Le Frido 2023,
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 2024. 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`

ISBN : 979-10-97085-34-6

Index thématique

1 : cardinalité
2 : morphismes et compagnie
3 : arithmétique modulo, théorème de Bézout
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 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 : compacts
33 : densité
34 : application réciproque
35 : applications continues et bornées
36 : suite de Cauchy, espace complet
37 : caractérisations séquentielles
38 : valeurs propres, définie positive
39 : norme matricielle, norme opérateur et rayon spectral
40 : série de matrices
41 : décomposition de matrices
42 : systèmes d'équations linéaires
43 : réduction, diagonalisation
44 : déterminant
45 : espaces de fonctions
46 : fonctions Lipschitz
47 : suites et séries
48 : suite de fonctions
49 : exponentielle
50 : logarithme
51 : fonction puissance
52 : sommation finie et infinie
53 : polynôme de Taylor
54 : formule des accroissements finis
55 : dérivation
56 : différentiabilité
57 : équations différentielles
58 : convexité
59 : espaces de Hilbert, base hilbertienne
60 : analyse complexe, fonctions holomorphes
61 : permuter des limites
62 : déduire la nullité d'une fonction depuis son intégrale
63 : inversion locale, fonction implicite
64 : points fixes
65 : changement de variables
66 : techniques de calcul
67 : méthodes de calcul
68 : méthode de Newton
69 : prolongement d'applications
70 : opérations sur les distributions
71 : convolution
72 : séries de Fourier
73 : transformée de Fourier
74 : gaussienne
75 : lemme de transfert
76 : invariants de similitude
77 : isométries
78 : enveloppes
79 : intégration sur des variétés
80 : dénombrements
81 : caractérisation de distributions en probabilités
82 : théorème central limite
83 : indépendance d'événements et de variables aléatoires
84 : probabilités et espérances conditionnelles
85 : chaine de Markov

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

1. Ici je mets la référence [1] ; pas parce qu'elle est utile ici, mais parce que je veux être sûr qu'elle soit numéro 1 de façon à être facilement reconnaissable. Elle indique les affirmations à propos desquelles le lecteur doit être doublement attentif.

subpotence, et démontrer un certain nombre de résultats en utilisant sans retenue le lemme de Zorn 1.22.

(1) Ensemble infini, définition 1.112.
(2) Ensemble dénombrable, définition 1.124.
(3) Cardinal d'un ensemble fini, définition 1.121.
(4) Définition d'équipotence, surpotence et subpotence, notations $A \succ B$ et $A \approx B$, définition 1.110.
(5) Toute partie d'un ensemble fini est finie, lemme 1.114.
(6) Si A est un ensemble fini ou dénombrable, alors il existe une surjection $\mathbb{N} \to A$, lemme 1.126.
(7) Si A est un ensemble infini et si $f\colon A \to B$ est une application injective, alors $f(A)$ est infini, proposition 1.119.
(8) Toute partie infinie de $\mathbb{N}$ est dénombrable, proposition 1.127
(9) Une bijection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, proposition 1.130.
(10) Une décomposition de $\mathbb{N}$ en une infinité de parties équipotentes à $\mathbb{N}$, corolaire 1.131.
(11) Si il existe une surjection $\mathbb{N} \to A$, alors A est fini ou dénombrable, lemme 1.132.
(12) Une union dénombrable d'ensembles finis ou dénombrables est finie ou dénombrable, proposition 1.133
(13) Tout ensemble infini contient une partie en bijection avec $\mathbb{N}$, proposition 1.136.
(14) Toute partie d'un ensemble fini est finie, et toute partie d'un ensemble dénombrable est finie ou dénombrable, proposition 1.137.
(15) Si $A \geq B$ et $B \geq A$, alors $A \approx B$, théorème de Cantor-Schröder-Bernstein 1.140
(16) Le théorème de Cantor 1.143 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 1.145).
(17) Si A est infini et si $A \geq B$, alors $A \approx A \cup B$ par le lemme 1.147.
(18) Si S est un ensemble infini alors il existe une bijection $\varphi\colon \{0,1\} \times S \to S$, proposition 1.148.
(19) Si A est infini, alors $A \times \mathbb{N} \approx A$, proposition 1.150.
(20) Si A est infini et si $B \prec A$, alors $A \backslash B \approx A$, lemme 1.152.
(21) Si A est infini, alors $A \approx A \times A$, théorème 1.156.

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 6.134 affirme que tout corps admet une unique clôture algébrique. La preuve utilise pas mal de cardinalité ainsi que le lemme de Zorn 1.22.

Thème 2 : morphismes et compagnie

(1) 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.
(2) Morphisme de module, définition 1.323.
(3) Morphisme de groupes, définition 1.36.
(4) Un isomorphisme d'espaces topologiques est une application continue, inversible, dont l'inverse est continue, 7.37. On dit aussi un homéomorphisme.
(5) Un difféomorphisme est différentiable d'inverse différentiable, définition 11.224.
(6) Un C^k-difféomorphisme est une application C^k d'inverse C^k. Définition 11.224.

Le mot « homomorphisme » signifie exactement « morphisme », et, sauf incohérence de ma part, il n'est pas utilisé dans le Frido.

Thème 3 : arithmétique modulo, théorème de Bézout

(1) Pour $\mathbb{Z}^*$ c'est le théorème 1.229.

(2) Théorème de Bézout dans un anneau principal : corolaire 3.68.

