Définition 9.80 (Espace topologique séparable)**.**
Un espace topologique est ***séparable*** *si il possède une partie dénombrable[30] dense[31].*

LEMooXNSCooQYkmAN

Lemme 9.81 ([1])**.**
Un singleton d'un espace Hausdorff[32] est fermé.

Démonstration. Soit un espace topologique séparé X. Nous prouvons que $X\backslash\{a\}$ est ouvert. Soit $x \in X\backslash\{a\}$. Vu que X est séparé, il existe un voisinage V de a et U de x tels que $V \cap U = \varnothing$. En particulier $U \subset X \setminus \{a\}$. Donc $X \setminus \{a\}$ contient un voisinage de chacun de ses points et est donc ouvert. □

9.4 Suites et convergence

9.82.
À propos de notations. La pire notation possible pour une suite est $(a_n)_n$. Mais que vient faire le second indice n ? Il peut être raisonnable d'écrire $(a_n)_{n\in I}$ lorsqu'on veut dire dans quel ensemble se déplace n. Si nous parlons de *suite*, il faut une sérieuse raison de prendre autre chose que $\mathbb{N}$ comme ensemble d'indices.

[28] Voir la proposition 9.154.
[29] Définition 1.7.
[30] Définition 2.34.
[31] Définition 9.26.
[32] Hausdorff et séparé sont synonymes, définition 9.80.

Une suite étant une fonction, de la même façon qu'on ne devrait pas dire « la fonction $f(x)$ », mais « la fonction f » ou « la fonction $x \mapsto f(x)$ », nous devrions simplement écrire a pour désigner la suite dont les éléments sont a_n.

Par conséquent, il est parfaitement légal, et même conseillé, d'écrire « $a+b$ » pour la somme des suites a et b. Et il est tout aussi légal d'écrire « $\lim a$ » au lieu de $\lim_{n\to\infty} a_n$.

Le hic est que nous écrivons souvent x la limite de la suite $n \mapsto x_n$. Dans ce cas, nous sommes évidemment obligé d'écrire l'indice n pour parler de la suite.

Tout cela pour dire qu'il faut être souple avec les notations.

PROPooFSRRooYNNTvj

Proposition 9.83 (Les fonctions continues commutent avec les limites de suites[1])**.**
Soient des espaces topologiques X et Y ainsi qu'une fonction continue $f\colon X \to Y$. Si $x_k \xrightarrow{X} x$ alors

$$f(x_k) \xrightarrow{Y} f(x). \tag{9.85}$$

Démonstration. Soit un ouvert U autour de $f(x)$. Étant donné que f est continue, $f^{-1}(U)$ est un ouvert autour de x. Vu que $x_n \xrightarrow{X} X$, il existe un N tel que si $n \geqslant N$, alors $x_n \in f^{-1}(U)$. Pour ces n nous avons aussi $f(x_n) \in U$. Cela prouve que $(f(x_n))_{n\in\mathbb{N}}$ est une suite convergente dans Y vers $f(x)$. □

9.4.1 Convergence dans un fermé

PROPooBBNSooCjrtRb

Proposition 9.84 ([1])**.**
Une suite contenue dans un fermé ne peut converger[33] *que vers un élément de ce fermé.*

Démonstration. Soient un espace topologique X et un fermé F dans X. Nous supposons que la suite (x_k) soit contenue dans F. Nous allons prouver qu'aucun élément de F^c ne peut être limite.

Soit $a \in F^c$. Puisque le complémentaire de F est un ouvert, et d'après le théorème 9.8, il existe un ouvert $\mathcal{O}_a$ contenant a, et contenu dans F^c. Le voisinage $\mathcal{O}_a$ de a ne contient donc aucun élément de la suite (x_k), qui ne peut donc pas converger vers a. □

CorLimAbarA

Corolaire 9.85.
Soit A un sous-ensemble d'un espace topologique X. Toute suite d'éléments de A qui converge, admet pour limite un élément de $\mathrm{Adh}(A)$.

Démonstration. Une fois la suite (x_n) fixée, il suffit de remarquer que tous les x_n sont dans $\mathrm{Adh}(A)$, et puis d'appliquer la proposition 9.84. □

PROPooEXUMooAFbpVJ

Proposition 9.86 ([1])**.**
Soit un espace topologique X, et une partie $A \subset X$. Nous supposons que pour toute suite convergente $x_n \xrightarrow{X} x$ telle que $x_n \in A$, nous avons $x \in A$.
Alors A est fermé.

Démonstration. Soit $a \in \mathrm{Adh}(A)$. Il existe une suite convergente $x_n \xrightarrow{X} a$ avec $x_n \in A$. Par hypothèse nous avons alors $a \in A$. Cela prouve que $\mathrm{Adh}(A) \subset A$, et donc que A est fermé. □

LemPESaiVw

Lemme 9.87.
Soit $A \subset X$ muni de la topologie induite de X et (x_n) une suite dans A. Si (x_n) converge vers un élément x dans A, alors elle converge aussi vers x dans X.

Démonstration. Soit $\mathcal{O}$ un ouvert autour de x dans X. Alors $A \cap \mathcal{O}$ est un ouvert autour de x dans A et il existe $N \in \mathbb{N}$ tel que si $n \geqslant N$, alors $x_n \in A \cap \mathcal{O} \subset \mathcal{O}$. □

LEMooAIVCooXTzWZi

Lemme 9.88.
soient un espace topologique X ainsi qu'une application continue $f\colon X \to X$. Alors

$$f(\bar{A}) \subset \overline{f(A)}. \tag{9.86}$$

Démonstration. Soit $y \in f(\bar{A})$. Il existe $x \in \bar{A}$ tel que $y = f(x)$. Il existe alors une suite (x_n) dans A telle que $x_n \to x$. Par continuité de f et la proposition 9.83 nous avons :

$$f(x_n) \to f(x) = y. \tag{9.87}$$

Pour chaque n nous avons $f(x_n) \in f(A)$ et donc $\lim_n f(x_n) \in \overline{f(A)}$. Donc $y = \lim f(x_n) \in \overline{f(A)}$. □

[33] Définition 9.14.

LEMooSCIIooRyRrHA

Lemme 9.89.
Soient un espace topologique X, une bijection continue $f\colon X \to X$ telle que f^{-1} est continue et $A \subset X$ tel que $f(A) = A$. Alors

$$f(\bar{A}) = \bar{A}. \tag{9.88}$$

Démonstration. En deux étapes.

(1) $\underline{f(\bar{A}) \subset \bar{A}}$ Par hypothèse nous avons $f(A) \subset A$. En prenant la fermeture des deux côtés : $\overline{f(A)} \subset \bar{A}$. Mais par le lemma 9.88 nous savons que $f(\bar{A}) \subset \overline{f(A)}$. Donc

$$f(\bar{A}) \subset \overline{f(A)} \subset \bar{A}. \tag{9.89}$$

(2) $\underline{\bar{A} \subset f(\bar{A})}$ Soit $x \in \bar{A}$. Il existe une suite (x_n) dans A telle que $x_n \to x$. Étant donné que $A = f(A)$, nous pouvons choisir pour chaque n un $y_n \in A$ tel que $x_n = f(y_n)$. Étant donné que f^{-1} est une bijection continue, la suite $y_n = f^{-1}(x_n)$ est également convergente. Notons y sa limite. Vu que f est continue, elle commute avec la limite (proposition 9.83) :

$$x = \lim f(y_n) = f(\lim y_n) = f(y). \tag{9.90}$$

Notons que $y_n \in A$ pour tout n, donc $y \in \bar{A}$. Donc $x \in f(\bar{A})$. Nous avons démontré que $\bar{A} \subset f(\bar{A})$.

□

9.4.2 Pour des limites uniques : séparabilité

PropUniciteLimitePourSuites

Proposition 9.90.
Dans un espace topologique séparé, si une suite converge, alors sa limite est unique.

Démonstration. Supposons que la suite (x_k) converge vers deux éléments distincts x et y. L'espace étant séparé, il existe deux ouverts $\mathcal{O}_x$ et $\mathcal{O}_y$, disjoints, contenant respectivement x et y. La suite convergeant à la fois vers x et y, il existe k_x et k_y, tels que, si $k \geqslant \max\{k_x, k_y\}$, l'élément x_k est (à la fois) dans $\mathcal{O}_x$ et $\mathcal{O}_y$. Cela est en contradiction avec le fait que ces deux ensembles sont disjoints. □

9.91.
Donc, on pourra parler, avec des espaces séparés, de « la limite d'une suite ». On notera $x_n \to a$, ou $\lim_{n\to\infty} x_n = a$, pour signifier que la suite (x_n) converge vers a.

LEMooMDTNooThlHJl

Lemme 9.92 ([1]).
Soit $a \neq 0$ dans un espace vectoriel topologique[34] *Hausdorff*[35]*. Il existe un voisinage V de 0 tel que $a \notin \bar{V}$.*

Démonstration. Étant donné que l'espace topologique est Hausdorff, nous pouvons considérer des voisinages V de 0 et W de a tels que $V \cap W = \varnothing$.

Dans ce cas nous avons $a \notin \bar{V}$ (voir la définition 9.19 de la fermeture de V). □

PROPooNRRIooCPesgO

Proposition 9.93 ([1]).
La convergence de suite pour la topologie de l'espace produit[36] *est équivalente à la convergence des suites « composante par composante ».*

Démonstration. En deux parties

(1) **Sens direct** Pour simplifier les notations, nous allons considérer le produit de deux espaces. Soit donc $(x_k, y_k) \xrightarrow{X\times Y} (x, y)$ et des ouverts $\mathcal{O}_1$ dans X autour de x et $\mathcal{O}_2$ autour de y dans Y.

La partie $\mathcal{O}_1 \times \mathcal{O}_2$ est ouverte dans $X \times Y$. Donc il existe K tel que $k \geqslant K$ implique $(x_k, y_k) \in \mathcal{O}_1 \times \mathcal{O}_2$.

Nous avons prouvé que pour tout ouvert $\mathcal{O}_1$ autour de x il existe K tel que $k \geqslant K$ implique $x_k \in \mathcal{O}_1$. Donc $x_k \xrightarrow{X} x$. Idem pour y.

(2) **Dans l'autre sens** Nous considérons l'espace produit[37] $X = \prod_{i=1}^{n} X_i$. Nous supposons pour chaque i, avoir une suite convergente $(x_i)_k \xrightarrow{X_i} x_i$.

[34] Définition 9.239.
[35] Définition 9.79
[36] Définition 9.66.
[37] Pour les notations, ça va être le sport : $(x_i)_k$ désigne une suite dans X_i, mais x_i désigne la limite de cette suite.

Nous allons prouver que

$$\big((x_1)_k,\dots,(x_n)_k\big) \xrightarrow{X} (x_1,\dots,x_n). \tag{9.91}$$

Soit un ouvert $\mathcal{O}$ de X autour de $(x_1,\dots,x_n)$. Nous considérons des ouverts U_i de X_i tels que $x_i\in U_i$ et $U_1\times\dots\times U_n\subset\mathcal{O}$.

Vu que $(x_i)_k \xrightarrow{X_i} x_i$, il existe $K_i\in\mathbb{N}$ tel que $k>K_i$ implique $(x_i)_k\in U_i$. Si $k\geqslant \max_i\{K_i\}$, alors $(x_i)_k\in U_i$ pour tout i et nous avons

$$\big((x_1)_k,\dots,(x_n)_k\big)\in U_1\times\dots\times U_n\subset\mathcal{O}. \tag{9.92}$$

□

LEMooSJKMooKSiEGq

Lemme 9.94 ([1]).
Soit un espace topologique X. Soient dans X une suite (x_n) et un élément x tels que toute sous-suite de (x_n) contient une sous-suite convergente vers x. Alors $x_n\to x$.

Démonstration. Supposons que (x_n) ne converge pas vers x. Il existe alors un ouvert $\mathcal{O}$ autour de x tel que pour tout $N>0$, il existe $n\geqslant N$ tel que x_n n'est pas dans $\mathcal{O}$.

Cela nous permet de construire une sous-suite de (x_n) composée d'éléments hors de $\mathcal{O}$. Aucune sous-suite de cette sous-suite ne peut converger vers x. □

9.4.3 Topologie induite

PROPooAHIMooYhOwUf

Proposition 9.95 ([1]).
Soient un espace topologique X et une partie $A\subset X$. Nous munissons A de la topologie induite depuis X.

ITEMooLXGWooYgPqoT

(1) Si X est Hausdorff[38], alors A est Hausdorff.

ITEMooOQZDooGztljW

(2) Si X est à base dénombrable de topologie[39], alors A est à base dénombrable.

Démonstration. En deux parties.

(1) **Pour (1)** Soient $a,b\in A$. Vu que X est Hausdorff, il existe des voisinages ouverts $\mathcal{O}_1$ de a et $\mathcal{O}_2$ de b tels que $\mathcal{O}_1\cap\mathcal{O}_2=\varnothing$. Les paries $A\cap\mathcal{O}_1$ et $A\cap\mathcal{O}_2$ sont des ouverts disjoints de A.

(2) **Pour (2)** Soit une base $\{B_i\}_{i\in I}$ de la topologie de X. Nous supposons que I est dénombrable. Nous démontrons que $\{B_i\cap A\}_{i\in I}$ et une base de la topologie de A.

En effet soit $a\in A$ et un ouvert S de A tel que $a\in S$. Il existe un ouvert $\mathcal{O}$ de X tel que $S=\mathcal{O}\cap A$. Vu que $\{B_i\}_{i\in I}$ est une base de la topologie de X, il existe $i\in I$ tel que $a\in B_i\subset\mathcal{O}$.

Vu que $\mathcal{O}\subset B_i$, nous avons

$$a\in S=A\cap\mathcal{O}\subset B_i\cap\mathcal{O}. \tag{9.93}$$

□

9.4.4 Fonctions équivalentes

DEFooWDSAooKXZsZY

Proposition-Définition 9.96 ([240]).
Soit un espace topologique X et $D\subset X$. Soient encore des fonctions $f,g\colon D\to\mathbb{C}$ et un point $a\in \mathrm{Adh}(D)$[40].

Nous définissons sur $\mathrm{Fun}(D,\mathbb{C})$ la relation $f\sim g$ lorsque qu'il existe un voisinage V de a dans X et une fonction $\alpha\colon V\to\mathbb{R}$ telles que

(1) $\lim_{x\to a}\alpha(x)=0$,

(2) pour tout $x\in(V\cap D)\setminus\{a\}$,

$$f(x)=\big(1+\alpha(x)\big)g(x). \tag{9.94}$$

EQooQXKYooSDPpNq

Cette relation est une relation d'équivalence.

*Lorsque $f\sim g$, nous disons que f et g sont **équivalentes** en a.*

Démonstration. Nous devons prouver les trois conditions de la définition 1.55 de relation d'équivalence.

[38] Définition 9.79.
[39] Base de topologie, proposition 9.2.
[40] Adhérence ou fermeture, c'est la même chose. Voir la définition 9.19 et le lemme 9.20.

(1) **Réflexive** Il suffit de poser $\alpha(x) = 0$.

(2) **Symétrique** Si $f \sim g$, il existe une fonction α vérifiant ce qu'il faut telle que

$$f(x) = \big(1 + \alpha(x)\big)g(x). \tag{9.95}$$

Comme $\lim_{x\to a} \alpha(x) = 0$, il y a un voisinage de a sur lequel $|\alpha(x)| < 1$; il n'y a donc pas de problème de dénominateur en écrivant

$$g(x) = \frac{1}{1 + \alpha(x)} f(x). \tag{9.96}$$

Nous posons alors $\beta(x) = -\alpha(x)/\big(1 + \alpha(x)\big)$. Cela vérifie

$$g(x) = \big(1 + \beta(x)\big)f(x). \tag{9.97}$$

Et

$$\lim_{x\to a} \beta(x) = 0 \tag{9.98}$$

parce que $\lim_{x\to a} \big(1 + \alpha(x)\big) = 1$ et $\lim_{x\to a} -\alpha(x) = 0$.

(3) **Transitive** Soit $f \sim g$ et $g \sim h$. Sur un voisinage V de a nous avons

$$f(x) = \big(1 + \alpha(x)\big)g(x), \tag{9.99}$$

sur un voisinage W de a nous avons

$$g(x) = \big(1 + \beta(x)\big)h(x). \tag{9.100}$$

Sur le voisinage $V \cap W$ nous avons

$$f(x) = \big(1 + \beta(x) + \alpha(x) + (\alpha\beta)(x)\big)h(x). \tag{9.101}$$

Donc la fonction $\gamma(x) = \beta(x) + \alpha(x) + (\alpha\beta)(x)$ fait l'affaire.

□

Notons que la notion d'équivalence de fonctions, de même que la notion de limite, ne dépend pas des valeurs exactes atteintes par les fonctions au point.

Lemme 9.97.
Si f et g sont équivalentes en a, et si g ne s'annule pas sur un voisinage de a, alors pour tout $\epsilon > 0$, il existe r tel que

$$\frac{f(x)}{g(x)} \in B(1, \epsilon) \tag{9.102}$$

pour tout $x \in B(a, r)$.

Démonstration. Nous considérons un voisinage V de a sur lequel en même temps :

- la fonction α de la définition d'équivalence est définie,
- $|\alpha(x)| < \epsilon$ pour tout $x \in V$,
- $g(x) \neq 0$, pour tout $x \in V$.

Ensuite nous considérons $r > 0$ tel que $B(a, r) \subset V$. En divisant la condition (9.94) par $g(x)$ nous trouvons

$$\frac{f(x)}{g(x)} = 1 + \alpha(x). \tag{9.103}$$

Donc

$$\Big|\frac{f(x)}{g(x)} - 1\Big| = |\alpha(x)| \leqslant \epsilon, \tag{9.104}$$

ce qu'il fallait prouver. □

9.5 Espace topologique normal et complètement normal

DEFooNNKVooLtzImT

Définition 9.98 (Espace normal).
*Un **espace topologique normal** est un espace topologique séparé dont les ouverts séparent strictement les fermés disjoints.*

Autrement dit, si F_1 et F_2 sont des fermés disjoints de X, alors il existe des ouverts disjoints $\mathcal{O}_1$ et $\mathcal{O}_2$ tels que $F_1 \subset \mathcal{O}_1$ et $F_2 \subset \mathcal{O}_2$.

PROPooWSKZooHKvuob

Proposition 9.99.
L'espace topologique $\mathbb{R}^n$ est normal.

PROPooBYJGooWkbcRo

¡¡ Avertissement/question au lecteur !! 9.100
J'ai écrit le lemme 9.101 de façon adhoc pour une utilisation dans le théorème d'Urysohn. J'avoue n'être pas certain qu'il soit vrai. Si vous en trouvez une preuve, écrivez-moi.

LEMooVVASooEXYKOZ

Lemme 9.101 ([1, 226]).
Soit un espace topologique normal X. Si $\mathcal{O}$ est ouvert dans X et si F est un fermé contenu dans $\mathcal{O}$, alors il existe un ouvert U tel que

$$F \subset U \subset \bar{U} \subset \mathcal{O}. \tag{9.105}$$

DEFooTLVHooYWvDIu

Définition 9.102 ([241]).
*Un espace topologique X est **complètement normal** si pour toutes parties $A, B \subset X$ telles que $A \cap \bar{B} = B \cap \bar{A} = \varnothing$, il existe deux ouverts U, V tels que*

(1) $A \subset U$

(2) $B \subset V$

(3) $U \cap V = \varnothing$.

Si A et B sont des parties d'un espace topologique, nous notons

$$A \mid B \tag{9.106}$$

pour dire que les ouverts séparent A et B, c'est-à-dire si il existe des ouverts U et V tels que $A \subset U$, $B \subset V$ et $U \cap V = \varnothing$.

LEMooWORZooAFZSDS

Lemme 9.103 ([226]).
Soient deux parties A et B dans l'espace topologique X. Nous avons $A \mid B$ si et seulement si il existe un voisinage V de B tel que $\bar{V} \cap A = \varnothing$.

Démonstration. En deux parties.

(1) $\Rightarrow$ Si $A \mid B$, nous considérons $U, V \in \tau_X$ séparant A et B. Notons que $V \subset X \setminus U$. Étant donné que $X \setminus U$ est fermé, nous avons aussi $\bar{V} \subset X \setminus U$. Donc $\bar{V} \cap U = \varnothing$ et à fortiori, $\bar{V} \cap A = \varnothing$.

(2) $\Leftarrow$ Soit $V \in \tau_X$ tel que $B \subset V$ et $\bar{V} \cap A = \varnothing$. En posant $U = X \setminus \bar{V}$, nous avons que U est ouvert et que $U \cap V = \varnothing$ et que $A \subset U$.

□

LEMooTEZYooOvzGcl

Lemme 9.104 ([242, 1]).
Soit un recouvrement ouvert $\{U_i\}_{i \in I}$ de l'espace topologique (X, τ_X). Sur chacun de U_i nous considérons la topologie induite[41] τ_i. Soit une partie $A \subset X$.

ITEMooSVJRooTCEyog

(1) A est ouvert dans X si et seulement si $A \cap U_i$ est ouvert de U_i.

ITEMooDXAIooSWqaPp

(2) A est fermé dans X si et seulement si $A \cap U_i$ est fermé de U_i.

Démonstration. En Plusieurs parties.

(1) **Pour (1), $\Rightarrow$** Si $A \in \tau_X$, alors $A \cap U_i \in \tau_i$ par définition de la topologie induite.

[41] Définition 9.30.

(2) **Pour (1), $\Leftarrow$** SPITEMooMLEFooQrWsbE Nous supposons que $A \cap U_i \in \tau_i$ pour tout i. Soit $a \in A$. Vu que $\{U_i\}_{i\in I}$ recouvre X, nous avons un i tel que $a \in U_i$. Donc $a \in U_i \cap A$. Étant donné que $U_i \cap A \in \tau_i$, il existe $S_i \in \tau_X$ tel que $A \cap U_i = S_i \cap U_i$. Nous avons

$$a \in A \cap U_i = S_i \cap U_i. \tag{9.107}$$

En tant qu'intersection d'ouverts, $S_i \cap U_i$ est ouvert. Soit un ouvert $V \in \tau_X$ contenant a et contenu dans $S_i \cap U_i$. Nous avons

$$a \in V \subset S_i \cap U_i = A \cap U_i, \tag{9.108}$$

et en particulier $V \subset A$. Donc A contient un voisinage de chacun de ses éléments. Donc A est ouvert.

(3) **Pour (2), $\Rightarrow$** Nous avons les égalités

$$U_i \setminus (A \cap U_i) = U_i \setminus A = U_i \cap A^c. \tag{9.109}$$ EQooNCIAooDBMSYy

Supposons que A est fermé. Alors A^c est ouvert et donc $U_i \cap A^c \in \tau_i$ pour tout i. Donc $U_i \cap A^c$ est ouvert de U_i, donc

$$U_i \setminus (A \cap U_i) \tag{9.110}$$

est ouvert de U_i Donc $A \cap U_i$ est fermé de U_i (complémentaire d'un ouvert).

(4) **Pour (2), $\Leftarrow$** Nous supposons que $A \cap U_i$ est fermé de U_i pour tout $i \in I$. Donc le complémentaire (dans U_i) est ouvert de U_i :

$$U_i \setminus (A \cap U_i) \in \tau_i. \tag{9.111}$$

Encore par (9.109) nous avons $U_i \cap A^c \in \tau_i$. Par le point (2), A^c est ouvert de X, ce qui signifie que A est fermé de X.

□

DEFooERRQooNOpCXD

Définition 9.105 (Famille localement finie)**.**
*Soit un espace topologique X. Une famille $\{U_i\}_{i\in I}$ est **localement finie** si pour tout $x \in X$, il existe un voisinage V de x tel que*

$$\{i \in I \text{ tel que } U_i \cap V \neq \varnothing\} \tag{9.112}$$

est fini.

PROPooKDMWooVyOkUE

Proposition 9.106 ([242])**.**
Soient un espace topologique X et une famille localement finie de fermés $\{F_i\}_{i\in I}$. Alors

$$F = \bigcup_{i\in I} F_i \tag{9.113}$$

est fermé.

Démonstration. Vu que $\{F_i\}_{i\in I}$ est localement finie, pour chaque $x \in X$ nous pouvons considérer un ouvert U_x tel que

$$I_x = \{i \in I \text{ tel que } F_i \cap U_x \neq \varnothing\} \tag{9.114}$$

est fini. Nous avons

$$F \cap U_x = \bigcup_{i\in I_x} (F_i \cap U_x). \tag{9.115}$$

La partie $F_i \cap U_x$ est fermée dans U_x (topologie induite, voir le lemme 9.31). En tant qu'union finie de fermés, $F \cap U_x$ est un fermé de U_x (pour tout x). Nous en déduisons que F est fermé dans X par le lemme 9.104. □

PROPooRDVDooFYHgPV

Proposition 9.107 ([226])**.**
Si $\{A_i\}_{i\in I}$ est localement fini, alors

$$\overline{\bigcup_{i\in I} A_i} = \bigcup_{i\in I} \bar{A}_i. \tag{9.116}$$

Démonstration. En deux parties.

(1) $\overline{\bigcup_{i\in I} A_i} \subset \bigcup_{i\in I} \bar{A}_i$ Nous savons par le lemme 9.20(1) que $\overline{\bigcup_{i\in I} A_i}$ est un fermé contenu dans n'importe quel fermé contenant $\bigcup_{i\in I} A_i$. Étant donné que chacun des $\bar{A}_i$ est fermé, la proposition 9.106 nous dit que $\bigcup_{i\in I} \bar{A}_i$ est un fermé qui contient $\bigcup_{i\in I} A_i$.

(2) $\bigcup_{i\in I}\bar{A}_i \subset \overline{\bigcup_{i\in I} A_i}$ C'est la proposition 9.25 qui est valable même si $\{A_i\}_{i\in i}$ n'est pas localement finie.

□

DefParacompact

Définition 9.108.
*Un espace topologique est **paracompact** si tout recouvrement ouvert admet un sous-recouvrement localement fini*[42].

PROPooLFPXooUBytkm

Proposition 9.109.
Tout ouvert de $\mathbb{R}^n$ est paracompact.

PROPooJOYRooSIIDtK

Proposition 9.110 ([226]).
Tout espace séparé paracompact[43] *est normal*[44].

Démonstration. Soit un espace topologique séparé paracompact X. Soient deux fermés disjoints A et B. Nous faisons deux parties.

(1) **Si $A \mid \{b\}$ pour tout $b \in B$** Nous commençons par supposer que le ouverts séparent A et $\{b\}$ pour tout b dans B. Le lemme 9.103 nous permet, pour chaque $b \in B$ de choisir un voisinage ouvert V_b tel que $\bar{V}_b \cap A = \varnothing$.

En posant $L = B \cup \{o\}$ et $V_o = X \setminus B$, les ensembles $\{V_l\}_{l\in L}$ forment un recouvrement de X par des ouverts. Par paracompacité de X nous pouvons en extraire un sous recouvrement localement fini

$$\{W_i\}_{i\in I}. \tag{9.117}$$

Nous posons $J = \{i \in I \text{ tel que } W_i \cap B \neq \varnothing\}$ et nous définissons

$$V = \bigcup_{j\in J} W_j. \tag{9.118}$$

C'est un ouvert et $B \subset V$ parce que $\{W_i\}_{i\in I}$ recouvre tout X et qu'avec J on a sélectionné les parties qui recouvrent B. Pour tout $j \in J$ nous avons $\bar{W}_j \cap A = \varnothing$ parce que chaque W_j est un des V_b. Notez que $V_o = X \setminus B$ fait partie de ceux qui ne sont pas sélectionnés par J.

La proposition 9.107 nous dit que $\bar{V} = \bigcup_{j\in J} \bar{W}_j$ et donc que $\bar{V} \cap A = \varnothing$.

(2) **Cas général** Soient A et B fermés dans X. Nous fixons un $b \in X \setminus A$. La partie $X \setminus A$ est ouverte. Pour chaque $a \in A$, les ouverts séparent a et b de telle sorte à avoir un ouvert U_a autour de a et un ouvert V_a autour de b tels que $U_a \cap V_a = \varnothing$.

Les parties $\{U_a\}_{a\in A}$ et $X \setminus A$ forment un recouvrement de X par des ouverts. Nous pouvons en extraire un sous-recouvrement localement fini. Soit donc A' fini dans A tel que $\{U_a\}_{a\in A'}$ recouvre A de façon localement finie. Nous posons

$$U = \bigcup_{a\in A'} U_a. \tag{9.119}$$

Soit un voisinage W_0 de b tel que

$$A'' = \{a \in A' \text{ tel que } U_a \cap W_0 \neq \varnothing\} \tag{9.120}$$

soit fini. Nous posons

$$V = \bigcap_{a\in A''} (V_a \cap W_0). \tag{9.121}$$

Par construction, $b \in W_0$ et $b \in V_a$ pour tout a. Donc $b \in V$. De plus V est ouvert en tant qu'intersection finie d'ouverts.

Montrons que $U \cap V = \varnothing$. Pour cela nous considérons $x \in U \cap V$. Vu que $x \in W_0$, il existe $a \in A''$ tel que $x \in U_a$. Mais $x \in V_a$ pour tout $a \in A''$, donc $x \in U_a \cap V_a$, ce qui n'est pas possible.

□

[42] Définition 9.105.
[43] Définition 9.108.
[44] Définition 9.98.

9.6 Connexité

L'idée de la connexité, c'est de s'assurer qu'un ensemble est « d'un seul tenant ».

PROPooNLXDooVTZLan

Proposition-Définition 9.111 (Espace topologique connexe[243]).
Soit un espace topologique X. Les propositions suivantes sont équivalentes :

(1) X n'est pas la réunion de deux ouverts non vides disjoints.

(2) X n'est pas la réunion de deux fermés non vides disjoints.

(3) Les seuls ouverts-fermés de X sont X et $\varnothing$.

(4) Toute application continue $X \to \{1,2\}$ (munie de la topologie discrète) est constante.

*Quand un espace topologique vérifie ces conditions, nous disons que X est **connexe**.*

DEFooQGESooKSVtmt

Définition 9.112 (Partie connexe[243]).
*Une partie d'un espace topologique est **connexe** si elle est connexe pour la topologie induite.*

DEFooJYCDooGNEDoC

Définition 9.113 (Partie o-connexe[1]).
*Une partie Q d'un espace topologique X est **o-connexe** si pour tout ouverts A, B tels que*

(1) $Q \subset A \cup B$

(2) $A \cap Q \neq \varnothing$ et $B \cap Q \neq \varnothing$,

nous avons $A \cap B \neq \varnothing$.

PROPooQHJXooMNrxOJ

Proposition 9.114 ([1]).
Tout connexe est o-connexe.

Démonstration. Soient un espace topologique (X, τ_X) ainsi qu'une partie $Q \subset X$ munie de la topologie induite τ_Q. Nous supposons que Q n'est pas o-connexe, et nous montrons que Q n'est pas connexe.

Si Q n'est pas o-connexe, il existe $A, B \in \tau_X$ tels que $Q \subset A \cup B$, $A \cap B = \varnothing$, $A \cap Q \neq \varnothing \neq B \cap Q$.

Les parties $A \cap Q$ et $B \cap Q$ sont des ouverts de (Q, τ_Q). Elles sont disjointes, non vides et recouvrent Q. Donc Q n'est pas connexe. □

PROPooAHWNooXhrqnd

Proposition 9.115 ([244]).
Dans un espace complètement normal[45], tout o-connexe est connexe.

Démonstration. Soient un espace topologique complètement normal X, et une partie $Q \in X$.

(1) **Contraposée** Par contraposée nous supposons que Q n'est pas connexe : il existe $G_0, G_1 \in \tau_Q$ tels que

(1a) $Q = G_0 \cup G_1$
(1b) $G_0 \neq \varnothing \neq G_1$
(1c) $G_0 \cap G_1 \neq \varnothing$

Par définition de la topologie induite τ_Q, il existe des ouverts $U_0, U_1 \in \tau_X$ tels que $G_0 = U_0 \cap Q$ et $G_1 = U_1 \cap Q$.

(2) $U_0 \cap G_1 = \varnothing$ Nous avons

$$U_0 \cap G_1 = U_0 \cap U_1 \cap Q \subset U_0 \cap Q = G_0. \tag{9.122}$$

Donc un élément de $U_0 \cap G_1$ serait dans $G_0 \cap G_1$, ce qui n'est pas possible.

(3) **Fermeture** Vu que U_0 est ouvert dans X et que $U_0 \cap G_1 = \varnothing$, le lemme 9.39 dit que $U_0 \cap \mathrm{Adh}_X(G_1) = \varnothing$. Et comme $G_0 \subset U_0$,

$$G_0 \cap \mathrm{Adh}_X(G_1) = \varnothing. \tag{9.123}$$

De même

$$G_1 \cap \mathrm{Adh}_X(G_0) = \varnothing. \tag{9.124}$$

(4) **Complètement normal** Vu que X est complètement normal, il existe des ouverts disjoints $V_0, V_1 \in \tau_X$ tels que $G_0 \subset V_0$ et $G_1 \subset V_1$.

[45] Définition 9.102.

(5) **Conclusion** Nous concluons que Q n'est pas o-connexe parce que $\{V_0, V_1\}$ est un recouvrement disjoint de Q par des ouverts de X.

□

¡¡ Avertissement/question au lecteur !! 9.116
Il y a peut-être une réciproque. J'ai entendu à quelques endroits sur internet que si tous les o-connexes sont connexes, alors l'espace est complètement normal. Voici une tentative de démonstration, pas complète. Si vous pouvez donner une démonstration complète ou un contre-exemple (un espace non complètement normal dans lequel tous les o-connexes sont connexes), écrivez-moi.

THOooMULNooNYeHAj

pseudo-théorème 9.117 ([244, 245]).
Un espace topologique dans lequel tous les o-connexes sont connexes est complètement normal.

Démonstration. Soient des parties $A, B \subset X$ telles que $A \cap \bar{B} = B \cap \bar{A} = \varnothing$. Nous notons $Q = A \cup B$.

(1) **B est ouvert dans $Q = A \cup B$** Nous savons que $X \setminus \bar{B}$ est ouvert dans X. Vu que $B \cap \bar{A} = \varnothing$ nous avons $B \subset Q \cap (X \setminus \bar{A})$, et donc $B \subset X \setminus \bar{A}$ et donc $B = Q \cap (X \setminus \bar{A})$. La partie B est donc bien l'intersection entre Q et un ouvert de X. Donc B est ouvert dans Q.

Donc $A \cup B$ est l'union de deux ouverts disjoints (pour sa topologie induite), et n'est donc pas connexe.

(2) **Utilisation de l'hypothèse** Vu que Q n'est pas connexe, il n'est pas non plus o-connexe. Il existe des ouverts U et V tels que

(2a) $Q \subset U \cup V$
(2b) $U \cap Q \neq \varnothing \neq V \cap Q$
(2c) $U \cap V = \varnothing$.

Ce serait bien que $A \subset U$ et que $B \subset V$. Mais rien n'est moins sûr. Nous considérons donc quelques cas possibles.

(3) **Si A est connexe** Dans ce cas, $\{U, V\}$ est un recouvrement de A par des ouverts disjoints. Donc $A \subset U$ et $A \cap V = \varnothing$ (ou le contraire).

(4) **Si A a un nombre fini de composantes connexes** Soient $\{C_i\}_{1=1,\dots,n}$ les composantes connexes[46] de A. Pour chaque i nous avons $C_1 \cap \bar{B} = B \cap \bar{C}_i = \varnothing$ et donc (en reprenant toute la démonstration jusqu'ici avec C_i au lieu de A), nous avons des ouverts U_i et V_i tels que $C_i \subset U_i$, $B \subset V_i$ et $U_i \cap V_i = \varnothing$. Nous posons alors $U = \bigcup_{i=1}^{n} C_i$ et $V = \bigcap_{i=1}^{n} V_i$.

(4a) $V \cap U = \varnothing$ En effet si $x \in V \cap U$ nous avons $V \in C_i$ pour un certain i. Pour ce même i nous avons $x \in V_i$ (c'est pour ça qu'on a dit que V serait l'intersection). Or $V_i \cap U_i = \varnothing$; un tel x ne peut pas exister.

(4b) $V \neq \varnothing$ Parce que chacun des V_i contient B.

(4c) V **est ouvert** Parce que c'est une intersection finie d'ouverts[47].

(5) **Le problème** Si A et B ont tous les deux un nombre infini de composantes connexes, on ne peut pas déduire que U et V sont ouverts. Donc le démonstration coince dans ce cas.

Bref. Preuve pas terminée. Écrivez-moi si vous êtes capable de terminer.

□

DefIRKNooJJlmiD

Définition 9.118.
*Lorsque X est un espace topologique, nous disons qu'un sous-ensemble A est **non connexe** quand on peut trouver des ouverts O_1 et O_2 disjoints tels que*

$$A = (A \cap O_1) \cup (A \cap O_2), \tag{9.125}$$

EqDefnnCon

*et tels que $A \cap O_1 \neq \varnothing$, et $A \cap O_2 \neq \varnothing$. Si un sous-ensemble n'est pas noo-connexe, alors on dit qu'il est **connexe**.*

Une autre façon d'exprimer la condition (9.125) est de dire que A n'est pas connexe quand il est contenu dans la réunion de deux ouverts disjoints qui intersectent tous les deux A.

[46] Définition 9.120.
[47] C'est la propriété 9.1(3).

PROPooBCFXooRlMvch

Proposition 9.119 ([246]).
Soit un espace topologique X. Soient $(C_i)_{i\in I}$ des connexes de X tels que $\bigcap_{i\in I} C_i \neq \varnothing$. Alors $\bigcup_{i\in I} C_i$ est connexe.

Démonstration. Nous notons $C = \bigcup_{i\in I} C_i$. Soient des ouverts disjoints $A, B \in \tau_C$ recouvrant C. Nous devons démontrer que soit $A\cap C$ soit $B\cap C$ est vide. Par définition de la topologie induite τ_C, il existe des ouverts $A', B' \in \tau_X$ tels que $A = C\cap A'$ et $B = C\cap B'$.

Nous notons $A_i = C_i \cap A$ et $B_i = C_i \cap B$. Les parties A_i et B_i recouvrent C_i et nous avons $A_i \cup B_i = C_i$. De plus

$$A_i = C_i \cap^C \cap A' = C_i \cap A', \tag{9.126}$$

donc A_i est ouvert dans C_i. Vu que C_i est ouvert, soit A_i soit B_i est vide.

Par hypothèse, $\bigcap_{i\in I} C_i$ est non vide. Soit x un élément de cette intersection. Soit $x \in A$ et alors $x \in A_i$ pour tout i ; soit $x \in B$ et alors $x \in B_i$ pour tout i.

Dans le premier cas, $x \in A_i$ pour tout i, de telle sorte que $B_i = \varnothing$ pour tout i. Nous avons alors

$$\varnothing = \bigcup_{i\in I} B_i = \bigcup_{i\in I} (C_i \cap B) = B \cap C. \tag{9.127}$$

Dans le second cas nous obtenons de même que $A\cap C = \varnothing$. □

DEFooFHXNooJGUPPn

Proposition-Définition 9.120 ([247]).
Soient un espace topologique X et un point $x \in X$.

ITEMooBZAQooNwuzaS

(1) La réunion de toutes les parties connexes de X contenant x est connexe.

(2) Cette réunion est la plus grande (au sens de la relation d'inclusion) de toutes les parties connexes de X contenant x.

*La réunion de toutes les parties connexes de X contenant x est nommée **composante connexe** de x dans X.*

Démonstration. La réunion de toutes les parties connexes contenant x est connexe par la proposition 9.119.

Nous notons C la réunion de toutes les parties connexes contenant x. Si D est un connexe contenant x, alors $D \subset C$ parce que C est une union de tous les connexes, y compris D. □

PropHSjJcIr

Proposition 9.121 ([1]).
Soit X un espace topologique. Les conditions suivantes sont équivalentes.

ITEMooXHIKooGqrgTs

(1) L'espace X est connexe.

ITEMooRTNPooADKVnw

(2) Si $X = O_1 \cup O_2$ avec O_1 et O_2 des ouverts disjoints, alors soit $O_1 = \varnothing$ soit $O_2 = \varnothing$.

ITEMooOEZYooFBNaOZ

(3) Si $X = F_1 \cup F_2$ avec F_1 et F_2 fermés disjoints dans X, alors $F_1 = \varnothing$ ou $F_2 = \varnothing$.

ITEMooNIPZooIDPmEf

(4) Si $A \subset X$ avec A ouvert et fermé en même temps, alors $A = \varnothing$ ou $A = X$.

Démonstration. En quatre parties.

(1) **(1) implique (2)** Par rapport à la définition 9.118, nous prenons la partie X de l'espace X. Supposons que O_1 et O_2 sont tout deux non vides. Dans ce cas nous avons

$$X = O_1 \cup O_2 = (O_1 \cap X) \cup (O_2 \cap X), \tag{9.128}$$

ce qui prouverait que X est non connexe. Contradiction. Un des O_i est vide.

(2) **(2) implique (3)** Soit une union disjointe de fermés $X = F_1 \cup F_2$. Puisque l'union est disjointe, nous avons $F_1 = X \setminus F_2$ et $F_2 = X \setminus F_1$, ce qui fait que F_1 et F_2 sont également ouverts. Nous en déduisons que $X = F_1 \cup F_2$ est une union disjointe d'ouverts. L'hypothèse indique que $F_1 = \varnothing$ ou $F_2 = \varnothing$.

(3) **(3) implique (4)** Soit A une partie ouverte et fermée de X. Nous supposons que A est ouvert et fermé, donc $X \setminus A$ est également ouvert et fermé : c'est la définition 9.3 d'un fermé. Nous avons évidemment l'union $X = A \cup (X \setminus A)$ qui est une union disjointe de fermés. Par hypothèse nous avons soit $A = \varnothing$ soit $X \setminus A = \varnothing$.

(4) **(4) implique (1)** Supposons que X ne soit pas connexe. Il existe donc des ouverts disjoints O_1 et O_2 tels que $X = O_1 \cup O_2$. Étant donné que $O_1 = X \setminus O_2$, la partie O_1 est fermée comme complémentaire d'ouvert. Donc O_1 est fermé et ouvert (et O_2 aussi d'ailleurs). Par hypothèse nous concluons que O_1 est soit X soit $\varnothing$.

□

Nous verrons plus tard (proposition 9.294) une autre caractérisation de la connexité basée sur la continuité des fonctions $X \to \mathbb{Z}$.

PROPooSCKNooRbewdv

Proposition 9.122 ([1]).
Soient un espace topologique X ainsi que $S \subset X$. Si $U \subset X$ est connexe[48] *et si $U \subset S \subset \bar{U}$, alors S est connexe.*

Démonstration. Supposons que S ne soit pas connexe. Il existe des ouverts disjoints A et B tels que $S \subset A \cup B$ et $S \cap A \neq \varnothing$, $S \cap B \neq \varnothing$. Nous prouvons que ces ouverts fonctionnent aussi pour prouver que U est non connexe (donc on aura une contradiction).

D'abord A et B recouvrent U parce que $U \subset S \subset A \cup B$. Ensuite prouvons que $U \cap A \neq \varnothing$. Soit $x \in S \cap A$. Vu que $x \in S \subset \bar{U}$, tout voisinage de x intersecte U (c'est la définition 9.19 de l'adhérence). De plus $x \in A$ et A est ouvert. Soit donc un voisinage V de x contenu dans A. Nous avons $V \subset A$ et $V \cap U \neq \varnothing$. Donc $A \cap U \neq \varnothing$.

Le même raisonnement tient pour B. □

PropIWIDzzH

Proposition 9.123.
Stabilité de la connexité par union.

ITEMooLVSSooTGstBz

(1) Une union quelconque de connexes ayant une intersection non vide est connexe.

(2) Pour tout $n \in \mathbb{N}, n > 0$, si $A_1, \dots, A_n$ sont des connexes de X avec $A_i \cap A_{i+1} \neq \varnothing$, alors l'union $\bigcup_{i=1}^{n} A_i$ est connexe.

Démonstration. Point par point.

(1) Soient $\{C_i\}_{i \in I}$ un ensemble de connexes et un point p dans l'intersection : $p \in \bigcap_{i \in I} C_i$. Supposons que l'union ne soit pas connexe. Alors nous considérons A et B, deux ouverts disjoints recouvrant tous les C_i et ayant chacun une intersection non vide avec l'union.

Supposons pour fixer les idées que $p \in A$ et prenons $x \in B \cap \bigcup_{i \in I} C_i$. Il existe un $j \in I$ tel que $x \in C_j$. Avec tout cela nous avons

(1a) $C_j \subset A \cup B$ parce que $A \cup B$ recouvre tous les C_i,

(1b) $C_j \cap A \neq \varnothing$ parce que p est dans l'intersection,

(1c) $C_j \cap B \neq \varnothing$ parce que x est dans cette intersection.

Cela contredit le fait que C_j soit connexe.

(2) Pour la seconde partie nous procédons de proche en proche[49]. D'abord $A_1 \cup A_2$ est connexe par la première partie, ensuite $(A_1 \cup A_2) \cup A_3$ est connexe parce que les connexes $A_1 \cup A_2$ et A_3 ont un point d'intersection par hypothèse, et ainsi de suite.

□

9.7 Compacité

La compacité est le thème 33.

[48] Définition 9.118.
[49] Parce qu'on a la flemme de rédiger correctement une récurrence.

9.7.1 Définition et notions connexes

Soit E, un sous-ensemble de $\mathbb{R}$. Nous pouvons considérer les ouverts suivants :

$$\mathcal{O}_x = B(x, 1) \tag{9.129}$$

pour chaque $x \in E$. Évidemment,

$$E \subseteq \bigcup_{x \in E} \mathcal{O}_x. \tag{9.130}$$

Cette union contient en général de nombreuses redondances. Si par exemple $E = [-10, 10]$, l'élément $3 \in E$ est contenu dans $\mathcal{O}_{3.5}$, $\mathcal{O}_{2.7}$ et bien d'autres. Pire : même si on enlève par exemple $\mathcal{O}_2$ de la liste des ouverts, l'union de ce qui reste continue à être tout E. La question est : *est-ce qu'on peut en enlever suffisamment pour qu'il n'en reste qu'un nombre fini ?*

Définition 9.124.
Soit E, un sous-ensemble de $\mathbb{R}$. Une collection d'ouverts $\mathcal{O}_i$ est un ***recouvrement*** *de E si $E \subseteq \bigcup_i \mathcal{O}_i$.*

DefJJVsEqs

Définition 9.125.
Une partie A d'un espace topologique est ***compacte*** *si elle vérifie la propriété de Borel-Lebesgue : pour tout recouvrement de A par des ouverts (c'est-à-dire une collection d'ouverts dont la réunion contient A) on peut extraire un recouvrement fini.*

Remarque 9.126.
Certaines sources (dont Wikipédia) disent que pour être compact il faut aussi être séparé[50]. Pour ces sources, un espace qui ne vérifie que la propriété de Borel-Lebesgue est alors dit **quasi-compact**.

9.127.
La définition 9.125 en cache deux. En effet, si la partie A est l'espace topologique lui-même, cela définit un espace topologique compact. Un espace topologique est compact *en soi* lorsque de tout recouvrement par des ouverts, nous pouvons extraire un sous-recouvrement fini. Dans ce cas, si X est l'espace et si $\{A_i\}_{i \in I}$ est le recouvrement, nous avons $X = \bigcup_{i \in I} A_i$ et non une simple inclusion $X \subset \bigcup_{i \in I} A_i$.

LEMooVYTRooKTIYdn

Lemme 9.128.
Si K est une partie compacte de l'espace topologique X, alors K est un espace topologique compact pour la topologie induite[51] *de X.*

Démonstration. Nous notons τ la topologie de X et τ_K la topologie induite de X vers K, c'est-à-dire

$$\tau_K = \{\mathcal{O} \cap K \text{ tel que } \mathcal{O} \in \tau\}. \tag{9.131}$$

Soient des ouverts $A_i \in \tau_K$ ($i \in I$ où I est un ensemble quelconque) tels que $\bigcup_i A_i = K$. Pour chaque $i \in I$, il existe un $\mathcal{O}_i \in \tau$ tel que $A_i = K \cap \mathcal{O}_i$. Nous avons

$$K = \bigcup_{i \in I} (K \cap \mathcal{O}_i) \subset \bigcup_{i \in I} \mathcal{O}_i. \tag{9.132}$$

Donc les $\mathcal{O}_i$ forment un recouvrement de K par des ouverts de X. Puisque K est une partie compacte de X, il existe un sous-ensemble fini J de I tel que

$$K \subset \bigcup_{j \in J} \mathcal{O}_j. \tag{9.133}$$

Nous avons donc aussi

$$K \subset \bigcup_{j \in J} K \cap \mathcal{O}_j = \bigcup_{j \in J} A_j. \tag{9.134}$$

Nous avons prouvé que $\{A_j\}_{j \in J}$ est un recouvrement fini de K par des ouverts de K. Donc K est un espace topologique compact. □

PROPooOXKSooEDzCRZ

Proposition 9.129 ([248]).
Soit K compact dans $\mathbb{C}$. Si $\mathcal{O}$ est une composante connexe[52] *de $\mathbb{C} \setminus K$, alors $\partial\mathcal{O} \subset K$.*

[50] Définition 9.79.
[51] Définition 9.30.
[52] Définition 9.120.

Démonstration. Supposons que $\partial\mathcal{O}$ n'est pas inclus dans K, et considérons $w \in \partial\mathcal{O} \setminus K$. Nous posons $A = \mathcal{O} \cup \{w\}$. Vu que $w \in \partial\mathcal{O}$, nous avons $w \in \bar{\mathcal{O}}$. Donc

$$\mathcal{O} \subset A \subset \bar{\mathcal{O}}. \tag{9.135}$$

La proposition 9.122 fait que A est connexe parce que $\mathcal{O}$ est connexe. Donc A est un connexe de $\mathbb{C} \setminus K$ contenant strictement $\mathcal{O}$. Impossible parce que $\mathcal{O}$ est une composante connexe de $\mathbb{C} \setminus K$. Contradiction.

Nous en déduisons que $\partial\mathcal{O} \subset K$. □

9.7.2 Autres compacité

DEFooTVDOooZbwOFK

Définition 9.130 (Séquentiellement compact)**.**
Nous disons qu'un espace topologique est ***séquentiellement compact*** *si toute suite admet une sous-suite convergente.*

DEFooSOLWooWlSiUn

Définition 9.131 ([249])**.**
Un espace topologique est ***σ-compact*** *si il est union dénombrable de sous-espaces compacts.*

On dit aussi ***dénombrable à l'infini****.*

Définition 9.132.
Une famille $\mathcal{A}$ de parties de X a la ***propriété d'intersection finie non vide*** *si tout sous-ensemble fini de $\mathcal{A}$ a une intersection non vide.*

PropXKUMiCj

Proposition 9.133.
Soient X un espace topologique et $K \subset X$. Les propriétés suivantes sont équivalentes :

ItemXYmGHFai

(1) K est compact.

ItemXYmGHFaii

(2) Si $\{F_i\}_{i\in I}$ est une famille de fermés telle que $\bigcap_{i\in I} F_i \cap K = \varnothing$, alors il existe une partie finie non vide A de I tel que $\bigcap_{i\in A} F_i \cap K = \varnothing$.

ItemXYmGHFaiii

(3) Si $\{F_i\}_{i\in I}$ est une famille de fermés telle que pour tout choix de A fini dans I nous ayons $\bigcap_{i\in A} F_i \cap K \neq \varnothing$, alors l'intersection complète est non vide : $\bigcap_{i\in I} F_i \cap K \neq \varnothing$.

ItemXYmGHFaiv

(4) Toute famille de fermés de X, à laquelle K est joint, et qui a la propriété d'intersection finie non vide, a une intersection non vide.

Démonstration. Les propriétés (3) et (2) sont équivalentes par contraposition. De plus le point (4) est une simple[53] reformulation en français de la propriété (3).

Prouvons (1) ⇒ (2). Soit $\{F_i\}_{i\in I}$ une famille de fermés tels que $K \bigcap_{i\in I} F_i = \varnothing$. Les complémentaires $\mathcal{O}_i$ de F_i dans X recouvrent K et donc on peut en extraire un sous-recouvrement fini :

$$K \subset \bigcup_{i\in A} \mathcal{O}_i \tag{9.136}$$

pour un certain sous-ensemble fini A de I. Pour ce même choix A, nous avons alors aussi

$$\bigcap_{i\in A} F_i \cap K = \varnothing. \tag{9.137}$$

L'implication (2) ⇒ (1) est la même histoire de passage aux complémentaires. □

Le théorème 9.372 est en général celui qu'on nomme « théorème des fermés emboîtés », mais le corolaire suivant en mériterait également le nom.

CORooQABLooMPSUBf

Corolaire 9.134 ([1])**.**
Soient un espace topologique compact X et une suite $(F_i)_{i\in\mathbb{N}}$ de fermés emboîtés[54] *dans X telle que*

$$\bigcap_{i\in\mathbb{N}} F_i = \varnothing. \tag{9.138}$$

Alors il existe $j_0 \in \mathbb{N}$ tel que $F_i = \varnothing$ pour tout $i \geqslant j_0$.

[53] Enfin, simple… il faut remarquer que dans la formulation de (4), les intersections peuvent ne pas faire intervenir K, mais, au final, on s'en moque.

[54] C'est-à-dire que $F_{i+1} \subset F_i$.

Démonstration. La proposition 9.133 nous dit qu'il existe une partie finie non vide J de $\mathbb{N}$ telle que $\bigcup_{j\in J} F_j = \varnothing$. Si $j_0 = \min(J)$, alors $F_j \subset F_{j_0}$ pour tout $j \in J$ et nous avons

$$\varnothing = \bigcap_{j\in J} F_j = F_{j_0}. \tag{9.139}$$

Dès que $F_{j_0} = \varnothing$, tous les suivants sont également vides. □

9.7.3 Quelques propriétés

LemOWVooZKndbI

Lemme 9.135.
Une partie K d'un espace topologique est compacte si et seulement si de tout recouvrement par des ouverts d'une base de topologie nous pouvons extraire un sous-recouvrement fini.

Remarquons que la partie qui est réellement à prouver est que, si « ça marche » pour des ouverts d'une base de topologie, alors « ça marche » pour tous types d'ouverts.

Démonstration. Soit K une partie d'un espace topologique et $\{\mathcal{O}_i\}_{i\in I}$ un recouvrement de K par des ouverts. Chacun des $\mathcal{O}_i$ est une union d'éléments de la base de topologie par la proposition 9.2 : disons $\mathcal{O}_i = \bigcup_{j\in J_i} A_{(i,j)}$. Soit $J = \{j = (i, j_i) | i \in I, j_i \in J_i\}$; alors nous obtenons $\bigcup_{j\in J} A_j = \bigcup_{i\in I} \mathcal{O}_i$.

Par hypothèse nous pouvons extraire un ensemble fini $J_0 \subset J$ tel que $K \subset \bigcup_{j\in J_0} A_j$. Par construction chacun des A_j est inclus dans (au moins) un des $\mathcal{O}_i$. Le choix d'un élément de I pour chacun des éléments de J_0 donne une partie finie I_0 de I telle que $K \subset \bigcup_{j\in J_0} A_j \subset \bigcup_{i\in I_0} \mathcal{O}_i$. □

Exemple 9.136 (Un compact non fermé)**.**
En général, un compact n'est pas toujours fermé. Si nous prenons par exemple un ensemble X de plus de deux points muni de la topologie grossière $\{\varnothing, X\}$. Toutes les parties de cet espace sont compactes, mais les seuls fermés sont $\{\varnothing, X\}$. Toutes les autres parties sont alors compactes et non fermées. △

LemnAeACf

Lemme 9.137 (Compacts et fermés[250])**.**
À propos de parties fermées dans un compact.

ITEMooNKAKooQoNddr

(1) Une partie fermée d'un compact est compacte.

ITEMooAZWVooLyPDeY

(2) Tout compact d'un espace topologique séparé est fermé.

Démonstration. En deux parties.

(1) **Pour (1)** Soient F fermé dans un compact K et $\{\mathcal{O}_i\}_{i\in I}$ un recouvrement de F par des ouverts. Puisque F est fermé, F^c est ouvert et $\{\mathcal{O}_i\}_{i\in I} \cup \{K \setminus F\}$ est un recouvrement de K par des ouverts. Si nous en extrayons un sous-recouvrement fini, c'est un recouvrement de F, et en supprimant éventuellement l'ouvert $K\setminus F$, ça reste un sous-recouvrement fini de F tout en étant extrait de $\{\mathcal{O}_i\}_{i\in I}$.

(2) **Pour (2)** Soient X un espace séparé et K compact dans X. Nous considérons $y \in K^c$ et, par hypothèse de séparation, pour chaque $x \in K$ nous considérons un voisinage ouvert V_x de x et un voisinage ouvert [55] W_x de y tels que $V_x \cap W_x = \varnothing$. Bien entendu les V_x forment un recouvrement de K par des ouverts dont nous pouvons extraire un sous-recouvrement fini : soit S fini dans K tel que

$$K \subset \bigcup_{x\in S} V_x. \tag{9.140}$$

L'ensemble $W = \bigcap_{x\in S} W_x$ est une intersection finie d'ouverts autour de y et est donc un ouvert autour de y.

Montrons que $W \cap K = \varnothing$. Soit $a \in K$; par définition de S, il existe $s \in S$ tel que $a \in V_s$. Par conséquent, a n'est pas dans W_s et donc pas non plus dans W.

L'ouvert W prouve que y est dans l'intérieur du complémentaire de K, et comme y est arbitraire, nous concluons que le complémentaire de K est ouvert (théorème 9.8), en d'autres termes, que K est fermé.

□

CORooSSFFooNkNmlS

Corolaire 9.138 ([3, 251])**.**
Dans un espace topologique, une intersection d'un compact avec un fermé est compacte.

[55] Oui, la notation du voisinage peut surprendre, mais elle est quand même pratique pour ce qu'on veut en faire.

Démonstration. Soit un espace topologique X. Soient K compact dans X et F fermé dans X. Soit un recouvrement $\{U_i\}_{i\in I}$ de $K\cap F$ par des ouverts de X. Vu que $K=(K\cap F)\cup(K\setminus F)$, la famille

$$\big\{\{U_i\}_{i\in I},X\setminus F\big\}\tag{9.141}$$

recouvre K. Par compacité de K, nous pouvons en extraire un sous-recouvrement fini. Il existe une partie finie $I_0\subset I$ tel que

$$\big\{\{U_i\}_{i\in I_0},X\setminus F\big\}\tag{9.142}$$

recouvre K. Cette famille recouvre donc aussi $K\cap F$. Mais comme $X\setminus F$ n'intersecte surement pas $K\cap F$, la famille $\{U_i\}_{i\in I_0}$ recouvre $K\cap F$. Nous avons donc bien extrait un sous-recouvrement fini pour $K\cap F$. □

PROPooFXCXooXNeXWl

Proposition 9.139 (Théorème des compacts emboîtés[252])**.**
Soit un espace topologique séparé X. Soient des compacts emboîtés non vides $(K_n)_{n\in\mathbb{N}}$. Alors l'intersection est compacte et non vide.

Démonstration. En deux parties.

(1) **L'intersection est non vide** Nous utilisons la proposition 9.133(3). Vu que K_0 est compact, nous considérons la famille de fermés[56] $\{K_i\}_{i\in\mathbb{N}}$. Si I est fini dans $\mathbb{N}$, alors

$$K_{\max(I)+1}\subset\bigcap_{i\in I}K_i,\tag{9.143}$$

de telle sorte que $\bigcap_{i\in I}K_i$ est non vide. La proposition 9.133(3) dit alors que l'intersection $\bigcap_{i\in\mathbb{N}}K_i$ est non vide.

(2) **L'intersection est compacte** Nous posons $K=\bigcap_{i\in\mathbb{N}}K_i$. Soit un recouvrement $\{A_i\}_{i\in I}$ de K par des ouverts.

(2a) **$X\setminus K$ est ouvert** Vu que K_i est compact, il est fermé et $X\setminus K_i$ est ouvert. Le lemme 1.46(5) dit que

$$X\setminus K=\bigcup_{i\in\mathbb{N}}(X\setminus K_i).\tag{9.144}$$

Donc $X\setminus K$ est ouvert en tant que union d'ouverts.

(2b) **Un recouvrement pour K_0** Nous avons :

$$\begin{aligned}K_0&=(K_0\cap K)\cup(K_0\setminus K)&(9.145a)\\&\subset K\cup(K_0\setminus K)&(9.145b)\\&\subset\Big(\bigcup_{i\in I}A_i\Big)\cup(E\setminus K).&(9.145c)\end{aligned}$$

Donc $\{A_i,E\setminus K\}$ est un recouvrement de K_0 par des ouverts. Il existe donc un J fini dans $\mathbb{N}$ tel que

$$K_0\subset\big(\bigcup_{j\in J}A_j\big)\cup(X\setminus K).\tag{9.146}$$

(2c) **Le recouvrement fini de K** Si $x\in K$, alors $x\in K_0$, mais x n'est pas dans $X\setminus K$. Donc $x\in\bigcup_{j\in J}A_j$. Nous avons démontré que $\{A_j\}_{j\in J}$ était un recouvrement fini de K.

□

LEMooFJZDooSxYWVW

Lemme 9.140 ([1])**.**
Toute union finie de compacts est compacte.

Démonstration. Soient $(K_i)_{i=1,\dots,n}$ des compacts dans X. Si $\{\mathcal{O}_s\}_{i\in S}$ est un recouvrement de $\bigcup_{i\in I}K_i$ par des ouverts, à fortiori, ce sera un recouvrement de chacun des K_i. Pour chaque i, il existera donc une partie finie S_i de S telle que $\{\mathcal{O}_s\}_{s\in S_i}$ recouvre K_i.

L'union finie de parties finies S_i est une partie finie de S, et nous avons

$$\bigcup_i K_i\subset\bigcup_{s\in\bigcup_i S_i}\mathcal{O}_s.\tag{9.147}$$

□

[56] Tout compact d'un espace séparé est fermé, lemme 9.137(2).

PROPooQWHSooXeJOkT

Proposition 9.141 ([253]).
Dans un espace séparé, toute intersection de compacts est compacte.

Démonstration. Soit un espace topologie séparé X et des compacts $\{K_i\}_{i\in I}$ dans X (I est un ensemble quelconque). Chacun des K_i est fermé par le lemme 9.137(2). Donc l'intersection

$$K = \bigcap_{i\in I} K_i \tag{9.148}$$

est un fermé de X par le lemme 9.6(1). Soit i dans I. Nous avons $K \subset K_i$. Donc K est un fermé dans le compact K_i ; il est donc compact par le lemme 9.137. □

Exemple 9.142 (Intersection de compacts non compacte[253]).
Un exemple d'intersection de compacts qui n'est pas compacte. Vu la proposition 9.141, il va falloir chercher un espace non séparé. Soit $X = \mathbb{N} \cup \{x_1, x_2\}$ où x_1 et x_2 sont deux éléments distincts hors de $\mathbb{N}$. Nous définissons une topologie sur X en disant que les ouverts sont les parties suivantes :

- les parties de $\mathbb{N}$,
- la partie $\mathbb{N} \cup \{x_1\}$,
- la partie $\mathbb{N} \cup \{x_2\}$,
- la partie $\mathbb{N} \cup \{x_1, x_2\}$.

Nous considérons les parties $K_1 = \mathbb{N} \cup \{x_1\}$ et $K_2 = \mathbb{N} \cup \{x_2\}$.

(1) K_i **est compact** Soit $\{\mathcal{O}_i\}_{i\in I}$ un recouvrement de K_1 par des ouverts de X. Alors il existe $i_0 \in I$ tel que $x_1 \in \mathcal{O}_{i_0}$. Vue la liste des ouverts, $\mathcal{O}_{i_0}$ est soit $\mathbb{N} \cup \{x_1\}$ soit $\mathbb{N} \cup \{x_1, x_2\}$. Dans les deux cas, $\{\mathcal{O}_{i_0}\}$ est un sous-recouvrement fini de K_1.

(2) $K_1 \cap K_2 = \mathbb{N}$ C'est immédiat parce que x_1 et x_2 sont distincts.

(3) $\mathbb{N}$ **n'est pas compact** Il peut être recouvert par les ouverts $\{\{i\}\}_{i\in\mathbb{N}}$ dont on ne peut pas extraire de sous-recouvrements finis.

△

PropGBZUooRKaOxy

Proposition 9.143.
Si V est une partie de l'espace topologique X muni de la topologie induite[57] *τ_V de celle de X, et si K est un compact de (V, τ_V) alors K est un compact de (X, τ_X).*

Démonstration. Soient $\{\mathcal{O}_\alpha\}_{\alpha\in A}$ des ouverts de X recouvrant K. Alors les ensembles $V \cap \mathcal{O}_\alpha$ recouvrent également K, mais sont des ouverts de V. Donc il en existe un sous-recouvrement fini. Soient donc $\{V \cap \mathcal{O}_i\}_{i\in I}$ recouvrant K avec I un sous-ensemble fini de A. Les ensembles $\{\mathcal{O}_i\}_{i\in I}$ recouvrent encore K et sont des ouverts de X. □

Proposition 9.144 ([1]).
Soient des espaces topologiques X et Y. Nous considérons des ouverts A de X et B de Y. Soit un compact M dans $A \times B$[58]*. Il existe des compacts K et L dans A et B tels que $M \subset K \times L$.*

Démonstration. Nous considérons les « projections » de M sur A et B :

$$K = \{a \in A \text{ tel que } \exists b \in B \text{ tel que } (a, b) \in M\}, \tag{9.149}$$

et

$$L = \{b \in B \text{ tel que } \exists a \in A \text{ tel que } (a, b) \in M\}. \tag{9.150}$$

Nous avons $M \subset K \times L$; il reste à montrer que K et L sont des compacts de leurs espaces respectifs. Soit un recouvrement $\{U_i\}_{i\in I}$ de K par des ouverts de X et $\{V_j\}_{j\in J}$ de L par des ouverts de Y. Alors

$$\{U_i \times V_j\}_{\substack{i\in I\\ j\in J}} \tag{9.151}$$

[57] Définition 9.30.
[58] Topologie produit, définition 9.66

est un recouvrement de M par des ouverts de $X \times Y$. Puisque M est un compact de $X \times Y$, nous pouvons en extraire un sous-recouvrement fini, c'est-à-dire I_0 fini dans I et J_0 fini dans J tels que

$$\{U_i \times V_j\}_{\substack{i \in I_0 \\ j \in J_0}} \tag{9.152}$$

soit encore un recouvrement de $K \times L$. Nous prouvons à présent que $\{U_i\}_{i \in I_0}$ est un recouvrement de K, ce qui montrera que K est un compact.

Soit $a \in K$. Il existe $b \in B$ tel que $(a, b) \in M$. Donc il existe $i_0 \in I_0$ et $j_0 \in J_0$ tels que $(a, b) \in U_{i_0} \times V_{j_0}$. En particulier $a \in U_i$.

Le même raisonnement montre que $\{V_j\}_{j \in J_0}$ est un recouvrement de L. □

9.7.4 Espace relativement compact

DEFooBODRooEFhzeT

Définition 9.145 (Partie relativement compacte[254])**.**
Une partie d'un espace topologique est ***relativement compact*** *si elle est contenue dans un compact.*

PROPooXKBXooUIwTiO

Proposition 9.146 ([254])**.**
Une partie d'un espace séparé est relativement compacte si et seulement si sa fermeture est compacte.

LEMooJXGUooXDGIXG

Lemme 9.147 (Union finie de relativement compacts[1])**.**
Dans un espace séparé[59]*, une union finie de parties relativement compactes*[60] *est relativement compacte.*

Démonstration. Soit des paries relativement compactes A_i. Notre objectif est de prouver que $\overline{\bigcup_{i=1}^n A_i}$ est compact. La partie $\bigcup_{i=1}^n \bar{A}_i$ est compacte comme union finie de compacts (lemme 9.140) ; elle est donc fermée par le lemme 9.137(2) :

$$\overline{\bigcup_{i=1}^n \bar{A}_i} = \bigcup_{i=1}^n \bar{A}_i. \tag{9.153}$$

Nous avons donc

$$\overline{\bigcup_{i=1}^n A_i} \subset \overline{\bigcup_{i=1}^n \bar{A}_i} = \bigcup_{i=1}^n \bar{A}_i. \tag{9.154}$$

Autrement dit, la partie $\overline{\bigcup_{i=1}^n A_i}$ est un fermé dans un compact. Elle est donc compacte par le lemme 9.137(1). □

LEMooNIJEooMdvkuA

Lemme 9.148 (Les ouverts séparent les points et les compacts[1])**.**
Soit un espace séparé X. Soient un compact K et un point $a \notin K$. Alors il existe des ouverts A et B tels que $a \in A$, $K \subset B$ et $A \cap B = \varnothing$.

Démonstration. Pour chaque $x \in K$ nous séparons x et a : il existe A_x ouvert contenant a, B_x ouvert contenant x tels que $A_x \cap B_x = \varnothing$. Les $\{B_x\}_{x \in K}$ forment un recouvrement de K par des ouverts. Nous en extrayons un sous-recouvrement fini : il existe $x_1, \ldots, x_n \in K$ tels que $K \subset \bigcup_{i=1}^n B_{x_i}$. Nous notons $A_i = A_{x_i}$ et $B_i = B_{x_i}$.

Nous posons

$$\begin{aligned} A &= \bigcap_{i=1}^n A_i \\ B &= \bigcup_{i=1}^n B_i. \end{aligned} \tag{9.155}$$

En tant qu'intersection finie d'ouverts, A est ouvert, et comme union d'ouverts, B est ouvert. Par construction, $K \subset B$ et $a \in A$. Il reste à voir que $A \cap B = \varnothing$. Si $y \in A \cap B$, nous avons $y \in B$ et donc nous avons $y \in B_j$ pour un certain j. Mais $y \in A_i$ pour tout i, et en particulier $y \in A_j$. Donc $y \in A_i \cap B_i$. Impossible parce que nous avons choisit $A_i \cap B_i = \varnothing$. Donc $A \cap B$ est vide. □

9.7.5 Propriété d'intersection finie

DEFooCESGooZkACqs

Définition 9.149 (Propriété d'intersection finie[255])**.**
Soit un ensemble X. Une famille non vide $\mathcal{A}$ de parties de X a la ***propriété d'intersection finie*** *si toutes intersection finie d'éléments de $\mathcal{A}$ est non vide.*

[59] Séparé et Hausdorff sont synonymes, définition 9.79.
[60] Définition 9.145.

THOooCQSQooDuasqo

Théorème 9.150 ([255, 256]).
Un espace est compact si et seulement si toute famille de parties fermées ayant la propriété d'intersection finie[61] *a une intersection non vide.*

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que X est un espace topologique compact et nous considérons une famille $\{F_i\}_{i\in I}$ de fermés ayant la propriété d'intersection finie. Nous supposons par l'absurde que $\bigcap_{i\in I} F_i = \varnothing$ et nous allons contredire la propriété d'intersection finie.

Nous avons, en utilisant le lemme 1.50 :

$$X = \varnothing^x = \left(\bigcap_{i\in I} F_i\right)^c = \bigcup_{i\in I} F_i^c. \tag{9.156}$$

Vu que les F_i sont fermés, les F_i^c sont ouverts. Donc $\{F_i^c\}_{i\in I}$ est un recouvrement de X par des ouverts. Par compacité, il existe J fini dans I tel que $\bigcup_{j\in J} F_j^c = X$. Mais alors

$$X = \bigcup_{j\in J} F_j^c = \left(\bigcap_{j\in J} F_j\right)^c, \tag{9.157}$$

de telle sorte que $\bigcap_{j\in J} F_j = \varnothing$, qui contredit la propriété d'intersection finie.

(2) $\Leftarrow$ Nous supposons que toute famille de fermés ayant la propriété d'intersection finie a une intersection finie. Et nous allons prouver que X est compact. Pour cela nous considérons un recouvrement $\{A_i\}_{i\in I}$ de X par des ouverts. Nous y allons par contradiction en disant que pour tout J fini dans I nous avons $\bigcup_{j\in J} A_j \neq X$ (càs que X n'est pas compact), et nous allons trouver une contradiction.

Si J est fini dans I nous avons

$$\bigcap_{j\in J} A_j^c = \left(\bigcup_{j\in J} A_j\right)^c \neq \varnothing. \tag{9.158}$$

EQooCBAZooIoQumE

Mais les A_i^c sont des fermés, donc par propriété d'intersection finie,

$$\varnothing \neq \bigcap_{i\in I} A_i^c = \left(\bigcup_{i\in I} A_i\right)^c; \tag{9.159}$$

la première inégalité est parce que la famille $\{A_i^c\}_{i\in I}$ sont des fermés a toutes ses intersections finies non vides (c'est (9.158)), et donc a une intersection non vide par hypothèse.

Cela contredit le fait que $\bigcup_{i\in I} A_i$ est un recouvrement de X.

□

9.8 Limite de fonction

DefYNVoWBx

Définition 9.151 (Limite d'une fonction, thème 29[257]).
*Soient des espaces topologiques X et Y ainsi que $\Omega \subset X$ et $a \in \mathrm{Adh}(\Omega)$. Soit une application $f\colon \Omega \to Y$. Nous disons que l'élément ℓ de Y est une **limite** de f en a lorsque pour tout ouvert V contenant ℓ, il existe un voisinage ouvert U de a tel que*

$$f\Big(\big(U\cap\Omega\big)\setminus\{a\}\Big) \subset V. \tag{9.160}$$

EQooXLJJooZDcQtU

Si un tel élément est unique[62]*, alors nous disons que cet élément est la **limite** de f et nous notons*

$$\lim_{x\to a} f(x) = \ell. \tag{9.161}$$

9.152.
Il aurait été tout aussi bien de définir la limite d'une fonction $f\colon X \to Y$ définie sur tout X, puis de considérer Ω avec la topologie induite depuis X.

[61] Définition 9.149.
[62] Rappelons que ce n'est pas toujours le cas, mais que ça l'est si l'espace topologique est séparé – définition 9.79.

Dans ce cas, nous aurions écrit (9.160) sous la forme

$$f\Big(U \setminus \{a\}\Big) \subset V \tag{9.162}$$

en disant que U est un voisinage de a, et en laissant le lecteur deviner que ici, « voisinage » signifie « voisinage au sens de la topologie induite ». Vu que nous considérons la fonction f uniquement définie sur Ω, c'est la seule interprétation possible, et il n'y aurait pas au d'ambigüité[258]. Mais bon… si ça va sans dire, ça va encore mieux en le disant.

Remarque 9.153.
Nous ne saurions trop insister sur le fait que la valeur de f en a n'intervient pas dans la définition de la limite de f en a. Il n'est même pas nécessaire que f soit définie en a pour que l'on puisse parler de limite de f en a. Par exemple nous avons

$$\lim_{x\to 1} \frac{x^2-1}{x-1} = 2, \tag{9.163}$$

alors que la fonction n'est pas définie en $x = 1$.

Plus généralement, un peu par principe, toutes les fois que la notion de limite apporte une information, le point où l'on prend la limite est spécial. Sinon on ne calculerait pas la limite, mais on regarderait directement la valeur de la fonction. Cela est typiquement le cas lorsque nous aborderons les dérivées. En effet, regardons (en faisant semblant d'anticiper) la définition (12.298). Dans la formule

$$f'(a) = \lim_{x\to a} \frac{f(x)-f(a)}{x-a}, \tag{9.164}$$

la fonction sur laquelle nous prenons la limite n'est *jamais* définie en $x = a$.

PropFObayrf

Proposition 9.154 (Unicité de la limite pour un espace séparé)**.**
Soient X un espace topologique, A une partie de X et Y un espace topologique séparé[63]*. Nous considérons une fonction $f\colon A \to Y$. Si $a \in \mathrm{Adh}(A)$, alors f admet au plus une limite en a.*

Démonstration. Soient y et y' des limites de f en a, ainsi que des voisinages V et V' de y et y'. Nous prenons également les voisinages W et W' correspondants :

$$\begin{cases} f(W \cap A) \subset V & \text{(9.165a)} \\ f(W' \cap A) \subset V'. & \text{(9.165b)} \end{cases}$$

Quitte à prendre des sous-ensembles nous pouvons supposer que W et W' sont ouverts. Il s'ensuit alors que :

- l'ensemble $W \cap W'$ est un ouvert contenant a et intersecte donc A ;
- l'ensemble $(W \cap W') \cap A$ est donc non vide ;
- et donc, $f(W \cap W' \cap A)$ est, lui aussi, non vide.

Mais

$$f(W \cap W' \cap A) \subset f(W \cap A) \subset V, \tag{9.166}$$

et

$$f(W \cap W' \cap A) \subset f(W' \cap A) \subset V', \tag{9.167}$$

d'où V et V' ont une intersection. Puisque ces ensembles sont arbitraires, nous avons prouvé que tout voisinage de y et tout voisinage de y' ont une intersection non vide ; étant donné que Y est séparé, nous devons avoir $y = y'$. □

9.9 Topologie, distances et normes

Certains ensembles ont plus de structures qu'une topologie. Nous fixons quelques bases maintenant, et nous détaillerons certains résultats plus tard.

[63] Définition 9.79.

9.9.1 Distance et topologie métrique

DefMVNVFsX

Définition 9.155.
*Si E est un ensemble, une **distance** sur E est une application $d: E\times E\to\mathbb{R}$ telle que pour tout $x,y\in E$,*

(1) $d(x,y)\geqslant 0$

(2) $d(x,y)=0$ *si et seulement si* $x=y$,

(3) $d(x,y)=d(y,x)$

(4) $d(x,y)\leqslant d(x,z)+d(z,y)$.

*La dernière condition est l'**inégalité triangulaire**.*

*Un couple (E,d) formé d'un ensemble et d'une distance est un **espace métrique**.*

DEFooGLTUooJjaSmI

Définition 9.156 (Espace vectoriel topologique métrisable[259])**.**
*Un espace topologique est **métrisable** si il existe une distance[64] compatible avec la topologie.*

Le lemme suivant est similaire à la proposition 9.233.

LEMooXCXHooVtrkvl

Lemme 9.157 (Inégalité triangulaire inversée[2])**.**
Si (E,d) est un espace métrique et si $a,b,x\in E$, nous avons

$$d(a,b)\geqslant \big|d(a,x)-d(x,b)\big| \tag{9.168}$$

Démonstration. Nous écrivons l'inégalité triangulaire pour $d(a,x)$ et $d(b,x)$:

$$\begin{cases} d(a,x)\leqslant d(a,b)+d(b,x) & (9.169a)\\ d(b,x)\leqslant d(b,a)+d(a,x). & (9.169b)\end{cases}$$

Nous isolons alors $d(a,b)$ dans chacune de ces inégalité, et nous utilisons la symétrie de d :

$$\begin{cases} d(a,b)\geqslant d(a,x)-d(x,b) & (9.170a)\\ d(a,b)\geqslant d(b,x)-d(a,x). & (9.170b)\end{cases}$$

En vertu du lemme 1.122(7), nous avons alors

$$d(a,b)\geqslant |d(a,x)-d(x,b)|. \tag{9.171}$$

□

La définition suivante donne une topologie sur les espaces métriques en partant des boules.

ThoORdLYUu

Théorème-Définition 9.158 (Topologie métrique)**.**
*Soit (E,d) un espace métrique. Nous définissons les **boules ouvertes** par*

$$B(a,r)=\{x\in E \text{ tel que } d(a,x)<r\}. \tag{9.172}$$

EQooYCWSooIhibxd

pour tout $a\in E$ et $r>0$. Alors en posant

$$\tau_d=\big\{\mathcal{O}\subset E \text{ tel que } \forall a\in\mathcal{O},\exists r>0 \text{ tel que } B(a,r)\subset\mathcal{O}\big\} \tag{9.173}$$

EqGDVVooDZfwSf

nous définissons une topologie sur E.

*Cette topologie sur E est la **topologie métrique** de (E,d). En présence d'une distance, sauf mention explicite du contraire, c'est toujours cette topologie-là que nous utiliserons.*

Démonstration. D'abord $\varnothing\in\tau_d$ parce que tout élément de l'ensemble vide … heu … enfin parce que, d'accord hein[65]. Ensuite si les $\{A_i\}_{i\in I}$ sont des éléments de τ_d et si $x\in\bigcup_{i\in I}A_i$ alors il existe $k\in I$ tel que $x\in A_k$. Par hypothèse il existe une boule $B(x,r)\subset A_k\subset\bigcup_{i\in I}A_i$.

Enfin si les $\{A_i\}_{i\in\{1,\ldots,n\}}$ sont des éléments de $\mathcal{T}$ alors pour tout i il existe $r_i>0$ tel que $B(x,r_i)\subset A_i$. En prenant $r=\min\{r_i\}_{i=1,\ldots,n}$ nous avons $B(x,r)\subset\bigcap_{i=1}^n A_i$. □

PROPooZXTXooEMLgMn

Proposition 9.159.
La topologie sur un espace métrique[66] est la topologie engendrée[67] par ses boules ouvertes.

[64] Distance, définition 9.155.
[65] Pour qui ne serait pas d'accord, ajoutez $\varnothing$ dans la définition des ouverts et puis c'est tout.
[66] Définition 9.158.
[67] Définition 9.13

Démonstration. Nous notons (E,d) l'espace métrique. Nous notons τ_d la topologie métrique, et τ_B celle engendrée par les boules ouvertes.

(1) $\tau_d \subset \tau_B$ Soit $a \in \tau_d$. Pour tout $a \in A$, nous avons une boule $B(a,r_a)$ inclue dans A, et donc

$$A = \bigcup_{a\in A} B(a,r_a) \in \tau_B. \tag{9.174}$$

(2) $\tau_B \subset \tau_d$ Soient $a_i \in E$ et $r_i > 0$.

(2a) $\bigcap_{i=1}^n B(a_i,r_i) \in \tau_d$ Soit $x \in \bigcap_{i=1}^n B(a_i,r_i)$. Pour chaque i, nous avons $d(x,a_i) < r_i$. Il existe donc $\alpha_i > 0$ tel que $d(x,a_i) < \alpha_i < r_i$. En posant $\epsilon_i < r_i - \alpha_i$ nous avons $B(x,\epsilon_i) \subset B(a_i,r_i)$. En posant $\epsilon < \min_i(\epsilon_i)$ nous avons

$$B(x,\epsilon) \subset \cap_{i=1}^n B(a_i,r_i). \tag{9.175}$$

(2b) **Et donc** Nous avons prouvé que

$$\bigcap_{i=1}^n B(a_i,r_i) \in \tau_d. \tag{9.176}$$

Tout élément de τ_B est une union de tels éléments. Vu que τ_d est stable par union, nous avons $\tau_B \subset \tau_d$.

□

Proposition 9.160.
À propos de séparation.

(1) Tout espace métrique[68] *est séparé.*

(2) Si une suite dans un espace métrique possède une limite, alors elle est unique.

Démonstration. Si deux éléments x et y sont distincts, alors en posant $r = d(x,y)/3 > 0$, les boules $B(x,r)$ et $B(y,r)$ sont disjointes.

En ce qui concerne les limites, ce sont les propositions 9.90 et 9.154. □

9.161.
Nous allons maintenant voir deux résultats disant que si une fonction est continue, alors elle peut être permutée avec une limite de suite. Dans le cas des espaces métriques, la proposition 9.173 montrera la réciproque : si pour toute suite $x_n \to a$, nous avons $\lim_{n\to\infty} f(x_n) = y$, alors f a une limite en a qui vaut y.

fContEstSeqCont

Proposition 9.162 (Permuter limite et fonction continue[1])**.**
Soient deux espaces topologiques X et Y ainsi qu'une fonction $f\colon X \to Y$. Soit $a \in X$ et $\ell \in Y$. Si

$$\lim_{x\to a} f(x) = \ell, \tag{9.177}$$

alors, pour toute suite (x_k) telle que $x_k \to a$, on a

$$\lim f(x_k) = \ell. \tag{9.178}$$

Démonstration. Nous considérons une suite (x_k) qui converge vers a dans X. Soient V un voisinage de ℓ et W un voisinage de a tels que $f(W) \subset V$ (définition 9.151 de la continuité en un point). Par la convergence $x_k \to a$, il existe N tel que pour tout $k \geqslant N$, $x_k \in W$, et donc tel que $f(x_k) \in V$, ce qui donne la continuité séquentielle de f. □

9.9.2 Précompact

DEFooLZDTooZlAtdL

Définition 9.163.
Une partie A d'un espace topologique métrique[69] *est* ***précompact*** *si pour tout $\epsilon > 0$, il peut être recouvert par un nombre fini de boules de rayon ϵ.*

PROPooDWUDooGrgZpP

Proposition 9.164 ([260])**.**
L'adhérence d'un précompact est précompacte.

[68] Définition 9.155.
[69] Topologie métrique, définition 9.158.

Démonstration. Soit un précompact A ; fixons $\epsilon > 0$. La partie A peut être recouverte par les boules $\{B(a_i, \epsilon)\}_{i=1,\dots,n}$. Soit maintenant $x \in \mathrm{Adh}(A)$. Il existe $a \in A$ tel que $d(a,x) < \epsilon$. De plus ce a est dans une des boules ; c'est-à-dire que il existe $i = 1, \dots, n$ tel que $d(a_i, a) < \epsilon$. Nous avons donc

$$d(a_i, x) \leqslant d(a_i, a) + d(a, x) \leqslant 2\epsilon. \tag{9.179}$$

Donc les boules $\{B(a_i, 2\epsilon)\}_{i=1,\dots,n}$ recouvrent $\mathrm{Adh}(A)$. □

PROPooZRXDooUyFBFG

Proposition 9.165.
Soient un espace topologique X ainsi que $A \subset X$. Si A est précompact et complet, alors A est compact.

9.9.3 Caractérisations séquentielles

9.9.3.1 Continuité séquentielle

DefENioICV

Définition 9.166.
*Si X et Y sont deux espaces topologiques, une fonction $f : X \to \mathbb{R}$ est **séquentiellement continue** en un point a si pour toute suite convergente $x_n \to a$ dans X nous avons $f(x_n) \to f(a)$ dans Y.*

9.9.4 Suites et espaces métriques

PROPooJYOOooZWocoq

Proposition 9.167 (Caractérisation séquentielle de la limite[1])**.**
Soient deux espaces métriques X et Y ainsi qu'une fonction $f : X \to Y$. Soit $a \in X$ et $\ell \in Y$. On a

$$\lim_{x \to a} f(x) = \ell, \tag{9.180}$$

EqLimooJYOOooZWocoqC

si et seulement si, pour toute suite (x_k) telle que $x_k \to a$, on a

$$\lim f(x_k) = \ell. \tag{9.181}$$

EqLimooJYOOooZWocoqS

Par ailleurs, l'une des deux limites existe si et seulement si l'autre existe.

Démonstration. Le sens direct est la proposition 9.162. Pour la réciproque, nous passons par la contraposée. C'est-à-dire que nous supposons que ℓ n'est pas une limite de f pour $x \to a$. Il existe un ϵ tel que pour tout δ, il existe un x vérifiant $d_X(x;a) < \delta$ et $d_Y(f(x);\ell) > \epsilon$.

Nous construisons à présent une suite de la manière suivante. Pour $\delta = \frac{1}{n}$ nous considérons x_n tel que $d_X(x_n;a) < \delta$ et $d_Y(f(x_n);\ell) > \epsilon$. Cette suite converge vers a, mais la suite $f(x_n)$ ne converge manifestement pas vers ℓ : elle ne rentre jamais dans la boule $B(\ell, \epsilon)$. □

Une fonction continue est séquentiellement continue. Dans les espaces métriques la proposition suivante montre que la réciproque est également vraie et la continuité est équivalente à la continuité séquentielle. Cela n'est cependant pas vrai pour n'importe quel espace topologique.

PROPooBHRBooJMZYSg

Corolaire 9.168 (Caractérisation séquentielle de la continuité en un point[1])**.**
Si X et Y sont des espaces métriques, alors une fonction $f : X \to Y$ est continue en un point si et seulement si elle est séquentiellement continue en ce point.

Démonstration. Paraphrasons la preuve précédente. Nous supposons que X et Y sont métriques. Si f n'est pas continue en a, il existe $\epsilon > 0$ tel que pour tout $\delta > 0$, il existe x tel que $\|x - a\| \leqslant \delta$ et $\|f(x) - f(a)\| > \epsilon$. Nous considérons un tel ϵ et pour chaque $n \geqslant 1 \in \mathbb{N}$ nous considérons un x_n correspondant à $\delta = \frac{1}{n}$. Cela nous donne une suite $x_n \to a$ dans X mais $\|f(x_n) - f(a)\|$ reste plus grand que ϵ. Cela montre que f n'est pas non plus séquentiellement continue. □

Définition 9.169 (Fermeture séquentielle[261])**.**
*Une partie F d'un espace topologique X est dit **séquentiellement fermé** si la convergence d'une suite (x_n) de F vers x implique que x appartient à F.*

Les espaces métriques ont une propriété importante que la fermeture séquentielle est équivalente à la fermeture.

PropLFBXIjt

Proposition 9.170 (Caractérisation séquentielle d'un fermé)**.**
Soient X un espace métrique[70] et $F \subset X$. L'ensemble F est fermé si et seulement si toute suite contenue dans F et convergeant dans X converge vers un élément de F.

[70] Définition 9.155.

Démonstration. Une suite contenue dans un fermé ne peut converger que vers un élément de ce fermé : c'était la proposition 9.84. Le point le plus important est donc l'autre sens : si toute suite d'éléments de F converge dans F alors F est fermé.

Par contraposée, supposons que $X \setminus F$ ne soit pas ouvert. Alors il existe $x \in X \setminus F$ pour lequel tout voisinage intersecte F. En prenant $x_k \in B(x, \frac{1}{k})$, nous construisons une suite contenue dans F, convergeant vers x qui n'est pas dans F. □

Le lemme suivant est précisément la version « espace métrique » du corolaire 9.85 ; mais, donnons-en une preuve tout de même.

LemLimAbarA

Lemme 9.171.
Soit X un espace métrique[71], et soit (x_n) une suite convergente contenue dans un ensemble $A \subset X$. Alors la limite x_n appartient à $\bar{A}$.

Démonstration. Supposons que nous ayons une partie A de X, et une suite (x_n) dont la limite ℓ se trouve hors de $\bar{A}$. Dans ce cas, il existe un $r > 0$ tel que[72] $B(\ell, r) \cap A = \varnothing$. Si tous les éléments x_n de la suite sont dans A, il n'y en a donc aucun tel que $d(x_n, \ell) < r$. Cela contredit la notion de convergence $x_n \to \ell$. □

CorAdhEstLim

Corolaire 9.172.
Soit X un espace métrique, $A \subset X$ et $a \in \bar{A}$. Alors il existe une suite d'éléments dans A qui converge vers a.

Démonstration. Si $a \in A$, alors nous pouvons prendre la suite constante $x_n = a$. Si a n'est pas dans A, alors a est dans ∂A, et pour tout n, il existe un point de A dans la boule $B(a, \frac{1}{n})$. Si nous nommons x_n ce point, la suite ainsi construite est une suite contenue dans A et qui converge vers a (ce dernier point est laissé à la sagacité du lecteur.). □

En termes savants, ce corolaire signifie que la fermeture $\bar{A}$ est composé de A plus de toutes les limites de toutes les suites contenues dans A.

PropXIAQSXr

Proposition 9.173 (Caractérisation séquentielle de la continuité[1])**.**
Soient X et Y deux espaces topologiques séparés. Nous supposons que X est métrisable[73]. Une application $f : X \to Y$ est continue sur X si et seulement si elle est séquentiellement continue sur X.

Démonstration. En deux parties dont une déjà faite.

(1) $\Rightarrow$ C'est la proposition 9.162.

(2) $\Leftarrow$ Soit $\mathcal{O}$ un ouvert de Y ; nous allons voir que le complémentaire de $f^{-1}(\mathcal{O})$ est fermé dans X. Pour cela nous considérons une suite convergente $x_k \xrightarrow{X} x$ avec $x_k \in X \setminus f^{-1}(\mathcal{O})$ pour tout k. Nous allons montrer que $x \in X \setminus f^{-1}(\mathcal{O})$ et la caractérisation séquentielle[74] de la fermeture conclura que $X \setminus f^{-1}(\mathcal{O})$ est fermé.

Pour tout k, nous avons $f(x_k) \in X \setminus \mathcal{O}$, et $f(x_k) \xrightarrow{Y} f(x)$ parce que f est séquentiellement continue. Vu que $f(x_k)$ est une suite dans le fermé $Y \setminus \mathcal{O}$, la limite est également dans $Y \setminus \mathcal{O}$. Nous en déduisons que $f(x) \in Y \setminus \mathcal{O}$, de telle sorte que $x \in X \setminus f^{-1}(\mathcal{O})$.

□

PropCJGIooZNpnGF

Proposition 9.174.
Si X et Y sont deux espaces métriques et $f, g : X \to Y$ sont deux fonctions continues égales sur une partie dense de X alors $f = g$.

Démonstration. Les fonctions f et g sont séquentiellement continues (proposition 9.168). Soient A un ensemble dense dans X sur lequel f et g sont égales, et $x \notin A$. Vu que A est dense, il existe une suite a_n dans A telle que $a_n \to x$. La séquentielle continuité de f et g donnent

$$f(a_n) \to f(x) \tag{9.182a}$$
$$g(a_n) \to g(x), \tag{9.182b}$$

mais pour tout n, $f(a_n) = g(a_n)$. Par unicité de la limite[75] dans Y, $f(x) = g(x)$. □

[71] Définition 9.155.
[72] Une autre manière de dire la même chose : si $\ell \notin \bar{A}$, alors $d(\ell, A) > 0$.
[73] Définition 9.156 : il existe une distance compatible avec la topologie.
[74] Proposition 9.170, valable parce que la topologie de X provient d'une métrique.
[75] Proposition 9.154.

9.9.5 Continuité de la distance

PROPooSZMLooNdtLLj

Proposition 9.175 ([1]).
Soit un espace métrique (E,d). L'application $d\colon E\times E\to E$ est continue.

PROPooUXDJooCrWBbd

Proposition 9.176 ([1]).
Soient un espace métrique (E,d), ainsi qu'une suite convergente $a_n \xrightarrow{d} \ell$. Il existe $r>0$ tel que pour tout n nous ayons $d(\ell,a_n)<r$.

Démonstration. Soit $r_1>0$ et $N\in\mathbb{N}$ tel que $n\geqslant N$ implique $d(\ell,a_n)<r_1$. Ensuite nous posons $r_2=\max\{d(\ell,a_n)\}_{n=0,\dots,N}$.

Pour tout n nous avons $d(a_n,\ell)\leqslant r_1+r_2$. □

PROPooNOHQooTqBQLk

Proposition 9.177 ([1]).
Soient un espace topologique X, un espace topologique normé[76] Y. Soit une application continue $f\colon X\to Y$. Pour tout $x\in X$, il existe un voisinage ouvert de x sur lequel f est bornée.

Démonstration. Soit $\delta>0$. Nous considérons dans Y la boule $B\big(f(x),\delta\big)$. Par continuité de f, la partie $f^{-1}\Big(B\big(f(x),\delta\big)\Big)$ est ouverte dans X. Si y est dans cette partie, alors

$$f(y)\in B\big(f(x),\delta\big). \tag{9.183}$$

L'application f y est donc bornée. □

9.9.6 Topologie métrique et induite

LEMooKDMYooMIcFRI

Lemme 9.178.
Soit un espace vectoriel normé $\big(V,\|.\|\big)$ muni d'un sous-espace vectoriel M. La topologie induite de M depuis V est la même que la topologie de la norme induite $\big(M,\|.\|\big)$.

9.9.7 Intérieur, adhérence et frontière

9.179.
Choses déjà faites :

- Intérieur, définition 9.16.
- Adhérence, qui est la même chose que fermeture, définition 9.19, et précisé par le lemme 9.20.

Dans le cas de $\mathbb{R}^n$ dans lequel les boules forment une base de la topologie nous pouvons encore préciser de la façon suivante :

$$x\in \operatorname{Adh} A \overset{\text{def}}{\iff} \forall \epsilon>0, B(x,\epsilon)\cap A\neq\varnothing \tag{9.184}$$

PROPooZRFZooVqDFWD

Proposition 9.180.
Si A est une partie d'un espace topologique nous avons :

$$\operatorname{Int} A\subseteq A\subseteq \operatorname{Adh}(A) \tag{9.185}$$

Démonstration. Si $x\in\operatorname{Int}(A)$, alors x admet un voisinage contenu dans A ; ledit voisinage contient x, et donc x est dans A.

Si $x\in A$ alors tout voisinage de x intersecte A (au moins en x lui-même), donc $x\in\operatorname{Adh}(A)$. □

DEFooACVLooRwehTl

Définition 9.181.
*La **frontière** ou le **bord** de A est défini par $\partial A=\operatorname{Adh} A\setminus \operatorname{Int} A$.*

LEMooMPZWooGrqYIX

Lemme 9.182.
Soit une partie A d'un espace topologique.

ITEMooNBSCooXJcVos

(1) A est ouverte si et seulement si $A=\operatorname{Int}(A)$.

ITEMooDCIOooQAvCqI

(2) A est fermée si et seulement si $A=\operatorname{Adh}(A)$.

Et je rappelle que « adhérence » et « fermeture » c'est la même chose et que $\bar{A}$ et $\operatorname{Adh}(A)$ sont deux notations pour la fermeture.

[76] Topologie en 9.158.

Démonstration. Soient un espace topologique X et $A \subset X$.

(1) **Pour (1)** C'est une reformulation du théorème 9.8 parce que x a un voisinage dans A signifie exactement $x \in \text{Int}(A)$.

(2) **Pour (2)** En deux parties.

(2a) **Si A est fermé** Nous devons prouver que $A = \bar{A}$ en sachant que A^c est ouvert. Nous écrivons la proposition 9.21 avec A^c :

$$X = \text{Int}(A^c) \cup \overline{X \setminus A^c} = A^c \cup \bar{A}. \tag{9.186}$$

Nous avons utilisé le fait que $\text{Int}(A^c) = A^c$ en vertu de (1) et que A^c est ouvert. Étant donné que l'union est disjointe, $A^c = (\bar{A})^c$, ce qui signifie que $A = \bar{A}$ comme il fallait.

(2b) **Si $A = \bar{A}$** Nous écrivons encore 9.21 avec A^c :

$$X = \text{Int}(A^c) \cup \bar{A} = \text{Int}(A^c) \cup A. \tag{9.187}$$

Vu que l'union est disjointe, $\text{Int}(A^c) = A^c$, ce qui signifie que A est ouvert par (1).

□

PROPooFHURooGXcekV

Proposition 9.183 ([1]).
Un ouvert n'intersecte pas sa frontière.

Démonstration. Soit un ouvert A. Nous avons $\partial(A) = \bar{A} \setminus \text{Int}(A)$. Oh mais comme A est ouvert, $\text{Int}(A) = A$. Donc les éléments de A sont exclus de ∂A. □

PROPooGXYCooRcnHDD

Proposition 9.184 ([1]).
Si A est une partie de l'espace topologique X, alors

(1)

$$X \setminus \text{Int}(A) = \overline{X \setminus A} \tag{9.188}$$

(2)

$$\partial A = \bar{A} \setminus \overline{X \setminus A}. \tag{9.189}$$

EQooOKINooXiFiUX

Démonstration. Soit $x \in X \setminus \text{Int}(A)$. Vu que x n'est pas dans l'intérieur de A, tout voisinage de x contient un point hors de A, c'est-à-dire un point de $X \setminus A$. Donc $x \in \overline{X \setminus A}$.

Dans l'autre sens si $x \in \overline{X \setminus A}$, tout voisinage de x contient un élément de $X \setminus A$. Donc x n'est pas dans $\text{Int}(A)$.

En ce qui concerne (9.189). Il suffit d'utiliser ce qu'on vient de faire :

$$\begin{aligned} \partial A &= \bar{A} \setminus \text{Int}(A) && \text{(9.190a)} \\ &= \bar{A} \cap \big(X \setminus \text{Int}(A)\big) && \text{(9.190b)} \\ &= \bar{A} \cap \overline{X \setminus A} && \text{(9.190c)} \end{aligned}$$

□

PROPooTHOPooCOGmZD

Proposition 9.185 ([1]).
Toute frontière est fermée. Plus précisément : si S est une partie de l'espace topologique X, nous avons :

ITEMooCIGTooOyNTYt

(1) $\partial S = \bar{S} \cap \overline{E \setminus S}$.

ITEMooCSHKooHibSre

(2) ∂S est fermée.

Démonstration. Pour (1), nous utilisons la proposition 9.21 : $\overline{X \setminus S} = X \setminus \text{Int}(S)$. Donc

$$\bar{S} \cap \overline{X \setminus S} = \bar{S} \cap \big(X \setminus \text{Int}(S)\big) = \bar{S} \setminus \text{Int}(S) = \partial(S). \tag{9.191}$$

Nous avons utilisé le lemme 1.46(4).

En ce qui concerne (2), ∂S est fermé en tant qu'intersection de deux fermés. □

PROPooKQXDooEnNJyn

Proposition 9.186 (frontière de l'union et de l'intersection[262]).
Soient des parties A et B d'un espace topologique X. Nous avons

$$\partial(A\cup B)\subset \partial A\cup\partial B \tag{9.192}$$

et

$$\partial(A\cap B)\subset \partial A\cup\partial B. \tag{9.193}$$

Démonstration. Voici le calcul pour l'union :

$$\begin{aligned}
\partial(A\cup B)&=\overline{A\cup B}\cap\big(\overline{X\setminus(A\cup B)}\big) && \text{prop. 9.184.} && (9.194a)\\
&=\overline{A\cup B}\cap\big(\overline{(X\setminus A)\cap(X\setminus B)}\big) && && (9.194b)\\
&\subset\overline{A\cup B}\cap\big(\overline{X\setminus A}\cap\overline{X\setminus B}\big) && \text{prop. 9.24.} && (9.194c)\\
&=\bar{A}\cup\bar{B}\cap\overline{(X\setminus A)}\cap\overline{(X\setminus B)} && && (9.194d)\\
&=\big(\bar{A}\cap\overline{X\setminus A}\big)\cup\big(\bar{B}\cap\overline{X\setminus A}\big)\cap\overline{X\setminus B} && && (9.194e)\\
&=\big(\partial A\cap\overline{X\setminus B}\big)\cup\big(\bar{B}\cap\overline{X\setminus A}\cap\overline{X\setminus B}\big) && \text{prop. 9.184} && (9.194f)\\
&=\big(\partial A\cap\overline{X\setminus B}\big)\cup\big(\partial B\cap\overline{X\setminus A}\big) && && (9.194g)\\
&\subset\partial A\cup\partial B. && && (9.194h)
\end{aligned}$$

Et le calcul pour l'intersection :

$$\begin{aligned}
\partial(A\cap B)&=\overline{A\cap B}\cap\overline{\big(X\setminus(A\cap B)\big)} && && (9.195a)\\
&=\overline{A\cap B}\cap\Big(\overline{(X\setminus A)\cup(X\setminus B)}\Big) && && (9.195b)\\
&=\overline{A\cap B}\cap\big(\overline{(X\setminus A)}\cup\overline{(X\setminus B)}\big) && \text{par (9.15)} && (9.195c)\\
&=\big(\overline{A\cap B}\cap\overline{X\setminus A}\big)\cup\big(\overline{A\cap B}\cap\overline{X\setminus B}\big) && && (9.195d)\\
&\subset\big(\bar{A}\cap\overline{X\setminus A}\big)\cup\big(\bar{B}\cap\overline{X\setminus B}\big) && && (9.195e)\\
&=\partial A\cup\partial B. && && (9.195f)
\end{aligned}$$

□

PROPooIIRLooIPdjqO

Proposition 9.187 ([1]).
Soient un espace topologique X ainsi que $A,B\subset X$. Soit $x\in\partial A$. Nous suppposons qu'il existe un voisinage ouvert V_0 de x tel que $V_0\cap B=\varnothing$. Alors $x\in\partial(A\cup B)$.

Démonstration. Vu que $x\in\partial A$, nous avons $x\in\bar{A}\subset\overline{A\cup B}$. Il nous reste à prouver que x n'est pas dans l'intérieur de $A\cup B$. Soit un voisinage ouvert W de x. La partie $W\cap V_0$ est un ouvert contenant x et tel que $W\cap V_0=\varnothing$. De plus, étant donné que $x\in\partial A$, il existe $s\in W\cap V_0$ tel que $s\notin A$. Donc $s\notin A\cup B$. Et par conséquent il n'existe pas de voisinage de x contenu dans $A\cup B$; autrement dit, x n'est pas dans l'intérieur de $A\cup B$. □

PROPooYHIGooMDVKNy

Proposition 9.188 ([1]).
Soit une partie S d'un espace topologique X. Soit un ouvert $A\subset S$. Si $A\cap\partial S=\varnothing$, alors $\bar{A}\subset S$.

LEMooEUYEooYcUfKr

Lemme 9.189 (Caractérisation équivalente de la frontière).
Soient X un espace topologique et $S\subset X$. Un point $x\in X$ est dans ∂S si et seulement si tout voisinage de x contient un point de S et un point de S^c.

Démonstration. Supposons que tout voisinage de x contienne un point de S et un point de S^c. Alors $x\in Adh(S)$ (définition 9.19), mais pas dans l'intérieur de S parce que x ne possède pas de voisinage contenu dans S. Donc $x\in\partial S$.

À l'inverse, si $x\in\partial S$ alors x est dans l'adhérence de S et tout voisinage de x contient un point de S. Mais x n'est pas dans l'intérieur de S et tout voisinage de x contient un point qui n'est pas dans S, aka un point de S^c. □

Corolaire 9.190.
Un ensemble et son complémentaire ont même frontière.

Démonstration. Conséquence du lemme 9.189. Les points de $\partial(S^c)$ sont caractérisés par le fait que tout voisinage contient un point de S^c et un point de $(S^c)^c=S$. □

Exemple 9.191.
Soit $X = [0, 1]$ muni de la topologie de la distance $|x - y|$ (définition 9.158). Les points 0 et 1 *ne sont pas* dans la frontière de X. En effet une boule ouverte autour de 1 est un ensemble de la forme

$$B(1, r) = \{x \in X \text{ tel que } |x - 1| < r\} =]1 - r, 1] \tag{9.196}$$

où nous avons supposé $r < 1$.

Les points 0 et 1 sont par contre sur la frontière de $[0, 1]$ lorsque cet ensemble est vu comme partie de l'espace métrique $\mathbb{R}$. △

LEMooLKWEooItGnkP

Lemme 9.192 (Passage de douane[263, 264])**.**
Dans un espace topologique, toute partie connexe qui rencontre à la fois une partie A et son complémentaire rencontre nécessairement la frontière de A.