(3) Théorème de Bézout dans un anneau de polynômes : théorème 6.47.

(4) En parlant des racines de l'unité et des générateurs du groupe unitaire dans le lemme 19.6. Au passage nous y parlerons de solfège.

(5) La proposition 1.255 qui donne tout entier assez grand comme combinaisons de a et b à coefficients positifs est utilisée en chaines de Markov, voir la définition 38.33 et ce qui suit.

(6) PGCD et PPCM sont dans la définition 1.180.

(7) Calcul effectif du PGCD puis des coefficients de Bézout : sous-sections 3.2.1.1 et 3.2.1.2.

Thème 4 : divisibilité

(1) Si a divise bc et si a est premier avec c, alors a divise b. Lemme de Gauss 3.12.

(2) Si a divise b et b divise a, alors $a = b$, lemme 3.14.

Thème 5 : équations diophantiennes

(1) Équation $ax + by = c$ dans $\mathbb{N}$, équation (3.58).

(2) Dans 3.2.6, nous résolvons $ax + by = c$ en utilisant Bézout (théorème 1.229).

(3) L'exemple 3.86 donne une application de la pure notion de modulo pour $x^2 = 3y^2 + 8$. Pas de solutions.

(4) L'exemple 3.87 résout l'équation $x^2 + 2 = y^3$ en parlant de l'extension $\mathbb{Z}[i\sqrt{2}]$ et de stathme.

(5) Les propositions 3.91 et 3.93 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 26.99.

(7) La proposition 1.130 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.

Thème 6 : types d'anneaux

(1) Définition d'anneau : définition 1.39.

(2) La définition d'anneau principal est 1.221 ; pour un idéal principal, c'est 1.220.

(3) $\mathbb{Z}$ est intègre, lemme 1.245, principal et euclidien (proposition 1.248).

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

(5) Si A est un anneau intègre [2] qui n'est pas un corps, alors $A[X]$ n'est pas principal, lemme 1.249.

(6) L'anneau des fonctions holomorphes sur un compact donné est principal, proposition 26.68.

(7) L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel, exemple 3.64.

(8) L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est ni factoriel ni principal, exemple 3.77.

(9) Tous les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont principaux, mais $\mathbb{Z}/6\mathbb{Z}$ n'est pas principal. Exemple 1.241.

anneau principal

- Définition 1.221.
- Il est intègre, définition 1.221.
- Il est noetherien, lemme 3.73.
- il est factoriel, théorème 3.75.

anneau euclidien

2. Définition 1.192.

— Définition 1.244.

— Il est principal par 1.247

anneau intègre

— Définition 1.192.

anneau noetherien

— Définition 3.72.

anneau factoriel

— Définition 3.59.

— Il est intègre, définition 3.59.

corps

— Corps, définition 1.202.

— Il est un anneau intègre, lemme 1.193.

— Il est un anneau principal, proposition 3.76.

— Il est un anneau factoriel, proposition 3.76.

Dans un anneau intègre

— Un anneau fini intègre est un corps, proposition 3.57.

— A est intègre si et seulement si $A[X]$ est intègre, théorème 3.99.

— Si un pgcd [3] est inversible, tous les pgcd sont inversibles, lemme 1.195.

Dans un anneau principal

— p est premier si et seulement si il est irréductible si et seulement si l'idéal pA est maximal, proposition 1.227.

— Tous les idéaux sont principaux, définition 1.221.

— Si $\text{pgcd}(a,b)=1$, $\text{pgcd}(a,c)=1$, alors $\text{pgcd}(a,bc)=1$, lemme 3.70.

Dans un anneau factoriel

— Si p est irréductible et si $p \mid ab$, alors p divise a ou b, lemme 3.60.

— Tout élément irréductible est premier, proposition 3.61.

— Si p est irréductible, pA est un idéal premier, lemme 3.62.

— Si p est irréductible, A/pA est un anneau intègre, lemme 3.62 et proposition 1.224.

— P et Q sont primitifs si et seulement si PQ est primitif, lemme 3.114.

— Formule $c(PQ)=c(P)c(Q)$. Lemme 3.114.

— L'anneau des polynômes $\mathcal{P}(A)=A[X]$ est factoriel, théorème 6.35.

Dans un corps commutatif

— L'anneau $\mathbb{K}[X]$ est factoriel, proposition 6.36, euclidien et principal, lemme 3.105.

— Les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$, lemme 1.178.

— L'anneau $\mathcal{P}(\mathbb{K})$ est euclidien, lemme 3.105.

élément irréductible

— Définition 1.183

élément premier

— Définition 1.182

— Si A est intègre et unitaire, l'élément p est premier si et seulement si l'idéal pA est premier, proposition 1.194.

éléments associés

3. pgcd, définition 1.180.

— Définition 3.49.

Dans un anneau, un idéal est 1.177.

idéal premier

— Définition 1.222.

— Idéal premier si et seulement si A/I est anneau intègre, proposition 1.224.

idéal maximal

— Idéal maximal si et seulement si A/I est un corps, proposition 1.224.

idéal principal

— Définition 1.220.

— 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 1.194.

Thème 7 : sous-groupes

(1) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 9.305.

(2) Sous-groupes compacts de $\mathrm{GL}(n, \mathbb{R})$, lemme 13.40 ou proposition 13.41.

Thème 8 : groupe symétrique

(1) Définition 1.267.