Démonstration. Nommons C la partie connexe qui intersecte A et A^c. Les ouverts $\text{Int}(A)$ et $X \setminus \bar{A}$ ne peuvent pas recouvrir C parce que ce sont deux ouverts disjoints alors que C est connexe (voir la définition 9.118 de la connexité). Donc C doit contenir des points qui sont dans $\bar{A}$ mais pas dans $\text{Int}(A)$. C'est-à-dire des points de ∂A. □

On vérifiera que les notations et les dénominations sont cohérentes en prouvant la proposition suivante.

Proposition 9.193.
Pour $\epsilon > 0$,

(1) l'adhérence de $B(x, \epsilon)$ est $\bar{B}(x, \epsilon)$,

(2) l'intérieur de $\bar{B}(x, \epsilon)$ est $B(x, \epsilon)$,

(3) la boule ouverte $B(x, \epsilon)$ est un ouvert,

(4) la boule fermée $\bar{B}(x, \epsilon)$ est un fermé.

Nous avons également les liens suivants entre intérieur, adhérence, ouvert, fermé et passage au complémentaire (noté ^{c}) :

Proposition 9.194.
Si $A \subset \mathbb{R}^n$ et $A^c = \mathbb{R}^n \setminus A$, nous avons

(1) $(\text{Int}\, A)^c = \text{Adh}(A^c)$ et $(\text{Adh}\, A)^c = \text{Int}(A^c)$,

(2) A est ouvert si et seulement si A^c est fermé,

(3) $\text{Int}\, A$ est le plus grand ouvert contenu dans A,

(4) $\text{Adh}\, A$ est le plus petit fermé contenant A,

ExBFLooUNyvbw

Exemple 9.195.
Il n'est en général pas vrai que $\overline{A \cap B} = \bar{A} \cap \bar{B}$. Par exemple si $A = [0, 1[$ et $B =]1, 2]$. Dans ce cas, $A \cap B = \varnothing$ alors que $\bar{A} \cap \bar{B} = \{1\}$. △

9.9.8 Boules ouvertes, fermées, sphères

DEFooPDSJooFcUqKH

Définition 9.196.
Soit un espace métrique[77] *(E, d).*

*(1) Nous nommons **boule fermée** la fermeture de la boule ouverte, c'est-à-dire les parties de la forme $\overline{B(a, r)}$.*

*(2) La **sphère** de centre $a \in E$ et de rayon $r \in \mathbb{R}^+$ est la frontière*[78] *de la boule : $S(a, r) = \partial B(a, r)$.*

9.197.
Les différences entre boules ouverts, fermées et sphères sont très importantes. D'abord, les *boules* sont pleines tandis que la *sphère* est creuse. En comparant à une pomme, la boule ouverte serait la pomme « sans la peau », la boule fermée serait « avec la peau » tandis que la sphère serait seulement la peau.

[77] Définition 9.155.
[78] Frontière, définition 9.181.

9.9.9 Espace localement compact

DefEIBYooAWoESf

Définition 9.198.
*Un espace topologique est **localement compact** si tout élément possède un voisinage compact.*

LEMooAXESooYvyesg

Lemme 9.199.
Si X est un espace topologique localement compact et si K est compact dans X, il existe un ouvert V tel que $K \subset V$ et $\bar{V}$ est compact.

Démonstration. Pour chaque $x \in K$ nous considérons un voisinage compact L_x. Nous considérons un ouvert A_x dans L_x contenant x. Vu que les A_x recouvrent K, nous avons un sous-recouvrement fini, c'est-à-dire un choix de $\{x_1, \dots, x_n\}$ tels que

$$K \subset \bigcup_{i=1}^{n} A_{x_i}. \tag{9.197}$$

En posant $V = \bigcup_{i=1}^{n} A_{x_i}$ nous avons un ouvert qui vérifie $K \subset V$.

Montrons que V est compacte.

En tant qu'union finie de compacts, la partie $L = \bigcup_{i=1}^{n} L_{x_i}$ est compacte. Étant donné que X est séparé, L est fermé (lemme 9.137(2)). Par ailleurs $\bar{V}$ est l'intersection de tous les fermés contenant V (lemme 9.20(2)). Donc $\bar{V} \subset L$. La partie $\bar{V}$ est donc un fermé dans un compact. Elle est donc compacte par le lemme 9.137(1). □

PROPooACXGooHcQpxF

Proposition 9.200 ([2, 1])**.**
Soient un espace topologique X séparé et localement compact, un ouvert U et $x \in U$. Il existe un voisinage ouvert V de x tel que

(1) $\bar{V}$ soit compact,

(2) $\bar{V} \subset U$.

Démonstration. Vu que X est localement compact, nous considérons un voisinage compact K de x. Plus précisément, nous considérons un ouvert A et un compact K tels que

$$x \in A \subset K. \tag{9.198}$$

Vu que U est ouvert, $X \setminus U$ est fermé et donc

$$K \setminus U = K \cap (X \setminus U) \tag{9.199}$$

est fermé dans le compact K et est donc compact[79].

Deux possibilités : $K \setminus U$ est vide ou non.

(1) **Si $K \setminus U = \varnothing$** Dans ce cas $K \subset U$. En posant $V = A$ on est bon parce que

$$\bar{V} = \bar{A} \subset K \subset U. \tag{9.200}$$

Notez que $\bar{A}$ est l'intersection de tous les fermés contenant A. C'est pour ça que $\bar{A} \subset K$.

De plus $\bar{V}$ est compact en tant que fermé dans le compact K.

(2) **Si $K \setminus U \neq \varnothing$** Donc $K \setminus U$ est un compact qui ne contient pas x. Vu que les ouverts séparent les points et les compacts (lemme 9.148), nous avons des ouverts disjoints V_0 autour de x et W autour de $K \setminus U$ tels que $V_0 \cap W = \varnothing$. Nous posons

$$V = V_0 \cap A. \tag{9.201}$$

C'est encore un ouvert comme intersection d'ouverts. Nous avons

$$V \subset A \subset K. \tag{9.202}$$

Prouvons que $\bar{V} \subset U$. Pour cela nous supposons par l'absurde que $y \in \bar{V}$ avec $y \notin U$. Donc

$$y \in K \setminus U \subset W \tag{9.203}$$

Mais V et W sont des ouverts d'intersection vide, donc $\bar{V} \cap W$ est également vide (proposition 9.23). Donc $y \in W$ n'est pas possible. Contradiction. Nous en déduisons que $\bar{V} \subset U$.

Encore une fois $\bar{V}$ est compact parce que $V \subset K$.

[79] Nous avons utilisé 9.137 deux fois : une fois pour dire que K est fermé et une fois pour dire qu'un fermé dans un compact est compact.

□

PROPooAXUEooQxRGmr

Proposition 9.201 ([1]).
Soient des ouverts disjoints U et V d'un espace topologique. Alors

$$U \cap \overline{V} = \varnothing \tag{9.204a}$$
$$\bar{U} \cap V = \varnothing \tag{9.204b}$$

Démonstration. Soit $x \in U$. Étant donné que U est ouvert, nous avons un voisinage ouvert A de x tel que $A \subset U$. Un tel voisinage n'intersecte donc pas V. Donc $x \notin \bar{V}$. □

LEMooKYMKooPxZjWN

Lemme 9.202 ([1, 2]).
Soient un espace topologique séparé localement compact X, un compact K et un ouvert U tel que $K \subset U$. Il existe un ouvert V tel que

(1) $\bar{V}$ est compact,

(2) $K \subset V \subset \bar{V} \subset U$.

Démonstration. Pour chaque $x \in K$ la proposition 9.200 nous permet de considérer un ouvert V_x tel que $\bar{V}_x$ est compact et $\bar{V}_x \subset U$. Compactité, sous-recouvrement fini, tout ça, bref on a $x_1, \dots, x_n \in K$ tels que en posant $V_i = V_{x_i}$, et

$$V = \bigcup_{i=1}^{n} V_i, \tag{9.205}$$

on ait $K \subset V$. La proposition 9.24 nous dit que

$$\bar{V} = \bigcup_{i=1}^{n} \bar{V}_i. \tag{9.206}$$

En tant qu'union finie de compacts, $\bar{V}$ est compacte par le lemme 9.140. De plus pour tout $x \in K$ nous avons $\bar{V}_x \subset U$. Donc $\bar{V} \subset U$. □

PROPooVLOZooLlYNNa

Proposition 9.203 ([265, 266, 267]).
Soit un espace topologique séparé X. Les faits suivants sont équivalents :

ITEMooZLNUooHcTakl

(1) X est localement compact[80].

ITEMooYMKMooUkcNzd

(2) Tout éléments de X a un voisinage compact.

ITEMooXYYHooTCZMJr

(3) Tout point de X possède une base de voisinages formés d'ouverts à fermeture compactes.

ITEMooBTECooDDsTuo

(4) Tout point de X possède un voisinage ouvert à fermeture compacte.

Démonstration. Nous avons (1) ⇔ (2) parce que c'est la définition de localement compact. À part ça, on va faire un plusieurs parties.

(1) **(2) ⇒ (4)** Soit $X \in X$. Par (2) nous avons un ouvert A et un compact K tels que $x \in A \subset K$. La partie $\bar{A}$ est un fermé dans le compact K et est donc compacte par le lemme 9.137(1).

(2) **(4) ⇒ (2)** Soit $x \in X$. Si A est le voisinage ouvert à fermeture compacte, alors $\bar{A}$ est un voisinage compact.

(3) **(2) ⇒ (3)** Soit un ouvert U contenant x. Nous allons montrer qu'il existe un ouvert A autour de x tel que $\bar{A}$ est compact et $A \subset U$. Soit un point $x \in X$. Par (2), il possède un voisinage compact K.

Nous considérons la frontière $\partial(U \cap K)$. C'est une partie fermée de X par la proposition 9.185(2). Et comme $\partial(U \cap K)$ est contenu dans K, il est un fermé dans un compact. Donc $\partial(U \cap K)$ est compact.

Si $y \in \partial(U \cap K)$, alors $y \neq x$ parce que U est un ouvert et n'intersecte pas sa frontière[81]. Étant donné que X est séparé, pour chaque $y \in \partial(U \cap K)$, nous trouvons des voisinages ouverts V_y de y et W_y de x tels que $V_y \cap W_y = \varnothing$.

[80] Définition 9.198.
[81] Proposition 9.183.

Notons que $K \cap U$ contient un ouvert autour de x parce que K en contient un et que U en est un. Nous pouvons donc choisir $W_y \subset K \cap U$. L'ensemble de parties $\{V_y\}_{y\in\partial(U\cap K)}$ est un recouvrement du compact $\partial(U \cap K)$ par des ouverts. Nous pouvons donc choisir $y_1, \dots, y_n \in \partial(U \cap K)$ tel que

$$\partial(U \cap K) \subset \bigcup_{k=1}^{n} V_{y_k}. \tag{9.207}$$

Donc $A = W_{y_1} \cap \dots \cap W_{y_n}$ est un voisinage de x qui :

(3a) est inclut dans $U \cap K$,

(3b) n'intersecte aucun des V_{y_i},

(3c) n'intersecte donc pas $\partial(U \cap K)$.

La proposition 9.188 dit que la fermeture $\bar{A} = \overline{W_{y_1} \cap \dots \cap W_{y_n}}$ est encore dans $U \cap K$. Et comme $U \cap K$ est compact, nous déduisons que $\bar{A}$ est compact.

(4) **(3) ⇒ (4)** Si on a une base de voisinages, à fortiori, on a un voisinage.

□

9.9.10 Compactifié d'Alexandrov

PROPooHNOZooPSzKIN

Proposition-Définition 9.204 ([268]).
Soit un espace topologique séparé localement compact[82] X. *Nous considérons un élément* $\omega \notin X$ *et l'ensemble* $\hat{X} = X \cup \{\omega\}$. *Nous nommons « ouverts de* $\hat{X}$ *» les parties suivantes :*

- *les ouverts de* X,
- *les parties de la forme* $A \cup \{\omega\}$ *avec* $X \setminus A$ *compact dans* X.

Alors $\hat{X}$ *est un espace topologique compact (cela justifie le nom « ouvert » donné aux parties sus-définies).*

Démonstration. La première chose à faire est de prouver que $\hat{X}$ est bien un espace topologique (définition 9.1). Nous notons τ la topologie sur X et $\hat{\tau}$ l'ensemble des « ouverts » de $\hat{X}$. Le but est de prouver que $\hat{\tau}$ est une topologie.

(1) **L'espace lui-même** $\hat{X} \in \hat{\tau}$ parce que $\hat{X} = X \cup \{\omega\}$ et que $X \setminus X = \varnothing$ est compact.

(2) **Le vide** $\varnothing \in \tau \subset \hat{\tau}$.

(3) **Union quelconque** Soient A_i $(i \in I)$ des éléments de $\hat{\tau}$. Nous posons $I_1 = \{i \in I \text{ tel que } A_i \subset X\}$ et $I_2 = I \setminus I_1$. Nous avons

$$\bigcup_{i\in I} A_i = \big(\bigcup_{i\in I_1} A_i\big) \cup \big(\bigcup_{i\in I_2} A_i\big) = B \cup \big(\bigcup_{i\in I_2} B_i \cup \{\omega\}\big) \tag{9.208}$$

où B et les B_i sont des ouverts de X tels que $X \setminus B_i$ est compact dans X. Nous récrivons ça sous la forme

$$\bigcup_{i\in I} A_i = B \cup \big(\bigcup_{i\in I_2} B_i\big) \cup \{\omega\}. \tag{9.209}$$

La question est de savoir si

$$X \setminus \Big(B \cup \big(\bigcup_{i\in I_2} B_i\big)\Big) \tag{9.210}$$

est compact dans X. Un peu de réécriture :

$$X \setminus \Big(B \cup \big(\bigcup_{i\in I_2} B_i\big)\Big) = (X \setminus B) \cap X \setminus \big(\bigcup_{i\in I_2} B_i\big) = (X \setminus B) \cap \big(\bigcap_{i\in I_2} (X \setminus B_i)\big). \tag{9.211}$$

La partie $X \setminus B$ est fermée dans X parce que B est ouverte. La proposition 9.141 dit qu'une intersection de compacts est compacte (parce que X est séparé). Nous sommes donc en présence de l'intersection entre un compact et un fermé.

Tout compact d'un espace séparé est fermé[83]. Donc nous sommes en présence de l'intersection de deux fermés. Donc $(X \setminus B) \cap \big(\bigcap_{i\in I_2}(X \setminus B_i)\big)$ est fermé. Mais c'est contenu dans le compact $\bigcap_{i\in I_2}(X \setminus B_i)$. Fermé dans un compact, donc compact (lemme 9.137).

[82] Définition 9.198.
[83] Lemme 9.137(2).

(4) **Intersection finie** Nous considérons les « ouverts » $(A_i)_{i=1,\dots,n}$ de $\hat{X}$. Si ce sont tous des ouverts de X, l'intersection est un ouvert de X et on est bon.

Supposons que tous les A_i soient de la forme $A_i = B_i \cup \{\omega\}$ avec $X \setminus B_i$ compact. Alors

$$\bigcap_{i=1}^{n}(B_i \cup \{\omega\}) = \left(\bigcap_{i=1}^{n} B_i\right) \cup \{\omega\} \tag{9.212}$$

Mais le lemme 1.46 (appliqué un nombre fini de fois) donne

$$X \setminus \left(\bigcap_{i=1}^{n} B_i\right) = \bigcup_{i=1}^{n}(X \setminus B_i) \tag{9.213}$$

qui est compact en tant qu'union finie de compacts[84].

Enfin, nous supposons que les A_i sont un mélange des deux types, nous les séparons entre ceux qui sont directement des ouverts de X et les autres :

$$A_i = \begin{cases} B_i & \text{si } i \leqslant q \\ C_i \cup \{\omega\} & \text{si } q < i \leqslant n \end{cases} \tag{9.214}$$

où B_i sont ouverts et C_i sont des parties de X telles que $X \setminus C_i$ est compacte.

Nous avons

$$\bigcap_{i=1}^{n} A_i = \left(\bigcap_{i=1}^{q} B_i\right) \cap \left(\bigcap_{i=q+1}^{n} (C_i \cup \{\omega\})\right) \tag{9.215a}$$

$$= B \cap \left(\bigcap_{i=q+1}^{n} C_i\right). \tag{9.215b}$$

Justifications.

- Nous avons posé B est l'intersection des B_i.
- Vu que ω n'est pas dans B, nous pouvons l'oublier dans les $C_i \cup \{\omega\}$.

C'est le moment d'étudier $E = \bigcap_{i=q+1}^{n} C_i$. Nous avons

$$X \setminus E = X \setminus \left(\bigcap_{i=q+1}^{n} C_i\right) = \bigcup_{i=q+1}^{n} (X \setminus C_i). \tag{9.216}$$

Vu que $X \setminus C_i$ est compact, il est fermé[85]. La partie $X \setminus E$ est donc fermée comme union finie de fermés[86]. Et donc E est ouvert. Et finalement

$$\bigcap_{i=1}^{n} A_i = B \cap E \tag{9.217}$$

est un ouvert de X comme intersection d'ouverts. C'est donc aussi un ouvert de $\hat{X}$.

Nous avons fini de prouver que $(\hat{X}, \hat{\tau})$ est un espace topologique. Nous montrons à présent que $\hat{X}$ est compact.

Soit $\{A_i\}_{i\in I}$ un recouvrement de $\hat{X}$ par des ouverts. Pour au moins un $i_0 \in I$ nous avons $\omega \in A_{i_0}$. Nous posons $A_{i_0} = B \cup \{\omega\}$ avec $X \setminus B$ compact dans X.

Les ouverts $\{A_i\}_{i\in I}$ forment un recouvrement de $X \setminus B$ par des ouverts. Nous pouvons en extraire un sous-recouvrement fini :

$$X \setminus B \subset \bigcup_{i\in I_1} A_i. \tag{9.218}$$

Nous avons alors

$$\hat{X} \subset \bigcup_{i\in I_1\cup\{i_0\}} A_i. \tag{9.219}$$

EQooJQFMopKPXLkb

Et voilà que $\hat{X}$ est recouvert par un nombre fini des A_i. Notez que (9.219) est une égalité, mais nous n'en avons pas besoin. □

[84] Lemme 9.140.
[85] Par le lemme 9.137(2) et le fait que nous considérons un espace séparé.
[86] Par le lemme 9.6(2).

9.205.
Oh bien entendu, les plus férus de questions embarrassantes demanderont, si X est l'espace considéré, où prendre ce ω ? Quel « objet » existe en-dehors de X ? Qui m'assure que X n'est pas tellement grand que tout est dedans ? Le fait est qu'il n'existe pas d'ensemble contenant tous les ensembles (c'est le corolaire 1.90). Nous pouvons donc toujours trouver un ensemble ω qui n'est pas dans X.

En ce qui concerne $\mathbb{R}$ auquel nous pouvons attacher deux infinis ($+\infty$ et $-\infty$), ce sera la définition 14.26. Pour $\mathbb{C}$, nous donnerons une caractérisation de la limite en ∞ dans le lemme 14.87.

9.9.11 Continuité séquentielle

PropFnContParSuite

Corolaire 9.206 (Caractérisation séquentielle de la continuité en un point[1])**.**
Une application entre deux espaces topologiques continue en un point y est séquentiellement[87] *continue.*

Démonstration. Soit une application $f\colon X \to Y$ entre les espaces topologiques X et Y. Nous supposons que f est continue en $a \in X$. Soit une suite convergente $x_k \xrightarrow{X} a$. Nous devons prouver que $f(x_k) \to f(a)$.

Soit un voisinage V de $f(a)$ dans Y. Le fait que f soit continue en a signifie[88] que $f(a)$ est une limite de f en a, c'est-à-dire[89] qu'il existe un voisinage W de a tel que $f(W \setminus \{a\}) \subset V$.

Puisque $x_k \to a$, il existe N tel que $x_k \in W$ pour tout $k \geqslant N$. Pour ces valeurs de k, nous avons $f(x_k) \in V$.

Nous avons prouvé que pour tout voisinage V de $f(a)$ dans Y, il existe N tel que $f(x_k) \in V$ dès que $k \geqslant N$. Cela signifie exactement que $f(x_k) \to f(a)$. □

9.9.11.1 Les boules, une base de topologie

PropNBSooraAFr

Proposition 9.207.
Un espace métrique séparable[90] *accepte une base de topologie*[91] *dénombrable.*

Soit A dense et dénombrable dans l'espace métrique séparable (E, d). Si $\{a_i\}_{i\in\mathbb{N}}$ est une énumération de A et $\{r_i\}_{i\in\mathbb{N}}$ une énumération de $\mathbb{Q}$, alors

$$\mathcal{B} = \{B(a_i, r_j)\}_{i,j\in\mathbb{N}} \tag{9.220}$$

est une base de la topologie[92] *de E.*

Démonstration. Soient $x \in E$ et V un voisinage de x. Ce dernier contient une boule $B(x, r)$ et quitte à prendre r un peu plus petit nous supposons que $r \in \mathbb{Q}$ (existence d'un tel rationnel par le lemme 4.60).

Soit $a \in A$ avec $\|a - x\| < \frac{r}{3}$ (existe par densité de A dans E) ; nous avons $B(a, \frac{2r}{3}) \subset B(x, r)$ parce que si $y \in B(a, \frac{2r}{3})$ alors

$$\|y - x\| \leqslant \|y - a\| + \|a - x\| < \frac{2}{3}r + \frac{1}{3}r = r. \tag{9.221}$$

La seconde inégalité est stricte parce que les boules sont ouvertes. Le tout montre que $y \in B(x, r)$. Par ailleurs $x \in B(a, \frac{2}{3}r)$ et nous avons trouvé un élément de $\mathcal{B}$ contenant x tout en étant inclus dans V. Cela prouve que $\mathcal{B}$ est bien une base de la topologie de E. □

RemIPVLooHUXyeW

Remarque 9.208.
Il est vite vu que les cubes ouverts forment aussi une base de la topologie de $\mathbb{R}^n$. Cela est à mettre en rapport avec le fait que toutes les normes sont équivalentes sur $\mathbb{R}^n$ (proposition 12.70).

Voir aussi le corolaire 16.276 qui donnera tout ouvert comme union de pavés presque disjoints.

DefEnsembleBorne

Définition 9.209.
*Soit (X, d) un espace métrique. Un sous-ensemble $A \subset X$ est **borné** si il existe une boule de X contenant A.*

PROPooJIOAooWqzKMu

Proposition 9.210.
Toute réunion finie de parties bornés est bornée. Toute partie d'un ensemble borné est un ensemble borné.

[87] Définition 9.166.
[88] C'est la définition 9.48 de la continuité en un point.
[89] Définition 9.151 d'une limite.
[90] Qui possède une partie dense dénombrable, définition 9.80.
[91] Base de topologie, définition 9.2.
[92] Définition 9.2.

Démonstration. Soient des parties bornées $\{A_i\}_{i=1,\dots,n}$. Si m_i est un majorant de A_i, alors $M = \max\{m_i\}_{i=1,\dots,n}$ est un majorant de $\bigcup_{i=1}^n A_i$. Notons que M est bien défini par le lemme 2.31.

Pour la seconde affirmation, si A est borné (notons m un majorant de A) et si $B \subset A$, alors m est un majorant de B. □

9.9.12 Continuité et compacité

Un résultat important dans la théorie des fonctions sur les espaces vectoriels normés est qu'une fonction continue sur un compact est bornée et atteint ses bornes. Ce résultat sera énormément utilisé pour trouver des maximums et minimums de fonctions. Le théorème exact est le suivant.

LemQFXOWyx

Lemme 9.211 (de Lebesgue[269])**.**
Soit (X, d) un espace métrique tel que toute suite ait une sous-suite convergente à l'intérieur de l'espace. Si $\{V_i\}$ est un recouvrement par des ouverts de X, alors il existe ϵ tel que pour tout $x \in X$, nous ayons $B(x, \epsilon) \subset V_i$ pour un certain i.

Démonstration. Par l'absurde, nous supposons que pour tout n, il existe un $x_n \in X$ tel que la boule $B(x_n, \frac{1}{n})$ n'est contenue dans aucun des V_i. De ces x_n, nous extrayons une sous-suite convergente (que nous nommons encore (x_n)) et nous posons $x_n \to x$. Pour n assez grand ($\frac{1}{n} < \epsilon$) nous avons $x_n \in B(x, \epsilon)$, donc tous les x_n suivants sont dans le V_i qui contient x. □

LemMGQqgDG

Lemme 9.212 ([269])**.**
Soit (X, d) un espace métrique tel que toute suite possède une sous-suite convergente. Pour tout $\epsilon > 0$, il existe un ensemble fini $\{x_i\}_{i\in I}$ tel que les boules $B(x_i, \epsilon)$ recouvrent X.

Démonstration. Soit par l'absurde un $\epsilon > 0$ contredisant le lemme. Il n'existe pas de parties finies de X autour des points desquels les boules de taille ϵ recouvrent X.

Nous construisons par récurrence une suite ne possédant pas de sous-suite convergente. Le premier terme, x_0 est pris arbitrairement dans X. Ensuite si nous avons déjà N termes de la suite, nous savons que les boules de rayon ϵ centrées sur les points $\{x_i\}_{i=1,\dots,N}$ ne recouvrent pas X. Donc nous prenons x_{N+1} hors de l'union de ces boules.

Ainsi nous avons une suite (x_n) dont tous les termes sont à distance plus grande que ϵ les uns des autres. Une telle suite ne peut pas contenir de sous-suite convergente. Contradiction. □

ThoBWFTXAZNH

Théorème 9.213 (Bolzano-Weierstrass[269], thème 33)**.**
Un espace métrique est compact si et seulement si toute suite admet une sous-suite qui converge à l'intérieur de l'espace.

Démonstration. Soient X un espace métrique compact et (x_n) une suite dans X. Nous considérons la suite de fermés emboîtés

$$X_n = \overline{\{x_k \text{ tel que } k > n\}}. \tag{9.222}$$

Ce sont des fermés ayant la propriété d'intersection finie non vide, et donc la proposition 9.133 nous dit qu'ils ont une intersection non vide. Un élément de cette intersection est automatiquement un point d'accumulation de la suite[93].

Nous passons à l'autre sens. Nous supposons que toute suite dans X contient une sous-suite convergente, et nous considérons $\{V_i\}_{i\in I}$, un recouvrement de X par des ouverts. Par le lemme 9.211, nous considérons un ϵ tel que pour tout x, il existe un $i \in I$ avec $B(x, \epsilon) \subset V_i$. Par le lemme 9.212, nous considérons un ensemble fini $\{y_i\}_{i\in A}$ tel que les boules $B(y_i, \epsilon)$ recouvrent X.

Par construction, chacune de ces boules $B(y_i, \epsilon)$ est contenue dans un des ouverts V_i. Nous sélectionnons donc parmi les V_i le nombre fini qu'il faut pour recouvrir les $B(y_i, \epsilon)$ et donc pour recouvrir X. □

ExEFYooTILPDk

Exemple 9.214 (Non compacité de la boule unité en dimension infinie)**.**
Le théorème de Bolzano-Weierstrass permet de voir tout de suite que la boule unité n'est pas compacte dans un espace vectoriel de dimension infinie : la suite des vecteurs de base ne possède pas de sous-suite convergente. △

Le théorème de Bolzano–Weierstrass 9.213 a l'importante conséquence suivante.

ThoWeirstrassRn

Théorème 9.215 (Weierstrass)**.**
Une fonction continue à valeurs réelles définie sur un compact est bornée et atteint ses bornes.

[93] Définition 9.46.

Démonstration. Soient K un compact et $f\colon K \to \mathbb{R}$ une fonction continue. Nous désignons par A l'ensemble des valeurs prises par f sur K :

$$A = f(K) = \{f(x) \text{ tel que } x \in K\}. \tag{9.223}$$

Nous considérons le supremum $M = \sup A = \sup_{x\in K} f(x)$ avec la convention suivante : si A n'est pas borné supérieurement, nous posons $M = \infty$ (voir définition 4.85).

Nous allons maintenant construire une suite (x_n) de deux façons différentes selon que $M = \infty$ ou non.

(1) Si $M = \infty$, nous choisissons, pour chaque $n \in \mathbb{N}$, un $x_n \in K$ tel que $f(x_n) > n$. C'est certainement possible parce que si A n'est pas borné, nous pouvons y trouver des nombres aussi grands que nous voulons.

(2) Si $M \neq \infty$, nous savons que pour tout ε, il existe un $y \in A$ tel que $y > M - \varepsilon$. Pour chaque n, nous choisissons donc $x_n \in K$ tel que $f(x_n) > M - \frac{1}{n}$.

Quel que soit le cas dans lequel nous sommes, la suite (x_n) est une suite dans K qui est compact, et donc nous pouvons en extraire une sous-suite convergente à l'intérieur de K par le théorème de Bolzano-Weierstrass 9.213. Afin d'alléger la notation, nous allons noter (x_n) la sous-suite convergente. Nous avons donc

$$x_n \to x \in K. \tag{9.224}$$

Par la proposition 9.206, nous savons que f prend en x la valeur

$$f(x) = \lim_{n\to\infty} f(x_n). \tag{9.225}$$

Donc $f(x) < \infty$. Évidemment, si nous avions été dans le cas où $M = \infty$, la suite x_n aurait été choisie pour avoir $f(x_n) > n$ et donc il n'aurait pas été possible d'avoir $\lim_{n\to\infty} f(x_n) < \infty$. Nous en concluons que $M < \infty$, et donc que f est bornée sur K.

Afin de prouver que f atteint sa borne, c'est-à-dire que $M \in A$, nous considérons les inégalités

$$M - \frac{1}{n} < f(x_n) \leqslant M. \tag{9.226}$$

En passant à la limite $n \to \infty$, ces inégalités deviennent

$$M \leqslant f(x) \leqslant M, \tag{9.227}$$

et donc $f(x) = M$, ce qui prouve que f atteint sa borne M au point $x \in K$. □

LEMooQLVAooICaPvR

Lemme 9.216 ([1]).
Soient des compacts A, B et une fonction continue $f\colon A \times B \to \mathbb{R}$. Alors

$$\sup_{(x,y)\in A\times B} |f(x,y)| = \sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big). \tag{9.228}$$

Démonstration. Pour chaque $x \in A$, la fonction $f_x\colon B \to \mathbb{R}$ donnée par $f_x(y) = |f(x,y)|$ est continue et atteint donc sa borne[94] en $y_M(x)$. Notons que cela ne définit pas de façon univoque $y_M(x)$ parce que f_x peut atteindre son maximum en plusieurs points. L'important est que pour tout x, le nombre $|f\big(x, y_M(x)\big)|$ ne dépend pas du choix de $y_M(x)$ parmi les y qui réalisent le maximum.

Notons (x_0, y_0) un point de $A \times B$ sur lequel $|f|$ réalise son maximum[95] :

$$\sup_{(x,y)\in A\times B} |f(x,y)| = |f(x_0,y_0)|. \tag{9.229}$$

EQooDDXDooVanlKG

Nous avons d'une part

$$\sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big) = \sup_{x\in A}|f\big(x,y_M(x)\big)| \leqslant |f(x_0,y_0)| \tag{9.230}$$

Et d'autre part, quelques calculs avec justifications en-dessous :

SUBEQooPYJPooBJyEgN

$$\begin{aligned}
\sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big) &\leqslant \sup_{x\in A}\sup_{y\in B}|f(x_0,y_0)| && \text{(9.231a)}\\
&= |f(x_0,y_0)| && \text{(9.231b)}\\
&\leqslant |f\big(x_0,y_M(x_0)\big)| && \text{(9.231c)}\\
&\leqslant \sup_{x\in A}|f\big(x,y_M(x)\big)| && \text{(9.231d)}\\
&\leqslant \sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big). && \text{(9.231e)}
\end{aligned}$$

SUBEQooAKPQooPdkyMJ
SUBEQooDYVPooUsQpfD
SUBEQooVOEAooNtzSpt

Justifications.

[94] Théorème 9.215.
[95] Encore une fois, ce point n'est pas déterminé de façon unique par cette propriété.

- Pour (9.231a). Le point (x_0, y_0) est un maximum de $|f|$.
- Pour (9.231c). y_M est définie pour maximiser, en fonction de x, la quantité $|f(x, y_M(x))|$.
- Pour (9.231d). Au lieu de conserver la valeur x_0 fixé, nous prenons le maximum sur tous les x possibles.

Vu que les premiers et derniers termes des inégalités (9.231) sont égaux, toutes les inégalités sont en réalité des égalités. En particulier, en reprenant (9.229),

$$\sup_{(x,y)\in A\times B} |f(x,y)| = |f(x_0,y_0)| = \sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big). \tag{9.232}$$

□

9.9.13 Distance à un ensemble

DEFooGNNUooFUZINs

Définition 9.217.
Si A est une partie de l'espace métrique (X, d), et si $b \in X$, nous définissons

$$d(b, A) = \inf_{y\in A} d(b, y). \tag{9.233}$$

LEMooEQIZooLpsbOe

Lemme 9.218 ([1]).
Soit un fermé F de l'espace métrique (X, d). Si $a \in X$ vérifie $d(a, F) = 0$, alors $a \in F$.

Démonstration. Supposons que $d(a, F) = 0$, c'est-à-dire que $\inf_{x\in F} d(a, x) = 0$. Il existe donc une suite (x_k) dans F telle que $d(a, x_k) \to 0$.

Cela signifie que $x_k \xrightarrow{(X,d)} a$. La proposition 9.84 nous dit alors que $a \in F$. □

Exemple 9.219 (Pas avec un ouvert).
En prenant l'ouvert $A =]0, 1[$ dans $\mathbb{R}$ nous avons $d(0, A) = 0$, alors que 0 n'est pas dans A. △

LEMooJNRTooZyKiFC

Lemme 9.220 ([1]).
Soient un espace métrique (X, d) ainsi qu'une partie $A \subset X$. Soit $r > 0$. La partie

$$\mathcal{O} = \{x \in X \text{ tel que } d(x, A) < r\} \tag{9.234}$$

est ouverte.

Démonstration. Soit $y \in \mathcal{O}$; nous avons $d(y, A) < r$. Autrement dit,

$$\inf_{a\in A} d(y, a) < r \tag{9.235}$$

et donc il existe $a \in A$ tel que $d(y, a) < r$. Soit $\delta = d(y, a) < r$. Nous montrons à présent que $B(y, r - \delta)$ est dans $\mathcal{O}$. En effet si $z \in B(y, r - \delta)$, alors

$$d(z, a) \leqslant d(z, y) + d(y, a) < r - \delta + \delta = r. \tag{9.236}$$

□

PROPooTXYMooDGnfKB

Proposition 9.221 (Inégalité triangulaire point-partie[270]).
Soit un espace métrique[96] (X, d) et soit une partie non vide $A \subset X$. Pour tout $x, y \in A$ nous avons :

$$d(x, A) \leqslant d(x, A) + d(x, y) \tag{9.237}$$

Démonstration. Par l'inégalité triangulaire pour tout $a \in A$ nous avons $d(x, a) \leqslant d(x, y) + d(y, a)$ et en arrangeant :

$$d(y, a) \geqslant d(x, a) - d(x, y). \tag{9.238}$$

Et maintenant on peut calculer deux secondes :

$$\begin{aligned} d(y, A) &= \sup_{a\in A} d(y, a) && \text{(9.239a)}\\ &\geqslant \sup_{a\in A}\big(d(x, a) - d(x, y)\big) && \text{(9.239b)}\\ &= \big(\sup_{a\in A} d(x, a)\big) - d(x, y) && \text{(9.239c)}\\ &= d(x, A) - d(x, y). && \text{(9.239d)} \end{aligned}$$

□

[96] Espace métrique, définition 9.155.

LEMooCFGTooIfdcfk

Lemme 9.222 ([1, 271]).
Soit une partie A de l'espace métrique (X, d). Alors

ITEMooDXSHooPhCXlR

(1) Pour tout $x, y \in X$ nous avons

$$|d(x, A) - d(y, A)| \leqslant d(x, y). \tag{9.240}$$

ITEMooGNSEooDVZrFp

La fonction

$$\begin{aligned} f\colon X &\to [0, \infty[\\ x &\mapsto d(x, A) \end{aligned} \tag{9.241}$$

est continue.

Démonstration. Nous utilisons l'inégalité triangulaire point-partie 9.221. D'abord $d(x, A) \leqslant d(x, y) + d(y, A)$ que nous récrivons

$$d(x, A) - d(y, A) \leqslant d(x, y). \tag{9.242}$$

EQooCJKBooXdbzts

Ensuite $d(y, A) \leqslant d(x, y) + d(x, A)$ que nous récrivons

$$d(y, A) - d(x, A) \leqslant d(x, y). \tag{9.243}$$

EQooKHPCooDSsfTh

Notez que les équations (9.242) et (9.243) sont de la forme

$$\begin{cases} u - v \leqslant \alpha & \text{(9.244a)} \\ v - u \leqslant \alpha, & \text{(9.244b)} \end{cases}$$

dont nous déduisons $|u - v| \leqslant \alpha$. Bref, nous avons

$$|d(x, A) - d(y, A)| \leqslant d(x, y). \tag{9.245}$$

EQooNAQCooJzmEoj

Voilà qui prouve déjà (1).

Pour prouver 9.222, nous considérons $x_n \xrightarrow{X} x$, et écrivons (9.245) pour x et x_n : pour tout n nous avons

$$|d(x_n, A) - d(x, A)| \leqslant d(x_n, x). \tag{9.246}$$

Vu que $d\colon X \times X \to X$ est continue, en prenant la limite $n \to \infty$, à droite nous avons zéro[97] et donc

$$\lim_{n\to\infty} |d(x_n, A) - d(x, A)| = 0, \tag{9.247}$$

ou encore

$$\lim_{n\to\infty} |f(x_n) - f(x)| = 0, \tag{9.248}$$

ce qui signifie que f est continue en x parce que la continuité séquentielle implique la continuité par la proposition 9.173. □

Si V est une partie d'un espace vectoriel métrique[98] E, d, nous posons

$$B(V, \delta) = \{x \in E \text{ tel que } d(x, V) < \epsilon\} \tag{9.249}$$

où la distance entre V et x est définie en 9.217.

PROPooYTMRooExvGrN

Proposition 9.223.
Soient un ouvert U de $\mathbb{R}^n$ et un compact $K \subset U$. Alors il existe $\epsilon > 0$ tel que

$$K \subset B(K, \epsilon) \subset U. \tag{9.250}$$

[97] Parce que d est continue, proposition 9.175.
[98] Définition 9.155.

9.9.14 Espace métrisable

PROPooXWBTooCvGLOj

Proposition 9.224 ([272]).
Soit un espace topologique métrisable[99] X.

ITEMooOXVRooBsKwuq

(1) *Tout fermé de X est une intersection dénombrable d'ouverts.*

(2) *Tout ouvert de X est une union dénombrable de fermés.*

Démonstration. Soit une métrique d compatible avec la topologie de X et un fermé A. Nous posons

$$V_n = \{x \in X \text{ tel que } d(x, A) < \frac{1}{n}\}. \tag{9.251}$$

Et juste pour faire simple nous notons $V_0 = X$.

(1) **Les parties V_n sont ouvertes** Soit $x \in V_n$. Trouvons un voisinage de x contenu dans V_n afin de pouvoir encore invoquer le théorème 9.8. D'abord, vu que $x \in V_n$, il existe $a \in A$ tel que $d(x, a) < \frac{1}{n}$ (ici les inégalités strictes sont importantes).

Soient $\epsilon > 0$ que nous fixerons plus bas, et $y \in B(x, \epsilon)$. L'inégalité triangulaire donne

$$d(y, a) \leqslant d(y, x) + d(x, a) < \epsilon + \frac{1}{n}. \tag{9.252}$$

Nous pouvons donc choisir ϵ de telle sorte que $d(y, a) < 1/n$. Avec ce ϵ, nous avons, pour tout $y \in B(x, \epsilon)$:

$$d(y, A) \leqslant d(y, a) < \frac{1}{n} \tag{9.253}$$

et donc $y \in V_n$.

(2) **A est l'intersection des V_n** Nous avons évidemment $A \subset V_n$ pour tout n. Et d'autre part, si $a \in \bigcap_{n\in\mathbb{N}} V_n$ alors $d(a, A) < \frac{1}{n}$ pour tout n. Cela implique $d(a, A) = 0$, et donc $a \in A$ par le lemme 9.218.

Ceci démontre le point (1).

En ce qui concerne la seconde partie, nous appliquons la première partie au complémentaire. Si $\mathcal{O}$ est ouvert, $\mathcal{O}^c$ est fermé et

$$\mathcal{O}^c = \bigcap_{n\in\mathbb{N}} V_n, \tag{9.254}$$

ce qui donne immédiatement

$$\mathcal{O} = \bigcup_{n\in\mathbb{N}} V_n^c \tag{9.255}$$

où les V_n^c sont fermés. □

CORooTWFYooCNMieM

Corolaire 9.225.
Si X est un espace topologique métrisable, alors X accepte une base dénombrable de topologie autour de chaque point.

Démonstration. Il s'agit seulement de remarquer que les singletons sont fermés et d'appliquer la proposition 9.224. □

9.9.15 Connexité

PROPooUQNTooAegKwA

Proposition 9.226 ([1]).
Tout espace métrique[100] *est complètement normal.*

Démonstration. Soient un espace métrique (X, d) ainsi que deux parties $A, B \subset X$ telles que $A \cap \bar{B} = B \cap \bar{A} = \varnothing$. Vu que $A \cap \bar{B} = \varnothing$, pour chaque $a \in A$, il existe une boule $B(a, r_a)$ telle que $B(a, r_a) \cap B = \varnothing$. Même histoire pour $b \in B$.

Nous posons $U = \bigcup_{a\in A} B(a, r_a/2)$ et $V = \bigcup_{b\in B} B(b, r_b/2)$. Les parties U et V sont ouvertes comme union d'ouverts. Nous avons évidemment $A \subset U$ et $B \subset V$.

[99] Définition 9.156.
[100] Définition 9.155.

Pour voir que $U\cap V=\varnothing$, supposons $x\in U\cap V$. Il existe $a\in A$ et $b\in B$ tel que $x\in B(a,r_a/2)\cap B(b,r_b/2)$. Remarquons que $d(a,b)>r_a$ et $d(a,b)>r_b$: nous avons choisi r_a et r_b pour cela. Nous avons le calcul

$$d(a,b)\leqslant d(a,x)+d(x,b)\leqslant\frac{r_a+t_b}{2}<d(a,b). \tag{9.256}$$

Cela est une contradiction. □

PROPooBMFBooIQJMNC

Proposition 9.227 ([1]).
Tout o-connexe[101] *d'un espace métrique est connexe*[102].

Démonstration. Une espace métrique est complètement normal (proposition 9.226) et tout o-connexe d'un espace complètement normal est connexe (proposition 9.115). □

9.9.16 Convexité

DEFooQQEOooAFKbcQ

Définition 9.228 (Partie convexe).
*Une partie A d'un espace vectoriel est **convexe** si pour tout $a,b\in A$ et pour tout $t\in[0,1]$, le point $ta+(1-t)b$ est dans A.*

Autrement dit, une partie est convexe lorsqu'elle contient tous les segments joignant ses points.

PROPooJOCEooUKhkqQ

Proposition 9.229 ([273]).
Toute intersection de convexes est convexe.

Démonstration. Soit un espace vectoriel E ainsi que des parties convexes $\{C_i\}_{i\in I}$ indexées par un ensemble quelconque I. Nous prouvons que $C=\bigcap_{i\in I}C_i$ est convexe.

Soient $x,y\in C$, ainsi que $i\in I$. Nous avons $x,y\in C_i$ et donc $\{tx+(1-t)y\}_{t\in[0,1]}\subset C_i$. Vu que cela est vrai pour tout i, nous avons

$$\{tx+(1-t)y\}_{t\in[0,1]}\subset\bigcap_{i\in I}C_i, \tag{9.257}$$

et donc le résultat attendu. □

PROPooJOXUooEZELna

Proposition 9.230 ([274]).
Si A et B sont des convexes d'un espace vectoriel topologique, alors $A-B$ est convexe.

Démonstration. Soient $a_1,a_2\in A$ et $b_1,b_2\in B$. Nous devons prouver que $t(a_1-b_1)+(1-t)(a_2-b_2)$ est dans $A-B$. C'est un simple calcul :

$$t(a_1-b_1)+(1-t)(a_2-b_2)=\underbrace{ta_1+(1-t)a_2}_{\in A}-\underbrace{\big(tb_1+(1-t)b_2\big)}_{\in B}\in A-B. \tag{9.258}$$

□

LEMooEFCCooOuStrb

Lemme 9.231.
L'intérieur d'un convexe est convexe.

Démonstration. Pas de preuve pour le moment. Vous pouvez aider en m'envoyant une preuve. □

9.9.17 Norme

DefNorme

Définition 9.232 ([275], thème 25).
*Soit E un espace vectoriel (pas spécialement de dimension finie) sur le corps $\mathbb{K}$ ($=\mathbb{R}$ ou $\mathbb{C}$). Une **norme** sur E est une application $N\colon E\to[0,\infty[$ telle que*

(1) $N(x)\geqslant 0$

(2) $N(x)=0$ *si et seulement si* $x=0$;

ItemDefNormeii

(3) $N(\lambda x)=|\lambda|N(x)$

ItemDefNormeiii

(4) $N(x+y)\leqslant N(x)+N(y)$

[101] Définition 9.113
[102] Définition 9.111

pour tout $x, y \in E$ et pour tout $\lambda \in \mathbb{K}$.

*La propriété (4) est appelée **inégalité triangulaire**.*

*Un espace vectoriel muni d'une norme est un **espace vectoriel normé**.*

En prenant $\lambda = -1$ dans la propriété (3), nous trouvons immédiatement que $N(-x) = N(x)$.

PropNmNNm

Proposition 9.233.
Toute norme N sur l'espace vectoriel E vérifie l'inégalité

$$\big|N(x) - N(y)\big| \leqslant N(x - y) \tag{9.259}$$

pour tout $x, y \in E$.

Démonstration. Nous avons, en utilisant le point (4) de la définition 9.232,

subEqNNNxyyya
$$N(x) = N(x - y + y) \leqslant N(x - y) + N(y), \tag{9.260a}$$
subEqNNNxyyyb
$$N(y) = N(y - x + x) \leqslant N(y - x) + N(x). \tag{9.260b}$$

Supposons d'abord que $N(x) \geqslant N(y)$. Dans ce cas, en utilisant (9.260a),

$$\big|N(x) - N(y)\big| = N(x) - N(y) \leqslant N(x - y) + N(y) - N(y) = N(x - y). \tag{9.261}$$

Si par contre $N(x) \leqslant N(y)$, alors nous utilisons (9.260b) et nous trouvons

$$\big|N(x) - N(y)\big| = N(y) - N(x) \leqslant N(y - x) + N(x) - N(x) = N(y - x) = N(x - y). \tag{9.262}$$

Dans les deux cas, nous avons retrouvé l'inégalité annoncée. □

Cette proposition signifie aussi que

EqNleqNNleqNvalabs
$$-N(x - y) \leqslant N(x) - N(y) \leqslant N(x - y). \tag{9.263}$$

Le lemme suivant dit que nous pouvons remplacer l'inégalité triangulaire par la convexité de la boule unité dans la définition de norme.

LEMooAVIJooFhdXXr

Lemme 9.234 ([276])**.**
Soit une application $N : E \to [0, \infty[$ telle que

(1) $N(x) \geqslant 0$ pour tout $x \in E$,

(2) $N(x) = 0$ si et seulement si $x = 0$,

(3) $N(\lambda x) = |\lambda| N(x)$.

Alors N est une norme si et seulement si la partie

$$B = \{x \in E \text{ tel que } N(x) \leqslant 1\} \tag{9.264}$$

est convexe[103].

Démonstration. Dans les deux sens.

(1) $\Rightarrow$ Nous supposons que N est une norme et nous prouvons que la boule B est convexe. Soient $x, y \in B$ et $\lambda \in [0, 1]$. Nous avons

$$\begin{aligned} N\big(\lambda x + (1 - \lambda)y\big) &\leqslant N(\lambda x) + N\big((1 - \lambda)y\big) && \text{(9.265a)}\\ &= \lambda N(x) + (1 - \lambda)N(y) && \text{(9.265b)}\\ &\leqslant \lambda + (1 - \lambda) && \text{(9.265c)}\\ &= 1. && \text{(9.265d)} \end{aligned}$$

Nous avons utilisé diverses propriétés de la norme, ainsi que la majoration $N(x), N(y) \leqslant 1$.

[103] Définition 9.228.

(2) $\Leftarrow$ Nous supposons que B est convexe, et nous prouvons que N vérifie l'inégalité triangulaire. Soient $x, y \in E$ que nous choisissons tous deux non nuls (sinon c'est trop facile). Nous posons

$$z = \frac{x+y}{N(x)+N(y)} \tag{9.266}$$

et la subtilité sera d'écrire z de telle sorte à être une somme de deux éléments de B. L'astuce est de poser

$$\lambda = \frac{N(x)}{N(x)+N(y)}. \tag{9.267}$$

Une simple vérification montre qu'alors

$$z = \lambda \frac{x}{N(x)} + (1-\lambda)\frac{y}{N(y)}. \tag{9.268}$$

Nous avons évidemment $x/N(x) \in B$ (et de même avec y). Puisque B est convexe, nous avons $z \in B$. Exprimons le fait que $z \in B$ à partir de la définition (9.266) :

$$\frac{N(x+y)}{N(x)+N(y)} \leqslant 1. \tag{9.269}$$

Cela signifie exactement $N(x+y) \leqslant N(x)+N(y)$.

□

9.235.
Afin de suivre une notation proche de celle de la valeur absolue, à partir de maintenant, la norme d'un vecteur v sera notée $\|v\|$ au lieu de $N(v)$. La proposition 9.233 s'énoncera donc

$$\big|\|x\| - \|y\|\big| \leqslant \|x-y\|. \tag{9.270}$$

Un espace vectoriel E muni d'une norme est, on l'a déjà dit, un **espace vectoriel normé** ; on le notera $(E, \|.\|)$ pour distinguer la norme fixée.

Une autre inégalité utile de temps en temps.

Corolaire 9.236.
Si a et b sont dans un espace vectoriel normé, alors

$$\big|\|a-b\| - \|b\|\big| \leqslant \|a\|. \tag{9.271}$$

Démonstration. Il s'agit seulement de la proposition 9.233 avec $x = a-b$ et $y = b$. □

Lemme-Définition 9.237 (Distance induite par une norme)**.**
Soit un espace vectoriel normé $(E, \|.\|)$. Nous posons

$$d(x,y) = \|x-y\|. \tag{9.272}$$

Alors

(1) d est invariante par translations : $d(a,b) = d(a+u, b+u)$

(2) d est une distance[104] *sur E.*

*C'est la **distance induite** par la norme.*

Démonstration. Le fait que la formule (9.272) soit invariante par translations est immédiat. En ce qui concerne le fait que ce soit une distance, le seul point délicat à vérifier est l'inégalité triangulaire. Mais, pour tous $x, y, z \in E$, on a

$$d(x,y) = \|x-y\| = \|x-z+z-y\| \leqslant \|x-z\| + \|z-y\| = d(x,z) + d(z,y). \tag{9.273}$$

□

[104] Définition 9.155.

9.9.18 Topologie

DEFooPMVFooPSYVNQ

Définition 9.238.
La topologie associée à une norme est celle associée à la distance donnée en 9.237 par le théorème 9.158.

9.10 Espaces vectoriels topologiques

DefEVTopologique

Définition 9.239.
Un espace vectoriel V sur le corps valué[105] $\mathbb{K}$ *muni d'une topologie est un* ***espace vectoriel topologique*** *si*

(1) *la somme de deux vecteurs est une application continue $V \times V \to V$*

(2) *la multiplication par un scalaire est une application continue $\mathbb{K} \times V \to V$.*

Ici, sur $V \times V$ et sur $\mathbb{K} \times V$ nous avons la topologie produit.

Dans toute la suite, nous supposons que $\mathbb{K}$ est un corps avec une topologie métrique.

On le redit quand même : le corps[106] lui-même doit avoir sa topologie. Dans la grande majorité des cas, ce corps est $\mathbb{R}$ ou $\mathbb{C}$ muni de la topologie usuelle.

Mine de rien, le fait que les deux opérations usuelles soient continues a de belles conséquences sur la topologie de l'espace…

PROPooDXLFooFghbWk

Proposition 9.240 ([277]).
Soit un espace vectoriel topologique V. Pour $x \in V$ et $\lambda \in \mathbb{K}$, $\lambda \neq 0$ fixés, les fonctions T_x et M_λ définies par :

$$T_x : V \to V \qquad \text{et} \qquad M_\lambda : V \to V \tag{9.274}$$
$$y \mapsto x + y \qquad\qquad y \mapsto \lambda y \tag{9.275}$$

sont des automorphismes[107] *de l'espace topologique V.*

Démonstration. Ce sont des bijections continues, dont les inverses sont respectivement T_{-x} et $M_{1/\lambda}$. □

PROPooJYLVooPpLWFX

Proposition 9.241.
Soit un espace vectoriel topologique X. Si $\mathcal{O}$ est un ouvert dans X, alors pour tout $x \in X$ et pour tout $\lambda \in \mathbb{K}$, les parties $\mathcal{O} + x$ et $\lambda\mathcal{O}$ sont des ouverts.

LEMooEZIYooBBxdJj

Lemme 9.242 ([1]).
Soit un espace vectoriel topologique V sur le corps $\mathbb{K}$. Si $\mathcal{O}$ est un ouvert autour de 0 dans V et si $\lambda \neq 0 \in \mathbb{K}$, il existe un ouvert U autour de 0 tel que $\lambda U \subset \mathcal{O}$.

Démonstration. La réponse est $U = \lambda^{-1}\mathcal{O}$. En effet par définition d'un espace vectoriel topologique, la fonction donnée par $f(x) = \lambda x$ est continue ; donc $U = f^{-1}(\mathcal{O})$ est un ouvert. De plus $\lambda U = \mathcal{O}$. □

PROPooHKGZooDaNaHU

Proposition 9.243 ([1]).
Une application linéaire entre espaces vectoriels topologiques est continue si et seulement si elle est continue en 0.

Démonstration. Soient deux espaces vectoriels topologiques. Soit une application linéaire $f : E \to F$. Nous supposons qu'elle est continue en 0 (définition 9.48(1)), et nous montrons qu'elle est alors continue en $a \in E$.

Soit un voisinage W de $f(a)$ dans F. Alors la proposition 9.241 dit que $W - f(a)$ est un voisinage de $0 = f(0)$ dans F. Vu que f est continue en 0, il existe un voisinage V de 0 dans E tel que $f(V) \subset W - f(a)$. Alors

$$f(V + a) = f(V) + f(a) \subset W, \tag{9.276}$$

et le voisinage $V + a$ de a dans E fait l'affaire.

Nous avons prouvé que f est continue en chaque point de E. La proposition 9.49 dit que f est alors continue sur E. □

PROPooRCSQooAgTRDi

Proposition 9.244 ([278]).
À propos de complétude.

[105] Définition 1.118.
[106] Définition 1.213
[107] Définition 9.54.

ITEMooVUXEooBQTpIM

(1) *Dans un espace vectoriel topologique Hausdorff, toute partie complète est fermée.*

(2) *Dans un espace vectoriel topologique, toute partie fermée est complète.*

9.10.1 De complexe à réel

Si E est un espace topologique sur $\mathbb{C}$, nous aurons besoin de le voir comme espace topologique sur $\mathbb{R}$.

PROPooAIMVooYtZVJV

Proposition 9.245 ([1]).
Soit un espace topologique complexe (X, τ, m_X, s_X) où τ est la topologie sur X, $m_X : \mathbb{C} \times X \to X$ est la multiplication et $s_X : X \times X \to X$ est la somme.

Alors en posant $E = X$ (comme ensembles) ainsi que

$$\begin{aligned} s_E : E \times E &\to E \\ (x, y) &\mapsto s_X(x, y), \end{aligned} \tag{9.277}$$

et

$$\begin{aligned} m_E : \mathbb{R} \times E &\to E \\ (\lambda, x) &\mapsto m_X(\lambda, x), \end{aligned} \tag{9.278}$$

la quadruplet (E, τ, m_E, s_E) est un espace topologique.

PROPooQMGXooBnJblx

Proposition 9.246 ([1]).
Soit X un espace vectoriel topologique sur $\mathbb{C}$. Si $f : X \to \mathbb{R}$ est $\mathbb{R}$-linéaire, nous posons

$$\phi(x) = f(x) - if(ix). \tag{9.279}$$

Alors

(1) *L'application ϕ est $\mathbb{C}$-linéaire.*

(2) *Nous avons $\|\phi\| = \|f\|$.*

(3) *Si f est continue, alors ϕ est continue.*

9.10.2 Base de topologie

Toute base de voisinage de 0 se transporte en tout point de l'espace vectoriel topologique.

PropInvarianceTopologie

Corolaire 9.247 (Invariance de la topologie[277]).
Soit un espace vectoriel topologique (X, τ). Si $\mathcal{B}_0$ est une base de topologie en 0, alors $\mathcal{B}_0 + a$ est une base de topologie en a.

Démonstration. Soit un ouvert U contenant a. Alors $U - a$ est un ouvert contenant 0 (proposition 9.241). Il existe donc $B \in \mathcal{B}_0$ tel que $0 \in B \subset U - a$. Nous avons alors $a \in B + a \subset U$. □

9.10.2.1 Somme directe topologique

PropKZDqTR

Proposition-Définition 9.248 ([279, 280, 1]).
Soit V un espace vectoriel topologique et une décomposition en somme directe[108] $V = V_1 \oplus V_2$. Alors les trois conditions suivantes sont équivalentes.

ITEMooMUELooWdJQeW

(1) *La bijection*

$$\begin{aligned} \psi : V_1 \times V_2 &\to V \\ (x_1, x_2) &\mapsto x_1 + x_2 \end{aligned} \tag{9.280}$$

est un homéomorphisme[109].

ITEMooDKOYooUpEfOR

(2) *Les parties V_1 et V_2 sont fermées dans V et la projection $s : V_2 \to V/V_1$ est un homéomorphisme.*

ITEMooFSSMooCQzTIc

(3) *Les parties V_1 et V_2 sont fermées dans V et la projection $\pi_2 : V \to V_2$ est continue.*

[108] Définition 6.157.
[109] C'est-à-dire isomorphisme d'espaces vectoriels : bijection continue de réciproque continue. En ce qui concerne la topologie sur $V_1 \times V_2$, elle est donné par la définition 9.66.

Lorsqu'une décomposition en somme directe vérifie ces conditions, nous disons que la décomposition est ***topologique****.*

Démonstration. Avant de commencer, nous rappelons les topologies.

- Sur V_1 et V_2 nous avons la topologie induite, définition 9.30.
- La topologie produit sur $V_1 \times V_2$ est la définition 9.66.
- La topologie quotient sur V/V_1 est la définition 9.72.

Voici quelques points qui ne dépendent pas des hypothèses (1), (2) ou (3).

(1) **La projection $p: V \to V/V_1$ est continue** La projection est toujours continue pour la topologie quotient ; c'est la définition même, voir 9.72.

(2) **ψ est une bijection continue** Le fait que ψ soit continue fait partie de la définition 9.239 d'un espace vectoriel topologique. Pour que ce soit une bijection, c'est le lemme 6.158.

(3) **s est injective** Soient $v, w \in V_2$ tels que $s(v) = s(w)$. Alors $\{v + x_1\}_{x_1 \in V_1} = \{w + y_1\}_{y_1 \in V_1}$. En particulier $v \in \{w + y_1\}_{y_1 \in V_1}$. Il existe donc $y_1 \in V_1$ tel que $v = w + y_1$. Donc $v - w \in V_1$. Mais comme V_2 est un espace vectoriel, nous avons aussi $v - w \in V_2$. Donc $v - w \in V_1 \cap V_2 = \{0\}$.

(4) **s est surjective** Soit $x \in V$. Nous devons trouver $v \in V_2$ tel que $s(v) = [x]$. Nous savons qu'il existe $x_1 \in V_1$ et $x_2 \in V_2$ tels que $x = x_1 + x_2$. Nous avons alors $[x] = s(x_2)$.

(5) **s est continue** Soit un ouvert $\mathcal{O}$ de V/V_1. La partie $p^{-1}(\mathcal{O})$ est ouverte dans V (proposition 9.73), et donc

$$s^{-1}(\mathcal{O}) = p^{-1}(\mathcal{O}) \cap V_2 \tag{9.281}$$

est ouvert dans V_2 parce que la topologie sur V_2 est celle induite[110] de la topologie de V.

Et maintenant on prouve les équivalences.

(1) **Si (1) alors V_1 est fermé** La partie $V_1 \times \{0\}$ est fermée dans $V_1 \times V_2$. Vu que ψ^{-1} est continue, nous en déduisons que $\psi\big(V_1 \times \{0\}\big)$ est fermée dans V par le lemme 9.55. Mais comme $\psi\big(V_1 \times \{0\}\big) = V_1$, nous avons que V_1 est fermé dans V.

(2) **(1) ⇒ (3)** Nous supposons que $\psi: V_1 \times V_2 \to V$ est un homéomorphisme. Nous considérons l'application

$$\begin{aligned} \sigma: V_1 \times V_2 &\to V_1 \times V_2 \\ (x, y) &\mapsto (0, y). \end{aligned} \tag{9.282}$$

Cette application est continue et permet d'écrire π_2 sous la forme $\pi_2 = \psi \circ \sigma$. En tant que composée d'applications continues, l'application π_2 est continue.

(3) **(3) ⇒ (2)** L'application $\pi: V \to V_2$ est constante sur les classes (modulo V_1). Donc elle descend aux classes[111] en l'application

$$\begin{aligned} \tilde{\pi}: V/V_1 &\to V_2 \\ [x] &\mapsto \pi(x). \end{aligned} \tag{9.283}$$

Cette application est continue parce que π l'est et parce que le lemme 9.75 le dit. Le point à remarquer est que $s^{-1} = \tilde{\pi}$ parce que pour tout $x \in V_2$ nous avons

$$s\Big(\tilde{\pi}\big([x]\big)\Big) = s\big(\pi(x)\big) = s(x) = [x] \tag{9.284}$$

parce que $\pi(x) = x$ du fait que $x \in V_2$. Vu que $\tilde{\pi}$ est continue, l'application s^{-1} est également continue.

(4) **(2) ⇒ (1)** Nous pouvons écrire la projection $\pi_2: V \to V_2$ comme composée $\pi_2 = s^{-1} \circ p$. En effet pour $v_1 \in V_1$ et $v_2 \in V_2$ nous avons $(s^{-1} \circ p)(v_1 + v_2) = s^{-1}\big([v_2]\big) = v_2 = \pi_2(v_1 + v_2)$.

Nous savons que p est continue (construction de la topologie et tout ça), et que s^{-1} est également continue par hypothèse. Donc π_2 est continue. Étant donné que $\pi_1 + \pi_2 = \mathrm{Id}$ et que l'identité est continue, nous déduisons que π_1 est également continue.

□

[110] Topologie induite, définition 9.30.
[111] Voir la définition 9.74.

9.249 ([281]).
Si V est normé, il existe une façon plus directe (mais pas spécialement plus simple) de prouver l'implication (1) $\Rightarrow$ (2), et en particulier la continuité de s^{-1}. Voyez 12.106.

Si V est de Banach, la continuité de s^{-1} peut venir du théorème d'isomorphisme de Banach 29.1 parce que s est une bijection continue entre espaces de Banach. Attention toutefois à vérifier que V/V_1 est de Banach[112].

CORooJHSGooUkGepQ

Corolaire 9.250 ([1]).
Tout sous-espace vectoriel d'un espace vectoriel topologique de dimension finie est fermé.

9.10.2.2 Limite dans un espace vectoriel topologique

LEMooAHIGooJhpPvo

Lemme 9.251 (Changement de variables).
Soient un espace vectoriel topologique[113] X *ainsi qu'un espace séparé* Y *et une application* $f\colon X \to Y$. *Nous supposons que* $\lim_{x\to a} f(x) = \ell$. *Alors* $\lim_{x\to b} f(x+a-b)$ *existe et vaut* ℓ.

Démonstration. Soit un voisinage V de ℓ dans Y. Il existe un voisinage U de a tel que $f(U) \subset V$. Nous posons $U' = U - a + b$. C'est un voisinage de b. En posant $g(x) = f(x+a-b)$ nous avons

$$g(U') = f(U - a + b + a - b) = f(U) \subset V. \tag{9.285}$$

Donc $\lim_{x\to b} g(x) = \ell$. C'est cette égalité qui signifie $\lim_{x\to b} f(x+a-b)$. □

PROPooXWNDooGHDXTa

Proposition 9.252 ([1]).
Soient un espace vectoriel topologique X, *un espace topologique* Y *et une application* $f\colon X \to Y$. *Si*

$$\lim_{x\to b} f(a+x) = l, \tag{9.286}$$

EQooMUQJooLClnMP

alors $\lim_{x\to a+b} f(x)$ *existe et vaut* l.

Démonstration. Soit un voisinage V de l. Nous devons prouver qu'il existe un voisinage U de $a+b$ tel que $f(U) \subset V$. Par (9.286), il existe un voisinage U' de b tel que $f(a+u) \in V$ pour tout $u \in U'$. La partie $U = U' + a$ est un voisinage de $a+b$ (parce que c'est un ouvert et qu'il contient $a+b$). Et si $x \in U$, alors $x = a + u$ pour un certain $u \in U'$. Nous avons $f(x) = f(a+u) \in V$.

Cela prouve que $f(U) \subset V$ comme nous le voulions. □

PROPooKNVHooXlQyVA

Proposition 9.253 (Limite de fonction composée[282]).
Soient des fonctions $f, g\colon \mathbb{R} \to \mathbb{R}$ *telles que*

$$\lim_{y\to l} f(y) = z \tag{9.287a}$$

$$\lim_{x\to a} g(x) = l. \tag{9.287b}$$

Nous supposons que f *est continue en* l.

Alors

$$\lim_{x\to a} (f \circ g)(x) = \lim_{y\to l} f(y) = z. \tag{9.288}$$

9.10.3 Corps topologique

DEFooWKLOooPdsxQl

Définition 9.254 (Anneau topologique[283]).
Un ***anneau topologique*** *est un anneau*[114] *muni d'une topologie dans laquelle l'addition et la multiplication sont continues*[115].

PROPooAWAKooKRmbGT

Proposition-Définition 9.255.
Si $(\mathbb{K}, |.|)$ *est un corps totalement ordonné avec sa valeur absolue usuelle*[116], *alors*

[112] Je ne l'ai pas fait, et au doigt mouillé je dirais que ça m'étonnerais que ce soit vrai pour tout choix de sous-espace vectoriel V_1. À vos risques et périls. Écrivez-moi si vous avez une idée.
[113] Définition 9.239.
[114] Définition 1.100.
[115] Définition 9.48(2).
[116] Définition 1.121.

ITEMooSSJRooNCfbXa

(1) *l'application*

$$\begin{aligned} d\colon \mathbb{K}\times\mathbb{K} &\to \mathbb{R}^+ \\ (x,y) &\mapsto |x-y| \end{aligned} \tag{9.289}$$

est une distance[117].

ITEMooONQPooDAXbBh

(2) *Un corps valué muni de sa topologie métrique*[118] *est un corps topologique*[119].

ITEMooFCDZooMilJfr

(3) *Le corps topologique* $\mathbb{K}^d$ *est complet.*

Démonstration. Les points (1) et (2) sont les différentes propriétés du lemme 1.122. □

9.10.4 Les applications linéaires sont continues

PROPooWZHBooFXDRKH

Proposition 9.256 ([284]).
Soit un espace vectoriel topologique E *sur le corps* $\mathbb{K}$*. Nous considérons une application linéaire* $f\colon E\to\mathbb{K}$ *non identiquement nulle. Il y a équivalence entre :*

(1) f *est continue,*

(2) $\ker(f)$ *est fermé dans* E*,*

(3) $\ker(f)$ *n'est pas dense dans* E*,*

(4) f *est borné sur un voisinage de* 0 *dans* E*.*

PROPooWZXCooXfyLMK

Proposition 9.257 ([1]).
Si $f_i\colon E_i\to F_i$ *sont des applications continues entre espaces vectoriels topologiques, alors l'application*

$$\begin{aligned} f_1\times\ldots\times f_n\colon E_1\times\ldots\times E_n &\to F_1\times\ldots\times F_n \\ (v_1,\ldots,v_n) &\mapsto \big(f_1(v_1),\ldots,f_n(v_n)\big) \end{aligned} \tag{9.290}$$

est continue

9.10.5 Voisinage symétrique et équilibré

DEFooKBMAooAhYQAm

Définition 9.258 (Partie symétrique[277]).
Une partie U *d'un espace vectoriel topologique est* ***symétrique*** *si* $x\in U$ *implique* $-x\in U$*.*

DEFooPNRIooEFAlii

Définition 9.259 (Partie équilibrée[277]).
Une partie U *d'un espace vectoriel topologique* V *est* ***équilibrée*** *si pour tout* $|\alpha|\leqslant 1$ *dans* $\mathbb{K}$*,* $\alpha U\subset U$*.*

DEFooMNZJooSIAVGZ

Définition 9.260 (Partie absorbante[285]).
Soit un espace vectoriel X*. Une partie* U *est* ***absorbante*** *si pour tout* $x\in X$*, il existe* $\rho_x>0$ *tel que* $\lambda x\in U$ *pour tout* $|\lambda|\leqslant\rho_x$*.*

DEFooYSWJooPkcrJe

Définition 9.261 (Partie absolument convexe).
Une partie est ***absolument convexe*** *si elle est convexe et équilibrée.*

LEMooXKOTooLWDXhp

Lemme 9.262.
Si A *est équilibré ou absorbant, alors* $0\in A$*.*

Démonstration. En deux parties.

(1) **Si A est équilibré** Pour tout $|\alpha|<1$, nous avons $\alpha A\subset A$. En particulier pour $\alpha=0$ nous voyons que $0\in A$.

(2) **Si A est absorbant** Si $x\in X$, alors il existe ρ tel que $\lambda x\in A$ pour tout $|\lambda|<\rho$. En particulier avec $\lambda=0$ nous avons encore $0\in A$.

□

[117] Distance, définition 9.155.
[118] Définition 9.158.
[119] Définition 9.254.

LEMooEEKYooVCnBMq

Lemme 9.263 ([286]).
Dans un espace vectoriel topologique sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, tout ouvert contenant 0 est absorbant[120].

Démonstration. Soient un ouvert U contenant 0 et $x_0 \in X$. Nous considérons l'application

$$\begin{aligned} m\colon \mathbb{K} \times X &\to X \\ (t,x) &\mapsto tx \end{aligned} \tag{9.291}$$

qui est continue par définition 9.239. La partie $m^{-1}(U) \subset \mathbb{K} \times X$ est un ouvert contenant $(0,x_0)$. Par définition 9.66 de la topologie produit, il existe un $r > 0$ et un ouvert B de X contenant x_0 tels que

$$(0,x_0) \in B(0,r) \times B \subset m^{-1}(U). \tag{9.292}$$

Si $\lambda < r$, alors nous avons

$$\lambda x_0 = m(\lambda, x_0) \in m\big(B(0,r), B\big) \subset U. \tag{9.293}$$

□

LEMooKBRIooUAAPXV

Lemme 9.264.
Si A est équilibré et si $\xi \neq 0$ (dans $\mathbb{R}$ ou $\mathbb{C}$), alors

$$\xi A = |\xi| A \tag{9.294}$$

Démonstration. Vu que le corps $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$, il existe $s \in \mathbb{K}$ tel que $|s| = 1$ et $\xi = s|\xi|$ (prendre $s = \xi/|\xi|$). Vu que $|s| = 1$ et que A est équilibré, $sA \subset A$ et donc $\xi A = s|\xi|A \subset |\xi|A$.

Pour l'inclusion dans l'autre sens, nous savons que $|s^{-1}| = 1$ et donc que $|\xi|A = s^{-1}\xi A \subset \xi A$. □

LEMooYSWXooNqAcOQ

Lemme 9.265 ([277, 1]).
Soit un espace vectoriel topologique.

ITEMooSWWQooTreWIE

(1) Soit un ouvert A autour de 0 dans l'espace vectoriel topologique V. Il existe $\delta > 0$ dans le corps $\mathbb{K}$ et un voisinage ouvert W de 0 tel que $\lambda W \subset A$ pour tout $|\lambda| < \delta$.

ITEMooXZNHooGVplpu

(2) Tout voisinage de 0 contient un ouvert équilibré.

ITEMooRLVSooGihcLc

(3) Tout voisinage de 0 contient un ouvert équilibré et symétrique.

Démonstration. En plusieurs parties.

(1) **Pour (1)** Nous savons que $0 \cdot 0 = 0$ et que l'application

$$\begin{aligned} f\colon \mathbb{K} \times V &\to V \\ \lambda, x &\mapsto \lambda x \end{aligned} \tag{9.295}$$

est continue. La partie $f^{-1}(A)$ contient $(0,0)$. Il existe donc un voisinage ouvert S de 0 dans $\mathbb{K}$ et un voisinage ouvert W de 0 dans V tel que $S \times W \subset f^{-1}(A)$.

Puisque $\mathbb{K}$ est un corps dont la topologie est métrique[121], il existe une boule $S' = B(0,\delta) \subset S$.

Donc nous avons $f(S' \times W) \subset A$ et pour tout $|\lambda| < \delta$, $\lambda W \subset A$.

(2) **Pour (2)** Soit un voisinage ouvert $\mathcal{O}$ de 0 dans V. Par le point (1), nous considérons un voisinage W de 0 et un $\delta > 0$ tel que $\lambda W \subset \mathcal{O}$ pour tout $|\lambda| < \delta$.

Nous posons

$$U = \{\lambda w < \text{ tel que } |\lambda| < \delta, w \in W\}. \tag{9.296}$$

Nous avons $U \subset \mathcal{O}$ par définition de W. De plus U est équilibré parce que si $|\mu| < 1$, et si $x \in U$, il existe $|\lambda| < \delta$ et $w \in W$ tels que $x = \lambda w$. Alors $\mu x = \mu\lambda w$. Nous avons $|\mu\lambda| < \delta$ et donc $\mu\lambda w \in U$.

(3) **Pour (3)** Nous considérons U équilibré comme dans (2). Ensuite nous posons $U' = U \cap (-U)$. La partie U' est symétrique, elle est ouverte (intersection d'ouverts). Et elle est équilibrée parce que si $x \in U'$ et $|\lambda| < 1$ alors :

- $x \in U$ et U est équilibré, donc $\lambda x \in U$.

[120] Définition 9.260.
[121] Le corps $\mathbb{K}$ est un corps valué, et donc métrique par la définition 9.255.

- $x \in -U$ et U est équilibré, donc il existe $y \in U$ tel que $x = -y$. Pour ce y nous avons $\lambda y \in U$ et donc $\lambda x = -\lambda y \in -U$. Donc $\lambda x \in -U$.
- Au final, $\lambda x \in U \cap (-U) = U'$ et U' est équilibré.

□

LEMooQEFRooHAxOys

Lemme 9.266 ([287]).
Soit un espace vectoriel topologique V ainsi qu'un voisinage ouvert $\mathcal{O}$ de 0 dans V. Il existe des voisinages ouverts U_1 et U_2 de 0 dans V tels que

$$U_1 + U_2 \subset \mathcal{O}. \tag{9.297}$$

Démonstration. Par définition d'un espace vectoriel topologique, l'application

$$\begin{aligned} f\colon V \times V &\to V \\ x, y &\mapsto x + y \end{aligned} \tag{9.298}$$

est continue. Donc la partie $f^{-1}(\mathcal{O})$ est un ouvert de $V \times V$ (c'est la définition 9.48(2) de la continuité). La définition 9.66 de la topologie produit, appliquée au point $(0,0) \in V \times V$ implique qu'il existe des voisinages U_1 et U_2 de 0 dans V tels que

$$U_1 \times U_2 \subset f^{-1}(\mathcal{O}). \tag{9.299}$$

Donc $f(U_1 \times U_2) \subset \mathcal{O}$ et en particulier $U_1 + U_2 \subset \mathcal{O}$. □

PROPSommeTopologique

Proposition 9.267 ([277, 1]).
Soit V un espace vectoriel topologique, et $\mathcal{O}$ un voisinage ouvert de 0. Il existe un voisinage ouvert U de 0 tel que

(1) U est symétrique[122],

(2) U est équilibré[123]

(3) U vérifie $U + U \subset \mathcal{O}$.

(4) U vérifie $U + U + U + U \subset \mathcal{O}$.

Démonstration. En plusieurs petits pas.

(1) **Le point de départ** Le lemme 9.266 donne des voisinages ouverts U_1 et U_2 de 0 dans V tels que $U_1 + U_2 \subset \mathcal{O}$.

(2) **Symétrique** En posant $U' = U_1 \cap U_2 \cap (-U_1) \cap (-U_2)$, on a un sous-ensemble symétrique de U_1 et U_2 qui vérifie $U' + U' \subset U_1 + U_2 \subset \mathcal{O}$. De plus U' est encore un voisinage ouvert de 0 dans V.

(3) **équilibré** C'est le moment d'utiliser le lemme 9.265. La partie U' contient un voisinage ouvert U'' de 0 qui est symétrique et équilibré. Ce U'' vérifie encore $U'' + U'' \subset \mathcal{O}$.

(4) **En 4 parties** Maintenant nous ré-appliquons tout ce que nous venons de faire à U'' pour obtenir un voisinage symétrique et équilibré de 0 tel que $U + U \subset U'$. Nous avons alors $U + U + U + U \subset \mathcal{O}$.

Notons que ce U vérifie à fortiori $U + U \subset \mathcal{O}$.

□

LEMooKLOKooEfKhgN

Lemme 9.268 ([285, 288]).
Soit une partie B d'un espace vectoriel topologique.

(1) Si B est équilibré, alors la fermeture $\bar{B}$ est équilibrée.

ITEMooLZZEooAqoQVO

(2) Si B est équilibré et si $0 \in \mathrm{Int}(B)$, alors $\mathrm{Int}(B)$ est équilibré.

Démonstration. Pas de preuve pour le moment. Vous pouvez aider en m'envoyant une preuve. □

[122] Définition 9.258.
[123] Définition 9.259.

9.10.6 Espace topologique localement convexe

DefPJokvAa

Définition 9.269 ([285]).
Un espace topologique est ***localement convexe*** *il admet une base de voisinages de l'origine dont les éléments sont des parties convexes.*

PROPooCZJGooRlyEOV

Proposition 9.270 ([289]).
Soit un espace topologique X. Nous avons équivalence entre les points suivants :

(1) X est localement convexe[124]*.*

(2) Pour tout ouvert U de X, les composantes connexes de U sont des ouverts de X.

(3) Les ouverts connexes forment une base des ouverts de E.

LEMooWGOCooHSoCzb

Lemme 9.271 ([290]).
Soit un espace topologique localement connexe X. Soient un fermé F de X, et D, une composante connexe de $X \setminus F$. Alors la frontière de D est dans F :

$$\partial D \subset F. \tag{9.300}$$

Démonstration. En plusieurs parties.

(1) **∂D est fermé** Par définition, $\partial D = \bar{D} \setminus D$. Utilisant 1.49(5) nous écrivons

$$X \setminus \partial D = (X \setminus \bar{D}) \cap D. \tag{9.301}$$

Vu que $\bar{D}$ est fermé, $X \setminus \bar{D}$ est ouvert. De plus D est ouvert par la proposition 9.270. Donc $X \setminus \partial D$ est ouvert.

(2) **Par l'absurde** Supposons qu'il existe $p \in \partial D \setminus F$. Vu que F est fermé, il existe $r > 0$ tel que $B(p, r) \cap F = \varnothing$. Étant donné que $p \in \partial D$, tout voisinage de p contient un point de D : il existe $x \in B(p, r) \cap D$.

Donc $B(p, r)$ et D sont des ouverts connexes qui ont une intersection non vide. La proposition 9.123 nous indique que $D \cup B(p, r)$ est un ouvert connexe strictement plus grand que D.

Cela contredit la maximalité de D en tant que composante connexe.

□

PROPooOAXHooOGhRbu

Proposition 9.272 ([285]).
Un espace vectoriel topologie localement convexe a une base de voisinage constituée d'éléments qui sont :

(1) ouverts

(2) absorbants

(3) convexes

(4) équilibrés

Démonstration. Soit un voisinage N de 0 dans l'espace vectoriel topologique X. Vu que X est localement convexe, il existe un voisinage convexe W de 0 contenu dans N. Par le lemme 9.265, W contient un ouvert équilibré U. Nous considérons enfin l'enveloppe convexe $S = \mathcal{C}\text{onv}(U)$ de U, et nous montrons que l'intérieur $\text{Int}(S)$ vérifie tout ce qu'il faut.

ouvert Parce que c'est un intérieur.

convexe L'intérieur d'un convexe est convexe par le lemme 9.231.

absorbant Tout ouvert contenant 0 est absorbant par le lemme 9.263

contient 0 La partie U contient 0 parce qu'elle est équilibrée et le lemme 9.262. Vu que U est ouvert, il contient un voisinage de tout ses points. Donc 0 est dans l'intérieur de U. Il est donc également dans l'intérieur de son enveloppe convexe.

équilibré Par le lemme 9.268(2) parce que c'est un ouvert contenant 0.

[124] Définition 9.269.

contenu dans N Nous avons les inclusions $U \subset W \subset N$. Étant donné que W est convexe, nous avons aussi $\mathcal{C}\text{onv}(U) \subset W$, et donc

$$\text{Int}(S) \subset S = \mathcal{C}\text{onv}(U) \subset W \subset N. \tag{9.302}$$

□

THOooPTLOooJLaHGE

Théorème 9.273 ([285]).
Soit un espace vectoriel topologique localement convexe[125]*. Il existe une base de voisinages $\mathcal{B}$ de 0 tels que :*

(1) les éléments sont absorbants et absolument convexes[126]*.*

(2) pour tout $A, B \in \mathcal{B}$, il existe $W \in \mathcal{B}$ tel que $W \subset A \cap B$,

(3) pour tout $A \in \mathcal{B}$, et pour tout $\rho > 0$, il existe $W \in \mathcal{B}$ tel que $W \subset \rho A$.

LEMooDVZWooWKRQWC

Lemme 9.274 ([1]).
Soit un espace vectoriel localement convexe[127] *X. Soient un compact $K \subset X$ et un ouvert U contenant 0. Il existe $\lambda \in \mathbb{R}$ tel que $K \subset \lambda U$.*

Démonstration. En deux parties.

(1) **Si U est convexe** Soit $x \in K$. Étant donné que $x/n \to 0$ et que U est un voisinage de 0, il existe n tel que $x/n \in U$. Pour chaque $x \in K$ nous considérons $\lambda \in \mathbb{R}^+$ tel que $x \in \lambda_x U$. Les parties $\{\lambda_x U\}_{x \in K}$ forment un recouvrement de K par des ouverts.

Nous en extrayons un sous-recouvrement fini, c'est-à-dire $x_1, \dots, x_n \in K$ tels que $K \subset \bigcup_{i=1}^n \lambda_{x_i} U$. Et au passage nous notons $\lambda_i = \lambda_{x_i}$. Et enfin nous posons

$$\lambda = \max\{\lambda_1, \dots, \lambda_n\}. \tag{9.303}$$

Nous montrons que si $y \in K$ alors $y \in \lambda U$. Soit $y \in K$. Vu que les $\lambda_i U$ forment un recouvrement de K, il existe i et $u \in U$ tels que

$$y = \lambda_i u = \frac{\lambda_i}{\lambda} \lambda U. \tag{9.304}$$

La partie λU est convexe et contient 0, donc $\mu(\lambda U) \subset \lambda U$ pour tout $\mu \in [0,1]$. Étant donné que $\lambda_i/\lambda \leqslant 1$ nous avons

$$y = \lambda_i u = \frac{\lambda_i}{\lambda}(\lambda u) \in \frac{\lambda_i}{\lambda} \lambda U \subset \lambda U. \tag{9.305}$$

(2) **Si U n'est pas convexe** Étant donné que X est localement convexe nous pouvons considérer un voisinage convexe U' de zéro tel que $U' \subset U$. Par le point précédent il existe $\lambda > 0$ tel que $K \subset \lambda U' \subset \lambda U$.

□

Voici une réciproque du théorème 9.273.

THOooKNXGooEebnxI

Théorème 9.275 ([285]).
Soit en espace vectoriel X et une collection $\mathcal{B}$ de parties de X vérifiant

(1) les éléments sont absorbants et absolument convexes.

(2) pour tout $A, B \in \mathcal{B}$, il existe $W \in \mathcal{B}$ tel que $W \subset A \cap B$,

(3) pour tout $A \in \mathcal{B}$, et pour tout $\rho > 0$, il existe $W \in \mathcal{B}$ tel que $W \subset \rho A$.

Alors il existe une unique topologie τ sur X telle que

(1) τ est compatible avec la structure vectorielle de X,

(2) (X, τ) est localement convexe

(3) la collection $\mathcal{B}$ est une base de voisinages de 0

[125] Définition 9.269.
[126] Absolument convexe : convexe et équilibrée.
[127] Définition 9.269.

PROPooUQLUooDQfYLT

Proposition 9.276.
Soit un espace vectoriel normé[128] $(V, \|.\|)$. *Pour tout* $a \in V$ *et* $r > 0$, *la boule* $B(a,r)$ *est convexe*[129]. *La boule fermée* $\overline{B(a,r)}$ *également.*

Démonstration. En deux parties.

(1) **La boule centrée en zéro** Soient $x, y \in B(0,r)$ et $\lambda \in]0,1[$. Alors

$$\|\lambda x + (1-\lambda)y\| \leqslant |\lambda|\|x\| + |1-\lambda|\|y\| < (|\lambda| + |1-\lambda|)r \leqslant r \tag{9.306}$$

où nous avons utilisé le fait que $|\lambda| = \lambda$ et $|1-\lambda| = 1-\lambda$.

Cela prouve que $\lambda x + (1-\lambda)y \in B(0,r)$. Notez l'inégalité stricte due au fait que $\|x\| < r$ et $\|y\| < r$. Dans le cas de la boule fermée, nous avons une inégalité large.

(2) **La boule centrée autre part**

Soient $x, y \in B(a,r)$. Alors $x-a$ et $y-a$ sont dans $B(0,r)$, de telle sorte que

$$\lambda(x-a) + (1-\lambda)(y-a) \in B(0,r) \tag{9.307}$$

par la première partie. En développant et simplifiant,

$$\lambda x + (1-\lambda)y - a \in B(0,r), \tag{9.308}$$

ce qui signifie que $\lambda x + (1-\lambda)y \in B(a,r)$.

□

PROPooBVWIooZocheH

Proposition 9.277.
Tout espace métrique est localement convexe[130].

Démonstration. Les boules ouvertes forment une base de topologie par 9.159. La proposition 9.276 dit que ces boules sont convexes. □

9.10.7 Limite de suites

9.278.
Si (x_n) est une suite dans un espace vectoriel topologique, rien ne garantit qu'elle ait une limite, ni qu'elle soit unique. Donc lorsque nous écrivons

$$x_n \xrightarrow{V} x, \tag{9.309}$$

nous sous-entendons seulement que x est une limite.

De même, dans la proposition 9.283, nous montrerons que $x_n + y_n \xrightarrow{V} x+y$ et $\lambda x_n \xrightarrow{V} \lambda x$. Cela signifie que si x et y sont des limites de (x_n) et (y_n), alors $x+y$ est une limite de (x_n+y_n) et que λx est une limite de (λx_n).

Si V est un espace vectoriel topologique dans lequel il n'y a pas unicité de la limite[131], nous ne pouvons pas exactement dire que le processus de limite est une opération linéaire sur l'ensemble des suites convergentes.

PROPooTJQPooMHtOAv

Proposition 9.279 ([1]).
Soit une suite (x_k) *dans l'espace vectoriel topologique* X. *L'élément* x *est une limite de* (x_k) *si et seulement si* 0 *est une limite de* $(x - x_k)$.

Démonstration. En deux parties.

(1) $\Rightarrow$ Supposons que x est une limite de (x_k). Soit un ouvert $\mathcal{O}$ autour de 0. La partie $\mathcal{O} + x$ est un ouvert autour de x (proposition 9.279). Donc il existe N tel que si $n \geqslant N$, alors $x_n \in \mathcal{O} + x$. Pour ces valeurs de n nous avons $x_n - x \in \mathcal{O}$.

(2) $\Leftarrow$ Soit un ouvert $\mathcal{O}$ autour de x. La partie $\mathcal{O} - x$ est un ouvert autour de 0. À partir de là la preuve fonctionne comme dans l'autre sens.

[128] Définition 9.232.
[129] Définition 9.228.
[130] Définition 9.269.
[131] La proposition 9.90 dit qu'il y a unicité de la limite dans les espaces topologiques séparés.

□

PROPooQIQSooHbNkIy

Proposition 9.280 ([1]).
Soient deux suites (x_k) et (y_k) dans l'espace vectoriel topologique X. Si x est une limite[132] *de (x_k) et si y est une limite de (y_k), alors $x+y$ est une limite de (x_k+y_k).*

Démonstration. En deux parties

(1) **Le cas $x=y=0$** Nous commençons avec $x=y=0$. Soit un ouvert A autour de 0. La proposition 9.267 nous permet de considérer un voisinage U de 0 tel que $U\subset A$ et $U+U\subset A$.

Vu que 0 est une limite de (x_k), il existe N tel que $x_n\in U$ pour tout $b\geqslant N$. Quitte à prendre le maximum, nous supposons aussi que $y_n\in U$ pour $n\geqslant N$. Avec ça, $x_n+y_n\in U+U\subset A$. Cela montre que 0 est une limite de (x_k+y_k).

(2) **Le cas général** Nous supposons que x est une limite de (x_k) et que y est une limite de (y_k). La proposition 9.279 nous dit que 0 est une limite de $x-x_k$ et de $y-y_k$. La première partie dit alors que 0 est une limite de

$$k\mapsto x-x_k+y-y_k=x_k+y_k-(x+y). \tag{9.310}$$

La proposition 9.279, prise dans l'autre sens nous dit alors que $x+y$ est une limite de $k\mapsto x_k+y_k$.

□

LEMooJDJVooHUKdSe

Lemme 9.281 ([1]).
Soient un espace vectoriel topologique V ainsi qu'une suite (x_n) dans V. Nous avons

$$x_n\xrightarrow{V}x \tag{9.311}$$

si et seulement si

$$x_n-x\xrightarrow{V}0. \tag{9.312}$$

Démonstration. En deux parties.

(1) $\Rightarrow$ soit un voisinage u de 0 dans x. La partie $U+x$ est un voisinage de x, et donc il existe $N>0$ tel que si $n\geqslant N$, alors $x_n\in U+x$. Si $x_n\in U+x$, alors $x_n-x\in U$. Cela signifie que $x_n-x\xrightarrow{X}0$.

(2) $\Leftarrow$ Même raisonnement, mais en partant d'un voisinage U de x.

□

9.282.
Dans la proposition 9.283, nous considérons un espace vectoriel topologique. Il n'y a pas de produit. Pour la convergence

$$x_ky_k\xrightarrow{xy}, \tag{9.313}$$

voir la proposition 11.27.

PROPooZRCBooKiJhDg

Proposition 9.283 ([1]).
Soit V, un espace vectoriel topologique. Soient deux suites convergentes $x_n\xrightarrow{V}x$ et $y_n\xrightarrow{V}y$ ainsi que $\lambda\in\mathbb{K}$. Alors

ITEMooSHPAooQyEkgT

(1)

$$x_n+y_n\xrightarrow{V}x+y. \tag{9.314}$$

ITEMooYHHYooYATzWE

(2)

$$\lambda x_n\xrightarrow{V}\lambda x. \tag{9.315}$$

Démonstration. En deux parties.

(1) **(1)** Nous allons montrer que $x_n+y_n-(x+y)\xrightarrow{V}0$; ce sera suffisant par le lemme 9.281.
Soit un ouvert $\mathcal{O}$ autour de 0. Soient des ouverts U_1 et U_2 autour de 0 tels que $U_1+U_2\subset\mathcal{O}$ (lemme 9.266).

Vues les convergences de (x_n) et de (y_n), il existe un N tel que $n\geqslant N$ implique $x_n-x\in U_1$ et $y_n-y\in U_2$. Dans ce cas, $x_n+y_n-(x+y)\in U_1+U_2\subset\mathcal{O}$.

Donc pour $n\geqslant N$ nous avons bien $x_n-y_n-(x+y)\in\mathcal{O}$, ce qui signifie que $x_n+y_n\xrightarrow{V}x+y$.

[132] Limite de suite, définition 9.14.

(2) **(2)** En plusieurs étapes.

(2a) $x_n - x \xrightarrow{V} 0$ C'est le lemme 9.281.

(2b) $\lambda x_n - \lambda x \xrightarrow{V} 0$ Soit un ouvert $\mathcal{O}$ autour de 0. Par le lemme 9.242, il existe un ouvert U autour de 0 tel que $\lambda U \subset \mathcal{O}$. Comme $x_n - x \xrightarrow{V} 0$, il existe N tel que $n \geqslant N$ implique $x_n - x \in U$. Pour ces N et n nous avons aussi $\lambda(x_n - x) \in \lambda U \subset \mathcal{O}$. Nous avons donc démontré que $\lambda x_n - \lambda x \xrightarrow{V} 0$.

(2c) **Conclusion** Encore le lemme 9.281 nous permet de déduire que $\lambda x_n \xrightarrow{V} \lambda x$.

□

9.11 Applications continues

9.11.1 Continuité

La définition de la continuité d'une fonction est donnée en 9.48.

9.284.
Lorsque nous écrivons $f\colon X \to Y$, nous entendons que f est définie sur tout X, mais pas qu'elle soit surjective sur Y. En particulier, pour que f soit continue en a, il faut que a soit dans le domaine de définition de f.

Dans le cas de fonctions $\mathbb{R} \to \mathbb{R}$, l'espace X sera la partie de $\mathbb{R}$ sur laquelle f sera définie, et la topologie sera la topologie induite de $\mathbb{R}$.

PROPooOXBCooIzLaPe

Proposition 9.285 ([291]).
Soient deux espaces topologiques X et Y. Une application $f\colon X \to Y$ est continue[133] *si et seulement si pour tout $x \in X$ et pour tout voisinage*[134] *V de $f(x)$, la partie $f^{-1}(V)$ est un voisinage de x dans X.*

Démonstration. En deux parties.

(1) $\Rightarrow$ Soient $x \in X$ et un voisinage V de $f(x)$ dans Y. Il existe alors un ouvert $\mathcal{O}$ de Y tel que $f(x) \in \mathcal{O} \subset V$.

La partie $f^{-1}(\mathcal{O})$ vérifie :

- $f^{-1}(\mathcal{O})$ est un ouvert de X parce que f est continue.
- $x \in f^{-1}(\mathcal{O})$
- $f^{-1}(\mathcal{O}) \subset f^{-1}(V)$.

Donc $f^{-1}(V)$ contient un ouvert contenant x. Donc $f^{-1}(V)$ est un voisinage de x dans X.

(2) $\Leftarrow$ Soit un ouvert $\mathcal{O}$ de Y. Nous devons prouver que $f^{-1}(\mathcal{O})$ est un ouvert de X. Pour cela nous prouvons que $f^{-1}(\mathcal{O})$ contient un ouvert autour de chacun de ses éléments et utilisons le théorème 9.8.

Soit donc $x \in f^{-1}(\mathcal{O})$. La partie $\mathcal{O}$ est un voisinage de $f(x)$. Donc $f^{-1}(\mathcal{O})$ est un voisinage de x. Il existe donc un ouvert V de X tel que

$$x \in V \subset f^{-1}(\mathcal{O}). \tag{9.316}$$

Nous en déduisons que $f^{-1}(\mathcal{O})$ contient bien un ouvert autour de chacun de ses points.

□

La proposition 9.371 donnera des détails sur ce qu'il se passe lorsque l'espace est métrique.

ThoESCaraB

Théorème 9.286.
Une fonction $f\colon X \to Y$ est une fonction continue si et seulement si elle est continue en chacun des points de X.

Démonstration. En deux parties.

[133] Définition 9.48.
[134] Définition 9.4

(1) $\Rightarrow$ Nous supposons que f est une fonction continue. Soient $a \in X$ et W un voisinage de $f(a)$. Nous considérons $\mathcal{O}$, un voisinage ouvert de $f(a)$ contenu dans W ; l'ensemble $f^{-1}(\mathcal{O})$ est alors un ouvert contenant a, et l'image de $f^{-1}(\mathcal{O})$ par f est bien entendu contenue dans W.

(2) $\Leftarrow$ Soit $\mathcal{O}$ un ouvert de Y. Pour prouver que $f^{-1}(\mathcal{O})$ est un ouvert de X, nous allons considérer un élément $a \in f^{-1}(\mathcal{O})$ et montrer qu'il existe un voisinage ouvert de a contenu dans $f^{-1}(\mathcal{O})$; le théorème 9.8 nous assurera alors que $f^{-1}(\mathcal{O})$ est ouvert.

L'ensemble $\mathcal{O}$ est un voisinage ouvert de $f(a)$ parce que a a été choisi dans $f^{-1}(\mathcal{O})$. Donc la continuité de f en a nous assure qu'il existe un voisinage W de a tel que $f(W) \subset \mathcal{O}$. En prenant un ouvert contenant a à l'intérieur de W nous avons un voisinage ouvert de a contenu dans $f^{-1}(\mathcal{O})$.

□

Remarque 9.287.
À cause de l'éventuelle non unicité de la limite, deux fonctions continues et égales sur un sous-ensemble dense ne sont pas spécialement égales. Ce sera vrai sur les espaces métriques et plus généralement pour les espaces séparés. Voir l'exemple 9.78 et la proposition 9.154.

LEMooCQQWooVSAWiy

Lemme 9.288 ([1]).
Soient une fonction $f\colon X \to Y$, et un point d'accumulation $a \in X$[135]. La fonction f est continue en a si et seulement si $f(a)$ est une limite de f en a.

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que f est continue en $a \in X$. Soit un ouvert V de Y contenant $f(a)$. Par continuité de f au point[136] a, il existe un voisinage U de a tel que $f(U) \subset V$. À fortiori, $f\big(U \setminus a\big) \subset W$ comme le demande la définition de la limite.

(2) $\Leftarrow$ Nous supposons que $f(a)$ est une limite de $f(x)$ lorsque x tend vers a. Si W est un ouvert de Y contenant $f(a)$, il existe un voisinage V de a dans X tel que $f\big(V \setminus a\big) \subset W$. Mais puisque $f(a) \in W$, nous avons $f(V) \subset W$.

□

LEMooQFISooYWkzPR

Lemme 9.289 ([1]).
Soient des espaces topologiques X et Y ainsi qu'une application continue $f\colon X \to Y$. Soient

(1) $a \in X$ et $b = f(a) \in Y$.

(2) Un voisinage ouvert V de b dans Y.

Alors il existe un voisinage ouvert U de a tel que $f(U) \subset V$.

9.11.1.1 Composition

PROPooCNTBooTkOJuK

Proposition 9.290 (Composée d'application continues[1]).
Soient des espaces topologiques X, Y, Z ainsi que des applications continues $f\colon X \to Y$ et $g\colon Y \to Z$. Alors l'application $g \circ f\colon X \to Z$ est continue.

Démonstration. Soit un ouvert $\mathcal{O}$ de Z. Nous avons

$$(g \circ f)^{-1}(\mathcal{O}) = (f^{-1} \circ g^{-1})(\mathcal{O}) = f^{-1}\big(g^{-1}(\mathcal{O})\big). \tag{9.317}$$

Vu que f est continue, la partie $g^{-1}(\mathcal{O})$ est ouverte dans Y. Et comme f est continue, $f^{-1}\Big(g^{-1}(\mathcal{O})\Big)$ est ouvert dans X. □

9.11.2 Continuité et topologie induite

PROPooNPLBooPfmmym

Proposition 9.291 ([1]).
Soit une fonction $f\colon X \to Y$, continue sur l'ouvert A de X au sens où elle est continue en chaque point de A. Alors la fonction restriction $\tilde{f}\colon A \to Y$ est également continue pour la topologie sur A, induite[137] de X.

[135] Un point d'accumulation de X n'est pas spécialement dans X, si X est un sous-espace d'un autre. Par exemple 0 est un point d'accumulation de $]0,1[$ dans $\mathbb{R}$. Ici nous supposons que $a \in X$, sinon il n'y a de toute façon pas de continuité en a.
[136] Continuité en un point, définition 9.48(1).
[137] Définition 9.30.

Démonstration. Soit $a \in A$, et montrons que $\tilde{f}$ est continue en a, c'est-à-dire que $\tilde{f}(a) = f(a)$ soit une limite de $\tilde{f}$ en a. Soit un voisinage V de $\tilde{f}(a)$ dans Y. Par la continuité de f, nous avons un ouvert W de X tel que

$$f\big(W \setminus \{a\}\big) \subset V. \tag{9.318}$$

La partie $W \cap A$ est un voisinage de a pour la topologie de A, et vérifie

$$f\big(W \cap A \setminus \{a\}\big) \subset V. \tag{9.319}$$

donc $f(a)$ est une limite de $\tilde{f}$ pour $x \to a$. La fonction $\tilde{f}\colon A \to Y$ est continue en chaque point de A. □

Au niveau de la notion de continuité, il n'y a pas trop de changements en passant de $\mathbb{R}$ à $\mathbb{Q}$ muni de la topologie induite.

EXooHWIlooYYbfGE

Exemple 9.292.
Que signifie d'être continue pour une fonction $f\colon \mathbb{Q} \to \mathbb{R}$? D'après le théorème 9.286, il s'agit d'être continue en chaque point de $\mathbb{Q}$. Il s'agit donc, par la définition 9.48 que pour tout $q \in \mathbb{Q}$, le nombre $f(q)$ soit une limite de f pour $x \to q$.

L'espace d'arrivée étant $\mathbb{R}$, un voisinage de $f(q)$ est pris comme une boule de taille ϵ. La continuité de f exige qu'il y ait un voisinage W de q dans $\mathbb{Q}$ tel que pour tout $q' \in W$ (différent de q), $|f(q) - f(q')| < \epsilon$.

Qu'est-ce qu'un ouvert dans $\mathbb{Q}$? D'après la définition 9.30 de la topologie induite, ce sont les ensembles $\mathbb{Q} \cap \mathcal{O}$ avec $\mathcal{O}$ ouvert dans $\mathbb{R}$. Tout cela pour dire que pour tout $\epsilon > 0$, il doit exister $\delta > 0$ tel que pour tout $q' \in \mathbb{Q}$ tel que $0 < |q - q'| < \delta$, nous ayons $|f(q) - f(q')| < \epsilon$.

Bref, c'est exactement le mécanisme usuel de la continuité sur $\mathbb{R}$, sauf qu'il ne faut considérer que les rationnels. △

LEMooHAODooYSPmvH

Lemme 9.293 (Application partielle[1])**.**
Soient trois espaces topologiques X_1, X_2 et Y. Nous considérons une fonction continue $f\colon X_1 \times X_2 \to Y$ ainsi que $x_1 \in X_1$. Alors l'application

$$\begin{aligned} g\colon X_2 &\to Y \\ x_2 &\mapsto f(x_1, x_2) \end{aligned} \tag{9.320}$$

est continue.

Démonstration. Soit un ouvert $\mathcal{O}$ de Y ; par hypothèse sur f, la partie $f^{-1}(\mathcal{O})$ est ouverte dans $X_1 \times X_2$. Notre but est de prouver que $g^{-1}(\mathcal{O})$ est un ouvert de X_2. Nous avons :

$$g^{-1}(\mathcal{O}) = \{x_2 \in X_2 \text{ tel que } (x_1, x_2) \in f^{-1}(\mathcal{O})\}. \tag{9.321}$$

Nous considérons $x_2 \in g^{-1}(\mathcal{O})$ et nous prouvons qu'il existe dans X_2 un voisinage de x_2 entièrement contenu dans $g^{-1}(\mathcal{O})$.

Étant donné que (x_1, x_2) est dans $f^{-1}(\mathcal{O})$ qui est ouvert, la définition 9.66 de la topologie sur $X_1 \times X_2$ nous donne des ouverts A_1 dans X_1 et A_2 dans X_2 tels que

$$(x_1, x_2) \in A_1 \times A_2 \subset f^{-1}(\mathcal{O}). \tag{9.322}$$

Nous montrons à présent que $A_2 \subset g^{-1}(\mathcal{O})$. Soit $y_2 \in A_2$. Par construction $(x_1, y_2) \in A_1 \times A_2 \subset f^{-1}(\mathcal{O})$, donc

$$g(y_2) = f(x_1, y_2) \in \mathcal{O}. \tag{9.323}$$

Cela termine la démonstration. □

9.11.3 Continuité et connexité

PropConnexiteViaFonction

Proposition 9.294.
Un espace topologique X est connexe si et seulement si toute application continue[138] *$X \to \mathbb{Z}$ est constante.*

Démonstration. En deux parties.

(1) $\Rightarrow$ Soit une fonction continue $f\colon X \to \mathbb{Z}$. Supposons qu'elle ne soit pas constante. Nous allons en déduire que X n'est pas connexe. En effet supposons que $f(a) = u$ et $f(b) = v$ avec $u \neq v$. Nous posons

$$\begin{aligned} A &= f^{-1}(u) \\ B &= X \setminus A. \end{aligned} \tag{9.324}$$

[138] La topologie sur $\mathbb{Z}$ est celle de l'ensemble des parties. C'est également la topologie induite de $\mathbb{R}$, mais ça n'a aucune importance pour l'instant.

La partie A est ouverte parce que $\{u\}$ est ouvert dans $\mathbb{Z}$. La partie B est également ouverte parce que c'est une union d'ouverts : $B = \bigcup_{n\neq u} f^{-1}(n)$. La parie A contient a, et B contient b.

Voilà. Ce sont deux parties ouvertes non vides, disjointes qui recouvrent X. Donc X n'est pas connexe.

(2) $\Leftarrow$ Encore par l'absurde nous supposons que X n'est pas connexe. Soient deux ouverts A et B qui font ce qu'il faut. Alors en définissant

$$\begin{aligned} f\colon X &\to \mathbb{Z} \\ x &\mapsto \begin{cases} 0 & \text{si } x\in A \\ 1 & \text{si } x\in B, \end{cases} \end{aligned} \tag{9.325}$$

nous avons une fonction continue non constante sur X à valeurs dans $\mathbb{Z}$.