(2) La signature $\epsilon\colon S_n \to \{-1, 1\}$ est l'unique morphisme surjectif de S_n sur $\{-1, 1\}$, proposition 1.293(1).

(3) La table des caractères du groupe symétrique S_4 est donné dans la section 16.5.

(4) Le groupe symétrique S_4 est le groupe des symétries affines du tétraèdre régulier [4], proposition 18.197.

(5) Le groupe alterné A_5 est l'unique groupe simple d'ordre [5] 60, proposition 5.54.

(6) La proposition 5.44 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.

Thème 9 : action de groupe

(1) Définition d'une action de groupe sur un ensemble : 1.360.

(2) Action du groupe modulaire sur le demi-plan de Poincaré, théorème 23.95.

(3) La formule de Burnside (théorème 2.40) 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, 18.10.15.1 et 18.10.15.2.

(5) Le groupe symétrique S_n agit sur l'anneau $\mathbb{K}[T_1, \ldots, T_n]$, lemme 1.361.

Thème 10 : classification de groupes

(1) Ordre d'un groupe, définition 1.260.

(2) Structure des groupes d'ordre pq, théorème 5.25.

(3) Le groupe alterné est simple, théorème 5.50.

(4) Définition 5.6 d'un p-groupe.

(5) Théorème de Sylow 5.11.

(6) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 9.305.

4. Définition 12.147.
5. Ordre d'un groupe, définition 1.260.

(7) $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, corolaire 19.32.

(8) Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, proposition 3.132.

(9) Le premier théorème d'isomorphisme 2.6 dit que si θ est un morphisme de groupes, alors $G/\ker(\theta) = \text{Image}(\theta)$.

(10) Le deuxième théorème d'isomorphisme 2.7 dit que si N est normal dans G, alors $NH/N = H/(H \cap N)$.

(11) Le troisième théorème d'isomorphisme 2.9 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 1.261.

(2) L'ordre d'un élément divise l'ordre du groupe, corolaire 2.14.

(3) Si H est normal dans G, alors $|G/H| = |G|/|G|$, théorème de Lagrange 2.13.

(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 3.26.

Thème 11 : Fonction indicatrice d'Euler

(1) Définition de $\varphi\colon \mathbb{N}^* \to \mathbb{N}^*$ dans 5.29.

(2) Propriétés genre $\varphi(pq) = \varphi(p)\varphi(q)$, corolaire 5.42.

(3) $\varphi(n) = \text{Card}(\Delta_n)$, proposition 19.12.

(4) $n = \sum_{d|n} \varphi(d)$, lemme 5.37.

(5) Le théorème de Euler-Fermat 5.33 donne $a^{\varphi(n)} \in [1]_n$ dès que a et n sont premiers entre eux.

(6) Si A et B sont premiers entre eux, il existe p, m tels que $A^p = mB + 1$, proposition 5.33.

Thème 12 : produit semi-direct de groupes

(1) Définition 2.47.

(2) Le corolaire 2.49 donne un critère pour prouver qu'un produit NH est un produit semi-direct.

(3) L'exemple 18.179 donne le groupe des isométries du carré comme un produit semi-direct.

(4) Le théorème 5.25 classifie les groupes d'ordre pq (p, q premiers distincts) à grands coups de produit semi-directs.

(5) Le théorème 18.81 donne les isométries de $\mathbb{R}^n$ par $\text{Isom}(\mathbb{R}^n) = T(n) \times_\rho O(n)$ où $T(n)$ est le groupe des translations.

(6) La proposition 18.83 donne une décomposition du groupe orthogonal $\text{O}(n) = \text{SO}(n) \times_\rho C_2$ où $C_2 = \{\text{Id}, R\}$ où R est de déterminant -1.

(7) La proposition 8.63 donne $\text{Aff}(\mathbb{R}^n) = T(n) \times_\rho \text{GL}(n, \mathbb{R})$ où $\text{Aff}(\mathbb{R}^n)$ est le groupe des applications affines bijectives de $\mathbb{R}^n$.

Thème 13 : théorie des représentations

(1) Définition 4.131.

(2) Table des caractères du groupe diédral, section 18.17.

(3) Table des caractères du groupe symétrique S_4, section 16.5.

Thème 14 : espaces vectoriels

(1) Les notations $\mathcal{L}(V, W)$, $L(V, W)$, $\text{GL}(V, W)$ ainsi que les notions de morphismes et d'isomorphismes d'espaces vectoriels normés sont dans la définition 11.230.

(2) Existence d'une base. Pour un espace vectoriel quelconque, proposition 4.23.

(3) Théorème de la base incomplète. Pour un espace vectoriel quelconque, théorème 4.24.

Thème 15 : rang

(1) Définition pour une application linéaire : 4.45, pour une matrice : 4.103. L'équivalence est la proposition 4.107.

(2) Le théorème du rang, théorème 4.46

(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 4.48.

(4) Pour prouver que des matrices sont équivalentes et pour les mettre sous des formes canoniques, nous avons le lemme 4.109 et son corolaire 4.110.

(5) Tout hyperplan de $\mathbb{M}(n,\mathbb{K})$ coupe $\mathrm{GL}(n,\mathbb{K})$, corolaire 4.110. Cela utilise la forme canonique sus-mentionnée.

(6) Le lien entre application duale et orthogonal de la proposition 9.187 utilise la notion de rang.

(7) Le lemme 9.295 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 9.296.

Thème 16 : formes bilinéaires et quadratiques

(1) Les formes bilinéaires sont définies en 9.119.