□

NORMooSCAWooPFnrVj

9.295.
Pour mettre les idées au clair, dire qu'une partie A n'est pas connexe[139] signifie qu'il existe des ouverts $\mathcal{O}_1$ et $\mathcal{O}_2$ vérifiant

ITEMooRACDooKLaVXP

(1) $\mathcal{O}_i \cap A \neq \varnothing$

ITEMooNCQVooNjAYCT

(2) $\mathcal{O}_1 \cap \mathcal{O}_2 = \varnothing$

ITEMooPIHJooNJYpQo

(3) $A \subset \mathcal{O}_1 \cup \mathcal{O}_2$.

LemConncontconn

Lemme 9.296.
L'image d'un connexe par une application continue est connexe.

Démonstration. Soit une application continue $f\colon X \to Y$ entre deux espaces topologiques.

Nous allons prouver la contraposée. Soit A une partie de Y telle que $f(A)$ ne soit pas connexe. Nous allons prouver que A elle-même n'est pas connexe. Vu que $f(A)$ n'est pas connexe, il existe des ouverts disjoints $\mathcal{O}_1$ et $\mathcal{O}_2$ recouvrant $f(A)$ et intersecant tous deux A. Nous prouvons que A n'est pas connexe en considérant les parties $A_1 = f^{-1}(\mathcal{O}_1)$ et $A_2 = f^{-1}(\mathcal{O}_2)$, et en vérifiant les propriétés de 9.295.

(1) **A_i est ouvert** Les parties A_i sont ouvertes parce qu'elles sont images inverses d'ouverts par une fonction continue (définition 9.48(2)).

(2) **Pour (1)** Nous devons prouver que $A_i \cap A \neq \varnothing$, c'est-à-dire qu'il existe un $x \in f^{-1}(\mathcal{O}_i) \cap A$.

Nous commençons par considérer $y \in \mathcal{O}_i \cap f(A)$. Nous avons d'une part $f^{-1}(y) \subset f^{-1}(\mathcal{O}_i) = A_i$. D'autre part, vu que $y \in f(A)$, nous avons $f^{-1}(y) \cap A \neq \varnothing$. Nous prenons donc $x \in f^{-1}(y) \cap A$.

Ce x vérifie $x \in f^{-1}(y) \cap A \subset A_i \cap A$.

(3) **Pour (2)** Si $x \in f^{-1}(\mathcal{O}_1) \cap f^{-1}(\mathcal{O}_2)$, alors $f(x) \in \mathcal{O}_1 \cap \mathcal{O}_2$, ce qui contredirait le fait que $\mathcal{O}_1$ et $\mathcal{O}_2$ sont disjoints. Il n'y a donc pas d'éléments dans l'intersection de $f^{-1}(\mathcal{O}_1)$ et de $f^{-1}(\mathcal{O}_2)$.

(4) **Pour (3)** Si $f^{-1}(\mathcal{O}_1)$ et $f^{-1}(\mathcal{O}_2)$ ne recouvrent pas A, il existe un x dans A qui n'est dans aucun des deux. Dans ce cas, $f(x)$ est dans $f(A)$, mais n'est ni dans $\mathcal{O}_1$, ni dans $\mathcal{O}_2$, ce qui contredirait le fait que ces deux derniers recouvrent $f(A)$.

Nous déduisons que A n'est pas connexe. Et donc le lemme. □

Une application de ce lemme sera le théorème des valeurs intermédiaires 11.92.

Exemple 9.297.
Les espaces topologiques $\mathbb{R}$ et $\mathbb{R}^2$ ne sont pas homéomorphes. △

Démonstration. Supposons par l'absurde que $f\colon \mathbb{R} \to \mathbb{R}^2$ soit un homéomorphisme. Nous posons $E = f\big(\mathbb{R}\setminus\{0\}\big)$ et $z_0 = f(0)$. Puisque f est bijective nous avons

$$E = \mathbb{R}^2 \setminus \{z_0\}, \tag{9.326}$$

qui est connexe.

Comme E est connexe et que f^{-1} est continue, le lemme 9.296 nous dit que $f^{-1}(E)$ est connexe. Mais par définition, $f^{-1}(E) = \mathbb{R}\setminus\{0\}$ qui n'est pas connexe. □

[139] Connexe, définition 9.118.

9.11.4 Continuité et compacité

La proposition 9.367 dira que l'image d'un compact par une application continue est compacte. Nous démontrons ici en général.

ThoImCompCotComp

Théorème 9.298.
L'image d'un compact[140] *par une fonction continue est un compact.*

Démonstration. Soit $K \subset X$, un ensemble compact, et étudions $f(K)$; en particulier, nous considérons Ω, un recouvrement de $f(K)$ par des ouverts. Nous avons

$$f(K) \subseteq \bigcup_{\mathcal{O}\in\Omega} \mathcal{O}. \tag{9.327}$$

Par construction, nous avons aussi

$$K \subseteq \bigcup_{\mathcal{O}\in\Omega} f^{-1}(\mathcal{O}), \tag{9.328}$$

en effet, si $x \in K$, alors $f(x)$ est dans un des ouverts de Ω, disons $f(x) \in \mathcal{O}$, et évidemment, $x \in f^{-1}(\mathcal{O})$. Les $f^{-1}(\mathcal{O})$ recouvrent le compact K, et donc on peut en choisir un sous-recouvrement fini, c'est-à-dire un choix de $\{f^{-1}(\mathcal{O}_1), \dots, f^{-1}(\mathcal{O}_n)\}$ tels que

$$K \subseteq \bigcup_{i=1}^{n} f^{-1}(\mathcal{O}_i). \tag{9.329}$$

Dans ce cas, nous avons

$$f(K) \subseteq \bigcup_{i=1}^{n} \mathcal{O}_i, \tag{9.330}$$

ce qui prouve la compacité de $f(K)$. □

9.11.5 Distance uniforme

PROPooNSCCooJuqOQe

Proposition 9.299 ([292]).
Soient un compact K et un espace métrique[141] *(E, d). Nous notons $C(K, X)$ l'ensemble des applications continues*[142] *de K vers X. Alors l'application*

$$\begin{aligned} d_\infty \colon C(K,E) \times C(K,E) &\to \mathbb{R} \\ (f,g) &\mapsto \sup_{x\in K} d\big(f(x), g(x)\big) \end{aligned} \tag{9.331}$$

est une distance.

9.11.6 Continuité de la réciproque sur un compact

LEMooPLGTooATIGov

Lemme 9.300 ([293]).
Soit une application continue et bijective $f \colon K \to X$ où K est compact et X est métrique. Alors la réciproque $f^{-1} \colon X \to K$ est continue.

Démonstration. Nous allons montrer que si F est fermé dans K, alors $(f^{-1})^{-1}(F)$ est fermé dans X. Le lemme 9.52 conclura. Si F est fermé dans K, alors F est compact (lemma 9.137(1)). Le théorème 9.298 dit que l'image d'un compact par une application continue est compacte. Donc $f(F)$ est compact dans X. Mais comme X est métrique, tout compact est fermé (lemme 9.137(2)). Bref, $f(F)$ est fermé. □

LEMooNEEVooSeHYzx

Lemme 9.301.
Soit un espace compact K et un espace topologique séparé X. Si $f \colon K \to X$ est une bijection continue, alors f est un isomorphisme d'espaces topologiques.

LEMooKSDKooDbKKeB

Lemme 9.302 ([1]).
Soit un espace vectoriel normé V ainsi qu'une application continue $f \colon [a, b] \to V$. Nous supposons que $f \colon [a, b[\to V$ est injective.

[140] Définition 9.125.
[141] Définition 9.155.
[142] Pour la topologie métrique 9.158.

Alors en posant $S = f\big([a,b[\big)$, l'application réciproque

$$f^{-1}: S \to [a,b[\tag{9.332}$$

est continue.

Démonstration. Pour tout $x \in [a,b]$ nous notons $V_x = f\big([a,x]\big)$.

Par hypothèse d'injectivité, l'existence de f^{-1} sur V_b est assurée. En ce qui concerne sa continuité, pour chaque $x \in]a,b[$, l'application $f: [a,x] \to V_x$ vérifie le lemme 9.300. Donc l'application réciproque $f^{-1}: V_x \to [a,x]$ est continue.

Le théorème 9.286 dit alors que l'application f^{-1} est donc continue en chaque point de V_x pour tout $a < x < b$. Elle est donc continue en chaque point de $f\big([a,b[\big)$ parce que chacun de ces points est dans un V_x. Le théorème 9.286 (dans l'autre sens) montre alors que $^{-1}: S \to [a,b[$ est continue. □

9.11.7 Espace vectoriel topologique

PROPooHUWQooPWYBUu

Proposition 9.303 ([1]).
Soient un espace vectoriel topologique E et une application linéaire $f \in \mathcal{L}(E,V)$ où V est un espace vectoriel normé. Si f est bornée sur un voisinage de 0, alors f est continue.

Démonstration. En plusieurs parties.

(1) **f est continue en 0** Nous vérifions la définition 9.48(1) d'une fonction continue en un point. Soit un ouvert $\mathcal{O}$ de V contenant $f(0) = 0$. Vu que V est normé, il existe $r > 0$ tel que $B(0,r) \subset \mathcal{O}$. Comme f est bornée sur un voisinage de 0, nous pouvons considérer un voisinage U de 0 dans E tel que $f(U) \subset B(0,m)$. Si nous prenons $\delta < r/m$, alors

$$f\big(\delta U\big) = \delta f(U) \subset \delta B(0,m) = B(0,\delta m) = B(0,r) \subset \mathcal{O}. \tag{9.333}$$

Donc le voisinage δU[143] de 0 fait fonctionner la définition 9.48(1).

(2) **Continue partout** C'est la proposition 9.243.

□

9.12 Produit fini d'espaces vectoriels normés

sec_prod

Dans cette section nous parlons de produits finis d'espaces. Cela ne signifie pas que chacun des espaces soient séparément de dimension finie.

9.12.1 Distance et norme produit

DefZTHxrHA

Proposition-Définition 9.304 (Distance produit).
Si (E_1,d_1),..., (E_n,d_n) sont des espaces métriques alors la formule

$$d(x,y) = \max_{i=1,\dots,n} d_i(x_i,y_i) \tag{9.334}$$

*définit une distance sur le produit cartésien $E = E_1 \times \dots \times E_n$. Elle est la **distance produit**.*

La définition de la norme sur un produit d'espaces vectoriels normés découle immédiatement de la définition de la distance 9.304 :

DefFAJgTCE

Lemme-Définition 9.305 ([294]).
Soient V et W deux espaces vectoriels sur $\mathbb{K}$. Si (v_1,w_1) et (v_2,w_2) sont des éléments de $V \times W$ et si λ est un élément de $\mathbb{K}$, alors les opérations suivantes donnent une structure d'espace vectoriel au produit $V \times W$:

- $(v_1,w_1) + (v_2,w_2) = (v_1 + v_2, w_1 + w_2)$
- $\lambda(v_1,w_1) = (\lambda v_1, \lambda w_1)$.

Démonstration. Il faut seulement faire les vérifications d'usage. □

LEMooFQMSooLmdIvD

Lemme-Définition 9.306 (Norme produit).
Soient deux espaces vectoriels normés V et W.

[143] C'est un voisinage par la proposition 9.241.

(1) *L'opération*

$$\|(v,w)\|_{V\times W}=\max\{\|v\|_V,\|w\|_W\}. \tag{9.335}$$

est une norme[144] *sur* $V\times W$.

(2) *La topologie de cette norme*[145] *est la même que la topologie produit*[146] *sur* $V\times W$.

Démonstration. En plusieurs parties.

(1) **Norme** On doit vérifier les trois conditions de la définition 9.232.

- Soit (v,w) dans $V\times W$ tel que $\|(v,w)\|_{V\times W}=\max\{\|v\|_V,\|w\|_W\}=0$. Alors $\|v\|_V=0$ et $\|w\|_W=0$, donc $v=0_V$ et $w=0_W$. Cela implique $(v,w)=(0_v,0_w)=0_{V\times W}$.
- Pour tout a dans $\mathbb{R}$ et (v,w) dans $V\times W$, la norme $\|a(v,w)\|_{V\times W}$ se calcule de la façon suivante :

$$\|a(v,w)\|_{V\times W}=\max\{\|av\|_V,\|aw\|_W\}=|a|\max\{\|v\|_V,\|w\|_W\}=|a|\|(v,w)\|_{V\times W}. \tag{9.336}$$

- Soient (v_1,w_1) et (v_2,w_2) dans $V\times W$.

$$\begin{aligned}\|(v_1,w_1)+(v_2,w_2)\|_{V\times W}&=\max\{\|v_1+v_2\|_V,\|w_1+w_2\|_W\}\\&\leqslant\max\{\|v_1\|_V+\|v_2\|_V,\|w_1\|_W+\|w_2\|_W\}\\&\leqslant\max\{\|v_1\|_V,\|w_1\|_W\}+\max\{\|v_2\|_V,\|w_2\|_W\}\\&=\|(v_1,w_1)\|_{V\times W}+\|(v_2,w_2)\|_{V\times W}.\end{aligned} \tag{9.337}$$

(2) **Équivalence**

Dans cette preuve, nous considérons la « topologie de $V\times W$ » comme étant la topologie produit et « la topologie métrique de $V\times W$ » la topologie de la norme produit.

(2a) **Dans un sens** La définition 9.66 de la topologie produit dit qu'une prébase de $V\times W$ est donnée par

$$\big\{B(v,r)\times B(w,s)\text{ tel que }v\in V;w\in W;r,s>0\big\}. \tag{9.338}$$

Nous prouvons maintenant que la partie $S=B(v_0,r)\times B(w_0,s)$ est un ouvert de l'espace $\big(V\times W,\|.\|_{V\times W}\big)$. Pour cela nous prouvons que tout élément de S contient un voisinage métrique contenu dans S.

Soit $(v_1,w_1)\in S$. Nous posons

$$d\big((v_1,w_1),(v_0,w_0)\big)=\delta<\max\{r,s\}. \tag{9.339}$$

Nous considérons $\epsilon>0$ et nous montrons que si ϵ est assez petit, $B\big((v_1,w_1),\epsilon\big)\subset S$. Pour cela nous considérons $(v,w)\in B\big((v_1,w_1),\epsilon\big)$ et nous calculons un tout petit peu :

$$d\big((v,w),(v_0,w_0)\big)\leqslant d\big((v,w),(v_1,w_1)\big)+d\big((v_1,w_1),(v_0,w_0)\big) \tag{9.340a}$$

$$<\epsilon+\delta. \tag{9.340b}$$

Si ϵ est assez petit, le tout reste plus petit que $\max\{r,s\}$.

Donc S est bien un ouvert métrique par le théorème 9.8. Vu que la topologie métrique contient une prébase de la topologie produit, tout ouvert de la topologie produit est un ouvert de la topologie métrique.

(2b) **Dans l'autre sens** Soient un ouvert métrique $\mathcal{O}$ ainsi que $(v_0,w_0)\in\mathcal{O}$; il existe $r>0$ tel que

$$B\big((v_0,w_0),r\big)\subset\mathcal{O}. \tag{9.341}$$

Nous affirmons que $B(v_0,r)\times B(w_0,r)$ est contenu dans $\mathcal{O}$, de telle sorte que $\mathcal{O}$ soit un ouvert de la topologie produit. Pour $(v_1,w_1)\in B(v_0,r)\times B(w_0,r)$ nous avons

$$d\big((v_1,w_1),(v_0,w_0)\big)=\max\{\|v_1-v_0\|,\|w_1-w_0\|\}<r \tag{9.342}$$

parce que $v_1\in B(v_0,r)$ et $w_1\in B(w_0,r)$.

Donc tout élément de $\mathcal{O}$ admet un voisinage « produit » contenu dans $\mathcal{O}$; donc $\mathcal{O}$ est ouvert pour le topologie produit.

[144] Définition 9.232.
[145] Topologie associée à une norme : c'est la topologie associée à la distance correspondante, définition 9.238.
[146] Topologie produit, définition 9.66.

□

9.307.
En particulier, pour la topologie de la norme maximum, la convergence d'une suite implique la convergence « composante par composante » par la proposition 9.93.

On remarque tout de suite que la norme $\|.\|_\infty$ sur $\mathbb{R}^2$ est la norme de l'espace produit $\mathbb{R} \times \mathbb{R}$. En outre cette définition nous permet de trouver plusieurs nouvelles normes dans les espaces $\mathbb{R}^p$. Par exemple, si nous écrivons $\mathbb{R}^4$ comme $\mathbb{R}^2 \times \mathbb{R}^2$ on peut munir $\mathbb{R}^4$ de la norme produit

$$\|(x_1, x_2, x_3, x_4)\|_{\infty,2} = \max\{\|(x_1, x_2)\|_\infty, \|(x_3, x_4)\|_2\}.$$

Les applications de projection de l'espace produit $V \times W$ vers les espaces «facteurs», V W sont notées $\mathtt{proj}_V$ et $\mathtt{proj}_W$ et sont définies par

$$\begin{aligned} \mathtt{proj}_V \colon V \times W &\to V \\ (v, w) &\mapsto v \end{aligned} \tag{9.343}$$

et

$$\begin{aligned} \mathtt{proj}_W \colon V \times W &\to W \\ (v, w) &\mapsto w. \end{aligned} \tag{9.344}$$

Les inégalités suivantes sont évidentes

$$\begin{aligned} \|\mathtt{proj}_V(v, w)\|_V &\leqslant \|(v, w)\|_{V\times W} \\ \|\mathtt{proj}_W(v, w)\|_W &\leqslant \|(v, w)\|_{V\times W}. \end{aligned} \tag{9.345}$$

La topologie de l'espace produit est induite par les topologies des espaces «facteurs». La construction est faite en deux passages : d'abord nous disons que une partie $A \times B$ de $V \times W$ est ouverte si A et B sont des parties ouvertes de V et de W respectivement. Ensuite nous définissons que une partie quelconque de $V \times W$ est ouverte si elle est une intersection finie ou une réunion de parties ouvertes de $V \times W$ de la forme $A \times B$.

Ce choix de topologie donne deux propriétés utiles de l'espace produit

(1) Les projections sont des **applications ouvertes**. Cela veut dire que l'image par $\mathtt{proj}_V$ (respectivement $\mathtt{proj}_W$) de toute partie ouverte de $V \times W$ est une partie ouverte de V (respectivement W).

(2) Pour toute partie A de V et B de W, nous avons $\operatorname{Int}(A \times B) = \operatorname{Int} A \times \operatorname{Int} B$.[PgovlABeqbAbB]

Une propriété moins facile à prouver est que pour toute partie A de V et B de W nous avons $\overline{A \times B} = \bar{A} \times \bar{B}$. Voir la proposition 12.108.

Ce que nous avons dit jusqu'ici est valable pour tout produit d'un nombre fini d'espaces vectoriels normés. En particulier, pour tout $m > 0$ l'espace $\mathbb{R}^m$ peut être considéré comme le produit de m copies de $\mathbb{R}$.

Exemple 9.308.
Si V et W sont deux espaces vectoriels, nous pouvons considérer le produit $E = V \times W$. Les projections $\mathtt{proj}_V$ et $\mathtt{proj}_W$, définies dans la section 9.12, sont des applications linéaires.

En effet, la projection $\mathtt{proj}_V \colon V \times W \to V$ est donnée par $\mathtt{proj}_V(v, w) = v$. Alors,

$$\begin{aligned} \mathtt{proj}_V\big((v, w) + (v', w')\big) &= \mathtt{proj}_V\big((v + v'), (w + w')\big) \\ &= v + v' \\ &= \mathtt{proj}_V(v, w) + \mathtt{proj}_V(v', w'), \end{aligned} \tag{9.346}$$

et

$$\mathtt{proj}_V\big(\lambda(v, w)\big) = \mathtt{proj}_V\big((\lambda v, \lambda w)\big) = \lambda v = \lambda\, \mathtt{proj}_V(v, w). \tag{9.347}$$

Nous laissons au lecteur le soin d'adapter ces calculs pour montrer que $\mathtt{proj}_W$ est également une projection[147]. △

PropDXR_KbaLC

Proposition 9.309.
Si $\mathcal{O}$ est un voisinage de (a, b) dans $V \times W$ alors $\mathcal{O}$ contient un ouvert de la forme $B(a, r) \times B(b, r)$.

[147] Écrivez-moi si ça pose un problème.

Démonstration. Puisque $\mathcal{O}$ est un voisinage, il contient un ouvert et donc une boule

$$B\big((a,b),r\big) = \{(v,w) \in V \times W \text{ tel que } \max\{\|v-a\|, \|w-b\|\} < r\}. \tag{9.348}$$

Évidemment l'ensemble $B(a,r) \times B(b,r)$ est dedans. □

CORooMWCUooKyoyZV

Corolaire 9.310.
Un espace vectoriel normé[148] *est un espace vectoriel topologique : en d'autres mots, l'addition et la multiplication par un élément du corps sont continues.*

Démonstration. Nous nommons $\mathbb{K}$ le corps de base, qui est $\mathbb{R}$ ou $\mathbb{C}$. Pour rappel, la topologie produit et la topologie de la norme produit sont identiques par le lemme 9.306. Nous allons donc considérer cette topologie sur $E \times E$ et sur $\mathbb{K} \times E$.

(1) **Pour l'addition**
Soit

$$\begin{aligned} s\colon E \times E &\to E \\ (x,y) &\mapsto x+y, \end{aligned} \tag{9.349}$$

et prouvons que s est continue. Soit un ouvert A de E ; nous montrons que $s^{-1}(A)$ est ouvert dans $E \times E$. Pour cela nous considérons $(a,b) \in s^{-1}(A)$. Vu que A est ouvert et que $a+b \in A$, il existe $r > 0$ tel que $B(a+b,r) \subset A$. Nous allons trouver $\epsilon > 0$ tel que

$$s\big(B(a,\epsilon) \times B(b,\epsilon)\big) \subset A. \tag{9.350}$$

Notez que le produit de boules est ouvert pour la définition 9.66 de la topologie produit. Si $x \in B(a,\epsilon)$, il existe $\delta \in E$ tel que $x = a+\delta$ avec $\|\delta\| < \epsilon$ et si $y \in B(b,\epsilon)$, nous avons $y = b+\mu$ avec $\|\mu\| < \epsilon$. Nous avons

$$s(x,y) = x+y = a+b+\delta+\mu \tag{9.351}$$

et donc[149]

$$\|(a+b) - s(x,y)\| = \|\delta+\mu\| \leqslant \|\sigma\| + \|\mu\| < 2\epsilon. \tag{9.352}$$

Il suffit donc de prendre $\epsilon < r/2$.

(2) **Pour la multiplication** Nous prouvons à présent que

$$\begin{aligned} m\colon \mathbb{K} \times E &\to E \\ (\lambda, x) &\mapsto \lambda x \end{aligned} \tag{9.353}$$

est continue. Soit A ouvert dans E, soit $(\lambda,a) \in m^{-1}(A)$. Nous cherchons comme avant un $\epsilon > 0$ tel que

$$m\big(B(\lambda,\epsilon) \times B(a,\epsilon)\big) \subset A. \tag{9.354}$$

Soient $\lambda+\mu \in B(\lambda,\epsilon)$ et $a+x \in B(x,\epsilon)$. Nous avons

$$\|m(\lambda+\mu, a+x) - m(\lambda,a)\| = \|\lambda x + \mu a + \mu x\| \tag{9.355a}$$
$$\leqslant |\epsilon|\big(|\lambda| + \|a\| + |\epsilon|\big). \tag{9.355b}$$

Nous considérons donc $r > 0$ tel que $B(\lambda a, r) \subset A$, puis $\epsilon > 0$ assez petit pour que

$$\epsilon|\big(|\lambda| + \|a\| + |\epsilon|\big) < r. \tag{9.356}$$

□

PROPooYMCUooERvDpk

Proposition 9.311.
La norme est une application continue sur un espace vectoriel normé.
Plus précisément, si $(E, \|.\|)$ est un espace vectoriel normé[150]*, alors l'application*

$$\begin{aligned} f\colon E &\to \mathbb{R} \\ x &\mapsto \|x\| \end{aligned} \tag{9.357}$$

est continue.

[148] Rappel que la définition 9.232 ne définit les espaces vectoriels normés que dans le cas où le corps de base est $\mathbb{R}$ ou $\mathbb{C}$.
[149] En utilisant 9.232(4).
[150] Dont la topologie métrique est donnée par 9.158.

Démonstration. Soit la boule $B(a,r)$ dans $\mathbb{R}$. Nous montrons que $f^{-1}(B(a,r))$ est un ouvert de E pour la topologie métrique. Soit $x_0 \in f^{-1}\big(B(a,r)\big)$. Nous prenons $\alpha \in \mathbb{R}$ tel que $\big|\|x_0\| - a\big| < \alpha < r$. Et nous considérons la boule $B_E(x_0,\epsilon)$ avec ϵ que nous allons fixer plus tard.

Pour tout $x \in B_E(x_0,\epsilon)$, nous avons

$$\big|\|x\| - a\big| \leqslant \big|\|x\| - \|x_0\|\big| + \big|\|x_0\| - a\big| \tag{9.358a}$$
$$< \alpha + \epsilon. \tag{9.358b}$$

En prenant ϵ tel que $\alpha + \epsilon < r$ nous avons $f(x) \in B(a,r)$. □

PROPooQUAZooGXskwF

Proposition 9.312.
La norme sur un espace vectoriel normé est une fonction de classe C^∞.

PROPooMHAVooRgJjMB

Proposition 9.313 ([1]).
Soient des espaces vectoriels normés v et w. Nous considérons des suites convergentes $v_k \xrightarrow{V} v$ et $w_k \xrightarrow{W} w$. Alors nous avons

$$(v_k, w_k) \xrightarrow{V\times W} (v,w). \tag{9.359}$$

L'espace $V \times W$ est l'espace vectoriel normé muni de la topologie de la norme produit.

Nous étudierons plus en détail les espaces vectoriels topologiques à partir de la définition 9.239.

9.13 Topologie réelle en dimension n

Nous considérons sur $\mathbb{R}$ la topologie donnée par la valeur absolue, et sur $\mathbb{R}^n$ celle de la topologie produit ou du maximum, qui sont identiques par le lemme 9.306.

En particulier, nous n'avons pas encore la norme donnée par $\|x\| = \sqrt{\sum_i x_i^2}$, parce qu'elle demande la racine carré, définie en 11.97.

9.13.1 Ouverts et fermés

La proposition suivante est évidemment à mettre en rapport avec le théorème 9.8.

PROPooEQYJooBbPiAj

Proposition 9.314.
Une partie A de $\mathbb{R}^n$ est ouverte si et seulement si pour tout $a \in A$ il existe $r > 0$ tel que $B(a,r) \subset A$.

Démonstration. C'est la définition 9.173 de la topologie métrique. □

LemMESSExh

Lemme 9.315.
Pour tout $x \in \mathbb{R}^n$ et tout $r > 0$ la boule[151] $B(x,r)$ est ouverte.

Démonstration. Afin de prouver que la boule est ouverte, nous prenons un point $p \in B(x,r)$, et nous allons montrer qu'il existe une boule autour de p qui est contenue dans $B(x,r)$.

Étant donné que $p \in B(x,r)$, nous avons $d(p,x) < r$. Prouvons que la boule $B\big(p, r - d(p,x)\big)$ est contenue dans $B(x,r)$. Pour cela, nous prenons $p' \in B\big(p, r - d(p,x)\big)$, et nous essayons de prouver que $p' \in B(x,r)$. En effet, en utilisant l'inégalité triangulaire,

$$d(x,p') \leqslant d(x,p) + d(p,p') \leqslant d(x,p) + r - d(p,x) = r. \tag{9.360}$$

□

9.13.2 Point d'accumulation, point isolé

Les définitions de point d'accumulation et de point isolé sont 9.46 et 9.47. Nous voyons maintenant ce que ces définitions donnent dans le cas de l'espace topologique $\mathbb{R}$.

Lemme 9.316.
Soit $D \subset \mathbb{R}$. Un point $a \in D$ est isolé dans D si et seulement si il existe $\varepsilon > 0$ tel que

$$[a - \varepsilon, a + \varepsilon] \cap D = \{a\}. \tag{9.361}$$

Autrement dit, il existe un intervalle autour de a dans lequel a est le seul élément de D.

[151] Définition 9.158.

Lemme 9.317.
Un point $a \in \mathbb{R}$ est un point d'accumulation de D si pour tout $\varepsilon > 0$,

$$\Big([a-\varepsilon, a+\varepsilon] \setminus \{a\}\Big) \cap D \neq \varnothing. \tag{9.362}$$

Autrement dit, quel que soit l'intervalle autour de a que l'on considère, le point a n'est pas tout seul dans D.

Exemple 9.318.
Prenons $D = [0,1[\cup]2,3]$. Cet ensemble n'a pas de point isolé, et l'ensemble de ses points d'accumulation est $[0,1] \cup [2,3]$.

Notez que les points 1 et 2 sont des points d'accumulation de D qui ne font pas partie de D. Il est possible d'être un point d'accumulation de D sans être dans D, mais pour être un point isolé dans D, il faut être dans D. △

Exemple 9.319.
Soit $D = \{\frac{1}{n}\}_{n\in\mathbb{N}}$. Tous les points de cet ensemble sont des points isolés (vérifier !). Aucun point de D n'est point d'accumulation. Cependant 0 est un point d'accumulation. △

EXooWOYQooJolaTV

Exemple 9.320.
Soit $D =]1,2[\cup \{12\}$. Le point 12 est adhérence, mais pas d'accumulation parce que le voisinage $]9,14[$ n'intersectionne pas $D \setminus \{12\}$. △

9.13.3 Limite de suite

Définition 9.321 (Limite d'une suite dans $\mathbb{R}^m$)**.**
*Une suite de points (x_n) dans $\mathbb{R}^m$ est dite **convergente** si il existe un élément $\ell \in \mathbb{R}^m$ tel que*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geqslant N,\ \|x_n - \ell\| < \varepsilon. \tag{9.363}$$

EqCondLimSuite

*Dans ce cas, nous disons que ℓ est la **limite** de la suite (x_n) et nous écrivons $\lim x_n = \ell$ ou plus simplement $x_n \to \ell$.*

Remarque 9.322.
Nous n'écrivons pas « $\lim_{n\to\infty} x_n$ » parce que, lorsqu'on parle de suites, la limite est *toujours* lorsque n tend vers l'infini. Il n'y a aucun intérêt à chercher par exemple $\lim_{n\to 4} x_n$ parce que cela vaudrait x_4 et rien d'autre.

Ceci est une différence importante avec les limites de fonctions.

Lemme 9.323 (Unicité de la limite)**.**
Il ne peut pas y avoir deux nombres différents qui satisfont à la condition (9.363). En d'autres termes, si ℓ et ℓ' sont deux limites de la suite (x_n), alors $\ell = \ell'$.

Démonstration. Soit $\varepsilon > 0$. Nous considérons N tel que

$$\|x_n - \ell\| < \varepsilon \tag{9.364}$$

pour tout $n \geqslant N$, et $N' > 0$ tel que

$$\|x_n - \ell'\| < \epsilon \tag{9.365}$$

pour tout $n > N'$. Maintenant, nous prenons n plus grand que N et N' de telle façon que les deux équations pour x_n soient vérifiées en même temps. Alors

$$\|\ell - \ell'\| = \|\ell - x_n + x_n - \ell'\| \leqslant \|\ell - x_n\| + \|x_n - \ell'\| < 2\varepsilon. \tag{9.366}$$

Cela prouve que $\|\ell - \ell'\| = 0$. □

Le théorème de Bolzano-Weierstrass 9.213 dit que dans le cas métrique, la compacité séquentielle est équivalente à la compacité.

9.14 Topologie et distance

LemDUJXooWsnmpL

Lemme 9.324.
Soient (X_1, d_1) et (X_2, d_2) des espaces métriques séparables. Alors $X_1 \times X_2$ admet une base dénombrable de

topologie constituée de produits de boules de X_1 par des boules de X_2. Plus précisément si A_i est dénombrable et dense dans X_i alors l'ensemble des produits

$$\big\{B(y_1,r_1)\times B(y_2,r_2)\big\}_{\substack{y_i\in A_i\\ r_i\in\mathbb{Q}^+}} \tag{9.367}$$

est une base de topologie pour $X_1\times X_2$.

Démonstration. Soit $\mathcal{O}$ un ouvert de $X_1\times X_2$ et $(x_1,x_2)\in\mathcal{O}$. Par définition de la topologie produit[152], il existe $r_1,r_2\in\mathbb{Q}^+$ tels que $B(x_1,r_1)\times B(x_2,r_2)\subset\mathcal{O}$. Les parties A_i étant denses, il existe $y_i\in B(x_i,r_i/2)\cap A_i$. Avec ces choix nous avons $x_i\in B(y_i,\frac{r_i}{2})$. Nous avons donc

$$(x_1,x_2)\in B(y_1,\frac{r_1}{2})\times B(y_2,\frac{r_2}{2}). \tag{9.368}$$

Il est facile de voir que $B(y_i,r_i/2)\subset B(x_i,r_i)$. En effet si $z_i\in B(y_i,r_i/2)$ alors

$$d_i(z_i,x_i)\leqslant d(z_i,y_i)+d(y_i,x_i)\leqslant\frac{r_i}{2}+\frac{r_i}{2}=r_i. \tag{9.369}$$

Au final,

$$(x_1,x_2)\in B(y_1,\frac{r_1}{2})\times B(y_2,\frac{r_2}{2})\subset\mathcal{O}. \tag{9.370}$$

□

Définition 9.325.
*Si (X,d_X) et (Y,d_Y) sont des espaces métriques, une **isométrie** est une application bijective $f\colon X\to Y$ telle que pour tout $x,y\in X$ nous ayons*

$$d_Y\big(f(x),f(y)\big)=d_X(x,y). \tag{9.371}$$ EQooVUOXopKJntMN

Remarque 9.326.
Une application vérifiant (9.371) est automatiquement injective. En pratique, il ne faut donc vérifier que la surjectivité.

Exemple 9.327 (Manque de surjectivité)**.**
Si $X=[0,\infty[$ et $f(x)=x+1$ alors f vérifie (9.371) pour la distance $d(x,y)=|x-y|$, mais n'est pas surjective. △

Proposition-Définition 9.328 (Groupe des isométries)**.**
Si (X,d) est un espace métrique,

(1) l'ensemble des isométries de X, noté $\mathrm{Isom}(X)$ *est un groupe pour la composition.*

(2) Ce groupe agit fidèlement[153] *sur X.*

PropLYMgVMJ

Proposition 9.329.
Une isométrie entre deux espaces métriques est continue.

Démonstration. Soient $f\colon X\to Y$ une application isométrique et $\mathcal{O}$ un ouvert de Y. Soit $a\in f^{-1}(\mathcal{O})$; si $d(a,b)<r$, alors $d\big(f(a),f(b)\big)<r$ et donc $b\in f^{-1}\big(B(f(a),r)\big)$. Donc autour de chaque point de $f^{-1}(\mathcal{O})$ nous pouvons trouver une boule ouverte contenue dans $f^{-1}(\mathcal{O})$, ce qui prouve que $f^{-1}(\mathcal{O})$ est ouvert. □

Exemple 9.330.
Si X est un ensemble, nous pouvons écrire la **distance discrète** :

$$d(x,y)=\begin{cases}0 & \text{si } x=y\\ 1 & \text{si } x\neq y.\end{cases} \tag{9.372}$$

La topologie résultante est la topologie discrète, côtoyée dans l'exemple 9.10[154].

Pour cette métrique, le groupe des isométries est le groupe symétrique de X, c'est-à-dire le groupe de toutes les bijections de X sur lui-même. △

[152] Définition 9.66.
[153] Si vous ne savez pas ce que c'est, alors vous avez zappé la définition 5.17.
[154] Vérifiez-le tout de même !

9.14.0.1 Distance point-ensemble

Définition 9.331.
*Si A est une partie de l'espace métrique (X, d) et si $x \in X$, nous disons que la **distance** entre A et x est le nombre*

$$d(x, A) = \inf_{a \in A} d(x, a). \tag{9.373}$$ EqdefDistaA

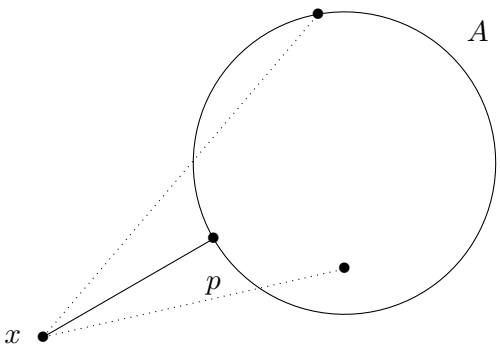


FIGURE 9.1 : La distance entre x et A est donnée par la distance entre x et p. Les distances entre x et les autres points de A sont plus grandes que $d(x, p)$. LabelFigDistanceEnsemble

9.15 Suites de Cauchy, métrique et espaces complets

9.15.1 Généralités

DefZSnlbPc

Définition 9.332 (Suite de τ-Cauchy, espace vectoriel topologique[274, 277])**.**
*Soit E un espace vectoriel topologique. Une suite (x_k) dans E est une **suite τ-Cauchy** si pour tout voisinage $\mathcal{U}$ de 0 il existe $N \in \mathbb{N}$ tel que $x_k - x_l \in \mathcal{U}$ pour tout $k, l \geqslant N$.*

DEFooVQDBooNxprFU

Définition 9.333 (Espace τ-complet)**.**
*Nous disons qu'une partie A d'un espace vectoriel topologique est **τ-complet** si toute suite τ-Cauchy d'éléments de A converge[155] vers un élément de A.*

DEFooXQYSooSPTRTn

Définition 9.334 (Suite de Cauchy, espace métrique)**.**
*Une suite (a_k) dans un espace métrique (V, d) est **de Cauchy** si pour tout $\epsilon > 0$ dans $\mathbb{R}$, il existe N tel que si $n, m \geqslant N$ alors $d(a_n, a_m) < \epsilon$.*

Notons qu'ici, même si l'espace V n'a rien à voir avec $\mathbb{R}$, nous prenons ϵ dans $\mathbb{R}$ et la distance à valeurs dans $\mathbb{R}$. Cela semble une évidence, mais il faut se rendre compte que $\mathbb{R}$ commence à prendre une place centrale dans nos constructions. Ce n'était pas le cas du temps où nous parlions de suites de Cauchy et de complétude dans des corps totalement ordonnés (définitions 3.249). Dans ce contexte, le ϵ était pris dans le corps lui-même.

DEFooHBAVooKmqerL

Définition 9.335 (Métrique complète)**.**
*Soit (E, d) un espace métrique. Nous disons que la métrique d est **complète** si toute suite de Cauchy dans (E, d) converge dans E.*

9.336.
Ces définitions méritent quelques remarques.

(1) Dans le cas des espaces vectoriels topologiques, nous définissons les notions de suite τ-Cauchy et d'espace topologique τ-complet. Nous ajoutons le préfixe τ pour indiquer que ce sont des notions topologiques.

(2) Dans le cas des espaces métriques, nous définissons la notion de *métrique* complète. C'est bien la métrique qui est complète, et non l'espace. En effet nous allons voir dans l'exemple 9.340 que le même espace topologique peut accepter plusieurs distances différentes (donnant la même topologie) donnant lieu à des suites de Cauchy différentes.

[155] Définition 9.14.

(3) Si un espace vectoriel a une topologie issue d'une distance, rien ne dit que ses suites τ-Cauchy et ses suites de Cauchy sont les mêmes. Ce sont deux notions à priori séparées. Si V est un espace vectoriel topologique que l'on peut munir de deux distances d_1, d_2 donnant toutes deux la topologie, dire que V est τ-complet, dire que d_1 est complète et dire que d_2 est complète sont trois choses différentes. Même si les trois topologies sont identiques.

(4) Nous allons bien entendu voir que dans de larges gammes d'exemples, les notions de suite de Cauchy et τ-Cauchy coincident.

PROPooTGCKooRsmoLx

Proposition 9.337 ([1]).
Tout compact d'un espace métrique est complet.

9.15.2 Espace de Banach

DEFooKSDFooGIBtrG

Définition 9.338.
*Soit un espace vectoriel E sur le corps $\mathbb{K}$. Son **dual topologique**, noté E', est l'ensemble des formes linéaires continues de E vers $\mathbb{K}$.*

DefVKuyYpQ

Définition 9.339 (espace de Banach, algèbre de Banach[295]).
*Un **espace de Banach** est un espace vectoriel normé complet*[156] *pour la topologie de la norme.*

*Une **algèbre de Banach** est une algèbre commutative et associative qui est un espace vectoriel normé complet.*

EXooNMNVooXyJSDm

Exemple 9.340 (La complétude n'est pas une propriété topologique[296]).
Le fait pour un espace d'être complet n'est pas une propriété topologique, mais une propriété métrique. Plus exactement, il existe des espaces topologiques isomorphes, mais dont l'un est complet et l'autre non.

Nous considérons la distance suivante sur $\mathbb{N}$:

$$d_1(x,y) = \left|\frac{1}{x} - \frac{1}{y}\right|. \tag{9.374}$$

Pour vérifier que cette formule définit bien une distance (définition 9.155), le seul point non immédiat est l'inégalité triangulaire :

$$d_1(x,y) = \left|\frac{1}{x} - \frac{1}{y}\right| \leqslant \left|\frac{1}{x} - \frac{1}{z}\right| + \left|\frac{1}{z} - \frac{1}{y}\right| = d_1(x,z) + d_1(z,y). \tag{9.375}$$

Au niveau de la topologie induite par cette distance, c'est la topologie discrète. En effet, soit $x \in \mathbb{N}$ et $\epsilon > 0$; nous voulons déterminer la boule $B(x,\epsilon)$ en résolvant l'équation

$$\left|\frac{1}{x} - \frac{1}{y}\right| < \epsilon \tag{9.376}$$

pour $y \in \mathbb{N}$. Nous trouvons que $\frac{1}{y} > \frac{1}{x} - \epsilon$ et $\frac{1}{y} < \frac{1}{x} + \epsilon$, soit

$$\begin{cases} y > \dfrac{1}{\frac{1}{x} + \epsilon} & \text{(9.377a)} \\ y < \dfrac{1}{\frac{1}{x} - \epsilon}. & \text{(9.377b)} \end{cases}$$

Si ϵ est assez petit, la seule solution entière est $y = x$. Les ouverts sont donc toutes les parties parce que tous les singletons sont ouverts.

L'espace topologique associé à $(\mathbb{N}, d_1)$ est donc la topologie discrète[157].

Si nous considérons par contre la distance usuelle sur $\mathbb{N}$, à savoir $d(x,y) = |x-y|$, nous obtenons encore la topologie discrète. Nous avons donc un isomorphisme d'espaces topologiques

$$(\mathbb{N}, d) \simeq (\mathbb{N}, d_1). \tag{9.378}$$

Nous pouvons même donner un isomorphisme explicite : $f(n) = n$.

La suite $(x_n) = n$ est une suite de Cauchy dans $(\mathbb{N}, d_1)$ parce que si $\epsilon > 0$ est donné, il suffit de prendre N assez grand pour avoir $\frac{1}{N} < \epsilon$ (possible par le lemme 4.60) nous avons, pour $n, m > N$:

$$\left|\frac{1}{n} - \frac{1}{m}\right| < \frac{1}{n} < \frac{1}{N} < \epsilon. \tag{9.379}$$

[156] Définition 9.335.
[157] Celle dont toutes les parties sont des ouverts.

Or cette suite ne converge pas. Soit en effet un candidat limite k. Calculons

$$d_1(x_n, k) = \left|\frac{1}{n} - \frac{1}{k}\right| \to \frac{1}{k} \neq 0. \tag{9.380}$$

L'espace $(\mathbb{N}, d_1)$ n'est pas complet.

Notons que cette suite n'est pas de Cauchy dans $(\mathbb{N}, d)$.

En résumé :

(1) Les espaces topologiques $(\mathbb{N}, d)$ et $(\mathbb{N}, d_1)$ sont isomorphes.

(2) Ils ont les mêmes notions de suites convergentes : une suite convergente pour l'un est convergente pour l'autre.

(3) Ils n'ont pas les mêmes notions de suites de Cauchy.

(4) Dans $(\mathbb{N}, d_1)$, il existe des suites de Cauchy qui ne convergent pas (pas complet).

(5) L'espace $(\mathbb{N}, d)$ est complet, mais $(\mathbb{N}, d_1)$ n'est pas complet.

(6) Le fait pour un espace topologique métrique d'être complet n'est pas intrinsèque à sa topologie : la complétude est une propriété de la distance. La complétude est une propriété de la métrique, et non de la topologie qui s'en suit.

△

LemCAIPooPMNbXg

Lemme 9.341.
Si E et F sont des espaces de Banach[158]*, l'espace $\mathcal{L}(E, F)$ est également de Banach.*

Démonstration. Soit (u_n) une suite de Cauchy dans $\mathcal{L}(E, F)$; si $x \in E$ il existe N tel que si $l, m > N$ alors $\|u_l - u_m\| < \epsilon$, c'est-à-dire que pour tout $\|x\| = 1$ on a $\|u_l(x) - u_n(x)\| < \epsilon$. Cela signifie que $u_n(x)$ est une suite de Cauchy dans l'espace complet F. Cette suite converge et nous pouvons définir l'application $u : E \to F$ par

$$u(x) = \lim_{n\to\infty} u_n(x). \tag{9.381}$$

Il suffit maintenant de prouver que u est linéaire, ce qui est une conséquence directe de la linéarité de la limite :

$$u(\alpha x + \beta y) = \lim_{n\to\infty} \big(\alpha u_n(x) + \beta u_n(y)\big). \tag{9.382}$$

□

9.15.3 Espace topologique métrique

Dans les espaces vectoriels topologiques métriques, il n'y a pas d'ambiguïté.

PropooUEEOooLeIImr

Proposition 9.342 (Caractérisations avec la distance d)**.**
Soit (E, d) un espace vectoriel topologique métrique.

ItemooROYMooAQCXnj

(1) Une suite (x_n) dans E est convergente[159] *vers x si et seulement si pour tout $\epsilon > 0$ il existe N_ϵ tel que pour tout $n \geqslant N_\epsilon$ nous avons $d(x_n, x) \leqslant \epsilon$.*

(2) Une suite (x_n) dans E est de Cauchy[160] *si pour tout $\epsilon \in \mathbb{R}$, il existe un N_ϵ tel que si $p, q \geqslant N_\epsilon$, nous avons $d(x_p, x_q) \leqslant \epsilon$.*

Démonstration. En ce qui concerne la convergence :

(1) **Sens direct**

Nous supposons que $x_k \to x$ dans E. Soit $\epsilon > 0$; vu que $B(x, \epsilon)$ est un ouvert contenant x, il existe un $N_\epsilon > 0$ tel que $k > N_\epsilon$ implique $x_k \in B(x, \epsilon)$. Cela signifie $d(x, x_k) \leqslant \epsilon$.

(2) **Réciproque**

Nous supposons que pour tout $\epsilon > 0$, il existe $N_\epsilon > 0$ tel que si $k > N_\epsilon$ alors $x_k \in B(x, \epsilon)$. Soit un ouvert $\mathcal{O}$ autour de x. Nous sommes dans un espace métrique ; ergo la topologie est donné par le théorème 9.158 et en particulier la liste des ouverts est donnée par (9.173). Il existe donc une boule $B(x, \epsilon)$ incluse à $\mathcal{O}$. Pour tout $k > N_\epsilon$ nous avons alors $x_k \in B(x, \epsilon) \subset \mathcal{O}$.

[158] Je crois qu'il ne faut pas que E soit complet.
[159] Définition 9.14.
[160] Définition 9.332.

En ce qui concerne les suites de Cauchy :

(1) **Sens direct** Si (x_n) est une suite de Cauchy et si $\epsilon > 0$ est donné, alors $B(0,\epsilon)$ est un voisinage de 0 et il existe N_ϵ tel que si $p, q \geqslant N_\epsilon$ alors $x_p - x_q \in B(0,\epsilon)$. Posons $u = x_p - x_q$; en utilisant l'invariance par translation (lemme 9.237(1)) nous avons

$$d(u,0) = d(x_p - x_q, 0) = d(x_p, x_q). \tag{9.383}$$

Par conséquent $d(x_p, x_q) \leqslant \epsilon$.

(2) **Réciproque** Soit $\mathcal{O}$ un voisinage de 0. Il existe ϵ tel que $B(0,\epsilon) \subset \mathcal{O}$. Par hypothèse il existe N_ϵ tel que $d(x_p, x_q) \leqslant \epsilon$ dès que $p, q \geqslant N_\epsilon$. En utilisant encore l'invariance par translation nous avons

$$d(x_p, x_q) = d(x_p - x_q, 0), \tag{9.384}$$

et comme cela est plus petit que ϵ, nous avons $x_p - x_q \in B(0,\epsilon) \subset \mathcal{O}$.

□

PROPooZZNWooHghltd

Proposition 9.343 ([297]).
Toute suite convergente dans un espace métrique est de Cauchy.

Démonstration. Nous utilisons les caractérisations de la proposition 9.342 des suites convergentes et de Cauchy.

Soit un espace métrique (X,d) et $x_n \to \ell$ une suite convergente. Si $\epsilon > 0$, la proposition 9.342(1), dit qu'il existe N tel que pour tout $n > N$ nous ayons $d(x_n, \ell) < \epsilon$. Par conséquent si $n, m > N$ alors

$$d(x_n, x_m) \leqslant d(x_m, \ell) + d(l, x_m) \leqslant 2\epsilon. \tag{9.385}$$

Cela prouve que (x_n) est une suite de Cauchy. □

9.15.4 Compacts, fermés

PROPooRMAOooZIgXwy

Proposition 9.344 (Séparation [277, 298]).
Soit V, un espace vectoriel topologique. Soient des parties K et F de V telles que :

(1) K est compact,

(2) F est fermé,

(3) $K \cap F = \varnothing$.

Alors il existe un voisinage U de 0 tel que

$$(K + U) \cap (F + U) = \varnothing. \tag{9.386}$$

Autrement dit, la topologie d'un espace vectoriel topologique sépare les fermés des compacts.

Démonstration. Soit un élément $x \in K$. La partie F^c est un ouvert qui contient x ; donc $F^c - x$ est un voisinage ouvert de 0.

(1) **Quelque chose sans intersection avec F** Par la proposition 9.267, il existe un ouvert symétrique U_x autour de 0 tel que

$$U_x + U_x + U_x + U_x \subset F^c - x. \tag{9.387}$$

En enlevant un des éléments de la somme, nous gardons la même inclusion :

$$U_x + U_x + U_x \subset F^c - x. \tag{9.388}$$

Et en passant le x de l'autre côté :

$$x + U_x + U_x + U_x \subset F^c. \tag{9.389}$$

Cela pour dire que nous avons, pour chaque $x \in K$ un voisinage ouvert U_x de 0 tel que

$$(x + U_x + U_x + U_x) \cap F = \varnothing. \tag{9.390}$$

EQooPXUVooVvUEoN

(2) $(x+U_x+U_x)\cap(U_x+F)=\varnothing$ Supposons $z\in(x+U_x+U_x)\cap(U_x+F)$, et déduisons une contradiction. En particulier $z\in U_x+F$ et donc il existe $u\in U_x$, $f\in F$ tel que $z=v+f$. Nous avons alors (nous utilisons le fait que U_x soit symétrique)

$$f=z-v\in z+U_x \tag{9.391}$$

Mais z est aussi dans $x+U_x+U_x$. Donc

$$f\in z+U_x\subset x+U_x+U_x+U_x. \tag{9.392}$$

Cela prouve que $x+U_x+U_x+U_x\cap F\neq\varnothing$, en contradiction avec (9.390). Nous en concluons que

$$(x+U_x+U_x)\cap(U_x+F)=\varnothing. \tag{9.393}$$

EQooNLCRooWTEoyc

(3) **Un sous-recouvrement fini** Fini de rigoler. Si nous avons un compact dans les hypothèses, il fallait que ça arrive. Pour chaque $x\in K$ nous avons un voisinage ouvert U_x de 0 et donc un voisinage ouvert $x+U_x$ de x. Du coup $\{U_x+x\}_{x\in K}$ forme un recouvrement de K par des ouverts. Et hop, sous-recouvrement fini (c'est la définition 9.125 d'un compact) : nous avons $\{x_i\}_{i=1,\dots,n}$ tels que

$$K\subset\bigcup_{i=1}^{n}(x_i+U_{x_i}). \tag{9.394}$$

Nous posons $U=\bigcap_{i=1}^{n}U_{x_i}$. Même si c'est évident, remarquez que U est un ouvert autour de 0 et que U est plus petit que chacun des U_{x_i}. Récrivons (9.393) pour chacun des x_i :

$$(x+U_{x_i}+U_{x_i})\cap(F+U_{x_i})=\varnothing. \tag{9.395}$$

EQooGEAGooENElCG

Lorsqu'on enlève des éléments dans une intersection vide, l'intersection reste vide. Donc en remplaçant des U_{x_i} par des U dans (9.395), nous conservons une intersection vide :

$$(x+U_{x_i}+U)\cap(F+U)=\varnothing. \tag{9.396}$$

(4) **Conclusion** Aucun ensemble de la forme $x+U_{x_i}+U$ n'intersecte $F+U$. L'union ne l'intersecte pas non plus :

$$\bigcup_{i=1}^{n}(x+U_{x_i})+U\cap(F+U)=\varnothing. \tag{9.397}$$

Et donc

$$(K+U)\cap(F+U)=\varnothing, \tag{9.398}$$

comme nous le voulions.

□

DEFooGTOZooRcvGHg

Définition 9.345.
*Une distance d sur un espace vectoriel topologique V est dite **compatible** avec la topologie si la topologie induite*[161] *de d est celle de V.*

DEFooEUXVooEBYhNU

Définition 9.346.
*Une distance d sur un espace vectoriel V est dite **invariante** si pour tout $x,y,a\in V$ nous avons*

$$d(x+a,y+a)=d(x,y). \tag{9.399}$$

Notons que lorsque nous parlons d'une distance compatible avec un espace vectoriel topologique, nous parlons de compatibilité avec la topologie, pas avec la structure vectorielle.

LEMooZNBAooOhEwJd

Lemme 9.347 ([1])**.**
Soit un espace vectoriel muni d'une distance invariante. Alors

$$B(a,r)+x=B(a+x,r). \tag{9.400}$$

Démonstration. Un élément de $B(a,r)+x$ est de la forme $y+x$ avec $d(a,y)<r$. Nous avons alors $d(y+x,a+x)=d(y,a)<r$, de telle sorte que $y+x\in B(a+x,r)$.

Dans le sens inverse, si $y\in V$ vérifie $d(a+x,y)<r$, alors je prétend que $y-x\in B(a,r)$. En effet $d(y-x,a)=d(y-x+x,a+x)=d(y,a+x)<r$. □

[161] Définition 9.158.

Une version plus complète du lemme suivant sera dans la proposition 12.195 et ce qui suit.

LEMooIQBXooUEtdoy

Lemme 9.348.
Nous introduisons l'ensemble $\mathbb{D}_2$ des suites finies[162] $\mathbb{N}\setminus\{0\}\to\{0,1\}$[163]. *Nous notons*

$$l(x)=\max\{i\in\mathbb{N}\text{ tel que }x_i\neq 0\}. \tag{9.401}$$

L'application

$$\begin{aligned}\varphi\colon\mathbb{D}_2&\to[0,1[\\ x&\mapsto\sum_{i=1}^{l(x)}\frac{x_i}{2^i}.\end{aligned} \tag{9.402}$$

est injective.

Démonstration. Le lemme 4.116 donne la somme partielle de la série géométrique. Dans notre cas, $q=1/2$. Si $x\in D_n$, alors en majorant chacun des c_i par 1,

$$x\leqslant\sum_{i=1}^{n}\left(\frac{1}{2}\right)^i=\frac{1-(1/2)^{n+1}}{1/2}-1=1-(1/2)^{n+1}<1. \tag{9.403}$$

Donc c'est bon pour dire que φ prend ses valeurs dans $[0,1[$.

Il reste à voir l'injectivité. Nous supposons que $\varphi(x)=\varphi(y)$. Quitte à alonger x ou y par des zéros, nous supposons qu'elles ont même longueur N. Enfin nous définissons n_0 le plus petit indice pour lequel $x_i\neq y_i$. Nous avons :

$$0=\frac{1}{2^{n_0}}+\sum_{i=n_0+1}^{N}\frac{x_i-y_i}{2^i}. \tag{9.404}$$

EQooEUKNooVoJfFC

Le deuxième terme est majoré de la façon suivante :

$$\begin{aligned}\left|\sum_{i=n_0+1}^{N}\frac{x_i-y_i}{2^i}\right|&\leqslant\sum_{i=n_0+1}^{N}\frac{|x_i-y_i|}{2^i}&(9.405a)\\ &\leqslant\sum_{i=n_0+1}^{N}\frac{1}{2^i}&(9.405b)\\ &=\sum_{i=1}^{N}\left(\frac{1}{2}\right)^i-\sum_{i=1}^{n_0}\left(\frac{1}{2}\right)^i&(9.405c)\\ &=\frac{1-(1/2)^{N+1}}{1/2}-\frac{1-(1/2)^{n_0+1}}{1/2}&(9.405d)\\ &=\frac{1}{2^{n_0}}-\frac{1}{2^N}&(9.405e)\\ &<\frac{1}{2^{n_0}}.&(9.405f)\end{aligned}$$

L'égalité (9.404) n'est donc pas possible. Nous déduisons que n_0 n'existe en fait pas et que $x=y$. D'où l'injectivité de φ. □

Pour faire les sommes dans $\mathbb{D}_2$, nous introduisons $\mathbb{D}_2'$, l'ensemble des suites finies $\mathbb{N}\to\{0,1\}$ et

$$\begin{aligned}\varphi'\colon\mathbb{D}_2'&\to[0,2[\\ x&\mapsto\sum_{i=0}^{l}(x)\frac{x_i}{2^i}.\end{aligned} \tag{9.406}$$

DEFooRJSFooDvbkrx

Définition 9.349 ([1]).
Si $x,y\in\mathbb{D}_2$, nous définissons $z,r\in\mathbb{D}_2'$ par récurrence (à l'envers) de la façon suivantes[164]. *D'abord, quitte à ajouter des zéros, nous supposons que x et y aient la même longueur l.*

D'abord posons $r_l=0$.

Ensuite, pour tout k nous considérons les trois cas possibles.

[162] Les suites donc nous parlons sont indexées en commençant à 1, et non à 0. C'est une précision importante.

[163] C'est en gros ce qui se fera dans 12.193 pour les développements de nombres dans une base donnée, sauf qu'ici nous n'avons pas besoin de subtilités sur les queues de suites.

[164] z va être la somme en binaire et r va être la suite des reports.

Si $x_k + y_k + r_k$ vaut 0 ou 1 *Dans ce cas nous posons*

- $z_k = x_k + y_k + r_k$
- $r_{k-1} = 0$

Si $x_k + y_k + r_k = 2$ *Nous posons*

- $z_k = 0$
- $r_{k-1} = 1$

Si $x_k + y_k + r_k = 3$ *Nous posons*

- $z_k = 1$
- $r_{k-1} = 1$.

Et enfin nous posons $z_0 = r_0$.

LEMooIUDHooNDlVtg

Lemme 9.350 ([1])**.**
Si $r_k = 1$, alors $z_k \neq x_k + y_k$.

Démonstration. Il y a seulement quelques cas à traiter.

x_k	y_k	r_k	z_k
0	0	1	$z_k = 1 \neq x_k + y_k$
0	1	1	$z_k = 0 \neq x_k + y_k$
1	0	1	$z_k = 0 \neq x_k + y_k$
1	1	1	$z_k = 1 \neq x_k + y_k$

□

PROPooGHPZooEwXqMH

Proposition 9.351 ([1])**.**
Soient $x, y \in \mathbb{D}_2$ ainsi que z défini par 9.349. Nous avons

$$\varphi(x) + \varphi(y) = \varphi'(z). \tag{9.407}$$

Démonstration. Nous supposons que x et y sont de longueur l, et nous faisons une récurrence à l'envers. D'abord

$$\varphi(x) + \varphi(y) = \sum_{i=1}^{l} \frac{x_i + y_i}{2^i} = \sum_{i=1}^{l-2} \frac{x_i + y_i}{2^i} + \frac{x_{l-1} + y_{l-1}}{2^{l-1}} + \frac{x_l + y_l}{2^l}. \tag{9.408}$$

Il y a deux possibilités. Si $x_l + y_l$ vaut 0 ou 1, alors $r_{l-1} = 0$ et $z_l = x_l + y_l$, de telle sorte que

$$\frac{x_{l-1} + y_{l-1}}{2^{l-1}} + \frac{x_l + y_l}{2^l} = \frac{x_{l-1} + y_{l-1} + r_{l-1}}{2^{l-1}} + \frac{z_l}{2^l}. \tag{9.409}$$

Si $x_l + y_l = 2$, alors $r_{l-1} = 1$ et $z_l = 0$ de telle sorte que

$$\frac{x_{l-1} + y_{l-1}}{2^{l-1}} + \frac{x_l + y_l}{2^l} = \frac{x_{l-1} + y_{l-1}}{2^{l-1}} + \frac{2}{2^l} \tag{9.410a}$$

$$= \frac{x_{l-1} + y_{l-1} + 1}{2^{l-1}} + \frac{z_l}{2^l} \tag{9.410b}$$

$$= \frac{x_{l-1} + y_{l-1} + r_{l-1}}{2^{l-1}} + \frac{z_l}{2^l}. \tag{9.410c}$$

En ce qui concerne la récurrence, il faut faire les trois cas pour montrer que dans tous les cas,

$$\frac{x_k + y_k}{2^k} + \frac{x_{k+1} + y_{k+1} + r_{k+1}}{2^{k+1}} = \frac{x_k + y_k + r_k}{2^k} + \frac{z_{k+1}}{2^{k+1}}. \tag{9.411}$$

□

LEMooEAIBooMxCDHF

Lemme 9.352 ([1])**.**
Soit $z \in \mathbb{D}'_2$. Nous avons $\varphi'(z) < 1$ si et seulement si $z_0 = 0$.

Démonstration. D'une part, si $z_0 = 0$, alors

$$\varphi'(z) = \varphi'(0, z_1, \dots, z_l) = \varphi(z_1, \dots, z_l) \in [0, 1[. \tag{9.412}$$

D'autre part, si $z_0 \neq 0$, c'est que $z_0 = 1$. Et dans ce cas, nous avons

$$\varphi'(z) = z_0 + \sum_{i=1}^{l}(z)\frac{z_i}{2^i} \geqslant z_0 = 1. \tag{9.413}$$

Cela prouve que si $z_0 \neq 0$, alors $\varphi'(z) \geqslant 1$. □

Toujours avec l'injection φ du lemme 9.348 nous avons ceci.

LEMooVDPWooWLQzbF

Lemme 9.353 ([1]).
Soient $s, t \in \varphi(\mathbb{D}_2)$ tels que $s + t < 1$. Alors $s + t \in \varphi(\mathbb{D}_2)$.

Démonstration. Nous considérons $x, y \in \mathbb{D}_2$ tels que $s = \varphi(x)$ et $t = \varphi(y)$. En considérant $z \in \mathbb{D}_2'$ et r comme avant, la proposition 9.351 donne $\varphi(x) + \varphi(y) = \varphi'(z)$. En particulier $\varphi'(z) < 1$. Le lemme 9.352 dit alors que $z_0 = 0$. En posant $z' = (z_1, \dots, z_l)$, nous avons

$$\varphi(z') = \varphi'(z) = \varphi(x) + \varphi(y). \tag{9.414}$$

Et donc z' est l'élément de $\mathbb{D}_2$ que nous cherchions : $s + t = \varphi(z')$. □

LEMooQYILooMimKHS

Lemme 9.354.
Soient $s, t \in \varphi(\mathbb{D}_2)$ tels que $s + t < 1$. Nous posons $x = \varphi^{-1}(s)$, $y = \varphi^{-1}(t)$ et $z = \varphi^{-1}(s + t)$. Si k est le plus petit entier tel que $z_k \neq x_k + y_k$, alors $x_k = y_k = 0$ et $z_k = 1$.

Démonstration. Il suffit de traiter les 8 cas possible de x_k, y_k et r_k et voir ceux qui vont. Voici le tableau à remplir :

x_k	y_k	r_k	z_k	r_{k-1}
0	0	1		
0	1	1		
1	0	1		
1	1	1		
0	0	0		
0	1	0		
1	0	0		
1	1	0		

Et voici le tableau rempli :

x_k	y_k	r_k	z_k	r_{k-1}
0	0	1	0	0
0	1	1	1	0
1	0	1	1	0
1	1	1	0	1
0	0	0	1	0
0	1	0	0	1
1	0	0	0	1
1	1	0	1	1

Par le lemme 9.350, nous voulons une ligne qui satisfait $z_k \neq x_k + y_k$ et $r_{k-1} = 0$. Cherchez un peu et vous verrez qu'il y a une seule ligne, et c'est celle qui donne $x_k = y_k = 0$, $r_k = 1$, $z_k = 1$ et $r_{k-1} = 0$. □

THOooAGBXooZnvQLK

Théorème 9.355 (Espace topologique métrisable[277, 1]).
Si V est un espace vectoriel topologique. Nous supposons :

(1) Tout point admet une base dénombrable de topologie[165].

(2) Le singleton $\{0\}$ est fermé[166].

[165] Définition 9.2.

[166] Attention : dans [277], cela fait partie de la définition d'un espace vectoriel topologique et n'est donc pas listé dans les hypothèses de ce théorème.

Alors il existe une distance d sur V telle que

(1) d est compatible avec la topologie de V,

(2) d est invariante par translation.

Démonstration. Vu que V admet une base dénombrable de topologie, nous en considérons une autour de 0 dans V : $\{A_i\}_{i\in\mathbb{N}}$.

(1) **Nouvelle base de topologie** Nous construisons une nouvelle base de topologie $\{U_i\}_{i\in\mathbb{N}}$ autour de 0 de la façon suivante. La proposition 9.267 donne un ouvert symétrique équilibré dans A_0. Nous le nommons U_0 :

$$U_0 \subset A_0. \tag{9.415}$$

Pour les suivants, U_{k+1} est un ouvert symétrique équilibré dans $U_k \cap A_k$ vérifiant

$$U_{k+1} + U_{k+1} + U_{k+1} + U_{k+1} \subset A_k \cap U_k. \tag{9.416}$$

Le fait est que $A_k \cap U_k$ est un ouvert autour de 0 ; donc la proposition 9.267 permet de construire un ouvert symétrique et équilibré U_{k+1} autour de 0 ayant la propriété demandée.

(2) **C'est bien une base** Notons d'abord que $U_k \subset A_k$. Si $\mathcal{O}$ est un ouvert autour de 0, il existe k tel que $A_k \subset \mathcal{O}$: c'est la définition 9.2 d'une base de topologie. Nous avons donc $U_k \subset A_k \subset \mathcal{O}$, et les $\{U_k\}$ forment une base dénombrable de la topologie autour de 0.

(3) **Quelques inclusions** Notons au passage quelques inclusions. Pour tout $n \in \mathbb{N}$ nous avons

$$U_{n+1} + U_{n+1} + U_{n+1} + U_{n+1} \subset U_n. \tag{9.417}$$

À fortiori nous avons

$$U_{n+1} \subset U_n \tag{9.418}$$

et pour tout $n, k \in \mathbb{N}$, nous obtenons alors

$$U_{n+1} + U_{n+2} + \cdots + U_{n+(k-1)} + U_{n+k} \subset U_{n+1} + U_{n+1} \subset U_n. \tag{9.419}$$

(4) **L'ensemble D** Nous considérons l'ensemble $\mathbb{D}_2$ et l'application φ du lemme 9.348. Nous notons $D = \varphi(\mathbb{D}_2) \subset [0,1[$. L'application $\varphi\colon \mathbb{D}_2 \to D$ est injective, et nous pouvons donc parler de $\varphi^{-1}(r)$ pour tout $r \in D$.

(5) **La fonction ϕ**

Nous définissons maintenant une fonction à valeurs dans la topologie τ_V de V :

$$\begin{aligned}\phi\colon D \cup [1,+\infty[&\to \tau_V \\ r &\mapsto \begin{cases} V & \text{si } r \geqslant 1; \\ \sum_i \varphi^{-1}(r)_i U_i & \text{si } r \in D. \end{cases}\end{aligned} \tag{9.420}$$

La dernière somme est toujours une somme finie et est un ouvert parce que la multiplication par un scalaire et l'addition sont des ouverts.

Notez aussi que plus r est petit, plus ce sont les grands i qui tendront à avoir $\varphi^{-1}(r) \neq 0$. En effet, pour $r = 1/8$, nous avons $\varphi^{-1}(1/8) = (0,0,0,1)$, et plus généralement pour $r < 1/2^N$, les N premiers termes de $\varphi^{-1}(r)$ seront nuls.

Quelques remarques sur cette fonction.

(5a) **Une égalité facile** Si je ne me trompe pas d'un off-by-one, nous avons

$$\phi(1/2^N) = U_N. \tag{9.421}$$

(5b) **$0 \in \phi(r)$ pour tout r** En effet, $\phi(r)$ n'est jamais vide, c'est toujours un voisinage de 0.

(5c) **$\phi(r) + \phi(s) \subset \phi(r+s)$** Si $r + s \geqslant 1$, c'est clair. Sinon, nous posons $u = \varphi^{-1}(r)$, $v = \varphi^{-1}(s)$ et $w = \varphi^{-1}(r+s)$. Dans la suite, nous prolongeons u et v pour qu'elles aient le même nombre d'éléments que nous notons N.

Deux cas se produisent : soit $w_i = u_i + v_i$ pour tout i soit non.

(5c.i) **Premier cas** Si $w_i = u_i + v_i$ pour tout i, alors en particulier les u_i et v_i ne peuvent pas être 1 en même temps et nous pouvons séparer clairement les termes de la somme :

$$\phi(r+s) = \sum_i w_i U_i = \sum_i u_i U_i + \sum_i v_i U_i = \phi(r) + \phi(s); \tag{9.422}$$

(5c.ii) **Second cas** Sinon, posons k le plus petit entier tel que $w_k \neq u_k + v_k$. Alors le lemme 9.354 dit que $u_k = v_k = 0$ et $w_k = 1$. Nous avons d'abord

$$\phi(r) = \sum_{i=1}^{k-1} u_i U_i + \sum_{i=k+1}^{n} u_i U_i \subset \sum_{i=1}^{k-1} u_i U_i + U_{k+1} + U_{k+1} \tag{9.423}$$

où nous avons utilisé (9.418) pour tous les derniers termes. De même nous avons :

$$\phi(s) = \sum_{i=1}^{k-1} v_i U_i + \sum_{i=k+1}^{n} v_i U_i \subset \sum_{i=1}^{k-1} v_i U_i + U_{k+1} + U_{k+1}. \tag{9.424}$$

En combinant, et en utilisant (9.417),

$$\phi(r) + \phi(s) = \sum_{i=1}^{k-1} u_i U_i + \sum_{i=1}^{k-1} v_i U_i + \underbrace{U_{k+1} + U_{k+1} + U_{k+1} + U_{k+1}}_{\subset U_k} \tag{9.425a}$$

$$\subset \sum_{i=1}^{k-1} w_i U_i + U_k \tag{9.425b}$$

$$= \sum_{i=1}^{k} w_i U_i \tag{9.425c}$$

$$\subset \phi(r+s). \tag{9.425d}$$

Pour (9.425c) nous avons utilisé le fait que $w_k = 1$. Au final nous avons bien $\phi(r) + \phi(s) \subset \phi(r+s)$.

(5d) **ϕ est croissante** Dans notre contexte « croissante » signifie que si $r < s$ alors $\phi(r) \subset \phi(s)$. Il suffit d'écrire

$$\phi(r) \subset \phi(r) + \phi(s-r) \subset \phi(s). \tag{9.426}$$

(6) **Définition de la distance (enfin !)** Nous définissons l'application

$$\begin{aligned} f\colon V &\to \mathbb{R} \\ x &\mapsto \inf\{r \text{ tel que } x \in \phi(r)\}, \end{aligned} \tag{9.427}$$

et ensuite ce qui va être notre distance :

$$d(x,y) = f(y-x). \tag{9.428}$$

Notons que cet infimum est un réel, et qu'il n'est pas spécialement dans $\varphi(\mathbb{D}_2)$. Nous devons prouver que ce d est une distance invariante par translation et compatible avec la topologie.

(7) **d est invariante par translation** Il s'agit seulement d'écrire $d(x+a, y+a)$ et de remarquer que $(y+a) - (x+a) = y - x$.

$d(x,x) = 0$ Oui, car 0 est dans $\phi(r)$, pour tout r, puisque les U_i sont des voisinages de 0.

(8) **$d(x,y) = 0$ implique $x = y$** Nous montrons que $f(x) \neq 0$ dès que $x \neq 0$. Rappellez-vous que nous avons posé l'hypothèse que $\{0\}$ est un fermé dans V. Vu que $\{x\}$ est un compact[167], la proposition 9.344 nous indique qu'il existe un voisinage A de 0 qui ne contient pas x.

Vu que les $\{U_k\}_{k\in\mathbb{N}}$ forment une base de la topologie autour de 0, il existe un n_0 tel que $x \notin U_{n_0}$. Et comme $U_{k+1} \subset U_k$ nous avons

$$x \notin U_k \tag{9.429}$$

[167] Les singletons sont toujours des compacts dans les espaces topologiques.

pour tout $k \geqslant n_0$. Nous savons aussi que ϕ est croissante et que $\phi(1/2^N) = U_N$. Donc pour tout $\epsilon < \frac{1}{2^k}$, nous avons

$$\phi(\epsilon) \subset U_k \tag{9.430}$$

et donc $x \notin \phi(\epsilon)$. Donc

$$f(x) \geqslant \frac{1}{2^k} > 0 \tag{9.431}$$

la dernière inégalité est stricte et c'est important.

En ce qui concerne la distance, si $d(x,y) = 0$, alors $f(y-x) = 0$. Cela signifie que $y - x = 0$ et donc que $x = y$. Ok.

(9) $d(x,y) = d(y,x)$ Oui, car tous les voisinages considérés sont symétriques. Donc $x - y \in \phi(r)$ si et seulement si $y - x \in \phi(r)$.

(10) $d(x,z) \leqslant d(x,y) + d(y,z)$ Nous supposons que x, y et z sont trois points distincts, de telle sorte que les trois distances soient strictement positives.

Soit $\epsilon > 0$. Par définition des distances comme infimums, et grâce au corolaire 4.65, il existe r et s dans $\varphi(\mathbb{D}_2)$ tels que :

$$d(x,y) < r < d(x,y) + \frac{\epsilon}{2} \quad \text{et} \quad d(y,z) < s < d(y,z) + \frac{\epsilon}{2}. \tag{9.432}$$

En sommant :

$$d(x,y) + d(y,z) < r + s < d(x,y) + d(y,z) + \epsilon. \tag{9.433}$$

Vu que ϕ est croissante, on a $y - x \in \phi(r)$ et $z - y \in \phi(s)$; donc

$$z - x = (y - x) + (z - y) \in \phi(r) + \phi(s) \subset \phi(r + s) \tag{9.434}$$

Ainsi, pour tout $\epsilon > 0$, on a

$$d(x,z) \leqslant r + s < d(x,y) + d(y,z) + \epsilon. \tag{9.435}$$

(11) **Compatibilité avec la topologie** Nous devons montrer que les d-ouverts sont les mêmes que les ouverts de la topologie de V. Nous allons utiliser la proposition 9.2.

(11a) **Les ouverts sont des d-ouverts** Soit un ouvert $\mathcal{O}$ contenant $x \in V$. Alors $\mathcal{O} - x$ est un ouvert contenant 0, et il existe un n tel que

$$U_n \subset \mathcal{O} - x. \tag{9.436}$$

Nous avons alors

$$B(0, \frac{1}{2^n}) \subset U_n \subset \mathcal{O} - x. \tag{9.437}$$

Nous utilisant le lemme 9.347 pour additionner x dans toutes les inclusions :

$$B(x, \frac{1}{2^n}) = B(0, \frac{1}{2^n}) + x \subset \mathcal{O}. \tag{9.438}$$

Les boules forment donc une base de la topologie de V. Donc tous les ouverts de V sont des unions de boules et sont donc des d-ouverts.

(11b) **Les d-ouverts sont des ouverts**

Considérons une boule $B(0,r)$. Il existe un n tel que $B(0, 1/2^n) \subset B(0,r)$ et donc tel que

$$U_n \subset B(0,r). \tag{9.439}$$

En procédant par translations et tout ça, on en déduit que les $\{U_n + x\}_{n\in\mathbb{N}, x\in V}$ forment une base de la d-topologie. Donc les d-ouverts sont des ouverts.

□

9.15.5 Équivalence entre Cauchy et $\tau-$Cauchy

LEMooIAHSooFkXjvr

Lemme 9.356.
Soit un espace vectoriel topologique[168] V *et une distance* $d\colon V\times V\to\mathbb{R}^+$ *compatible*[169] *avec la topologie de* V. *Si* d *est invariante*[170], *alors les suites de Cauchy pour* d *et les suites* τ*-Cauchy sont les mêmes.*

Démonstration. Nous avons deux implications à prouver.

(1) **Cauchy pour d implique τ-Cauchy** Soit (x_n), une suite de Cauchy dans V pour d, et un voisinage U de 0. Vu que d est compatible avec la topologie de V, il existe une boule ouverte $B(0,\epsilon)$ incluse à U. Soit $N>0$ tel que $m,n>N$ implique $d(x_n,x_m)<\epsilon$. Par invariance de la métrique, nous avons aussi
$$d(0,x_m-x_n)<\epsilon, \tag{9.440}$$
c'est-à-dire $x_m-x_n\in B(0,\epsilon)\subset U$. La suite (x_n) est donc τ-Cauchy.

(2) **τ-Cauchy implique Cauchy pour d** Soit (x_n), une suite τ-Cauchy dans V et $\epsilon>0$. Vu que $B(0,\epsilon)$ est un voisinage de 0 dans V, il existe N tel que $m,n>N$ implique $x_n-x_m\in B(0,\epsilon)$. Cela signifie que $d(0,x_n-x_m)<\epsilon$ et toujours par invariance, que $d(x_n,x_m)<\epsilon$.

□

Tout ceci nous mène à donner une large classe d'espaces vectoriels topologiques sur lesquelles les notions de suites de Cauchy pour une distance et τ-Cauchy coïncident.

THOooGQZSooAmQolf

Théorème-Définition 9.357.
Soit V *un espace vectoriel topologique métrisable*[171], *alors il admet une métrique* d *compatible avec la topologie telle que une suite dans* V *est de Cauchy pour* d *si et seulement si elle est* τ*-Cauchy.*

Une ***suite de Cauchy*** *dans un espace vectoriel métrique* (E,d) *est une suite* τ*-Cauchy ou de Cauchy pour* d.

Démonstration. Soit d une métrique sur V satisfaisant au théorème 9.355. Vu qu'elle est invariante par translation, les suites d-Cauchy sont exactement les suites τ-Cauchy par le lemme 9.356. □

REMooUFQYooUVCCjs

Remarque 9.358.
Même si V est métrisable, si on choisit la métrique n'importe comment, on ne peut rien espérer.

9.359.
Sur les espaces vectoriels topologiques métrisables, nous pouvons donc parler de suite de Cauchy sans préciser si nous parlons de τ-Cauchy ou de d-Cauchy, parce que nous sous-entendons avoir choisi une métrique non seulement compatible avec la topologie, mais également invariante par translation.

Il reste cependant à traiter le cas d'un espace vectoriel topologique non métrisable. Dans ce cas, il n'y a pas de métrique, et la question de l'équivalence des définitions ne se pose pas.

Le théorème suivant donne la complétude de $\mathbb{R}$ et le critère de Cauchy pour les définitions métriques et topologiques usuelles. Lorsqu'on dit que $\mathbb{R}$ est complet, le plus souvent nous parlons de ce théorème, et non de 4.78 qui en est un lemme indispensable mais qui parle de notions différentes, bien que très liées.

THOooNULFooYUqQYo

Théorème 9.360 (Complétude de $\mathbb{R}$, critère de Cauchy[39])**.**
Nous avons :

(1) L'espace métrique $(\mathbb{R},d)$ *est complet (définition 9.335).*

ITEMooUUFCooIVtGgz

(2) Une suite dans $\mathbb{R}$ *est convergente (définition 9.14) si et seulement si elle est de Cauchy (définition 9.357).*

Démonstration. Tout ce théorème se base sur le fait que la définition de suite de Cauchy dans $(\mathbb{R},d)$ et de suite convergente dans $(\mathbb{R},d)$ coïncident avec les définitions correspondantes dans $\mathbb{R}$ vu comme simple corps ordonné (définitions 3.249).

Donc si (x_n) est de Cauchy dans $(\mathbb{R},d)$, elle est de Cauchy dans le corps ordonné $(\mathbb{R},\leqslant)$. Donc le théorème 4.78 nous dit que (x_n) est convergente dans $(\mathbb{R},\leqslant)$. Et donc convergente dans $(\mathbb{R},d)$.

Toutes les autres affirmations se prouvent de la même manière. □

[168] Définition 9.239.
[169] Définition 9.345.
[170] Définition 9.346.
[171] Voir la proposition 9.355 pour une condition suffisante.

Si vous n'êtes pas sûr ou si vous ne voulez pas étudier les notations de convergence et de suites de Cauchy dans les corps, vous pouvez simplement recopier la démonstration du théorème 4.78 en remplaçant partout $\mathbb{Q}$ par $\mathbb{R}$, et aussi en remplaçant les $|x-y|$ par $d(x,y)$.

9.361.
Nous pouvons également mettre une structure d'espace métrique sur $\mathbb{C}$ en posant

$$d(z,z') = |z-z'|. \tag{9.441}$$

PROPooOIQKooPtyXgm

Proposition 9.362.
L'espace métrique $(\mathbb{C},d)$ est complet.

Démonstration. Commençons par nous rendre compte que pour tout $z\in\mathbb{C}$ nous avons $|\operatorname{Re}(z)|\leqslant|z|$. C'est bon ? Vous vous en êtes rendu compte ? Ok. Continuons.

Soit une suite de Cauchy (z_k) dans $\mathbb{C}$ et $\epsilon>0$. Si nous posons $x_j=\operatorname{Re}(z_j)$, nous avons

$$|x_k-x_l| = |\operatorname{Re}(z_k-z_l)| \leqslant |z_k-z_l|. \tag{9.442}$$

Vu que (z_k) est de Cauchy, il existe un N tel que si $k,l\geqslant N$,

$$|x_k-x_l|\leqslant|z_k-z_l|\leqslant\epsilon. \tag{9.443}$$

Donc la suite des parties réelles converge par la complétude de $(\mathbb{R},d)$ du théorème 9.360. Notez que le d ici n'est pas tout à fait le même, et que la démonstration fonctionne parce que la distance prise sur $\mathbb{R}$ est la restriction à $\mathbb{R}$ de la distance prise sur $\mathbb{C}$. Notons x la limite de (x_k).

De la même manière la suite des parties imaginaires $y_k=\operatorname{Im}(z_k)$ converge vers un réel que nous notons y. Avec tout cela, la suite z_k converge dans $\mathbb{C}$ vers $x+iy$. En effet pour ϵ donné et pour un k suffisament grand,

$$|z_k-(x+iy)| = \big|\operatorname{Re}(z_k)-x+i(\operatorname{Im}(z_k)-y)\big| \leqslant |x_k-x|+|y_k-y|\leqslant\epsilon. \tag{9.444}$$

□

9.16 Norme, espace vectoriel normé

SECooWKJNooKOqpsx

La valeur absolue est essentielle pour introduire les notions de limite et de continuité pour les fonctions d'une variable. Par exemple nous verrons dans la proposition 11.81 que la fonction $f:\mathbb{R}\to\mathbb{R}$ est continue en a si et seulement si pour tout $\varepsilon>0$, il existe un $\delta>0$ tel que

$$|x-a|\leqslant\delta \Rightarrow |f(x)-f(a)|\leqslant\varepsilon. \tag{9.445}$$

La quantité $|x-a|$ donne la « distance » entre x et a ; la définition de la continuité signifie que pour tout ε, il existe un δ tel que si a et x sont au plus à la distance δ l'un de l'autre, alors $f(x)$ et $f(a)$ ne seront éloignés au plus d'une distance ε.

La valeur absolue, dans $\mathbb{R}$, nous sert donc à mesurer des distances entre les nombres. Les principales propriétés de la valeur absolue sont :

(1) $|x|=0$ implique $x=0$,

(2) $|\lambda x|=|\lambda||x|$,

(3) $|x+y|\leqslant|x|+|y|$

pour tout $x,y\in\mathbb{R}$ et $\lambda\in\mathbb{R}$.

Afin de donner une notion de limite pour les fonctions de plusieurs variables, nous devons trouver un moyen de définir les notions de « taille » d'un vecteur et de distance entre deux points de $\mathbb{R}^n$, avec $n>1$. La notion de « taille » doit satisfaire propriétés analogues à celles de la valeur absolue.

La première notion de « taille » pour un vecteur de $\mathbb{R}^2$ que nous vient à l'esprit est la longueur du segment entre l'origine et l'extrémité libre du vecteur. Cela peut être calculée à l'aide du théorème de Pythagore :

$$\text{taille de } (a,b) = \sqrt{a^2+b^2}. \tag{9.446}$$

Nous pouvons introduire une notion de distance entre les éléments de $\mathbb{R}^2$ de façon similaire :

$$d\big((a_x,a_y),(b_x,b_y)\big) = \sqrt{(a_x-b_x)^2+(a_y-b_y)^2}. \tag{9.447}$$

Cette définition a l'air raisonnable ; est-elle mathématiquement correcte ? Peut-elle jouer le rôle de la valeur absolue dans $\mathbb{R}^2$? Est-elle la seule définition possibles de « taille » et distance en $\mathbb{R}^2$?

Nous voulons formaliser les notions de « taille » et de distance dans $\mathbb{R}^n$, et plus généralement dans un espace vectoriel V de dimension finie. Pour cela nous nous inspirons des propriétés de la valeur absolue.

9.16.0.1 Critère de Cauchy

THOooRDYOooJHLfGq

Théorème 9.363 (Bolzano-Weierstrass, thème 33)**.**
Toute suite contenue dans un compact admet une sous-suite convergente.

Démonstration. Nous faisons la preuve par l'absurde en supposant que (x_k) n'admette pas de sous-suite convergente. Soit $a \in K$; aucune sous-suite de (x_k) ne converge vers a. En particulier, il existe un voisinage ouvert $\mathcal{O}_a$ de a et une partie finie I_a de $\mathbb{N}$ tel que $x_k \in \mathcal{O}_a$ seulement pour $k \in I_a$.

Les ouverts $\mathcal{O}_a$ recouvrent K ; nous pouvons en extraire un sous-recouvrement fini (c'est la définition 9.125 de la compactié). Nous avons donc des points $a_1, \dots, a_n$ tels que

$$K \subset \bigcup_{i=1}^{n} \mathcal{O}_{a_i} \tag{9.448}$$

et tels que pour chaque $\mathcal{O}_{a_i}$, nous avons $x_k \in \mathcal{O}_{a_i}$ seulement pour $k \in I_{a_i}$. Bien entendu, toute la suite est dans K et donc dans l'union.

En conclusion, nous avons $\mathbb{N} = \bigcup_{i=1}^{n} I_{a_i}$, ce qui prouve que $\mathbb{N}$ est un ensemble fini. Contradiction avec la proposition 1.176 qui dit que $\mathbb{N}$ est infini. □

CORooBTIPooUYWucb

Corolaire 9.364 ([1])**.**
Une suite dans un compact dont toutes les sous-suites convergentes convergent vers la même limite est convergente.

Démonstration. Soient un espace topologique X, un compact K et une suite (x_k) dans K. Nous supposons que toutes les sous-suites convergentes de (x_k) convergent vers $a \in X$. Nous devons montrer que $x_k \xrightarrow{X} a$.

Supposons que ce ne soit pas le cas. Alors il existe un voisinage V de a tel que pour tout $N \in \mathbb{N}$, il existe k tel que $x_k \notin V$. Cela produit une sous-suite hors de V. Cette sous-suite est encore dans K et possède donc une sous(-sous)-suite convergente (théorème 9.363). Par hypothèse, cette sous-sous-suite doit converger vers a, ce qui est impossible.

Contradiction et le corolaire est prouvé. □

Lemme 9.365.
Une suite de Cauchy[172] *dans un espace vectoriel normé admettant une sous-suite convergente est elle-même convergente vers la même limite.*

Démonstration. Soit (a_n) une suite de Cauchy dans un espace vectoriel normé E et ℓ la limite d'une sous-suite de (a_n). Soit $\epsilon > 0$ et $N \in \mathbb{N}$ tel que $\|a_m - a_p\| < \epsilon$ dès que $m, p \geqslant N$. Nous allons montrer que si $k > N$ alors $\|a_k - \ell\| < 2\epsilon$. Pour cela nous considérons un $n > N$ tel que $\|a_n - \ell\| \leqslant \epsilon$ et nous calculons

$$\|a_k - \ell\| \leqslant \|a_k - a_n\| + \|a_n - \ell\| \leqslant 2\epsilon. \tag{9.449}$$

□

Dans le cas des espaces de dimension finie, le fait d'être complet est automatique, comme le montre la proposition suivante.

PROPooGJDTooXOoYfw

Proposition 9.366.
Soit $\big(E, \|.\|\big)$ un espace vectoriel normé de dimension finie sur un corps $\mathbb{K}$ qui est complet[173]*. Alors E est complet*[174]*.*

Pour rappel, la complétude de l'espace métrique $\mathbb{R}$ est la proposition 4.22.

Démonstration. Nous considérons une suite de Cauchy (f_n) dans E et si $\{e_\alpha\}$ est une base orthonormée de E nous définissons les coefficients $f_n = \sum_\alpha a_{n\alpha} e_\alpha$. La somme sur α est finie par hypothèse sur la dimension de E.

Nous avons

$$\|f_n - f_m\| = \|\sum_\alpha (a_{n\alpha} - a_{m\alpha}) e_\alpha\| = \sum_\alpha |a_{n\alpha} - a_{m\alpha}|^2. \tag{9.450}$$

[172] Définition 9.334.
[173] La définition est 3.249, mais si vous n'avez pas envie de vous embarquer trop loin, dites juste « toutes les suites de Cauchy convergent ». Typiquement c'est $\mathbb{R}$ ou $\mathbb{C}$.
[174] Définition 9.335.

Soit $\epsilon > 0$. Il existe N tel que si $m, n > N$ alors $\|f_n - f_m\| < \epsilon$. Avec ces conditions sur N, n et m nous avons

$$\sum_\alpha |a_{n\alpha} - a_{m\alpha}|^2 < \epsilon. \tag{9.451}$$

Pour chaque α nous avons donc $|a_{n\alpha} - a_{m\alpha}| < \sqrt{\epsilon}$.

Autrement dit, pour chaque α, la suite $(a_{n\alpha})_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{K}$ et converge donc dans $\mathbb{K}$. Soit a_α la limite et définissons $f = \sum_\alpha a_\alpha e_\alpha$. Nous avons alors

$$\|f_n - f\| = \|\sum_\alpha (a_{n\alpha} - a_\alpha)e_\alpha\|, \tag{9.452}$$

dont la limite $n \to \infty$ est bien zéro. Donc la suite (f_n) converge vers $f \in E$. L'espace E est alors complet. □

PropContinueCompactBorne

Proposition 9.367.
Soient V et W deux espaces vectoriels normés. Soient K une partie compacte de V et $f\colon K \to W$ une fonction continue. Alors l'image $f(K)$ est compacte dans W.

Ce résultat est démontré dans un cadre plus général par le théorème 9.298.

Démonstration. Nous allons prouver que $f(K)$ est fermée et bornée.

(1) $f(K)$ **est fermé** Nous allons prouver que si (y_n) est une suite convergente contenue dans $f(K)$, alors la limite est également contenue dans $f(K)$. Dans ce cas, nous aurons que l'adhérence de $f(K)$ est contenue dans $f(K)$ et donc que $f(K)$ est fermé. Pour chaque $n \in \mathbb{N}$, le vecteur y_n appartient à $f(K)$ et donc il existe un $x_n \in K$ tel que $f(x_n) = y_n$. La suite (x_n) ainsi construite est une suite dans le fermé K et possède donc une sous-suite convergente (proposition 9.363). Notons (x'_n) cette sous-suite convergente, et a sa limite : $\lim(x'_n) = a \in K$. Le fait que la limite soit dans K provient du fait que K est fermé.

Nous pouvons considérer la suite $f(x'_n)$ dans W. Cela est une sous-suite de la suite (y_n), et nous avons $\lim f(x'_n) = f(a)$ parce que f est continue. Par conséquent nous avons

$$f(a) = \lim f(x'_n) = \lim y_n. \tag{9.453}$$

Cela prouve que la limite de (y_n) est dans $f(K)$ et par conséquent que $f(K)$ est fermé.

(2) $f(K)$ **est borné** Si $f(K)$ n'est pas borné, nous pouvons trouver une suite (x_n) dans K telle que

$$\|f(x_n)\|_W > n \tag{9.454}$$

EqfxnWgeqn

Mais par ailleurs, l'ensemble K étant compact (et donc fermé), nous avons une sous-suite (x'_n) qui converge dans K. Disons $\lim(x'_n) = a \in K$.

Par la continuité de f nous avons alors $f(a) = \lim f(x'_n)$, et donc

$$\|f(a)\|_W = \lim \|f(x'_n)\|_W. \tag{9.455}$$

La suite $f(x'_n)$ est alors une suite bornée, ce qui n'est pas possible au vu de la condition (9.454) imposée à la suite de départ (x_n).

□

CorFnContinueCompactBorne

Corolaire 9.368.
Si $f\colon K \to \mathbb{R}$ est une application continue où K est une partie compacte d'un espace vectoriel normé, alors $f(K)$ est borné.

Démonstration. En effet, la proposition 9.367 montre que $f(K)$ est compact et donc borné. □

9.17 Espaces métriques

9.17.1 Espaces métrisables

Définition 9.369.
*Un espace topologique est **métrisable** si il est homéomorphe à un espace métrique.*

PROPooKNVUooMbLZoy

Proposition 9.370.
Une fonction séquentiellement continue sur un espace métrisable et à valeurs dans un espace métrique est continue.

Démonstration. Soient E un espace métrique et $\phi\colon X \to (E,d)$ un homéomorphisme. Nous supposons que $f\colon X \to Y$ est séquentiellement continue. Nous considérons l'application $\tilde{f} = f \circ \phi^{-1}$, c'est-à-dire

$$\begin{aligned} \tilde{f}\colon E &\to Y \\ a &\mapsto f\big(\phi^{-1}(a)\big). \end{aligned} \tag{9.456}$$

L'application ϕ^{-1} est continue et donc séquentiellement continue. De plus $\tilde{f}$ est séquentiellement continue. En effet si $a_k \xrightarrow{E} a$, alors

$$\tilde{f}(a_k) = f\big(\phi^{-1}(a_k)\big), \tag{9.457}$$

mais ϕ^{-1} est séquentiellement continue, donc $\phi^{-1}(a_k) \xrightarrow{X} \phi^{-1}(a)$, ce qui signifie que $\phi^{-1}(a_k)$ est une suite convergente dans X et donc

$$\lim_{k\to\infty} \tilde{f}(a_k) = \lim_{k\to\infty} f\big(\phi^{-1}(a_k)\big) = f\big(\phi^{-1}(a)\big) = \tilde{f}(a). \tag{9.458}$$

L'application $\tilde{f}$ est donc séquentiellement continue. Mais étant donné que $\tilde{f}$ est définie sur un espace métrique (E) et à valeurs dans un métrique, elle est continue par la proposition 9.173. L'application $f = \tilde{f} \circ \phi$ est donc continue en tant que composée d'applications continues. □

9.17.2 Fonctions continues

La propriété suivante donne des caractérisations importantes de la continuité dans le cas des espaces métriques.

PropQZRNpMn

Proposition 9.371 (Continuité, ouverts et voisinages et limite[299])**.**
Soient $f\colon E \to F$ une application entre espaces métriques et $a \in E$. Alors nous avons équivalence entre les choses suivantes :

ItemCBUoRWJi
(1) *f est continue en a,*

ItemCBUoRWJii
(2) *Pour tout voisinage ouvert W de $f(a)$, il existe un voisinage ouvert V de a tel que $f(V) \subset W$.*

ItemCBUoRWJiii
(3) *Pour toute boule $W' = B\big(f(a),\epsilon\big)$, il existe une boule $V' = B(a,\delta)$ telle que $f(V) \subset W'$.*

ItemCBUoRWJiv
(4) *$\forall \epsilon > 0$, $\exists \delta > 0$ tel que $f\big(B(a,\delta)\big) \subset B\big(f(a),\epsilon\big)$.*

ItemYNQpikrii
(5) *$\lim_{x\to a} f(x) = f(a)$ où la limite est donnée par la définition 9.151,*

ItemYNQpikriii
(6) *Pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que $\|x-a\| < \delta$ implique $\|f(x) - f(a)\| < \epsilon$.*

La proposition 9.419 nous montrera que ces équivalences tiennent encore lorsque l'espace a une topologie de seminormes.

Démonstration. L'équivalence (1) ⇔ (2) est la définition 9.48. L'équivalence (3) ⇔ (4) est une simple paraphrase.

Montrons (2) ⇒ (3). Si $W' = B\big(f(a),\delta\big)$, nous avons un voisinage V de a tel que $f(V) \subset W'$. L'ensemble V contenant une boule autour de chacun de ses points[175], il en contient un autour de a : $V' = B(a,\delta) \subset V$. A fortiori nous avons $f(V') \subset W$.

Montrons (3) ⇒ (2). Si W est un ouvert autour de $f(a)$, il contient une boule autour de $f(a)$: $B\big(f(a),\epsilon\big) \subset W$. Il existe donc une boule $V' = B(a,\delta)$ telle que $f(V') \subset B\big(f(a),\epsilon\big) \subset W$.

L'équivalence (1) ⇔ (5) est la définition 9.48 de la continuité en un point couplée à l'unicité de la limite due à la proposition 9.154 parce qu'un espace métrique est séparé.

Prouvons (5) ⇒ (6). Soient $\epsilon > 0$ et $V = B\big(f(a),\epsilon\big)$. Étant donné que $f(a)$ est une limite de f pour $x \to a$, il existe un voisinage W de a tel que $f(W) \subset V$. Soit $\delta > 0$ tel que $B(a,\delta) \subset W$; alors si $\|x-a\| < \delta$ nous avons $x \in B(x,\delta) \subset W$ et donc $f(x) \in B\big(f(a),\epsilon\big)$, c'est-à-dire $\|f(a) - f(x)\| < \epsilon$.

Enfin l'implication (2) ⇒ (5) est une réécriture de la définition de la limite en un point. □

[175] Cela est le théorème-définition 9.158 des ouverts dans un espace métrique, à ne pas confondre avec le théorème 9.8.

Voici un théorème qui parle de fermés emboîtés dans un espace métrique. Le corolaire 9.134 parle du cas $\cap_i A_i = \varnothing$ dans un compact.

ThoCQAcZxX

Théorème 9.372 (Théorème [300]).
Soit (E, d) un espace métrique. Il est complet si et seulement si toute suite décroissante de fermés non vides dont le diamètre tend vers zéro a une intersection qui se réduit à un seul point.

Démonstration. En deux parties.

(1) **Condition suffisante**

Soit $\{F_n\}_{n\in\mathbb{N}}$ une telle suite de fermés emboités. Si nous choisissons des points $x_n \in F_n$, nous obtenons une suite (x_n) de Cauchy et qui est par conséquent convergente vu que l'espace est par hypothèse complet. De plus, pour chaque $N \geqslant n$, la queue de suite $(x_n)_{n\geqslant N}$ est contenue dans F_N et donc converge vers un élément de F_N (parce que ce dernier est fermé). Donc la limite de (x_n) est dans $\bigcap_{n\in\mathbb{N}} F_n$.

De plus cette intersection a diamètre nul parce que le diamètre de $\bigcap_{n\in\mathbb{N}} F_n$ est majoré par tous les diamètres des F_n, lesquels sont arbitrairement petits par hypothèse. Donc l'intersection est réduite a un point.

(2) **Condition nécessaire**

Soit (x_n) un suite de Cauchy. Nous considérons les ensembles

$$F_n = \overline{\{x_i \text{ tel que } i \geqslant n\}}. \tag{9.459}$$

Le fait que la suite soit de Cauchy implique que $\operatorname{diam}(F_n) \to 0$. Par hypothèse, nous avons alors

$$\bigcap_{n\in\mathbb{N}} F_n = \{a\}. \tag{9.460}$$

Pour s'assurer que a est bien la limite de (x_n), il suffit de remarquer que

$$d(x_n, a) \leqslant \operatorname{diam} F_n \to 0. \tag{9.461}$$

□

PropGULUooNzqZKj

Proposition 9.373.
Soient (X, d) un espace topologique métrique et F un fermé de X. Nous avons $d(x, F) = 0$ si et seulement si $x \in F$.

Démonstration. Si $x \in F$ alors $d(x, F) = 0$ parce que $d(x, x)$ fait partie de l'ensemble sur lequel nous prenons l'infimum.

Si réciproquement $d(x, F) = 0$, cela signifie que pour tout ϵ, il existe $x_\epsilon \in F$ tel que $d(x_\epsilon, x) \leqslant \epsilon$. En prenant $\epsilon = 1/k$ nous construisons une suite (x_k) d'éléments dans F vérifiant $d(x_k, x) = \frac{1}{k}$. Cela signifie que $\lim_{k\to\infty} x_k = x$ par la proposition 9.342(1).

Par la caractérisation séquentielle des fermés (un fermé contient les limites de toutes ses suites, proposition 9.170), la suite (x_k) étant dans F, la limite est dans F. Donc $x \in F$. □

LemooynkH

Lemme 9.374.
Soit A_n une suite décroissante de fermés non vides dans un espace métrique[176] compact K. Alors

$$C = \bigcap_{n\in\mathbb{N}} A_n \tag{9.462}$$

est non vide.

Démonstration. Soit (x_n) une suite dans K telle que $x_n \in A_n$. La suite étant contenue dans A_1, et A_1 étant compact (lemme 9.137), elle possède une sous-suite $(y_n = x_{\sigma_1(n)})$ convergente dont la limite est dans A_1 par le théorème de Bolzano-Weierstrass 9.213. Une queue de la suite y_n est dans A_2 et nous considérons donc une sous-suite convergente dans A_2 donnée par

$$z_n = y_{\sigma_2(n)} = x_{\sigma_1\sigma_2(n)}. \tag{9.463}$$

[176] L'hypothèse métrique provient de l'utilisation de Bolzano-Weierstrass, lequel est vrai pour les espaces séquentiellement compacts, dont les espaces métriques.

En continuant ainsi nous construisons une suite convergente dans A_k. Nous considérons enfin la suite

$$y_n = x_{\sigma_1 \dots \sigma_n(n)}. \tag{9.464}$$

Pour tout k, une queue de cette suite est une sous-suite de $x_{\sigma_1 \dots \sigma_k(n)}$ et par conséquent cette suite converge dans A_k. La limite de cette suite est donc dans l'intersection demandée. □

Remarque 9.375.
Cette propriété est fausse pour les ouverts. Par exemple

$$\bigcap_{n>1}]0, \frac{1}{n}[= \varnothing. \tag{9.465}$$

LemKIcAbic

Lemme 9.376.
Si K est un compact dans un espace métrique et F un fermé disjoint de K, alors $d(K,F) > 0$.

Démonstration. La fonction

$$\begin{aligned} K &\to \mathbb{R} \\ x &\mapsto d(x,F) \end{aligned} \tag{9.466}$$

est une fonction continue sur K, et donc atteint son minimum par le théorème de Weierstrass 9.215. Soit $x_0 \in K$ un point de K qui réalise ce minimum. Si $d(x_0,F) = 0$, alors on aurait une suite (x_n) dans F qui convergerait vers x_0, mais F étant fermé cela signifierait que x_0 serait dans F, ce qui contredirait l'hypothèse que F et K sont disjoints. □

PropLHWACDU

Proposition 9.377.
Soient (X,d) un espace métrique compact et (u_n) une suite de X telle que

$$\lim_{n\to\infty} d(u_n, u_{n+1}) = 0. \tag{9.467}$$

Alors l'ensemble des points d'accumulation[177] *de (u_n) est connexe.*

Démonstration. Nous notons Γ l'ensemble des points d'accumulation de la suite.

(1) **Γ est compact** Nous notons $A_p = \{u_n \text{ tel que } n \geqslant p\}$ et nous avons

$$\Gamma = \bigcap_{p\in\mathbb{N}} \overline{A_p} \tag{9.468}$$

parce que si $x \in \Gamma$, alors pour tout n, il existe $m > n$ tel que $x_m \in B(x,\epsilon)$, et donc tel que $x \in B(x_m,\epsilon)$. Donc pour tout ϵ et pour tout p, l'intersection $B(x,\epsilon) \cap A_p$ est non vide.

En tant qu'intersection de fermés, Γ est fermé (lemme 9.6). En tant que fermé dans un compact, Γ est compact (lemme 9.137).

(2) **Recouvrement par deux compacts**

Supposons que Γ ne soit[178] pas connexe. Nous pouvons alors considérer S et O, deux ouverts disjoints recouvrant Γ et intersectant tous deux Γ. Nous posons alors

$$A = S \cap \Gamma \tag{9.469a}$$
$$B = O \cap \Gamma, \tag{9.469b}$$

et nous avons évidemment $\Gamma = A \cup B$. Montrons que A est fermé (B le sera aussi par le même raisonnement). Soit une suite d'éléments de $S \cap \Gamma$ convergent dans X. Alors la limite est dans $\bar{\Gamma} = \Gamma$ et donc elle est donc O ou S, mais elle est certainement dans $\bar{S}$. Cependant $\bar{S}$ n'intersecte pas O. En effet si $x \in \bar{S} \cap O$, alors tout voisinage de x intersecterait S, mais il y a des voisinages de x étant inclus dans O parce que O est ouvert ; cela donnerait une intersection entre O et S, ce qui est impossible. Donc la limite n'est pas dans O et donc elle est dans S. Au final la limite est dans $S \cap \Gamma$, ce qui prouve son caractère fermé.

Comme d'habitude, $\Gamma \cap S$ est compact parce que fermé dans un compact[179].

[177] Définition 9.46.
[178] est-ce qu'il faut vraiment un subjonctif ici ?
[179] Lemme 9.137.