(2) Forme quadratique, définition 9.120.

(3) Équivalence de forme quadratiques, définition 9.244. Deux formes quadratiques sont équivalentes si et seulement si elles ont même signature, proposition 9.245.

(4) Une isométrie d'une forme bilinéaire est affine ou linéaire, théorème 9.152.

(5) Forme bilinéaire dégénérée, définition 9.124.

(6) Une forme bilinéaire est non-dégénérée si et seulement si sa matrice associée est inversible, c'est la proposition 9.221.

(7) Une isométrie d'une forme bilinéaire est linéaire ou affine par le théorème 9.152.

(8) Toute forme quadratique admet des bases orthogonales, théorème 9.237 pour le cas général ; proposition 9.248 pour le cas de $\mathbb{R}^n$, en se basant sur le théorème spectral.

(9) Base q-orthogonale pour une forme quadratique, théorème 9.237.

(10) Le concept de projection orthogonale est la définition 12.142 en dimension finie et la définition 25.7 dans le cas des espaces de Hilbert.

(11) Produit hermitien, définition 9.170. Opérateur hermitien ($A^\dagger = A$), opérateur unitaire ($A^\dagger A = 1$), définition 9.173

matrice

(1) Matrice d'une forme quadratique, définition 9.143.

(2) Théorème de Sylvester à propos de signature (définition 9.158) de forme quadratique réelle : 9.243.

orthogonalité

(1) Il existe une base q-orhogonale, proposition 9.235 et théorème 9.237.

(2) Définition de l'orthogonal $A^\perp$ et du noyau $\ker(b)$, définitions 9.126, 9.127.

(3) Diverses propriétés comme $A^\perp = \mathrm{Span}(A)^\perp$ et $V \cap V^\perp = \ker(b_V)$, propositions 9.128 et 9.129.

(4) En dimension finie, $(V^\perp)^\perp = V$, lemme 9.132.

(5) Nous avons $\dim(V) + \dim(V^\perp) = \dim(E)$, lemme 9.131.

(6) Pour une forme quadratique strictement définie positive ou négative, $E = F \oplus E^\perp$, lemme 9.134.

Thème 17 : endomorphismes cycliques

(1) Définition 9.99.

(2) Groupe cyclique, définition 1.319.

(3) Son lien avec le commutant donné dans la proposition 9.293 et le théorème 9.296.

(4) Utilisation dans le théorème de Frobenius (invariants de similitude), théorème 9.284.

Thème 18 : extension de corps et polynômes

(1) Définition d'une extension de corps 6.59.

(2) Définition de polynôme minimal : 6.64.

(3) Pour l'extension du corps de base d'un espace vectoriel et les propriétés d'extension des applications linéaires, voir la section 9.14.

(4) Extension de corps de base et similitude d'application linéaire (ou de matrices, c'est la même chose), théorème 9.298.

(5) Extension de corps de base et cyclicité des applications linéaires, corolaire 9.297.

(6) À propos d'extensions de $\mathbb{Q}$, le lemme 6.181.

(7) Corps de rupture : définition 6.113 existence par la proposition 6.119. Il n'y a pas unicité.

(8) Corps de décomposition : définition 6.140. Attention : le plus souvent nous parlons de corps de décomposition d'un seul polynôme. Cette définition est un peu surfaite. Existence par la proposition 6.141 qui le donne même comme extension par toutes les racines, et unicité à isomorphisme près par le théorème 6.143, énoncé de façon plus simple (mais pas indépendante !) en la proposition 6.144.

(9) 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 6.79.

Un trio de résultats d'enfer est :

(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[6] (proposition 1.237).

(2) Dans un anneau, un idéal I est maximal si et seulement si A/I est un corps (proposition 1.213)

(3) Si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est principal (lemme 3.105).

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 1.352. Le produit et l'évaluation sont définis en 1.355 et la formule $(PQ)(x) = P(x)Q(x)$ dans 1.356.

(2) Si $\mathbb{A}$ est commutatif, alors $\mathbb{A}[X]$ est également commutatif, lemme 1.357.

(3) En ce qui concerne la notation $A[X]$, elle ne devrait pas être utilisée, voir 1.19.2. L'ensemble des polynômes sera noté $\mathcal{P}(A)$ et ceux de degré n (définition 1.354), $\mathcal{P}_n(A)$.

(4) $A[X]$, définition 1.352 ; 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 1.355.

(5) Liens entre $\mathbb{K}[\alpha]$, $\mathbb{K}[X]$, $\mathbb{K}(\alpha)$ et $\mathbb{K}(X)$ lorsque α est transcendant, proposition 6.99. Et la proposition 6.102 pour le cas où α est algébrique[7].

(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 3.97.

6. Irréductibilité, y compris polynôme irréductible, définition 1.183.
7. Définition 6.71.

(7) $\mathbb{K}(X)$, le corps des fractions de $\mathbb{K}[X]$, définition 6.83. Si $R = P/Q$ dans $\mathbb{K}(X)$, l'évaluation est $R(\alpha) = P(\alpha)Q(\alpha)^{-1}$, définition 6.84.

(8) $\mathbb{K}(\alpha)_{\mathbb{L}}$ est le plus petit corps de $\mathbb{L}$ contenant $\mathbb{K}$ et α, définition 6.85.

(9) À propos de polynômes à plusieurs variables.

— Anneau de polynômes : $A[X_1, \dots, X_n]$ est la définition 3.45.