(3) **Décomposition en trois morceaux**

Vu que A et B sont des compacts disjoints, nous avons $d(A,B)=\alpha>0$ pour un certain α par le lemme 9.376. Nous notons

$$A'=\{x\in X \text{ tel que } d(x,A)<\frac{\alpha}{3}\} \tag{9.470a}$$

$$B'=\{x\in X \text{ tel que } d(x,B)<\frac{\alpha}{3}\} \tag{9.470b}$$

Nous avons $A'=\bigcup_{x\in A}B(x,\frac{\alpha}{3})$ et donc en tant qu'union d'ouverts, A' est ouvert (définition de la topologie). Même chose pour B'.

Enfin nous notons

$$K=X\setminus(A'\cup B') \tag{9.471}$$

qui est fermé en tant que complémentaire d'ouvert, et donc compact. Étant donné que $A\subset A'$ et $B\subset B'$, nous avons $K\cap\Gamma=\varnothing$.

L'idée est maintenant de montrer que K contient un point d'accumulation de (u_n).

(4) **Sous-suites de (u_n)**

L'hypothèse sur la suite (u_n) nous indique qu'il existe un N_0 tel que $\forall n\geqslant N_0$,

$$d(u_n,u_{n+1})<\frac{\alpha}{3}. \tag{9.472}$$ EqIHioHiW

Soient $N>N_0$ et $x_0\in A$. Étant donné que x_0 est point d'accumulation de la suite, il existe $n_1>N$ tel que $d(x_0,u_{n_1})<\frac{\alpha}{3}$. Même chose dans B : nous prenons $y_0\in B$ et un naturel $n_2>n_1$ tel que $d(y_0,u_{n_2})<\frac{\alpha}{3}$. Nous avons $u_{n_1}\in A'$ et $u_{n_2}\in B'$.

Soit n_0 le plus petit naturel supérieur à n_1 tel que $u_{n_0}\notin A'$. Cela existe parce que $u_{n_2}\in B'$ et $B'\cap A'=\varnothing$, mais n_0 n'est pas n_2 lui-même parce que $d(A',B')\geqslant\frac{\alpha}{3}$ alors que nous considérons $n_0,n_1,n_2>N_0$ et donc pour tous les i entre n_1 et n_2 (compris), $d(u_i,u_{i+1})<\frac{\alpha}{3}$. Notons qu'ici le strict dans la condition (9.472) est important. Nous avons donc $N_0<n_1<n_0<n_2$.

Nous allons maintenant montrer que u_{n_0} est dans K. C'est fait pour : il est loin en même temps de A' et de B'. En utilisant l'inégalité triangulaire à l'envers, nous avons

$$\begin{aligned}d(u_{n_0},B)&\geqslant d(u_{n_0-1},B)-d(u_{n_0-1},u_{n0})\\&\geqslant d(A,B)-d(u_{n_0-1},A)-d(u_{n_0-1},u_{n_0})\\&\geqslant\alpha-\frac{\alpha}{3}-\frac{\alpha}{3}\\&=\frac{\alpha}{3}.\end{aligned} \tag{9.473}$$

Pour la dernière inégalité nous avons utilisé le fait que u_{n_0-1} n'est pas dans A'. Bref, nous avons montré que u_{n_0} n'est pas dans B' (dans la définition de ce dernier nous avons bien une inégalité stricte). Vu que par définition u_{n_0} n'est pas non plus dans A', nous avons $u_{n_0}\in K$.

Nous avons montré jusqu'à présent que pour tout $N\geqslant N_0$, il existe un $n_0\geqslant N$ tel que $u_{n_0}\in K$. Cela nous construit donc une sous-suite (v_n) de (u_n) contenue dans K. En tant que suite dans le compact K, la suite (v_n) admet un point d'accumulation dans K. Ce point est également point d'accumulation de la suite (u_n) complète, ce qui donne un point d'accumulation de (u_n) dans K et donc une contradiction.

Nous concluons que Γ est connexe. □

Encore une petite conséquence sans ambition du théorème de Bolzano-Weierstrass.

PropHNylIAW

Proposition 9.378.
Si (x_n) est une suite dans un compact telle que toute sous-suite convergente ait le même point x comme limite. Alors la suite entière converge vers x.

Démonstration. Supposons que ce ne soit pas le cas. Alors il existe un ϵ tel que pour tout $N>0$, il existe $n>N$ avec $d(x_n,x)>\epsilon$. Cela nous donne une sous-suite de (x_n) composée d'éléments tous à une distance de x supérieure à ϵ. Nous la nommons (y_n) ; c'est une suite dans un compact qui admet donc une sous-suite convergente (et une telle sous-suite est une sous-suite de (x_n)) dont la limite devrait être x, mais c'est impossible par construction. □

LemGDeZlOo

Lemme-Définition 9.379 ([301]).
Soit Ω un ouvert dans un espace métrique E. Il existe une suite (K_n) de compacts tels que

(1) $K_n \subset \Omega$

(2) $\bigcup_{n=0}^{\infty} K_n = \Omega$

(3) $K_n \subset \text{Int}(K_{n+1})$.

Une telle suite de compacts vérifie alors

(1) Il existe δ_n tel que pour tout $z \in K_n$, $B(z, \delta_n) \subset K_{n+1}$.

ITEMooBPYPooEMhSmY

(2) Tout compact de Ω est inclus dans $\text{Int}(K_n)$ pour un certain n.

*Une telle suite de compacts est une **suite exhaustive** de compacts pour Ω.*

Démonstration. Nous considérons les ensembles

$$V_n = \{z \in E \text{ tel que } |z|\} \cup \bigcup_{a \notin \Omega} B(a, \frac{1}{n}), \tag{9.474}$$

et nous définissons $K_n = V_n^c$. Vérifions que ces ensembles vérifient tout ce qu'il faut.

(1) $\underline{K_n \subset \Omega}$ Si $a \notin \Omega$ alors a est dans tous les V_n et donc dans aucun des K_n ; nous avons donc bien $\overline{K_n \subset \Omega}$.

(2) $\underline{\bigcup_{n=0}^{\infty} K_n = \Omega}$ Nous avons déjà prouvé que $\bigcup_{n=0}^{\infty} K_n \subset \Omega$. Pour avoir l'inclusion dans l'autre sens, soit $z \in \Omega$. Nous prenons $n_1 > |z|$ puis n_2 tel que $B(z, \frac{1}{n_2}) \subset \Omega$. Alors $z \in K_n$ avec $n > \max(n_1, n_2)$. Pour ce choix de n, nous avons $z \in K_n$. Cela prouve que $\Omega \subset \bigcup_{n=0}^{\infty} K_n$.

(3) $\underline{K_n \subset \text{Int}(K_{n+1})}$ Soit $z \in K_n$. L'élément z vérifie $d(z, \Omega^c) \geqslant \frac{1}{n}$. Du coup si nous prenons δ tel que

$$\frac{1}{n+1} < \delta < \frac{1}{n} \tag{9.475}$$

alors $B(z, \delta) \subset K_{n+1}$.

(4) $\underline{\textbf{Les } K_n \textbf{ sont compacts}}$ Enfin, les K_n sont tous compacts. En effet ils sont bornés parce que $K_n \subset \overline{B(0, n)}$ et ensuite K_n est fermé en tant que complémentaire d'un ouvert (V_n est ouvert en tant qu'union d'ouverts).

Nous passons maintenant aux propriétés, qui sont indépendantes de la façon dont nous avons construit les K_n vérifiant les conditions.

(1) Nous pouvons considérer la fonction $K_n \to \mathbb{R}$ donnée par $z \mapsto d(z, K_{n+1}^c)$. Vu que $K_n \subset \text{Int}(K_{n+1})$, c'est une fonction (continue sur le compact K_n) prenant des valeurs strictement positives. Elle a donc un minimum strictement positif. Si δ_n est plus petit que ce minimum nous avons $B(z, \delta_n) \subset K_{n+1}$ pour tout $z \in K_n$.

(2) D'abord nous avons $\Omega = \bigcup_{n=0}^{\infty} \text{Int}(K_n)$. En effet nous avons

$$\Omega = \bigcup_{n=0}^{\infty} K_n \subset \bigcup_{n=0}^{\infty} \text{Int}(K_{n+1}) \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \tag{9.476}$$

L'inclusion dans l'autre sens est facile.

Soit K compact dans Ω. Vu que Ω est l'union des $\text{Int}(K_n)$, nous avons

$$K \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \tag{9.477}$$

Cela donne à K un recouvrement par des ouverts dont nous pouvons extraire un sous-recouvrement fini par compacité. Les K_n étant croissants, du recouvrement fini, il suffit de prendre le plus grand (disons K_m) et nous avons $K \subset \text{Int}(K_m)$.

□

Notons qu'avec la suite de K_n telle que construite, le dernier point est réglé en prenant

$$\frac{1}{n+1} < \delta_n < \frac{1}{n}. \tag{9.478}$$

LEMooWRIXooSBHavt

Lemme 9.380 ([302]).
Soient un compact $K \subset \mathbb{R}^d$ ainsi que des ouverts $\{\Omega_i\}_{i=1,\dots,n}$ tels que $K \subset \bigcup_{i=1}^n \Omega_i$.
Il existe des compacts $\{K_i\}_{i=1,\dots,n}$ tels que

- $K_i \subset \Omega_i$,
- $K \subset \bigcup_{i=1}^n K_i$.

Démonstration. Soit $x \in K$. Vu que les Ω_i recouvrent K, il existe un $k(x) \in \{1,\dots,n\}$ tel que $x \in \Omega_{k(x)}$. De plus, vu que $\Omega_{k(x)}$ est ouvert, il existe un voisinage de x contenu dans $\Omega_{k(x)}$ (théorème 9.8). Autrement dit, il existe $r(x) > 0$ tel que

$$\overline{B\big(x, r(x)\big)} \subset \Omega_{k(x)}. \tag{9.479}$$

Vu que l'ensemble $\{B\big(x, r(x)\big)\}_{x\in k}$ est un recouvrement de K par des ouverts, nous pouvons en extraire un sous-recouvrent fini[180]. Soient donc $x_1, \dots, x_m \in K$ tels que

$$K \subset \bigcup_{i=1}^m B\big(x_i, r(x_i)\big). \tag{9.480}$$

EQooETROooCMUsx

Pour chaque $j = 1, \dots, n$, nous posons

$$A_j = \big\{l \in \{1,\dots,m\} \text{ tel que } k(x_l) = j\big\}. \tag{9.481}$$

Et enfin nous définisssons, pour $j = 1, \dots, n$ les parties

$$K_j = \bigcup_{l\in A_j} \overline{B\big(x_l, r(x_l)\big)} \tag{9.482}$$

et il nous reste à prouver que ces ensembles répondent bien à la question.

(1) $\bigcup_{j=1}^n A_j = \{1,\dots,m\}$ **est une union disjointe** Un élément l de $A_i \cap A_j$ devrait vérifier $i = k(x_l) = j$. Si $s \in \{1,\dots,m\}$, alors $s \in A_{k(x_s)}$. Donc oui, l'union des A_j est tout $\{1,\dots,m\}$.

(2) $K_j \subset \Omega_j$ Nous avons

$$K_j = \bigcup_{l\in A_j} \overline{B\big(x_l, r(x_l)\big)} \subset \bigcup_{l\in A_j} \Omega_{k(x_l)} = \bigcup_{l\in A_j} \Omega_j = \Omega_j. \tag{9.483}$$

(3) $K \subset \bigcup_{i=1}^n K_i$. Par (9.480), et vu que $\{1,\dots,m\} = \bigcup_{j=1}^n A_j$,

$$\begin{aligned}
K &\subset \bigcup_{i=1}^m B\big(x_i, r(x_i)\big) && \text{(9.484a)}\\
&= \bigcup_{j=1}^n \bigcup_{l\in A_j} B\big(x_l, r(x_l)\big) && \text{(9.484b)}\\
&= \bigcup_{j=1}^n \underbrace{\bigcup_{l\in A_j} \overline{B\big(x_l, r(x_l)\big)}}_{K_j} && \text{(9.484c)}\\
&= \bigcup_{j=1}^n K_j. && \text{(9.484d)}
\end{aligned}$$

□

[180] C'est la définition 9.125 d'un compact.

9.17.3 Théorème de Tykhonov

Pour des versions plus simples du théorème de Tykhonov, voir le thème 33.

ThoFWXsQOZ

Théorème 9.381 (Tykhonov)**.**
Un produit quelconque d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

PROPooDXUIooUUmgYN

Proposition 9.382 ([1])**.**
Soient des espaces topologiques $\{X_i\}_{i\in I}$ et des parties compactes $K_i \subset X_i$. Alors $\prod_{i\in I} K_i$ est compact dans $\prod_{i\in I} X_i$.

9.17.4 Ensembles enchainés

Soit (X, d) un espace métrique.

Définition 9.383.
*Une **ϵ-chaine** joignant les points a et b de X est une suite finie $(u_0, \dots, u_n)$ dans X telle que $u_0 = a$, $u_n = b$ et pour tout $0 \leqslant i \leqslant n-1$ nous avons $d(u_n, u_{n+1}) \leqslant \epsilon$.*

*Une partie A de X est **bien enchainée** si pour tout $\epsilon > 0$ et pour tout $a, b \in A$, il existe une ϵ-chaine joignant a et b dans A.*

Lemme 9.384.
Les rationnels dans $\mathbb{R}$ sont bien enchainés.

Démonstration. Soient p et q des rationnels avec $p < q$, ainsi que $\epsilon > 0$. Le lemme 4.60 nous permet de considérer un rationnel δ vérifiant $0 < \delta < \epsilon$. Et nous définissons les rationnels

$$r_k = p + k\delta. \tag{9.485}$$

Vu que $\mathbb{Q}$ est archimédien[181], il existe K tel que $r_K > q$. D'autre part, $r_0 = p < q$. Donc il existe $N = \max\{k \in \mathbb{N} \text{ tel que } r_k < q\}$.

Nous considérons la chaine $(r_0, \dots, r_N, q)$. Elle débute à $r_0 = p$ et termine à q ; pas de problèmes avec ça. À part pour le dernier pas, nous avons

$$|r_n - r_{n-1}| = \delta < \epsilon, \tag{9.486}$$

donc c'est bien une ϵ-chaine. Il reste à voir $|q - r_N|$. Nous avons $r_N \leqslant q \leqslant r_{N+1}$, et donc

$$0 \leqslant q - r_N \leqslant r_{N+1} - r_N = \delta \leqslant \epsilon. \tag{9.487}$$

Donc ok aussi pour ce dernier pas. □

PROPooBUNOooIvfugn

Proposition 9.385 ([303, 1])**.**
Un espace métrique connexe[182] est bien enchainé.

Démonstration. Soit un espace métrique X et $\epsilon > 0$. La relation $x \sim y$ si et seulement si x et y peuvent être reliés par une ϵ-chaine est une relation d'équivalence.

Soit $x \in X$. Nous prouvons que la classe $[x]$ est ouverte. En effet soit $y \in [x]$, si $z \in B(y, \epsilon)$ nous avons $z \in [y]$, et donc $z \in [x]$. Nous en déduisons que $B(y, \epsilon) \subset [x]$, et donc que $[x]$ est ouvert par le théorème 9.8.

Donc les classes sont des ouverts.

Supposons que X n'est pas bien enchainé. Alors il existe ϵ pour lequel X possède plus qu'une classe d'équivalence. Soit $\{[x_k]\}_{k\in I}$ l'ensemble des classes d'équivalences.

Nous considérons un $i_0 \in I$ quelconque, et nous définissons les ouverts $A = [x_{i_0}]$ et

$$B = \bigcup_{k\in I\setminus\{i_0\}} [x_k]. \tag{9.488}$$

Ce sont deux ouverts disjoints qui recouvrent X qui n'est donc pas connexe. □

PROPooXHTWooZibddZ

Proposition 9.386.
La fermeture d'un ensemble bien enchainé dans un espace métrique compact (X, d) est connexe.

[181] Proposition 4.15.
[182] Définition 9.118.

Démonstration. Soit $A \subset X$ un ensemble bien enchainé, et soient $a, b \in \bar{A}$. Nous construisons une suite (u_k) dans A de la façon suivante. Pour chaque $n > 0$ nous prenons $a' \in B(a, \frac{1}{n}) \cap A$ et $b' \in B(b, \frac{1}{n}) \cap A$. Ensuite nous considérons une $\frac{1}{n}$-chaine $\{v_i^{(n)}\}_{i \in I_n}$ dans A entre a' et b'. Ici l'ensemble I_n est fini. La suite (u_k) est simplement construite en mettant bout à bout les éléments $v_i^{(n)}$.

La suite ainsi construite est une suite dans A admettant a et b comme points d'accumulation (les autres points d'accumulation sont également dans $\bar{A}$) et telle que $\lim_{k\to\infty} d(u_k, u_{k+1}) = 0$. Par conséquent la proposition 9.377 nous dit que l'ensemble des points d'accumulation de (u_k) est connexe dans X. Nous le notons $C_{a,b}$.

Si nous fixons $a \in \bar{A}$, alors nous avons

$$\bigcup_{x \in \bar{A}} C_{a,x} = \bar{A}. \tag{9.489}$$

Vu que le membre de gauche est une union de connexes, c'est un connexe par la proposition 9.123. □

CORooSIKCooTncoQm

Corolaire 9.387.
Un espace métrique compact est connexe si et seulement si il est bien enchainé.

Démonstration. Dans le sens direct, c'est la proposition 9.385. Dans l'autre sens, si X est compact, alors X est fermé par le lemme 9.137(2). Et vu qu'il est fermé et bien enchainé, la proposition 9.386 implique qu'il est connexe. □

9.17.5 Produit fini d'espaces métriques

Pour rappel, la distance sur un espace produit est donnée par la définition 9.304.

THOIYmxXuu

Théorème 9.388 ([1]).
Un produit fini d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

Démonstration. Soient K_1,..., K_n des compacts et $K = K_1 \times \ldots \times K_n$ le produit muni de sa métrique usuelle de la définition (9.304) (attention : chacun des K_i peut être de dimension infinie) :

$$d(\alpha, \beta) = \max\{d_i(\alpha_i, \beta_i)\} \tag{9.490}$$

où d_i est la distance sur K_i. Si (α_n) est une suite dans K alors la suite $(\alpha_n)_1$ est une suite dans le compact K_1 dont nous pouvons extraire une sous-suite convergente (Bolzano-Weierstrass 9.213). De la sous-suite de α correspondante nous extrayons la sous-suite pour la seconde composante, etc.

En fin de compte nous avons une sous-suite (que nous nommons α également) donc chacune des composantes est convergente. Notez que nous utilisons ici de façon cruciale le fait que nous ayons qu'un nombre fini de facteurs.

Autrement dit, pour chaque $i = 1, \ldots, n$, l'application $p \mapsto (\alpha_p)_i$ est une suite dans K_i, et cette suite converge vers ℓ_i.

Soit $\epsilon > 0$ pour chaque $i = 1, \ldots, n$, il existe $N_i > 0$ tel que si $p > N_i$ alors

$$d_i\big((\alpha_p)_i, \ell_i\big) \leqslant \epsilon. \tag{9.491}$$

En prenant $N = \max_k N_k$ et $n > N$ nous avons

$$d\big(\alpha_n, (\ell_1, \ldots, \ell_n)\big) \leqslant \epsilon. \tag{9.492}$$

Par conséquent de la suite (α) nous avons extrait une sous-suite convergente et la partie « réciproque » de Bolzano-Weierstrass nous assure alors que K est compact.

À l'inverse si un des facteurs n'est pas compact (mettons K_1) alors nous prenons un recouvrement $\{\mathcal{O}_i\}_{i \in I}$ de K_1 par des ouverts duquel il est impossible d'extraire un sous-recouvrement fini. Ensuite nous posons

$$\mathcal{P}_i = \mathcal{O}_i \times K_2 \times \ldots \times K_n, \tag{9.493}$$

qui est un recouvrement de K par des ouverts (de K) d'où aucun sous-recouvrement fini ne peut être extrait. □

Pour la culture générale, il y a bien entendu moyen de faire des produits dénombrables et pire d'espaces métriques.

Définition 9.389 ([304]).
Soient (E_n, d_n) des espaces métriques. Sur l'ensemble produit $E = \prod_{i=1}^{\infty} E_i$ nous définissons la métrique

$$d(x,y) = \sum_{k=1}^{\infty} \frac{1}{2^k} d'_k(x_i, y_i) \tag{9.494}$$

où $d'_i = \min(d_i, 1)$.

On peut montrer que ce d est bien une distance et que (E, d) devient un espace métrique.

ThoKKBooNaZgoO

Théorème 9.390 (Tykhonov dénombrable[304]).
Un produit dénombrable d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

Note : ce résultat est encore valable pour un produit quelconque, c'est le théorème de Tykhonov 9.381.

9.17.6 Équicontinuité

DEFooDHQDooFfIvsX

Définition 9.391 ([1, 305, 306]).
*Soient un espace topologique X et un espace vectoriel topologique Y. Une famille H d'applications $X \to Y$ est **équicontinue** en $a \in X$ si pour tout voisinage V de 0 dans Y, il existe un voisinage U de a dans X tel que*

$$h(U) \subset h(a) + V \tag{9.495}$$

pour tout $h \in H$.

Nous disons que H est équicontinue si elle est équicontinue en tout point.

LEMooMIHJooUhvPgM

Lemme 9.392 ([1]).
Soient un espace métrique X, un espace vectoriel normé Y ainsi qu'une famille H d'isométries linéaires $X \to Y$. Alors H est équicontinue.

Démonstration. Nous suivons la définition 9.391 de l'équicontinuité. Soient $a \in X$ et un voisinage V de 0 dans Y. Nous considérons $r > 0$ tel que $B(0,r) \subset V$, et nous posons $U = B(a,r)$.

Si $x \in U$ et $h \in H$, nous avons

$$\|h(x) - h(a)\| = \|h(x-a)\| = d(x,a) < r, \tag{9.496}$$

de telle sorte que $h(x) \in h(a) + B(0,r)$.

Donc H est équicontinue en a. Vu que a est arbitraire, H est équicontinue en tout point et donc équicontinue sur X. □

LEMooKEMRooYyqsBl

Lemme 9.393 ([306]).
Soit une famille de fonctions $f_i : X \to E$ indexée par un ensemble I où X est un espace topologique et E un espace métrique. Cette famille est équicontinue[183] en $x \in X$ si et seulement si pour tout $\epsilon > 0$, il existe un voisinage U de x tel que

$$\|f_i(x) - f_i(y)\| < \epsilon \tag{9.497}$$

pour tout $x \in U$ et $i \in I$.

Démonstration. En deux parties.

(1) $\Rightarrow$ Nous supposons que $\{f_i\}_{i\in I}$ est équicontinue en $a \in X$. Soit $\epsilon > 0$. La partie $B(0,\epsilon)$ est un voisinage de 0 dans E. Donc, par définition de l'équicontinuité, il existe un voisinage U de a dans X tel que $f_i(U) \subset f_i(a) + B(0,\epsilon)$ pour tout $i \in I$. C'est-à-dire que pour tout $x \in U$ nous avons

$$f_i(x) \in f_i(a) + B(0,\epsilon), \tag{9.498}$$

ce qui est équivalent à dire que $\|f_i(x) - f_i(a)\| < \epsilon$.

(2) $\Leftarrow$ Soit un voisinage V de 0 dans E. Nous considérons $\epsilon > 0$ tel que $B(0,\epsilon) \subset V$. Il existe un voisinage U de a tel que $\|f_i(a) - f_i(x)\| < \epsilon$ pour tout $x \in U$. Cela signifie que $f_i(x) \in f_i(a) + B(0,\epsilon)$, et à fortiori que $f_i(x) \in f_i(a) + V$.

□

[183] Définition 9.391.

La proposition suivante permet de montrer que certaines fonctions définies par une limite sont continues. Ce sera par exemple le cas de la fonction puissance, proposition 14.446.

PROPooICNNooAMjcut

Proposition 9.394 ([1, 306]).
Soit une suite équicontinue (f_i) de fonctions qui converge simplement vers f, alors f est continue.

Démonstration. Soit une suite équicontinue $f_i\colon X \to E$ convergeant simplement vers f. Soit $a \in X$. Nous prouvons que f est continue en a. Pour cela nous considérons $\epsilon > 0$ et, conformément à l'hypothèse équicontinuité un voisinage V de a tel que $|f_i(a) - f_i(x)| < \epsilon$ pour tout $x \in V$.

Nous avons la majoration

$$|f(x) - f(a)| \leqslant |f(x) - f_i(x)| + |f_i(x) - f_i(a)| + |f_i(a) - f(a)|. \tag{9.499a}$$

Plusieurs majorations.

- Vu que $f_i \to f$, il existe N_1 tel que $|f(x) - f_i(x)| < \epsilon$ pour tout $i > N_1$.
- De plus, par définition de V, nous avons aussi $|f_i(x) - f_i(a)| \leqslant \epsilon$.
- Vu que $f_i \to f$, il existe N_2 tel que $|f_i(a) - f(a)| < \epsilon$ pour tout $i > N_2$.

Donc en prenant $x \in V$ et $i > \max\{N_1, N_2\}$ nous avons

$$|f(x) - f(a)| \leqslant 3\epsilon. \tag{9.500}$$

□

9.17.7 Continuité uniforme

DEFooYIPXooQTscbG

Définition 9.395 ([307]).
*Soient deux espaces métriques (E, d) et (E', d'). Une application $f\colon E \to E'$ est **uniformément continue** si pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que $d(x, y) \leqslant \delta$ implique $d'\big(f(x), f(y)\big) \leqslant \epsilon$.*

Dans l'uniforme continuité, le α qui fait fonctionner ϵ doit le faire fonctionner pour tous les $x, y \in E$. C'est la différence avec la continuité simple dans laquelle nous pouvons choisir, pour un même ϵ, un δ différent en chaque point.

Nous parlons plus d'uniforme continuité dans la section 14.7.

9.18 Partie maigre et nulle part dense

Une des caractérisations 9.436 des espaces de Baire parle de parties maigres.

DEFooTYNBooIaQINO

Définition 9.396 (nulle part dense[308]).
Soit un espace topologique X et une partie $A \subset X$. Les propriétés suivantes sont équivalentes :

ITEMooFFSAooUdcUuV
(1) $\mathrm{Int}(\bar{A}) = \varnothing$

ITEMooYKDEooYwNblV
(2) Tout ouvert de X inclus dans $\bar{A}$ est vide.

ITEMooOYOCooLkyrFx
(3) A n'est dense dans aucun ouvert non vide de X.

ITEMooGYICooSAelba
(4) Pour tout ouvert non vide U de X, il existe un ouvert V non vide tel que $V \subset U$ et $V \cap A = \varnothing$.

*Une telle partie est **nulle part dense**.*

DEFooYKHUooPGZvLz

Définition 9.397 ([309]).
Soient un espace topologique X et une partie A de X. Les propriétés suivantes sont équivalentes :

(1) A est une réunion dénombrable de fermés d'intérieur vide.

(2) A est réunion dénombrable de parties nulle part denses[184]

*Une telle partie est dite **maigre**.*

ThoQGalIO

Théorème 9.398 (Baire[310]).
Une réunion dénombrable d'ensembles nulle part denses est d'intérieur vide.

[184] Définition 9.396.

Démonstration. Soient $a \in S$ et $\epsilon > 0$. Nous allons trouver un élément dans $B(a,\epsilon)$ qui n'est pas dans S. Nous commençons par choisir $x_1 \in B(a,\epsilon)$ et $r_1 < \frac{\epsilon}{2}$ tel que

$$B(x_1, r_1) \cap A_1 = \varnothing. \tag{9.501}$$

Ensuite nous choisissons $x_2 \in B(x_1, r_1)$ et $r_2 < \epsilon/4$ tel que $B(x_2, r_2) \subset B(x_1, r_1)$ et $B(x_2, r_2) \cap A_2 = \varnothing$. Notons que $B(x_2, r_2) \cap A_1 = \varnothing$ aussi, par construction.

Par récurrence nous construisons une suite d'éléments x_n et de rayons $r_n < \epsilon/2^n$ tels que

(1) $B(x_n, r_n) \cap A_j = \varnothing$ pour tout $j \leqslant n$,

(2) $\overline{B(x_n, r_n)} \subset B(x_{n-1}, r_{n-1})$.

Cette suite étant de Cauchy (parce que contenue dans des intervalles emboîtés de rayon décroissant vers zéro), elle converge[185] donc vers un point qui en particulier appartient à $B(a,\epsilon)$. Mais la limite n'est dans aucun des A_n et donc pas dans S. □

9.19 Seminormes

Les principaux espaces topologiques construit avec des seminormes seront les espaces de fonctions de la définition 32.14. Nous verrons également la topologie $*$-faible sur $\mathscr{D}'(\Omega)$ en la définition 32.30.

9.19.1 Seminorme

DefPNXlwmi

Définition 9.399.
*Si E est un espace vectoriel sur le corps $\mathbb{K}$ ($\mathbb{R}$ ou $\mathbb{C}$), une **seminorme** sur E est une application $p\colon E \to \mathbb{R}$ telle que*

ItemSHnimhDii

(1) $p(\lambda x) = |\lambda| p(x)$

ItemSHnimhDiii

(2) $p(x+y) \leqslant p(x) + p(y)$

pour tout $x, y \in E$ et pour tout $\lambda \in \mathbb{K}$.

Remarque 9.400.
Deux remarques.

(1) La seule différence avec une norme est qu'une seminorme peut s'annuler en des éléments non-nuls de l'espace.

(2) Une seminorme prend ses valeurs dans $\mathbb{R}$. En particulier pour que p soit une seminorme, il faut que $p(x) < \infty$ pour tout x.

LEMooHTOAooGmRGZL

Lemme 9.401 ([311, 285])**.**
Soit une seminorme[186] p. Nous avons

ITEMooFRCRooZBWTxH

(1) $p(0) = 0$,

ITEMooHVWHooAVZsTf

(2) $|p(x) - p(y)| \leqslant p(x-y)$.

ITEMooXCHBooDoBvpL

(3) $p(x) \geqslant 0$ *pour tout* $x \in X$.

ITEMooQIGMooVNDakF

(4) $\ker(p)$ *est un sous-espace vectoriel.*

Démonstration. En plusieurs parties.

(1) **Pour (1)** Pour la première affirmation, il suffit de poser $\lambda = 0$ dans l'inégalité de définition $p(\lambda x) = |\lambda| p(x)$.

(2) **Pour (2)** Nous avons d'une part $p(x+h) \leqslant p(x) + p(h)$ et d'autre part $p(x) \leqslant p(x+h) + p(-h) = p(x+h) + p(h)$. En isolant $p(x+h) - p(x)$ dans chacune ce des deux inégalités,

$$-p(h) \leqslant p(x+h) - p(x) \leqslant p(h) \tag{9.502}$$

ou encore

$$|p(x+h) - p(x)| \leqslant p(h) \tag{9.503}$$

qui donne le résultat demandé en posant $h = y - x$.

[185] Par la proposition 4.22
[186] Définition 9.399.

(3) **Pour (3)** Soit $x \in X$. Nous appliquons le point (2) avec $y = 0$, en nous souvenant que $p(0) = 0$: $|p(x) - p(0)| \leqslant p(x - 0)$, c'est-à-dire $0 \leqslant |p(x)| \leqslant p(x)$.

(4) **Pour (4)** Soient $x, y \in \ker(p)$ ainsi que $\alpha, \beta \in \mathbb{K}$. En utilisant les points précédents,

$$0 \leqslant p(\alpha x + \beta y) \leqslant |\alpha| p(x) + |\beta| p(y) = 0. \tag{9.504}$$

Vu que les inégalités commencent par 0 et finissent par zéro, ce sont toutes les égalités, et en particulier $p(\alpha x + \beta y) = 0$.

□

DEFooNFOAooRAUuOk

Définition 9.402 ([312]).
*Soit un espace vectoriel complexe X. Une application $f : X \to \mathbb{C}$ est **dominée** par la seminorme p si pour tout x dans X nous avons $|f(x)| \leqslant p(x)$.*

*Si M est un sous-espace vectoriel de X, nous disons qu'une application $f : M \to \mathbb{R}$ est **dominée par le dessus** par la seminorme p si $f(m) \leqslant p(m)$ pour tout $m \in M$.*

LEMooKTSKooIteFGq

Lemme 9.403 ([312]).
Une application linéaire est dominée par une seminorme si et seulement si sa partie réelle est dominée par le dessus[187].

Démonstration. Soit une application linéaire $f : X \to \mathbb{C}$. Nous la décomposons en parties réelles et imaginaires par

$$f(x) = u(x) + iv(x) \tag{9.505}$$

où u et v sont des applications à valeurs réelles.

(1) $\Rightarrow$ Nous supposons que $|f(x)| \leqslant p(x)$ pour tout $x \in X$. Nous avons les majorations

$$u(x) \leqslant |u(x)| \leqslant |f(x)| \leqslant p(x). \tag{9.506}$$

(2) $\Leftarrow$ Nous supposons que $u(x) \leqslant p(x)$, et nous devons prouver que $|f(x)| \leqslant p(x)$. Nous notons $z = f(x)$. Si $z = 0$ nous avons évidemment $|z| \leqslant p(x)$. Nous supposons que $z \neq 0$. Nous avons[188]

$$f(\frac{|z|}{z}x) = \frac{|z|}{z} f(x) = |z|. \tag{9.507}$$

En particulier $f(\frac{|z|}{z}x)$ est réel et est donc donné par u :

$$f(\frac{|z|}{z}x) = u(\frac{|z|}{z}x). \tag{9.508}$$

Nous avons alors le calcul

$$r = f(\frac{|z|}{z}x) = u(\frac{|z|}{z}x) \leqslant p(\frac{|z|}{z}x) = \big|\frac{|z|}{z}\big| p(x) = p(x). \tag{9.509}$$

□

9.19.2 Fonctionnelle de Minkowski

DEFooJQXHooGDaJtW

Définition 9.404 ([285]).
Soient un espace vectoriel X et une seminorme p sur X. Nous posons

$$\mathring{U}_p = \{x \in X \text{ tel que } p(x) < 1\} \tag{9.510a}$$
$$U_p = \{x \in X \text{ tel que } p(x) \leqslant 1\}. \tag{9.510b}$$

Notez qu'il n'y a aucune raison particulière de croie que U_p serait la fermeture de $\mathring{U}_p$ parce que pour l'instant nous n'avons aucune topologie sur X.

[187] Définition 9.402.
[188] Notez que si on écrit z en coordonnées polaires $z = re^{i\theta}$, le nombre $z/|z|$ est $e^{i\theta}$. Passez par les polaires pour simplifier les notations si cela vous chante, mais remarquez que le théorème 20.67 n'arrive que dans longtemps.

DEFooYQYBooRkAfjG

Définition 9.405 (Fonctionnelle de Minkowski[285]).
*Soient un espace vectoriel X ainsi qu'une partie $A \subset X$. La **fonctionnelle de Minkowski** de A est l'application*

$$\begin{aligned} p_A\colon X &\to \mathbb{R} \\ x &\mapsto \inf\{\lambda > 0 \text{ tel que } x \in \lambda A\}. \end{aligned} \tag{9.511}$$

Nous posons aussi $p_A(x) = \infty$ si l'ensemble est vide.

LEMooEIWEooPgoskd

Lemme 9.406 ([285]).
Soient un espace vectoriel X sur le corps $\mathbb{K}$ ($\mathbb{R}$ ou $\mathbb{C}$) ainsi qu'une partie $A \subset X$ qui est non vide, absorbante[189] *et absolument convexe*[190]. *Alors*

(1) La fonctionnelle de Minkowski p_A est une seminorme.

(2) Nous avons[191]

$$\mathring{U}_{p_A} \subset A \subset U_{p_A}. \tag{9.512}$$

*Note : le lemme 9.407 donnera la même inclusion en mieux parce qu'il n'y aura pas besoin de l'*absolue *convexité.*

Démonstration. En plusieurs parties.

C'est une seminorme.

(1) $p_A(x) < \infty$ **pour tout** x Nous avons supposé que A est absorbant. Soit $x \in X$. Il existe $\rho > 0$ tel que $\lambda x \in A$ pour tout $|\lambda| < \rho$. En particulier $\rho x \in A$, et donc $x \in \frac{1}{\rho}A$. L'ensemble $\{\lambda > 0 \text{ tel que } x \in \lambda A\}$ est donc non vide parce qu'il contient $1/\rho$. Nous en déduisons que $p_A(x) \leqslant 1/\rho < \infty$.

(2) $p_A(0) = 0$ Le lemme 9.262 nous dit que $0 \in A$, de telle sorte que $0 \in \lambda A$ pour tout $\lambda > 0$. Donc

$$p_A(0) = \inf\{\lambda > 0 \text{ tel que } 0 \in \lambda A\} = 0. \tag{9.513}$$

(3) **Condition pour** $\xi x \in \lambda A$ SPITEMooGDGDooMBDsPB Soit $x \in X$. Nous prouvons que $\xi x \in \lambda A$ si et seulement si $x \in \frac{\lambda}{|\xi|}A$. En utilisant le lemme 9.264, nous avons

$$\lambda A = \frac{\lambda}{|\xi|}|\xi|A = \frac{\lambda}{|\xi|}\xi A. \tag{9.514}$$

Donc $\xi x \in \lambda A$ si et seulement si $\xi x \in \frac{\lambda}{|\xi|}\xi A$ si et seulement si $x \in \frac{\lambda}{|\xi|}A$.

(4) $p_A(\xi x) = |\xi| p_A(x)$ Soient $x \in X$ et $\xi \in \mathbb{K}$ avec $\xi \neq 0$. Nous avons

$$\begin{aligned} p_A(\xi x) &= \inf\{\lambda > 0 \text{ tel que } \xi x \in \lambda A\} && && (9.515a)\\ &= \inf\{\lambda > 0 \text{ tel que } x \in \frac{\lambda}{|\xi|}A\} && \text{par (3)} && (9.515b)\\ &= \inf\{|\xi|\frac{\lambda}{|\xi|} > 0 \text{ tel que } x\frac{\lambda}{|x|}A\} && && (9.515c)\\ &= |\xi| \inf\{\frac{\lambda}{|\xi|} > 0 \text{ tel que } x \in \frac{\lambda}{|\xi|}A\} && && (9.515d)\\ &= |\xi| \inf\{\mu > 0 \text{ tel que } x \in \mu A\} && \text{cf. justif.} && (9.515e)\\ &= |\xi| p_A(x). && && (9.515f) \end{aligned}$$

SUBEQooIHJHooWLXBtA

Pour (9.515e). Si λ prend toutes les valeurs strictement positives, alors $\lambda/|\xi|$ aussi.

(5) $p_A(x+y) \leqslant p_A(x) + p_A(y)$ Soit $\epsilon > 0$. Nous notons $S_A(x) = \{\lambda > 0 \text{ tel que } x \in \lambda A\}$.
Vu que $p_A(x)$ et $p_A(y)$ sont définis comme des infimums, il existe $\lambda, \mu > 0$ tels que

$$\lambda \leqslant p_A(x) + \epsilon \tag{9.516a}$$
$$\mu \leqslant p_A(y) + \epsilon \tag{9.516b}$$

[189] Définition 9.260.
[190] Définition 9.261.
[191] Avec les notations de 9.404.

avec $x \in \lambda A$ et $y \in \mu A$.

Vu que A est convexe, et vu que

$$\frac{\lambda}{\lambda+\mu} + \frac{\mu}{\lambda+\mu} = 1, \tag{9.517}$$

pour tout $z, z' \in A$ nous avons

$$\frac{\lambda}{\lambda+\mu} z + \frac{\mu}{\lambda+\mu} z' \in A, \tag{9.518}$$

ou encore : $\lambda z + \mu z' \in (\lambda+\mu)A$. En particulier pour z et z' choisis tels que $\lambda z = x$ et $\mu z' = y$ nous avons $x + y \in (\lambda+\mu)A$. Nous avons alors

$$p_A(x+y) = \inf\{\delta > 0 \text{ tel que } x+y \in \delta A\} \leqslant \lambda + \mu \leqslant p_A(x) + p_A(y) + 2\epsilon. \tag{9.519}$$

Étant donné que ϵ est arbitraire, nous avons prouvé que $p_A(x+y) \leqslant p_A(x) + p_A(y)$.

(6) p_A **est une seminorme** Nous avons prouvé toutes les conditions de la définition 9.399.

$$\text{\_\_\_\_\_} \mathring{U}_{p_A} \subset A \subset U_{p_A} \text{\_\_\_\_\_}$$

(1) **Première inclusion** Soit $x \in \mathring{U}_{p_A}$, c'est-à-dire $p_A(x) < 1$, ou encore

$$\inf\{\lambda > 0 \text{ tel que } x \in \lambda A\} < 1. \tag{9.520}$$

Donc il existe $\lambda \in [0,1[$ tel que $x \in \lambda A$. Vu que A est équilibré (ça fait partie d'être absolument convexe) et que $\lambda < 1$, nous avons $\lambda A \subset A$. Bref,

$$x \in \lambda A \subset A. \tag{9.521}$$

Cela prouver que $x \in A$.

(2) **Seconde inclusion** Soit $x \in A$. Nous avons $1 \in \{\lambda > 0 \text{ tel que } x \in \lambda A\}$, et donc

$$p_A(x) = \inf\{\lambda > 0 \text{ tel que } x \in \lambda A\} \leqslant 1, \tag{9.522}$$

ce qui signifie que $x \in U_{p_A}$.

□

LEMooFUXVooJumScW

Lemme 9.407 ([313]).
Soit un espace vectoriel topologique X ainsi qu'une partie convexe et absorbante A. Alors

$$\{x \in X \text{ tel que } p_A(x) < 1\} \subset A \subset \{x \in X \text{ tel que } p_A(x) \leqslant 1\}. \tag{9.523}$$

Démonstration. Nous prouvons les deux inclusions séparément.

(1) **Première inclusion** Soit $x \in X$ vérifiant $p_A(x) < 1$. Nous avons

$$\inf\{\lambda > 0 \text{ tel que } x \in \lambda A\} < 1. \tag{9.524}$$

Soit $\lambda \in]0,1[$ tel que $x \in \lambda A$. En particulier $x/\lambda \in A$. Étant donné que A est convexe et que $0 \in A$ (toute partie absorbante contient 0), le segment joignant 0 à x/λ est contenu dans A. En particulier, nous avons

$$x = \lambda \left(\frac{1}{\lambda} x \right) + (1-\lambda)0 \in A \tag{9.525}$$

(2) **Seconde inclusion** Soit $x \in A$. Nous avons évidemment

$$1 \in \{\lambda > 0 \text{ tel que } x \in \lambda A\}. \tag{9.526}$$

Donc $p_A(x) = \inf\{\lambda > 0 \text{ tel que } x \in \lambda A\} \leqslant 1$.

□

LEMooFWCIooVwGutp

Lemme 9.408 ([285]).
Soit une seminorme q sur l'espace vectoriel X. Alors

(1) $\mathring{U}_q$ est absorbant.

(2) $\mathring{U}_q$ *est absolument convexe.*

(3) $q = p_{\mathring{U}_q}$.

Démonstration. En plusieurs points.

(1) $\mathring{U}_q$ **est absorbant** Soit $x \in X$. Nous devons montrer l'existence de $\rho_x > 0$ tel que pour tout $|\lambda| < \rho_x$, nous ayons $\lambda x \in \mathring{U}_q$.
Si $q(x) = 0$, alors $q(\lambda x) = |\lambda| q(x) = 0 < 1$ et donc n'importe quel $\rho_x > 0$ fait l'affaire.
Si $q(x) > 0$, alors il suffit de prendre $\rho_x \in]0, 1/q(x)[$. En effet si $|\lambda| < \rho_x$, nous avons

$$q(\lambda x) = |\lambda| q(x) \leqslant \frac{1}{q(x)} q(x) = 1, \tag{9.527}$$

et donc $\lambda x \in \mathring{U}_q$.

(2) $\mathring{U}_q$ **est équilibré** Soient $|\alpha| \leqslant 1$, et $x \in \mathring{U}_q$. Nous avons

$$q(\alpha x) = |\alpha| q(x) \leqslant q(x) < 1. \tag{9.528}$$

Donc $\alpha x \in \mathring{U}_q$.

(3) $\mathring{U}_q$ **est convexe** Soient $x, y \in \mathring{U}_q$ ainsi que $t \in [0, 1]$. Nous avons

$$\begin{aligned} q\big(tx + (1-t)y\big) &\leqslant q(tx) + q\big((1-t)y\big) && \text{(9.529a)}\\ &= |t| q(x) + |1-t| q(y) && \text{(9.529b)}\\ &\leqslant |t| + |1-t| && \text{(9.529c)}\\ &= t + (1-t) && \text{(9.529d)}\\ &= 1. && \text{(9.529e)} \end{aligned}$$

Donc $tx + (1-t)y \in \mathring{U}_q$.

(4) $q = p_{\mathring{U}_q}$ Soit $x \in X$. Nous avons

$$p_{\mathring{U}_q}(x) = \inf\{\lambda > 0 \text{ tel que } x \in \lambda \mathring{U}_q\} = \inf\{\lambda > 0 \text{ tel que } q(x) < \lambda\} = q(x). \tag{9.530}$$

□

LEMooQSAJooCgPNnD

Lemme 9.409 ([314])**.**
Soit un espace vectoriel X, ainsi qu'une seminorme p sur X. Nous posons[192]

$$\begin{aligned} B_p(0,1) &= \{x \in X \text{ tel que } p(x) < 1\}\\ \bar{B}_p(0,1) &= \{x \in X \text{ tel que } p(x) \leqslant 1\}. \end{aligned} \tag{9.531}$$

Alors pour tout $\epsilon > 0$ nous avons

$$\begin{aligned} \epsilon B_p(0,1) &= \{x \in X \text{ tel que } p(x) < \epsilon\}\\ \epsilon \bar{B}_p(0,1) &= \{x \in X \text{ tel que } p(x) \leqslant \epsilon\}. \end{aligned} \tag{9.532}$$

PROPooDDURooJHfHLw

Proposition 9.410 ([314, 315])**.**
Soit un espace vectoriel topologique X, ainsi qu'une seminorme p. Les faits suivants sont équivalents.

ITEMooCAOXooGNBeSB

(1) *p est continue.*

ITEMooWWUSooEPkoWU

(2) *p est continue en 0.*

ITEMooPKFLooTRlKwo

(3) *$B_p(0,1)$ est un voisinage de 0.*

ITEMooRTFZooUXUVnA

(4) *$\bar{B}_p(0,1)$ est un voisinage de 0.*

[192] Nous ne supposons pas de compatibilité particulière entre la topologie de X et p. Donc à priori $\bar{B}_p(0,1)$ n'est pas la fermeture de $B_p(0,1)$. Si ça avait été le cas, nous aurions écrit $\overline{B_p(0,1)}$.

Démonstration. Nous prouvons les implications dans l'ordre cyclique (1) ⇒ (3) ⇒ (4) ⇒ (2) ⇒ (1). Courage, c'est parti.

(1) **(1) ⇒ (3)** Nous avons

$$B_p(0,1) = \{x \in X \text{ tel que } p(x) < 1\} = p^{-1}\big(]-\infty,1[\big). \tag{9.533}$$

Vu que p est continue et que $]-\infty,1[$ est ouvert, la partie $B_p(0,1)$ est un ouvert contenant 0.

(2) **(3) ⇒ (4)** La partie $\bar{B}_p(0,1)$ contient $B_p(0,1)$ qui est un ouvert contenant 0.

(3) **(4) ⇒ (2)** Nous vérifions la condition de la définition 9.48(1). D'abord $p(0) = 0$. Nous considérons donc un ouvert W de $\mathbb{R}$ contenant 0, et nous allons chercher un voisinage V de 0 dans X tel que $p(V) \subset W$.

Soit $r > 0$ tel que $B(0,r) \subset W$. Par hypothèse $\bar{B}_p(0,1)$ est un voisinage de 0. Comme la topologie de X est vectorielle, la partie $\epsilon\bar{B}_p(0,1)$ est également un voisinage de 0 pour tout $\epsilon > 0$. Montrons que

$$p\Big(\frac{r}{2}\bar{B}_p(0,1)\Big) \subset B(0,r) \subset W. \tag{9.534}$$

Soit $x \in \frac{r}{2}\bar{B}_p(0,1)$. Nous avons $p(x) \leqslant r/2$ par le lemme 9.409, et donc $p(x) \in B(0,r) \subset W$.

Bref, en posant $V = \frac{r}{2}\bar{B}_p(0,1)$, nous avons bien $p(V) \subset W$.

(4) **(2) ⇒ (1)** Nous supposons que p est continue en $0 \in X$ et nous devons prouver qu'elle est continue en $a \in X$. Soient $x \in X$, et $r > 0$. Pour prouver la continuité de p en x (définition 9.48(1)), nous devons prouver l'existence d'un voisinage V de x tel que $f(V) \subset B\big(p(x),r\big)$.

Pour $\epsilon > 0$ nous posons

$$U_\epsilon = p^{-1}\big(B(0,\epsilon)\big). \tag{9.535}$$

Cette partie est ouverte parce que p est continue en 0 et que $p(0) = 0$. Nous allons prouver que si ϵ est assez petit, alors $p(x + E_\epsilon) \subset B\big(p(x),r\big)$.

Soit $z \in U_\epsilon$. Nous avons

$$\begin{aligned}
|p(x) - p(x+z)| &\leqslant p\big(x-(x+y)\big) && \text{lem.9.401} && (9.536a)\\
&= p(-z) && && (9.536b)\\
&= p(z) && && (9.536c)\\
&\subset B(0,\epsilon). && && (9.536d)
\end{aligned}$$

Donc $p(x+z) \in B\big(p(x),\epsilon\big)$ et nous avons montré que $p(x+U_\epsilon) \subset B\big(p(x),\epsilon\big)$. Donc en prenant $\epsilon \leqslant r$, c'est bon.

□

9.20 Topologie des seminormes

Soit $(p_i)_{i\in I}$ une famille de seminormes sur E. Il existe plusieurs façons de construire une topologie sur E à partir des seminormes.

9.20.1 Topologie initiale des seminormes

La première topologie qui nous tombe sous la main est celle de la topologie initiale[193] des p_i.

PROPooVUYTooJXkRYW

Proposition 9.411 ([1, 316])**.**
Soient un espace vectoriel X et une seminorme $p\colon X \to \mathbb{R}$. Soit $x_0 \in X$. En posant

$$B_\epsilon = \{x \in X \text{ tel que } |p(x) - p(x_0)| < \epsilon\}, \tag{9.537}$$

l'ensemble $\mathcal{B} = \{B_\epsilon\}_{\epsilon>0}$ est une base de voisinages de x_0 pour la topologie initiale de p.

[193] La topologie minimale rendant les p_i continue, définition 9.58.

Démonstration. Nous nommons τ la topologie initiale de p sur X. Posons $y_0 = p(x_0)$. Une base de voisinages de y_0 (dans $\mathbb{R}$) est $\{B(y_0, \epsilon)\}_{\epsilon>0}$. Donc la proposition 9.60 dit qu'une base de voisinages de x_0 dans X est donnée par

$$\{p^{-1}\Big(B\big(p(x_0), \epsilon\big)\Big)\}_{\epsilon>0}. \tag{9.538}$$

Or nous avons

$$p^{-1}\Big(B\big(p(x_0), \epsilon\big)\Big) = \{x \in X \text{ tel que } p(x) \in B\big(p(x_0), \epsilon\big)\} \tag{9.539a}$$

$$= \{x \in X \text{ tel que } |p(x) - p(x_0)| < \epsilon\}. \tag{9.539b}$$

□

La topologie initiale des seminormes n'est pas une bonne idée, parce qu'elle ne donne en général pas lieu à une structure d'espace vectoriel topologique[194].

Exemple 9.412 ([316]).
Nous considérons $\mathbb{R}$ avec la seminorme

$$\begin{aligned} p\colon \mathbb{R} &\to \mathbb{R} \\ x &\mapsto |x|. \end{aligned} \tag{9.540}$$

Nous considérons sur $\mathbb{R}$ la topologie initiale de cette seminorme. En vertu de la proposition 9.411, une base de topologie en $x_0 \in \mathbb{R}$ est donnée par les parties

$$B_\epsilon(x_0) = \{x \in \mathbb{R} \text{ tel que } \big||x| - |x_0|\big| < \epsilon\}. \tag{9.541}$$

Considérons la suite constante $x_k = 1$. Le nombre 1 est évidemment une limite de (x_k). Mais en y regardant bien, le nombre -1 est également une limite. En effet une base de voisinages autour de -1 est donnée par

$$B_\epsilon(-1) = \{x \in \mathbb{R} \text{ tel que } \big||x| - 1\big| < \epsilon\}. \tag{9.542}$$

Et donc $1 \in B_\epsilon(-1)$ pour tout ϵ.

Si $\mathbb{R}$ muni de cette topologie était un espace vectoriel topologique, la proposition 9.241 dirait que $-1+1 = 0$ serait une limite de $(x_k + x_k)$. La suite $(x_k + x_k)$ est la suite constante égale à 2. Or un voisinage typique autour de 0 est

$$B_\epsilon(0) = \{x \in \mathbb{R}' |x| < \epsilon\}. \tag{9.543}$$

Autant dire que la suite $(x_k + x_k) = 2$ n'y rentre pas souvent. △

9.20.2 Topologie avec des boules

DEFooROXMooCpmTwa

Définition 9.413.
Soit un espace vectoriel E sur lequel nous avons des seminormes $\{p_i\}_{i\in I}$. Pour chaque $i \in I$ nous posons

$$B_i(x, r) = \{y \in E \text{ tel que } p_i(y - x) < r\}. \tag{9.544}$$

Si J est une partie finie de I, nous considérons les parties

$$B_J(x, r) = \{y \in E \text{ tel que } p_j(y - x) < r \, \forall j \in J\}. \tag{9.545}$$

LEMooCNRNooWCejjZ

Lemme 9.414.
Soit un espace vectoriel E sur lequel nous avons des seminormes $\{p_i\}_{i\in I}$. Pour chaque $a \in E$, nous considérons la translation

$$\begin{aligned} t_a\colon E &\to E \\ x &\mapsto x + a. \end{aligned} \tag{9.546}$$

Pour toute partie finie $J \subset I$ nous avons

$$t_a\big(B_J(x, r)\big) = B_J(x + a, r) \tag{9.547}$$

Démonstration. D'une part si $y \in B_J(x + a, r)$, nous avons $p_j(y - x - a) < r$ pour tout $j \in J$. Dans ce cas, $y - a \in B_j(x, r)$, et nous avons donc bien $y = t_a(y - a) \in t_a\big(B_J(x, r)\big)$.