— Corps engendré : $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ est la définition 6.137.

— Corps des fractions rationnelles : $\mathbb{K}(X_1, \dots, X_n)$ est la définition 6.138.

contenu À propos de $c(P)$.

(1) Définition du contenu $c(P)$, 3.108.

(2) $c(PQ) = c(P)c(Q)$, lemme de Gauss 19.46, et lemme 3.114 pour un anneau factoriel.

(3) Si $c(P) = 1$, on dit que P est primitif au sens des pgcd, définition 3.110.

(4) Si $a \in A$ nous avons $c(aP) = ac(P)$ par le lemme 1.196.

(5) Un polynôme primitif est la définition 3.110.

Dérivation Plusieurs propriétés du polynôme dérivé P'.

(1) La définition 6.153 donne $P' = \sum_{k=1}^{n} ka_iX^{k-1}$.

(2) Règle de Leibnitz, lemme 6.154.

(3) Caractérisation de $P' = 0$ en fonction de la caractéristique de $\mathbb{K}$, lemme 6.155.

Coefficients dans un anneau commutatif (1) Les polynômes à coefficients dans un anneau commutatif sont à la section 3.7.

(2) Un anneau A est intègre si et seulement si $A[X]$ est intègre ; théorème 3.99.

Coefficients dans un corps Les polynômes à coefficients dans un corps sont à la section 6.3.

(1) Si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est euclidien et principal, lemme 3.105.

(2) Nous parlons de l'idéal des polynômes annulateurs dans le théorème 6.43.

(3) Le théorème 6.43 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 6.67.

(5) Quelques formules sur le pgcd, lemme 6.57.

Polynôme primitif (1) Un polynôme est irréductible sur A si et seulement si il est irréductible et primitif sur le corps des fractions, corolaire 3.129.

Polynôme d'endomorphisme C'est la section 9.6.

Racines et factorisation (1) Si $\mathbb{A}$ est un anneau, la proposition 3.118 factorise une racine.

(2) Si $\mathbb{A}$ est un anneau, la proposition 3.123 factorise une racine avec sa multiplicité.

(3) Si $\mathbb{A}$ est un anneau, le théorème 3.125 factorise plusieurs racines avec leurs multiplicités.

(4) Le théorème 3.125 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 6.100.

(6) Le théorème 6.110 annule un polynôme de degré n ayant $n + 1$ racines distinctes.

(7) La proposition 6.184 nous annule un polynôme à plusieurs variables lorsqu'il a trop de racines.

(8) En analyse complexe, le principe des zéros isolés 17.139 annule en gros toute série entière possédant un zéro non isolé.

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

Thème 20 : polynôme d'endomorphismes

(1) Endomorphismes cycliques et commutant dans le cas diagonalisable, proposition 9.293.
(2) Racine carrée d'une matrice hermitienne positive, proposition 13.27.
(3) Théorème de Burnside sur les sous-groupes d'exposant fini de $\mathrm{GL}(n,\mathbb{C})$, théorème 9.305.
(4) Décomposition de Dunford, théorème 9.257.
(5) Algorithme des facteurs invariants 4.111.

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

(1) Définition du dual, 4.123.
(2) Le dual d'un espace de Banach est de Banach, proposition 7.243.
(3) Définition de la base duale 4.124.
(4) $\dim(E) = \dim(E^*)$, lemme 4.124.
(5) Base préduale (existence, unicité) : proposition 4.128.
(6) Théorème de représentation de Riez 27.165 : $L^p = (L^q)'$, et en particulier $L^\infty = (L^1)'$.
(7) Il n'est pas vrai que $(L^\infty)' = L^1$, voir la proposition 27.211.
(8) Dans un espace de Banach [8], $\|x\| = \max_{\substack{\varphi\in E'\\ \|\varphi\|=1}} |\varphi(x)|$, proposition 27.153.

Dual topologique et algébrique Ils sont définis par 4.123. 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 7.313.

Nous comparons les topologies faibles et de la norme en la section 11.15.

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 9.130.
(2) Le théorème de représentation de Riesz 25.18 pour les espaces de Hilbert.
(3) La proposition 27.163 pour les espaces $L^p\big([0,1]\big)$ avec $1 < p < 2$.
(4) Le théorème de représentation de Riesz 27.165 pour les espaces L^p en général.

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

Thème 22 : injections

(1) L'espace de Sobolev $H^1(I)$ s'injecte de façon compacte dans $C^0(\bar{I})$, proposition 31.6.
(2) L'espace de Sobolev $H^1(I)$ s'injecte de façon continue dans $L^2(I)$, proposition 31.6.
(3) L'espace $L^2(\Omega)$ s'injecte continument dans $\mathscr{D}'(\Omega)$ (les distributions), proposition 30.28.

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

(1) Le plus souvent lorsque nous parlons de mesure est que nous parlons de mesure positive, définition 14.18 sur un espace mesuré avec une tribu, définition 14.1.
(2) Une mesure extérieure est la définition 14.10
(3) Une algèbre de partie : définition 14.13. Une mesure sur une algèbre de parties : définition 14.11. 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 14.77.
(4) Un λ-système : définition 14.30.

8. Espace de Banach, définition 7.241.

(5) Une mesure complexe : définition 14.232.

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

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

Voir les points 14.117 et 14.162 pour les conventions à ce propos.

À propos d'applications mesurables :

(1) Définition d'une application mesurable, définition 14.42.