Pour l'inclusion dans l'autre sens, c'est le même raisonnement. □

[194] Espace vectoriel topologique, définition 9.239.

DEFooZTKAooWYUyDa

Proposition-Définition 9.415 (Topologie et seminormes[317, 318, 285]).
Soient des seminormes $\{p_i\}_{i\in I}$ sur l'espace vectoriel E. Nous posons[195]

EQooNHMNooGJSeQr

$$\tau_B = \{\mathcal{O} \subset E \text{ tel que } \forall x \in \mathcal{O}, \exists J, r \text{ tel que } B_J(x,r) \subset \mathcal{O}\} \cup \{\varnothing\}. \tag{9.548}$$

Dans cette formule, les J sont des parties finies de I.

Pour chaque $i \in I$ et $x \in E$ nous posons

$$\begin{aligned} p_{i,x} \colon E &\to \mathbb{R} \\ y &\mapsto p_i(y-x). \end{aligned} \tag{9.549}$$

Alors

ITEMooQPVRooKyOBPi
(1) *Les parties τ_B forment une topologie sur E.*

ITEMooQIYWooAmPCdI
(2) *Les applications $p_i \colon E \to \mathbb{R}$ sont continues pour (E, τ_B).*

ITEMooYGNWooYhBzSa
(3) *Les applications $p_{i,x} \colon E \to \mathbb{R}$ sont continues pour τ_B.*

ITEMooMUUZooBKBhsH
(4) *Si τ est une topologie sur E dans laquelle tous les $p_{i,x}$ sont continus, alors $\tau_B \subset \tau$.*

ITEMooEGVFooNqDkdN
(5) *L'espace topologique (E, τ_B) est un espace vectoriel topologique localement convexe*[196].

*Cette topologie est la **topologie des seminormes** sur E.*

Démonstration. En plusieurs parties.

(1) **Pour (1)** Vérifier les trois conditions de la définition 9.1. D'abord E et $\varnothing$ sont dans τ_B. Ensuite si $\{\mathcal{O}_s\}_{s\in T}$ sont des éléments de τ_B, nous considérons $x \in \bigcup_{s\in T} \mathcal{O}_s$, et nous montrons que x est contenu dans une boule contenue dans $\bigcup_{s\in T} \mathcal{O}_s$. Nous considérons $s \in T$ tel que $x \in \mathcal{O}_s$. Vu que $\mathcal{O}_s \in \tau_B$, il existe J, r tels que

$$x \in B_J(x,r) \subset \mathcal{O}_s \subset \bigcup_{s\in T} \mathcal{O}_s. \tag{9.550}$$

Enfin pour l'intersection finie, l'intersection $B_J(x,r) \cap B_{J'}(x,r')$ contient la boule $B_{J\cup J'}(x,\delta)$ avec $\delta = \min\{r, r'\}$.

(2) **Pour (2)** Pour montrer que p_i est continue, nous montrons que l'image inverse d'un ouvert est ouverte. Soit $a \in \mathbb{R}$ ainsi que $r > 0$. Nous considérons l'ouvert $B(a,r)$ et nous montrons que $p_i^{-1}\big(B(a,r)\big) \in \tau_B$. Soit $x \in p_i^{-1}\big(B(a,r)\big)$. Nous allons montrer que si δ est assez petit, alors $B_i(x,\delta) \subset p_i^{-1}\big(B(a,r)\big)$.

Soit $y \in B_i(x,\delta)$. Par définition nous avons $p_i(y-x) < \delta$, et par le lemme 9.401,

$$|p_i(y) - p_i(x)| \leqslant p_i(x-y) < \delta. \tag{9.551}$$

D'autre part, vu que $x \in p_i^{-1}\big(B(a,r)\big)$, nous avons $|p_i(x) - a| < r$. Nous considérons $s > 0$ tel que $|p_i(x) - a| < r - s$. Avec tout ça,

$$\begin{aligned} |p_i(y) - a| &\leqslant |p_i(y) - p_i(x)| + |p_i(x) - a| && \text{(9.552a)} \\ &< \delta + r - s && \text{(9.552b)} \\ &< r && \text{(9.552c)} \end{aligned}$$

dès que nous choisissons $\delta < s$.

Nous avons donc montré que $p_i(y) \in B(a,r)$, et donc que $p_i\big(x,\delta\big) \subset B(a,r)$. Donc p_i est continue.

(3) **Les translations sont continues** Nous considérons les translations $t_a \colon E \to E$ données par $t_a(x) = x + a$. Soit un ouvert $\mathcal{O}$ dans E. Nous prouvons que $t_a^{-1}(\mathcal{O}) = t_{-a}(\mathcal{O})$ est ouvert. Pour cela nous considérons un élément $x \in t_{-a}(\mathcal{O})$ et nous prouvons qu'il existe une boule autour de x contenue dans $t_{-a}(\mathcal{O})$. Soit $y \in \mathcal{O}$ tel que $x = y - a$; vu que $\mathcal{O}$ est ouvert, il existe r, J tels que $B_J(y,r) \subset \mathcal{O}$. Nous avons alors

$$t_{-a}\big(B_J(y,r)\big) \subset t_{-a}(\mathcal{O}), \tag{9.553}$$

et donc

$$B_J(y-a,r) = t_{-a}\big(B_J(y,r)\big) \subset t_{-a}(\mathcal{O}). \tag{9.554}$$

[195] Nous ajoutons explicitement l'ensemble vide parce que nous n'avons pas envie de vérifier des propriétés du genre $\forall x \in \varnothing$, blah blah…Mais bon. En principe c'est pas obligatoire parce que l'ensemble vide est obtenu avec $r = 0$.
[196] Définition 9.269.

(4) **Pour (3)** Nous avons $p_{i,x} = p_i \circ t_{-x}$. Nous avons déjà prouvé que p_i et t_{-x} sont continues.

(5) **Pour (4)** Soit une topologie τ telle que toutes les applications $p_{i,a}$ sont continues. Nous avons

$$B_i(a,r) = \{y \in E \text{ tel que } p_i(y-a) < r\} = \{y \in E \text{ tel que } p_{i,a}(y) < r\} = p_{i,a}^{-1}\big(B(0,r)\big). \tag{9.555}$$

Étant donné que $B(0,r)$ est ouverte et que $p_{i,a}$ est continue, la partie $p_{i,a}^{-1}\big(B(0,r)\big)$ est ouverte. Donc τ contient toutes les boules de la forme $B_i(a,r)$.

Vu que τ est une topologie, elle contient toutes les intersections finies d'ouvert. En particulier si J est une partie finie de I, τ doit contenir toutes les boules de la forme $B_J(a,r)$.

(6) **Pour (5)** Le point (5), ce sont les points suivants.

(7) **L'addition est continue** Nous prouvons que l'application

$$\begin{aligned} a\colon E \times E &\to E \\ (x,y) &\mapsto x+y \end{aligned} \tag{9.556}$$

est continue pour la topologie τ_B. Soit $\mathcal{O} \in \tau_B$; nous devons prouver que la partie

$$a^{-1}(\mathcal{O}) = \{(x,y) \in E \times E \text{ tel que } x+y \in \mathcal{O}\} \tag{9.557}$$

est ouvert dans $E \times E$ (topologie produit). Soit $(x_0,y_0) \in a^{-1}(\mathcal{O})$. Vu que $x_0+y_0 \in \mathcal{O}$, il existe un r et un $i \in I$ tels que $B_i(x_0+y_0,r) \subset \mathcal{O}$.

Nous prouvons que si ϵ est assez petit,

$$B_i(x_0,\epsilon) \times B_i(y_0,\epsilon) \subset a^{-1}\Big(B_i(x_0,y_0,r)\Big) \subset a^{-1}(\mathcal{O}). \tag{9.558}$$

Nous avons

$$\begin{aligned} p_i\big((x+y)-(x_0+y_0)\big) &= p_i\big((x-x_0)+(y-y_0)\big) && && \text{(9.559a)}\\ &\leqslant p_i(x-x_0)+p_i(y-y_0) && \text{def. 9.399(2)} && \text{(9.559b)}\\ &\leqslant 2\epsilon. && && \text{(9.559c)} \end{aligned}$$

En prenant $\epsilon < r/2$ nous avons donc $a(x,y) \in B_i\big(x_0+y_0,r\big) \subset \mathcal{O}$.

(8) **La multiplication est continue** Nous considérons la multiplication

$$\begin{aligned} m\colon \mathbb{K} \times E &\to E \\ (\lambda,x) &\mapsto \lambda x, \end{aligned} \tag{9.560}$$

et nous montrons que c'est une application continue. Soit un ouvert $\mathcal{O} \subset E$, nous considérons $(\lambda_0,x_0) \in m^{-1}(\mathcal{O})$, et nous allons prouver que $\mathbb{K} \times E$ contient un ouvert contenant (λ_0,x_0) et contenu dans $m^{-1}(\mathcal{O})$.

Il existe $r>0$ et $i \in I$ tels que $B_i(\lambda_0 x_0,r) \subset \mathcal{O}$. Nous allons trouver une valeur de $\epsilon > 0$ telle que l'ouvert $B(\lambda_0,\epsilon) \times B_i(x_0,\epsilon)$ vérifie

$$(\lambda_0,x_0) \in B(\lambda_0,\epsilon) \times B_i(x_0,\epsilon) \subset m^{-1}\big(B_i(\lambda_0 x_0,r)\big) \subset m^{-1}(\mathcal{O}). \tag{9.561}$$

Soit $(\lambda,x) \in B(\lambda_0,\epsilon) \times B_i(x_0,\epsilon)$. Nous avons $|\lambda| < |\lambda_0| + \epsilon$ et le calcul suivant :

$$\begin{aligned} p_i(\lambda x - \lambda_0 x_0) &= p_i(\lambda x - \lambda x_0 + \lambda x_0 - \lambda_0 x_0) && \text{(9.562a)}\\ &= p_i\big(\lambda(x-x_0)+(\lambda-\lambda_0)x_0\big) && \text{(9.562b)}\\ &\leqslant |\lambda| p_i(x-x_0) + |\lambda-\lambda_0| p_i(x_0) && \text{(9.562c)}\\ &\leqslant \big(|\lambda_0|+\epsilon\big) \underbrace{p_i(x-x_0)}_{<\epsilon} + \underbrace{|\lambda-\lambda_0|}_{<\epsilon} p_i(x_0) && \text{(9.562d)}\\ &< \epsilon\big(|\lambda_0|+\epsilon\big) + \epsilon p_i(x_0) && \text{(9.562e)}\\ &= \epsilon^2 + \epsilon\big(|\lambda_0| + p_i(x_0)\big). && \text{(9.562f)} \end{aligned}$$

Il n'y a pas de problèmes pour trouver un $\epsilon > 0$ pour que le tout soit plus petit que r.

(9) **Espace vectoriel topologique** Nous avons prouvé que (E, τ_B) était un espace vectoriel topologique.

(10) **Localement convexe en 0** Nous montrons que $B_i(0,r)$ est convexe. Soient $x, y \in B_i(0,r)$ ainsi que $t \in [0,1]$. Nous avons

$$\begin{aligned} p_i\big(tx + (1-t)y\big) &\leqslant |t|p_i(x) + |1-t|p_i(y) && (9.563a)\\ &\leqslant tr + (1-t)r && (9.563b)\\ &= r. && (9.563c)\end{aligned}$$

Donc $tx + (1-t)y \in B_i(0,r)$.

(11) **Localement convexe** Soit $a \in E$, et montrons que $B_i(a,r)$ est convexe. Si t_a est la translation de vecteur a, le lemme 9.414 donne $B_i(a,r) = t_a\big(B_i(0,r)\big)$. Soient $x, y \in B_i(a,r)$. Nous avons $x-a, y-a \in B_i(0,r)$, et vu que la boule $B_i(0,r)$ est convexe,

$$t(x-a) + (1-t)(y-a) \in B_i(0,r). \tag{9.564}$$

Un tout petit peu de calcul :

$$\begin{aligned} t(x-a) + (1-t)(y-a) &= tx + (1-t)y - ta - (1-t)a && (9.565a)\\ &= tx + (1-t)y - a. && (9.565b)\end{aligned}$$

Cela prouve que $tx + (1-t)y - a \in B_i(0,r)$, et donc que $tx + (1-t)y \in B_i(a,r)$, ce qu'il fallait.

□

PROPooNAFAooShzixo

Proposition 9.416 ([285, 1])**.**
Soit un espace vectoriel X ainsi qu'un ensemble de seminormes $\{p_i\}_{i\in I}$. Il existe une unique topologie τ sur X telle que

(1) (X,τ) est un espace vectoriel topologique localement convexe.

(2) Une base de topologie de τ en 0 est donnée par

$$\mathcal{B}_0 = \{B_J(0,\epsilon) \text{ tel que } J \text{ est fini dans } I, \epsilon > 0\}. \tag{9.566}$$

Cette topologie est la topologie τ_B donnée en (9.548).

Démonstration. En ce qui concerne l'existence, la topologie τ_B donnée dans la proposition 9.415 fait l'affaire. Nous démontrons l'unicité. Soit une topologie τ sur X vérifiant les conditions. Nous allons prouver que $\tau = \tau_B$.

En deux inclusions.

(1) $\tau_B \subset \tau$ La topologie τ_B a une base formée de parties de la forme $B_J(x,r)$. Nous montrons que ces parties sont dans τ. En utilisant le lemme 9.414 et la proposition 9.241, nous avons

$$B_J(x,r) = B_J(0,r) + x \subset \mathcal{B}_0 + x \subset \tau. \tag{9.567}$$

Vu que τ contient une base de la topologie τ_B, nous avons $\tau_B \subset \tau$.

(2) $\tau \subset \tau_B$ Les $B_J(0,r)$ qui forment une base de topologie de τ en 0 sont des éléments de τ_B. Les $B_J(x,r) = B_J(0,r) + x$ forment une base de topologie de τ en x, et font aussi partie de τ_B.

□

PropQPzGKVk

Proposition 9.417.
Soit un ensemble E muni de la topologie des seminormes $\{p_i\}_{i\in I}$. Une suite (x_n) dans E converge vers x si et seulement si pour tout $i \in I$,

$$p_i(x - x_n) \to 0. \tag{9.568}$$

Démonstration. Si la suite (x_n) converge[197] vers x, alors pour tout ouvert $\mathcal{O}$ autour de x, il existe un N tel que si $n \geqslant N$, alors $x_n \in \mathcal{O}$. En particulier pour tout j et pour tout $\epsilon > 0$, il doit exister un $n \geqslant N_j$ tel que $x_n \in B_j(x,\epsilon)$.

[197] Définition 9.14.

Voyons l'implication inverse. Soit $\epsilon > 0$. Pour tout $i \in I$, il existe un N_i tel que $n \geqslant N_i$ implique $p_i(x - x_n) \leqslant \epsilon$. Si $\mathcal{O}$ est un ouvert, il doit contenir une boule du type $B_J(x, r)$ pour un certain ensemble fini $J \subset I$.

En prenant $N = \max\{N_j \text{ tel que } j \in J\}$, nous avons $p_j(x - x_n) \leqslant \epsilon$ pour tout j et donc $x_n \in B_J(x, r)$. □

PROPooGXGQooLRTwvH

Proposition 9.418 ([319, 1])**.**
Un espace vectoriel muni de seminormes sur un corps valué est un espace vectoriel topologique[198].

Démonstration. Soit un espace vectoriel E muni des seminormes $\{p_i\}_{i\in I}$. Sa topologie est donnée par la définition 9.415. Sur le corps $\mathbb{K}$, nous avons la topologie métrique 9.255.

(1) **Somme**

Nous commençons par prouver que

$$\begin{aligned} f\colon E \times E &\to E \\ (x, y) &\mapsto x + y \end{aligned} \tag{9.569}$$

est continue. Soit un ouvert A de E ; nous allons prouver que $f^{-1}(A)$ est ouvert dans $E \times E$ en prouvant qu'il contient un ouvert autour de chacun de ses points (théorème 9.8).

Soit $(a, b) \in f^{-1}(A)$. Vu que A est ouvert dans $(E, \{p_i\}_{i\in I})$, par définition de la topologie, il existe $i \in I$ et $r > 0$ tels que $B_i\big(f(a, b), r\big) \subset A$. Il nous faut un ouvert $U \in \tau_E$ autour de a et un ouvert $V \in \tau_E$ autour de b tels que $f(U \times V) \subset A$. Posons $U = B_i(a, \epsilon)$ et $V = B_i(b, \epsilon)$, considérons $x \in U$, $y \in V$ et montrons que $f(x, y) \in B_i\big(f(a, b), r\big)$. Nous avons

$$\begin{aligned} p_i\big(f(x, y) - f(a, b)\big) &= p_i\big((x - a) + (y - b)\big) && && (9.570a)\\ &\leqslant p_i(x - a) + p_i(y - b) && \text{def. 9.399(2)} && (9.570b)\\ &< 2\epsilon. && && (9.570c) \end{aligned}$$

En choisissant $\epsilon < r/2$ c'est bon.

(2) **Produit** Nous nommons $\mathbb{K}$ le corps de l'espace vectoriel E. Nous devons voir que l'application

$$\begin{aligned} f\colon \mathbb{K} \times E &\to E \\ (\lambda, x) &\mapsto \lambda x \end{aligned} \tag{9.571}$$

est continue.

La topologie sur $\mathbb{K}$ est sa topologie métrique, c'est-à-dire la topologie de son unique seminorme $\lambda \mapsto |\lambda|$. La topologie sur $\mathbb{K} \times E$ est donc celle des seminormes

$$\begin{aligned} q_i\colon \mathbb{K} \times E &\to \mathbb{R} \\ (\lambda, x) &\mapsto \max\{|\lambda|, p_i(x)\}. \end{aligned} \tag{9.572}$$

EQooFSBEooWDsHot

Nous pouvons donc reprendre le même cheminement que celui que nous avons pris pour la somme. Soit un ouvert $\mathcal{O}$ dans E ; nous considérons $(\lambda, a) \in f^{-1}(\mathcal{O})$. Vu que $f(\lambda, a) \in \mathcal{O}$, et que $\mathcal{O}$ est ouvert pour la topologie des $\{p_i\}_{i\in I}$, il existe[199] $i \in I$ et $r > 0$ tel que $B_i\big(f(\lambda, a), r\big) \subset \mathcal{O}$.

Nous allons prouver qu'il existe $s > 0$ tel que

$$f\Big(B_i\big((\lambda, a), s\big)\Big) \subset B_i(\lambda a, r). \tag{9.573}$$

Ici encore, à gauche B_i est la boule pour la seminorme q_i donnée en (9.572). Soit $(\mu, x) \in B_i\big((\lambda, a), s\big)$, c'est-à-dire

$$q_i\big((\mu, x) - (\lambda, a)\big) = \max\{|\lambda - \mu|, p_i(a - x)\} < s. \tag{9.574}$$

En particulier nous avons les deux inégalités

$$\begin{cases} |\lambda - \mu| < s, & (9.575a)\\ p_i(a - x) < s. & (9.575b) \end{cases}$$

[198] Définition 9.239.
[199] Voir la définition 9.415.

Nous avons le calcul suivant : SUBEQSooHWMSooBJsRgy

$$\begin{aligned} p_i\big(f(\mu,x),\lambda a\big) &= p_i(\mu x-\lambda a) && (9.576a)\\ &= p_i(\mu x-\lambda x+\lambda x-\lambda a) && (9.576b)\\ &\leqslant p_i\big((\mu-\lambda)x\big)+|\lambda|p_i(x-a) && (9.576c)\\ &= |\mu-\lambda|p_i(x)+|\lambda|p_i(x-a) && (9.576d)\\ &\leqslant sp_i(x)+|\lambda|s. && (9.576e)\end{aligned}$$

C'est le moment de chercher une majoration pour $p_i(x)$:

$$p_i(x)=p_i\big(a+(x-a)\big)\leqslant p_i(a)+p_i(x-a)\leqslant p_i(a)+s. \tag{9.577}$$

Nous pouvons continuer la majoration (9.576) tout en ne nous posant pas de questions sur le sens de l'inégalité parce que nous cherchons $s>0$:

$$\begin{aligned} p_i\big(f(\mu,x),\lambda a\big) &\leqslant sp_i(x)+|\lambda|s && (9.578a)\\ &\leqslant s\big(p_i(a)+s\big)+|\lambda|s && (9.578b)\\ &= s^2+\big(|\lambda|+p_i(a)\big)s. && (9.578c)\end{aligned}$$

Nous devons prouver l'existence d'un $s>0$ tel que $s^2+\big(|\lambda|+p_i(a)\big)s<r$; autrement dit nous devons résoudre l'inéquation

$$s^2+\big(|\lambda|+p_i(a)\big)s-r<0. \tag{9.579}$$

Nous sommes en présence d'un polynôme du second degré en s qui vaut $-r<0$ en $s=0$. Par continuité, il existe un voisinage de $s=0$ dans $\mathbb{R}$ sur lequel le polynôme reste strictement négatif. Il suffit de prendre un s positif dans ce voisinage.

□

La proposition suivante est pratiquement une copie de la proposition 9.371.

PropNGjQnqF

Proposition 9.419.
Soit $f:\mathbb{R}\to(E,p_i)_{i\in I}$ une application. Nous avons équivalence entre

ItemHNxGMpCi
(1) la fonction f est continue en $t_0\in\mathbb{R}$,

ItemHNxGMpCii
(2) si W est un voisinage ouvert de $f(t_0)$ il existe un voisinage ouvert V de t_0 (dans $\mathbb{R}$) tel que $f(V)\subset W$,

ItemHNxGMpCiii
(3) pour tout $i\in I$ et $\epsilon>0$ il existe $\delta>0$ tel que

$$f\big(B(t_0,\delta)\big)\subset B_i\big(f(t_0),\epsilon\big). \tag{9.580}$$

Démonstration. L'équivalence (1) ⇔ (2) est la définition 9.48.

Prouvons (2) ⇒ (3). Soient $i\in I$ et $\epsilon>0$. Considérons la boule $B_i\big(f(t_0),\epsilon\big)$, qui est un ouvert de E contenant $f(t_0)$. Il existe donc un ouvert V autour de t_0 tel que $f(V)\subset B_i\big(f(t_0),\epsilon\big)$. En particulier V contient une boule $B(t_0,\delta)$ et nous avons

$$f\big(B(t_0,\delta)\big)\subset f(V)\subset B_i\big(f(t_0),\epsilon\big). \tag{9.581}$$

Prouvons (3) ⇒ (2). Soit W un ouvert autour de $f(t_0)$. Il existe un $i\in I$ et $\epsilon>0$ tel que $B_i\big(f(t_0),\epsilon\big)\subset W$. Nous avons alors un $\delta>0$ tel que

$$f\big(B(t_0,\delta)\big)\subset B_i\big(f(t_0),\epsilon\big)\subset W. \tag{9.582}$$

□

Lorsqu'on a un espace E muni d'une quantité dénombrable de seminormes $\{p_k\}_{k\in I}$ nous définissons l'écart[200]

$$d(x,y)=\sup_{k\geqslant 1}\min\Big\{\frac{1}{k},p_k(x-y)\Big\}. \tag{9.583}$$ EqAAghiUR

Notons que cet écart est invariant par translation au sens où pour tout x,y,h dans E nous avons

$$d(x+h,y+h)=\sup_{k\geqslant 1}\min\Big\{\frac{1}{k},p_k(x-y)\Big\}=d(x,y). \tag{9.584}$$

[200] Dans le cas de $E=\mathscr{D}(K)$, la première seminorme est numérotée à zéro, donc il faudra poser $d(\varphi_1,\varphi_2)$ avec p_{k-1} au lieu de p_k.

9.20.3 Seminorme et métrisable

Définition 9.420 ([285]).
*Soit un espace vectoriel topologique X. Une famille $\{p_i\}_{i\in I}$ de seminormes est **séparante** si pour tout $x \in X \setminus \{0\}$, il existe $i \in I$ tel que $p_i(x) \neq 0$.*

PROPooMJEQooHtIyeX

Proposition 9.421.
Si X est un espace topologique dont la topologie est donnée par une famille dénombrable et séparante de seminormes[201]*, alors il est métrisable*[202]*.*

Démonstration. Nous utilisons le théorème 9.355. Nous considérons les seminormes $\{p_i\}_{i\in I}$ où I est dénombrable.

(1) **Base dénombrable** Vu que I est dénombrable, l'ensemble des parties finies de I est dénombrable[203]. Pour $a \in X$, l'ensemble des boules de la forme $B_J(a, 1/n)$ avec $n \in \mathbb{N}$ et J fini dans I est donc dénombrable et forme une base de topologie en a.

(2) **Singleton fermé** Prouvons que $\{0\}$ est fermé. Pour cela nous prouvons que le complémentaire est ouvert. Soit $a \neq 0$. Vu que $\{p_i\}_{i\in I}$ est séparante, il existe $i \in I$ tel que $p_i(a) \neq 0$. L'application p_i est continue par 9.415(2). Donc pour tout $\epsilon > 0$, la partie $p_i^{-1}\Big(B\big(p_i(a), \epsilon\big)\Big)$ est un ouvert contenant a.

En prenant $0 < \epsilon < p_i(a)$ et en tenant compte du fait que $p_i(0) = 0$,

$$|p_i(0) - p_i(a)| = |p_i(a)| > \epsilon, \tag{9.585}$$

et donc $p_i(0) \notin B\big(p_i(a), \epsilon\big)$ ou encore

$$0 \notin p_i^{-1}\Big(B\big(p_i(a), \epsilon\big)\Big). \tag{9.586}$$

Bref, l'ouvert $p_i^{-1}\Big(B\big(p_i(a), \epsilon\big)\Big)$ contient a mais pas 0.

□

9.20.4 Boules et topologie

PropLOwUvCO

Proposition 9.422 ([311]).
La topologie donnée par les boules

$$B_k(a, r) = \{x \in E \text{ tel que } \forall k \leqslant \frac{1}{r}, p_k(x - a) < r\} \tag{9.587}$$

EqGHfYIO

est la même que celle « usuelle » donnée par les seminormes. En disant « la même » nous entendons le fait que les ouverts sont les mêmes : A est ouvert pour une des deux topologies si et seulement si il est ouvert pour l'autre.

Démonstration. Pour cette démonstration nous allons préfixer par d les notions topologiques issues des boules (9.587) et par P celle des seminormes : P-continue, d-ouvert, etc.

D'abord nous avons

$$B(a, r) = \bigcap_{k\leqslant\frac{1}{k}} B_k(a, r). \tag{9.588}$$

EqRIURpQo

Si $\mathcal{O}$ est un d-ouvert, il contient une d-boule autour de chacun de ses points. Or d'après la formule (9.588), une d-boule est une intersection *finie* de P-ouverts et donc est un P-ouvert par définition. Donc $\mathcal{O}$ contient un P-ouvert autour de tous ses points et est donc P-ouvert.

Inversement nous supposons que $\mathcal{O}$ est un P-ouvert. Commençons par prouver que les seminormes p_k sont d-continues. En effet soient $k \in \mathbb{N}$, $\epsilon \leqslant \frac{1}{k}$ et $x, y \in E$ tels que $d(x, y) \leqslant \epsilon$; nous avons

$$\begin{aligned}
|p_k(y) - p_k(x)| &\leqslant p_k(x - y) && (9.589a)\\
&= \min\{\frac{1}{k}, p_k(x - y)\} && (9.589b)\\
&\leqslant d(x, y) && (9.589c)\\
&\leqslant \epsilon. && (9.589d)
\end{aligned}$$

[201] Topologie des seminormes, proposition 9.415.
[202] Métrisable, définition 9.156.
[203] Lemme 2.45.

Montrons à présent que $\mathcal{O}$ est d-ouverte. Si $a \in \mathcal{O}$, il existe k et r tels que $B_k(a,r) \subset \mathcal{O}$. Soit $x \in B_k(a,r)$. Montrons que si ϵ est suffisamment petit, la d-boule $B(x,\epsilon)$ est incluse à $B_k(a,r)$. Pour cela prenons $y \in B(x,\epsilon)$; nous avons

$$\big|p_k(a-x) - p_k(a-y)\big| \leqslant d(x,y) \leqslant \epsilon. \tag{9.590}$$

Par conséquent le nombre $p_k(a-y)$ est dans l'intervalle

$$p_k(a-x) \pm \epsilon \tag{9.591}$$

et il suffit de prendre $\epsilon < \frac{r - p_k(a-x)}{2}$. □

THOooTKWYooYYiBNa

Théorème 9.423 ([320]).
Soit une famille de seminormes $\{p_i\}_{i\in I}$ sur E. Pour une seminorme q sur E, les conditions suivantes sont équivalentes.

ITEMooHKNYooARXiXs

(1) L'application $q\colon E \to \mathbb{R}$ est continue.

ITEMooBBNCooGwHrUI

(2) Il existe une partie finie J de I et un nombre $M \in \mathbb{R}$ tels que

$$q(x) \leqslant M \max_{j\in J} p_j(x) \tag{9.592}$$

pour tout $x \in E$.

ITEMooWXSWooVfvSUy

(3) L'application q est bornée dans un voisinage de 0.

Démonstration. En trois parties.

(1) **(1) ⇒ (3)**
C'est la proposition 9.177.

(2) **(3) ⇒ (2)**
Soit un voisinage V de 0 sur lequel q est borné par μ. Ce voisinage contient une boule centrée en 0. Par la définition 9.415, nous avons une partie finie $J \subset I$ et $r > 0$ tels que q est bornée par μ sur $B_J(0,r)$.

Soit $x \in E$. Nous posons

$$t \in \left]0, \min_{j\in J} \frac{r}{p_j(x)}\right[. \tag{9.593}$$

Pour $l \in J$ nous avons alors

$$\begin{aligned}
p_l(tx) &= tp_l(x) && (9.594a)\\
&< \min_{j\in J} \frac{r}{p_j(x)} p_l(x) && (9.594b)\\
&< \frac{r}{p_l(x)} p_l(x) && (9.594c)\\
&= r. && (9.594d)
\end{aligned}$$

Donc $tx \in B_J(0,r)$. En ce qui concerne q nous avons alors $tq(x) = q(tx) < \mu$ et donc

$$q(x) < \frac{\mu}{t}. \tag{9.595}$$

En utilisant la proposition 4.70,

$$\begin{aligned}
q(x) &< \mu \frac{1}{t} && (9.596a)\\
&= \mu \frac{1}{\min_{j\in J} \frac{r}{p_j(x)}} && (9.596b)\\
&= \mu \max_{j\in J} \frac{p_j(x)}{r} && (9.596c)\\
&= \frac{\mu}{r} \max_{j\in J} p_j(x). && (9.596d)
\end{aligned}$$

En posant $M = \mu/r$ nous avons

$$q(x) \leqslant M \max_{j\in J} p_j(x), \tag{9.597}$$

comme demandé.

(3) **(2) ⇒ (1)**
Nous avons une partie finie $J \subset I$ et $M \in \mathbb{R}$ tels que $q(x) \leqslant M \max_{j\in J} p_j(x)$ pour tout $x \in E$.
Soit $x \in E$. Nous prouvons que q est continue en x. Pour tout y nous avons

$$|q(y) - q(x)| \leqslant q(x - y) \leqslant M \max_{j\in J} p_j(x - y). \tag{9.598}$$

Soit $\epsilon > 0$. Si nous prenons $y \in B_J(x, \epsilon)$, alors nous avons

$$|q(y) - q(x)| \leqslant M\epsilon. \tag{9.599}$$

Cela prouve que q est continue en x, et donc continue sur E par la proposition 9.49.

□

CORooSLUCooRaZyYK

Corolaire 9.424 ([320]).
Soient une famille de seminormes P sur E, ainsi qu'une famille Q de seminormes sur F. Une application linéaire $f : E \to F$ est continue si et seulement si $q \circ f$ est une seminorme continue sur E pour tout $q \in Q$.

CORooGMVHooNgYOaY

Corolaire 9.425 ([320]).
Soient des seminormes $P = \{p_i\}_{i\in I}$ sur E. Soit une application linéaire $f : E \to \mathbb{K}$. Elle est continue si et seulement si il existe une partie finie $J \subset I$ et $M \in \mathbb{R}$ tels que

$$|f(x)| < M \max_{j\in J} p_j(x) \tag{9.600}$$

pour tout $x \in E$.

9.20.4.1 Norme induite sur la topologie quotient

PROPooDUAVooEfrEGI

Proposition-Définition 9.426 (Norme quotient[321]).
Soient un espace vectoriel topologique normé E, et un sous-espace M. Pour $\alpha \in E/M$ nous posons

$$\|\alpha\|_{E/M} = d(\alpha, M) \tag{9.601}$$

où $d(\alpha, M)$ est la distance entre la partie α et la partie M.
Nous avons :

ITEMooQOZXooZiZdTn

(1) La formule $\|\alpha\| = \inf_{u\in\alpha} \|u\|_E$.

ITEMooFEOGooTTDgCj

(2) L'opération $\|.\|$ est une seminorme[204] sur l'espace vectoriel E/M.

ITEMooWCCSooMeqQHL

(3) C'est une norme si et seulement si M est fermé.

*Nous parlons de **(semi)norme quotient**.*

Démonstration. Point par point.

(1) **Pour (1)** La définition de $\|\alpha\|$ est $\|\alpha\| = d(\alpha, M) = \inf_{\substack{u\in\alpha\\ v\in M}} \|u - v\|$. Mais

$$\{u - v \text{ tel que } u \in \alpha, v \in M\} = \alpha, \tag{9.602}$$

donc

$$d(\alpha, M) = \inf_{u\in\alpha} \|u\|. \tag{9.603}$$

(2) **Pour (2)** Nous devons vérifier les propriétés de la définition 9.399. D'abord en tant que distance, nous avons $\|\alpha\| \geqslant 0$ pour tout α.
Si $\lambda \in \mathbb{R}$ nous avons aussi

$$\|\lambda\alpha\| = \inf_{u\in\lambda\alpha} \|u\| = \inf_{u\in\alpha} \|\lambda u\| = |\lambda| \inf_{u\in\alpha} \|u\| = |\lambda|\|\alpha\|. \tag{9.604}$$

Enfin si $\alpha, \beta \in E/M$, nous avons

$$\inf_{u\in\alpha+\beta} \|u\| \leqslant \inf_{\substack{u\in\alpha\\ v\in\beta}} \|u + v\| \leqslant \inf_{\substack{u\in\alpha\\ v\in\beta}} \big(\|u\| + \|v\|\big) = \inf_{u\in\alpha} \|u\| + \inf_{v\in\beta} \|v\| = \|\alpha\| + \|b\|. \tag{9.605}$$

[204] Définition 9.399.

(3) **Pour (3) en supposant que M est fermé** Nous supposons que M est fermé et nous montrons que $\|.\|$ est une norme. Nous supposons donc que $d(\alpha, M) = 0$ et nous prouvons que $\alpha = 0$. Soit $x \in E$ tel que $\alpha = [x]$. Nous avons donc

$$\alpha = \{x - v \text{ tel que } v \in M\} \tag{9.606}$$

Notez qu'on a écrit $-v$ et non $+v$. De toutes façons M est vectoriel ; ça ne change rien et ça tombera mieux plus bas.

Nous avons donc

$$0 = \|\alpha\| = d(\alpha, M) = \inf_{u \in \alpha} \|u\| = \inf_{v \in M} \|x - v\|. \tag{9.607}$$

Il existe donc une suite (v_n) dans M telle que $\|x - v_n\| \to 0$. La suite est donc convergente : $v_n \to x$. Comme M est fermé, la proposition 9.170 nous indique que la limite doit être dans M. Autrement dit : $x \in M$. Par définition des classes nous avons alors $\alpha = [x] = 0$.

(4) **Pour (3) en supposant que $\|.\|$ est une norme**

Supposons que M n'est pas fermé. Il ne contient donc pas son adhérence. Soit $a \in \text{Adh}(M) \setminus M$. Vu que M est vectoriel, nous supposons que $a \neq 0$.

Étant donné que a est dans l'adhérence de M nous avons $d(a, M) = 0$ et donc $\|[a]\| = 0$.

□

¡¡ Avertissement/question à la lectrice !! 9.427
Je ne suis pas certain de la proposition 9.428. Peut-être qu'il faut ajouter l'hypothèse que M est fermé.

PROPooKLXSooSOUZkc

Proposition 9.428.
Soient un espace vectoriel topologique normé E, et un sous-espace M. La topologie quotient[205] sur E/M est la même que celle de la seminorme induite[206].

9.20.5 Espace dual

Nous parlerons plus en détail d'espace dual d'un espace normé en la section 12.19.

DefHUelCDD

Lemme-Définition 9.429.
Soient F un espace métrique et E un espace topologique vectoriel. Pour chaque $v \in E$, l'application

$$\begin{aligned} p_v \colon \mathcal{L}(E, F) &\to \mathbb{R} \\ T &\mapsto \|T(v)\|_F \end{aligned} \tag{9.608}$$

est une seminorme.

*La **topologie $*$-faible** sur $\mathcal{L}(E, F)$ est la topologie des ces seminormes.*

9.430.
C'est une famille de seminormes indicées par les éléments de E. Si E est un espace métrique, c'est cette topologie qui sera considérée sur son dual topologique E' des applications continues $E \to \mathbb{R}$.

La topologie ainsi définie est, dans l'idée, celle qui sera choisie pour les espaces de distributions, voir la définition 32.30.

La proposition suivante indique qu'elle est un peu la topologie de la convergence ponctuelle.

PROPooQWOOooUBhBiG

Proposition 9.431.
Soient E un espace muni de la topologie des seminormes $\{p_i\}_{i \in I}$ et F un espace métrique. Soient une suite (T_n) dans $\mathcal{L}(E, F)$ et $T \in \mathcal{L}(E, F)$. Nous avons $T_n \xrightarrow{*} T$ si et seulement si $T_n(v) \xrightarrow{F} T(v)$ pour tout $v \in E$.

Démonstration. Nous avons équivalence entre les lignes suivantes :

$$T_n \xrightarrow{*} T \tag{9.609a}$$

$$p_v(T_n - T) \to 0 \, \forall v \in E \qquad \text{proposition 9.417} \tag{9.609b}$$

$$\|T_n(v) - T(v)\|_F \to 0 \, \forall v \in E \tag{9.609c}$$

$$T_n(v) \xrightarrow{E} T(v). \tag{9.609d}$$

□

[205] Topologie quotient, définition 9.72.
[206] Voir la définition 9.426.

9.20.6 Espace $C^k(\mathbb{R}, E')$

Nous revenons à nos histoires de limites de la définition 9.14.

PropRBCiHbz

Proposition 9.432 (Unicité de la limite dans un dual topologique)**.**
Soient E un espace métrique et E' son dual topologique muni de sa topologie de la définition 9.429. Il y a unicité de l'élément de E' vers lequel une fonction $u\colon \mathbb{R} \to E'$ peut converger.

Démonstration. Soit T un élément vers lequel u_t converge lorsque $t \to t_0$. Soient $\epsilon > 0$ et $x \in E$. La boule $B_x(T, \epsilon)$ de E' subordonnée à la norme p_x et centrée en T est un ouvert de E'. Étant donné que u converge vers T il existe $\delta > 0$ tel que $u_t \in B_x(T, \epsilon)$ dès que $|t - t_0| \leqslant \delta$. Nous avons donc, pour tout $x \in E$, la limite (dans $\mathbb{R}$) :

$$\lim_{t \to t_0} u_t(x) = T(x). \tag{9.610}$$

Cela prouve que la convergence de u vers T implique l'existence pour tout x de la limite de $u_t(x)$ dans $\mathbb{R}$. Si T' est un autre élément vers lequel u_t converge, nous avons par le même raisonnement que

$$\lim_{t \to t_0} u_t(x) = T'(x). \tag{9.611}$$

Par unicité de la limite dans $\mathbb{R}$ nous devons alors avoir $T(x) = T'(x)$ pour tout x, c'est-à-dire $T = T'$. □

PropVKSNfiB

Proposition 9.433.
Soit $u\colon \mathbb{R} \to E'$ une fonction continue. Alors

ItemLSJjfZdi

(1) pour tout $x \in E$ la fonction $t \mapsto u_t(x)$ est continue,

ItemLSJjfZdii

(2) pour tout $x \in E$ nous avons la limite dans $\mathbb{R}$

EqWKdEEVO

$$\lim_{t \to t_0} u_t(x) = u_{t_0}(x), \tag{9.612}$$

ItemLSJjfZdiii

(3) nous avons la limite dans E'

$$\lim_{t \to t_0} u_t = u_{t_0}. \tag{9.613}$$

Démonstration. Soient $x \in E$ et $\epsilon > 0$. Par la proposition 9.419 la continuité de u donne un $\delta > 0$ tel que

$$u_{B(t_0, \delta)} \subset B_x(u_{t_0}, \epsilon). \tag{9.614}$$

C'est-à-dire que si $|t - t_0| \leqslant \delta$ nous avons

$$\big|u_{t_0}(x) - u_t(x)\big| < \epsilon, \tag{9.615}$$

ce qui signifie bien que la fonction $t \mapsto u_t(x)$ est continue en tant que fonction $\mathbb{R} \to \mathbb{R}$. Cela est le point (1). Le théorème de limite et continuité dans $\mathbb{R}$ nous donne immédiatement la limite (9.612).

Nous passons à la preuve du point (3). Soit $\mathcal{O}$ un ouvert de E' contenant u_{t_0}. Il existe donc un $i \in I$ et $\epsilon > 0$ tel que $B_i(u_{t_0}, \epsilon) \subset \mathcal{O}$. Étant donné que u est continue, il existe $\delta > 0$ tel que

$$u_{B(t_0, \delta)} \subset B_i(u_{t_0}, \epsilon) \subset \mathcal{O}. \tag{9.616}$$

Cela signifie bien que

$$|t - t_0| \leqslant \delta \Rightarrow u_t \in \mathcal{O}, \tag{9.617}$$

c'est-à-dire que nous avons la limite $\lim_{t \to t_0} u_t = u_{t_0}$ dans E'. Pour dire cela nous avons utilisé la définition 9.151 de la limite et le résultat d'unicité 9.432. □

DefDZsypWu

Définition 9.434.
*Si nous avons une application $u\colon \mathbb{R} \to E'$ nous considérons sa **dérivée** donnée par la limite*

$$u'_{t_0} = \lim_{t \to t_0} \frac{u_t - u_{t_0}}{t - t_0}. \tag{9.618}$$

Cela est un nouvel élément de E' (pour peu que la limite existe). La fonction $u'\colon \mathbb{R} \to E'$ ainsi définie peut être continue ou non. Cela nous permet de définir les espaces $C^k(\mathbb{R}, E')$ et $C^\infty(\mathbb{R}, E')$.

Une des principales utilisations que nous ferons de ces espaces seront les espaces de fonctions à valeurs dans les distributions tempérées dont nous parlerons dans la section 32.4.

9.21 Espaces de Baire

LEMooRTXFooCMCaHC

Lemme 9.435 ([1]).
Soit un espace topologique X. Une partie A est un ouvert dense si et seulement si $X \setminus A$ est un fermé d'intérieur vide.

Démonstration. Nous savons, par définition que le complémentaire d'un ouvert est fermé et inversement. Soient une partie $A \subset X$ ainsi que son complémentaire $F = X \setminus A$. Nous avons équivalence entre :

- F est d'intérieur vide,
- aucun ouvert non vide n'est contenu dans F
- tout ouvert non vide intersecte $X \setminus F$
- tout ouvert non vide intersecte A
- A est dense dans X.

□

DEFooYEMNooLSXLYa

Proposition-Définition 9.436 (Espace de Baire[1, 322, 323]).
Soit un espace topologique X. Les propriétés suivantes sont équivalentes.

ITEMooBHOOooKyToBw

(1) Toute intersection dénombrable d'ouverts denses est dense.

ITEMooFMDAooUPaULP

(2) Toute union dénombrable de fermés d'intérieurs vides est d'intérieur vide.

ITEMooKSNYooIgzLey

(3) Le seul ouvert maigre[207] de X est le vide.

*Quand X vérifie ces propriétés, nous disons que X est une **espace de Baire**.*

Démonstration. En plusieurs parties.

(1) **(1) implique (2)** Soient des fermés d'intérieur vide $(F_i)_{i\in\mathbb{N}}$. Nous posons $A_i = X \setminus F_i$ et nous utilisons le lemme 1.50 pour dire que

$$\bigcup_i F_i = \bigcup_i (X \setminus A_i) = X \setminus \big(\bigcap_i A_i\big). \tag{9.619}$$

Par hypothèse, $\bigcap_i A_i$ est un ouvert dense. Par le lemme 9.435 son complémentaire est un fermé d'intérieur vide.

(2) **(2) implique (1)** Soient des ouverts denses $(A_i)_{i\in\mathbb{N}}$. En notant $F_i = X \setminus A_i$, nous avons

$$\bigcap_{i\in\mathbb{N}} A_i = \bigcap_{i\in\mathbb{N}} (X \setminus F_i) = X \setminus \big(\bigcup_{i\in\mathbb{N}} F_i\big). \tag{9.620}$$

Par hypothèse $\bigcup_i F_i$ est un fermé d'intérieur vide. Donc son complémentaire est un ouvert dense.

(3) **(1) implique (3)** Soient un espace de Baire X et un ouvert maigre $A \subset X$. Nous avons $A = \bigcup_{i\in\mathbb{N}} A_i$ où les A_i sont des parties nulle part denses[208]. Nous devons montrer que $A = \varnothing$.

Vu que A_i est nulle part dense, $\mathrm{Int}(\bar{A}_i) = \varnothing$ pour tout i. Nous avons :

$$\mathrm{Int}(A) \subset \mathrm{Int}\big(\bigcup_i A_i\big) \subset \mathrm{Int}\big(\bigcup_i \bar{A}_i\big) = \varnothing \tag{9.621}$$

parce que X étant de Baire, l'union de fermés d'intérieur vide est d'intérieur vide. Nous avons prouvé que $\mathrm{Int}(A) = \varnothing$. Mais A étant ouvert nous avons $\mathrm{Int}(A) = A$.

(4) **(3) implique (1)** Nous supposons que tout ouvert maigre de X est vide. Soient des fermés $(F_i)_{i\in\mathbb{N}}$ d'intérieurs vides. Nous considérons la partie $A = \mathrm{Int}\big(\bigcup_{i\in\mathbb{N}} F_i\big)$.

(4a) **A est ouvert** Parce que c'est l'intérieur d'une partie.

(4b) **F_i est nulle part dense** Vu que F_i est fermé nous avons $\bar{F}_i = F_i$ et donc $\mathrm{Int}(\bar{F}_i) = \mathrm{Int}(F_i) = \varnothing$.

[207] Définition 9.397
[208] Définition 9.396.

Donc l'ouvert A est une réunion dénombrable de parties nulle part denses. C'est donc un ouvert maigre, et nous en déduisons que $A = \varnothing$.

Par 9.436 nous savons que X est de Baire.

□

PROPooGVTDooRMaEUK

Proposition 9.437 ([229, 324]).
Plusieurs choses à propos d'espaces de Baire.

ITEMooYZKYooEvcLTx

(1) Tout espace de Baire Hausdorff[209] *sans point isolé est non dénombrable.*

ITEMooBZCAooIYQpvO

(2) Si U est une partie ouverte d'un espace de Baire X, alors toute partie maigre dans U (topologie induite) est maigre dans X.

ITEMooGHMTooDYUicn

(3) Si U est ouvert dans l'espace de Baire X, alors U est un espace de Baire pour la topologie induite.

Démonstration. Plusieurs points.

(1) **Pour (1)** Soit un espace de Baire Hausdorff. Un singleton est fermé par le lemme 9.81 et d'intérieur vide. En effet si U est un ouvert contenant a, il contient forcément autre chose que a parce que X n'a pas de points isolés. Donc il n'y a pas d'ouverts contenus dans $\{a\}$.

Une réunion dénombrable de fermés d'intérieurs vides est d'intérieur vide parce que X est de Baire (définition 9.436). Donc X n'est pas une union dénombrable de singletons.

(2) **Pour (2)** Soit une partie maigre M de X. Nous avons $M = \bigcup_{i\in\mathbb{N}} F_i$ où F_i est fermé d'intérieur vide dans U. Le lemme 9.38 nous dit que

$$\operatorname{Int}_X\big(\operatorname{Adh}_X(F_i)\big) = \varnothing. \tag{9.622}$$

En particulier $\operatorname{Adh}_X(F_i) \cap U$ est nulle part dense dans X (définition 9.396(1)).

La formule (9.33) dit que $F_i = \operatorname{Adh}_X(F_i) \cap U$, et donc

$$M = \bigcup_{i\in\mathbb{N}} \big(\operatorname{Adh}_X(F_i) \cap U\big) \tag{9.623}$$

est une union dénombrable de parties nulle part denses. Donc M est maigre dans X.

(3) **Pour (3)** Soit un ouvert maigre A de U. Par le point (2), A est maigre dans X et donc vide parce que X est de Baire. Cela prouve que tout ouvert maigre de U est vide et donc que U est de Baire (définition 9.436).

□

ThoBBIljNM

Théorème 9.438 (Théorème de Baire[323, 229, 324]).
Les espaces suivants sont de Baire :

(1) les espaces topologiques localement compacts[210]*,*

(2) les espaces métriques complets (donc ceux de Banach en particulier),

(3) tout ouvert d'un espace de Baire.

Démonstration. En plusieurs parties.

(1) **Espaces topologiques localement compacts** Nous allons utiliser les propriétés de 9.436. Soient un espace topologique localement compact X ainsi que des fermés F_i d'intérieurs vides. Nous posons $F = \bigcap_{i=0}^{\infty} F_i$, et nous prouvons que F est d'intérieur vide. Pour cela nous considérons un ouvert $U \subset X$ et nous prouvons que U n'est pas entièrement inclus dans F.

Par 9.203, il existe un ouvert à fermeture compacte $U_0 \subset U$. Vu que F_1 est fermé, $U_0 \setminus F_1$ est ouvert et comme F_1 est d'intérieur vide, il ne contient aucun ouvert, donc l'ouvert $U_0 \setminus F_1$ est non vide.

Si $x \in U_0 \setminus F_1$, alors $\{x\}$ est compact et le lemme 9.202 dit qu'il existe un ouvert V_1 tel que $\bar{V}_1$ est compact et tel que

$$x \in V_1 \subset \bar{V}_1 \subset U_0 \setminus F_1. \tag{9.624}$$

[209] Définition 9.79.
[210] Définition 9.198.

Maintenant V_1 étant ouvert, il n'est pas contenu dans $V_1 \setminus F_2$ qui est un ouvert non vide..

Bref, je vous laisse écrire la récurrence proprement, mais nous avons des ouverts V_n tels que $\bar{V}_n$ est compact et $\bar{V}_n \subset V_{n-1} \setminus F_n$.

Les parties $\bar{V}_n$ sont des compacts emboîtés non vides. La proposition 9.139 dit que $\bigcap_n \bar{V}_n$ est non vide. Soit $a \in \bigcap_n \bar{V}_n$. Pour tout $k \neq 1$ nous avons

$$a \in \bigcap_n \bar{V}_n \subset \bar{V}_k \subset V_{k-1} \setminus F_k. \tag{9.625}$$

Donc a n'est pas dans F_k. De plus $a \in \bar{V}_1 \subset U_0 \setminus F_1$. Donc a n'est pas non plus dans F_1. Bref, a n'est pas dans F.

Nous devons encore voir que $a \in U_0$. Cela est facile :

$$a \in \bigcup_n \bar{V}_n \subset \bar{V}_1 \subset U_0 \setminus F_1 \subset U_0. \tag{9.626}$$

(2) **Espaces métriques complets** Soit (E, d) un espace métrique complet. Soient V un ouvert quelconque de E et U_n une suite d'ouverts denses. Le but est de prouver que l'ensemble $\bigcap_{n\in\mathbb{N}} U_n$ intersecte V. Vu que V est ouvert dans un espace métrique, il contient une boule ouverte et donc une boule fermée B_0 de rayon strictement positif. L'ensemble U_1 est dense et intersecte donc un ouvert contenu dans B_0. L'intersection est un ouvert qui contient alors une boule fermée B_1 de rayon strictement positif. Continuant ainsi nous construisons une suite de fermés emboités B_n telle que

$$\bigcap_{n\in\mathbb{N}} U_n \cap V \tag{9.627}$$

contient l'intersection des B_n. Par le théorème 9.372 des fermés emboîtés (que nous utilisons parce que E est métrique et complet), cette intersection est non vide.

(3) **Ouvert d'un espace de Baire** C'est la proposition 9.437(3).

□

Parmi les applications du théorème de Baire, nous avons

- Le théorème de Banach-Steinhaus 12.202.
- Le théorème de l'application ouverte 12.211.