(2) Une fonction continue est borélienne, théorème 14.53.

(3) Si les f_n sont mesutables (au sens des boréliens), alors $\sup_n f_n$ est mesurable, lemme 14.97.

À propos de tribu induite :

(1) Définition 14.8.

(2) Les boréliens induits sont bien les boréliens de la topologie induite : $\mathcal{B}\text{or}(Y) = \mathcal{B}\text{or}(X)_Y$, théorème 14.54.

Tribu engendrée.

(1) Tribu engendrée par des parties, définition 14.4.

Thème 24 : théorie de la mesure

Mesure À propos de mesure.

(1) Tribu des boréliens, définition 14.47.

(2) Mesure positive, mesure finie et σ-finie, c'est la définition 14.18.

(3) Le produit de tribus est donné par la définition 14.124,

(4) Produit d'une mesure par une fonction, définition 14.205.

(5) le produit d'espaces mesurés est donné par la définition 14.240.

(6) Mesure de Lebesgue sur $\mathbb{R}$, définition 14.139.

(7) Une partie de $\mathbb{R}$ non mesurable au sens de Lebesgue : l'exemple 14.153.

(8) Mesure de Lebesgue sur $\mathbb{R}^N$, définition 14.242.

(9) Mesure à densité, définition 14.205.

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 14.115 dit qu'il existe une suite croissante de fonctions étagées qui converge vers f.

(2) Les fonctions simples sont denses dans L^p, proposition 27.47.

(3) Encadrement d'un borélien A par un fermé F et un ouvert V par le lemme 14.83 : $F \subset A \subset V$ avec $\mu(V \backslash F) < \epsilon$.

(4) Approximation L^p de la fonction caractéristique d'un borélien par une fonction continue par le théorème 14.235.

Produit (1) La tribu produit, définition 14.124.

(2) La mesure produit, définition 14.239.

Thème 25 : normes

Définitions (1) Espace vectoriel normé : définition 7.146.

(2) Produit scalaire, définition 9.162.

(3) Norme associée à un produit scalaire (cas réel), théorème 11.1.

(4) Norme associée à une forme sesquilinéaire (cas complexe), proposition 10.104.

(5) Produit scalaire sur $\mathbb{R}^n$, définition 9.167. Norme sur $\mathbb{R}^n$, définition 11.3.

(6) Forme hermitienne sur $\mathbb{C}^n$, définition 9.177. Norme sur $\mathbb{C}^n$, définition 10.105.

(7) La proposition 11.41 donne les normes $\|x\|_1$, $\|x\|_2$ et $\|x\|_\infty$ sur $\mathbb{R}^n$.

(8) Sur $\mathbb{R}^n$, la proposition 17.108 dit que $\|x\|_p$ est une norme.

Topologie (1) Métrique associée à une norme $d(x,y) = \|x-y\|$, définition 7.151.

(2) La topologie d'un espace vectoriel normé est la topologie métrique du théorème 7.108.

(3) Les boules sont les boules métrique définies en (7.97).

Inégalités (1) En général pour les normes $\|.\|_p$, il y a des inégalités dans 17.109 et 17.101.

(2) La proposition 17.114 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 11.43.

(2) La proposition 11.44 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 11.46.

Autres (1) Montrer que le problème $a-b$ est stable dans l'exemple 34.27.

(2) La proposition 12.114 donnant $\rho(A) \leqslant \|A\|$ utilise l'équivalence de toutes les normes sur un espace vectoriel de dimension finie (théorème 11.46.).

(3) La norme $x \mapsto \|x\|$ est une application continue, proposition 7.154.

Norme opérateur et d'algèbre voir le thème 39.

Thème 26 : inégalités Dans $\mathbb{C}$ nous avons $|a+b| \leqslant |a| + |b|$ par la proposition 10.95(6).

Inégalité de Young Nous avons

$$ab \leqslant \frac{a^p}{p} + \frac{b^q}{q} \tag{-2.1}$$

par la proposition 27.30.

Inégalité de Jensen (1) Une version discrète pour $f\big(\sum_i \lambda_i x_i\big)$, la proposition 17.105.

(2) Une version intégrale pour $f\big(\int \alpha d\mu\big)$, la proposition 27.31.

(3) Une version pour l'espérance conditionnelle, la proposition 36.72.

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

(1) Hölder pour L^p : $\|fg\|_1 \leqslant \|f\|_p\|g\|_q$, proposition 27.33.

(2) Hölder pour ℓ^p : $\|x\|_q \leqslant n^{\frac{1}{q}-\frac{1}{p}}\|x\|_p$, proposition 17.114.

(3) $\|x\|_\infty \leqslant \|x\|_p \leqslant n^{1/p}\|x\|_\infty$, théorème 17.109

(4) $\|x\|_p \leqslant n^{1/p}\|x\|_q$, corolaire 17.110.

Inégalité de Minkowsky (1) Pour une forme quadratique[9] q sur $\mathbb{R}^n$ nous avons $\sqrt{q(x+y)} \leqslant \sqrt{q(x)} + \sqrt{q(y)}$. Proposition 11.10.

(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 27.38.

9. Définition 9.120.

(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 27.40.

Transformée de Fourier Pour tout $f \in L^1(\mathbb{R}^n)$ nous avons $\|\hat{f}\|_\infty \leqslant \|f\|_1$, lemme 29.12.

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 27.60.

Thème 27 : constructions topologiques

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

(1) La définition de la topologie produit est 7.15.

(2) Pour les espaces vectoriels normés, le produit est donné par la définition 7.202.

(3) L'équivalence entre la topologie de la norme produit et la topologie produit est le lemme 7.202.

(4) Quand V et W sont des espaces métriques, la topologie considérée sur $V \times W$ est celle de la définition 7.202. C'est à la fois la topologie de la norme produit et la topologie produit.

(5) La convergence dans un espace vectoriel est si et seulement si il y a convergence composante par composante, proposition 7.59.

(6) Dans le cas d'espaces normés, la topologie produit est la même que celle de la norme produit, lemme 7.203.

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 7.24.

(2) Si X est un espace vectoriel normé, la topologie induite est celle de la norme restreinte : lemme 7.112.

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

(1) La topologie quotient est définie en 7.43.

(2) Si X est vectoriel normé, la topologie sur $X/\sim$ est aussi donnée par une norme quotient de la définition 7.310. La proposition 7.312 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 7.39.

Thème 28 : espaces métriques, normés

(1) Un espace métrique est un ensemble muni d'une distance, définition 7.106.

(2) La distance entre un point et un ensemble est la définition 7.138.

(3) Le théorème-définition 7.108 donne la topologie sur un espace métrique en disant que les boules ouvertes sont une base de la topologie (définition 7.2).

(4) La définition de la convergence d'une suite est la définition 7.13.

(5) Dans un espace vectoriel normé, une application est continue si et seulement si elle est bornée, proposition 11.62.

(6) Un espace vectoriel topologique [10] qui possède en tout point une base dénombrable de topologie accepte une distance, théorème 7.253.

Thème 29 : limite et continuité

(1) Limite d'une fonction en un point : définition 7.101. Il n'y a pas unicité en général comme le montre l'exemple 7.53 dans un espace non séparé.

(2) Caractérisation de la limite dans $\mathbb{R}$, proposition 12.1.

(3) Unicité de la limite d'une suite dans un espace séparé : proposition 7.56. Unicité de la limite d'une fonction, toujours dans le cas d'un espace séparé : proposition 7.104.

(4) La proposition 7.316 donne l'unicité de la limite dans le cas des espaces duaux pour la topologie $*$-faible. La proposition 7.104 nous dira qu'il y a unicité dès que l'espace d'arrivée est séparé.

(5) Définition de la continuité d'une fonction en un point et sur une partie de l'espace de départ : définition 7.32.

(6) Continuité sur une partie si et seulement si continue en chaque point, c'est le théorème 7.180.

(7) Voir l'exemple 12.57 traité en détail pour la (non) continuité d'une fonction qui fait un saut en un point.

(8) La fonction $f(x,y) = x + y$ est continue, lemme 10.29.

Thème 30 : intégration À propos d'intégration.

L'ordre dans lequel les choses sont faites — Nous commençons par considérer des fonctions $f\colon \Omega \to [0,+\infty]$ dans la définition 14.163.

— Nous donnerons ensuite quelques propriétés restreintes aux fonctions à valeurs positives, par exemple

(1) La convergence monotone 14.173,

(2) Lemme de Fatou 14.177.

(3) (presque) linéarité pour les fonctions positives, théorème 14.178.

— La définition pour les fonctions à valeurs dans $\mathbb{R}$ puis $\mathbb{C}$ est 14.181.

— Pour les fonctions à valeurs dans un espace vectoriel, c'est la définition 14.190.

primitive et intégrale (1) La définition 14.270 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 14.283.

Quelque résultats (1) Intégrale associée à une mesure, définition 14.163

(2) L'existence d'une primitive pour toute fonction continue est le théorème 12.431.

(3) La définition d'une primitive est la définition 12.201.

(4) Primitive et intégrale, proposition 14.271.

(5) Intégrale impropre, définition 14.283.

Intégrale et mesure (1) L'intégrale de la fonction 1 donne la mesure : $\int_B 1 d\mu = \mu(B)$, c'est le lemme 14.170.

(2) Le théorème de Radon-Nikodym 14.228 donne une densité pour certaines mesures.

10. Définition 7.158.

(3) Le produit d'une mesure par une fonction donnée par la définition 14.205 introduit aussi une densité : $(w \cdot \mu)(A) = \int_A w d\mu$.

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 14.187.

(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 14.203 et 14.204.

Thème 31 : connexité

(1) Définition 7.63

(2) L'image d'un connexe par une fonction continue est connexe, lemme 7.193.

(3) Connexité par arcs, définition 10.59.

(4) Si U est connexe et si $U \subset S \subset \bar{U}$, alors S est connexe, proposition 7.68.

(5) Une partie de $\mathbb{R}^2$ qui est connexe, mais pas connexe par arcs, proposition 21.56.

(6) Une partie de $\mathbb{R}$ est connexe si et seulement si elle est un intervalle, proposition 10.50.

(7) Le groupe $\mathrm{SL}(n, \mathbb{K})$ est connexe par arcs, proposition 13.18.

(8) Le groupe $\mathrm{GL}(n, \mathbb{C})$ est connexe par arcs, proposition 13.19.

(9) Le groupe $\mathrm{GL}(n, \mathbb{R})$ a exactement deux composantes connexes par arcs, proposition 13.20.

(10) Le groupe $\mathrm{O}(n, \mathbb{R})$ n'est pas connexe, lemme 13.15.

(11) Les groupes $\mathrm{U}(n)$ et $\mathrm{SU}(n)$ sont connexes par arcs, lemme 13.16.

(12) Pour tout $n \geqslant 2$, le groupe $\mathrm{SO}(n)$ est connexe, le groupe $\mathrm{O}(n)$ a deux composantes connexes, proposition 13.4.

(13) Connexité des formes quadratiques de signature donnée, proposition 17.120.

(14) Dans un espace vectoriel normé, les connexes par arcs sont connexes par arcs C^1, proposition 15.6.

Thème 32 : compacts

Propriétés générales Quelques propriétés de compacts.

(1) La définition d'un ensemble compact est la définition 7.73.

(2) Ne pas confondre le compactifié d'Alexandrov 7.97 avec la droite réelle achevée 12.27.

(3) 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 7.95.

(4) Un fermé dans un compact est compact, lemme 7.90

(5) Dans un espace Hausdorff[11], les compacts sont fermés, 7.90(2).

(6) Un espace est compact si et seulement si toute intersection finie de fermé est non vide, théorème 7.100.

(7) Tout compact d'un espace topologique séparé est fermé, lemme 7.90(2).

(8) Dans un espace vectoriel réel de dimension finie, les compacts sont les fermés bornés par le théorème 10.24.

(9) Le théorème de Borel-Lebesgue 10.19 dit qu'un intervalle[12] de $\mathbb{R}$ est compact si et seulement si il est de la forme $[a, b]$.

(10) Théorème des fermés emboîtés dans le cas compact, corolaire 7.87. À ne pas confondre avec celui dans le cas des espaces métrique, théorème 7.270.

(11) L'image d'un compact par une fonction continue est un compact, théorème 7.195.

11. Hausdorff, définition 7.54.
12. Définition 1.20.

(12) Si $f\colon K \to X$ est une bijection continue, sa réciproque est continue, lemme 7.197.

(13) Suites dans un compact

(13a) Toute suite dans un compact admet une sous-suite convergente, théorème 7.261.

(13b) Dans $\mathbb{R}^n$, toute suite dans un compact admet une sous-suite convergente, théorème 10.53. 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.

(13c) Un espace métrique est compact si et seulement si toute suite contient une sous-suite convergente. C'est le théorème de Bolzano-Weierstrass 7.134. La démonstration de ce théorème est indépendante.

(14) Une fonction continue sur un compact est bornée et atteint ses bornes, théorème 7.136.

(15) Une fonction continue sur un compact y est uniformément continue, théorème de Heine 12.81.

(16) Une bijection continue $f\colon K \to X$ entre un compact et un séparé est un isomorphisme, 7.196.

Produits de compacts À propos de produits de compacts. C'est un compact dans tous les cas métriques [13].

(1) Les produits d'espaces métriques compacts sont compacts. Il s'agit du théorème de Tykhonov que nous verrons ce résultat dans les cas suivants.

— $\mathbb{R}$, lemme 10.21.

— Produit fini d'espaces métriques compacts, théorème 7.286.

— Produit dénombrable d'espaces métriques compacts, théorème 7.288.

Composante connexe À propos de composantes connexes et de compacts.

(1) Si K est compact dans $\mathbb{C}$, alors la partie $\mathbb{C}\backslash K$ possède exactement une composante connexe non bornée. Lemme 26.49.

Thème 33 : densité

(1) Densité de $\mathbb{Q}$ dans $\mathbb{R}$, proposition 10.16.

(2) Densité des polynômes dans $\left(C^0([0,1]), \|.\|_\infty\right)$, théorème de Bernstein 36.168, ou une conséquence de Stone-Weierstrass 12.425.

(3) Densité des polynômes dans $\left(C^0(I), \|.\|_\infty\right)$ lorsque $I = [a,b]$, corolaire 36.169.

(4) Densité de $\mathscr{D}(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$ pour $1 \leqslant p < \infty$, théorème 27.50.

(5) Densité de $\mathscr{S}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 31.15.

(6) Densité de $\mathscr{D}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 31.17.
Cela est utilisé pour le théorème de trace 31.19.

(7) Les applications étagées dans les applications mesurables (qui plus est avec limite croissante), théorème fondamental d'approximation 27.53.

(8) Les fonctions continues à support compact dans $L^2(I)$, théorème 27.54.

(9) Les polynômes trigonométriques sont denses dans $L^p(S^1)$ pour $1 \leqslant p < \infty$. Deux démonstrations indépendantes par le théorème 28.8 et le théorème 27.74.

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 17.130.

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

13. Si vous connaissez des exemples non métriques de produits de compacts qui ne sont pas compacts, écrivez-moi.

— Le lemme 12.421 le donne pour la racine carré.

— Le théorème 12.427 donne la densité des polynômes dans les fonctions continues sur un compact.

— Le théorème 12.424 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 12.425 donne le même résultat pour la densité dans $C(X, \mathbb{C})$.

— Le lemme 28.1 est une version pour les polynômes trigonométriques.

— Le lemme 12.421 est un cas particulier du théorème 12.427, mais nous en donnons une démonstration indépendante afin d'isoler la preuve de la généralisation 12.425. Une version pour les polynômes trigonométriques sera donnée dans le lemme 28.1.

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 27.91.

Thème 34 : application réciproque

(1) Définition 7.187.

(2) Dans le cas des réels, des exemples sont donnés en 10.9.

(3) Continuité, théorème de la bijection 12.54.

(4) Continuité de la réciproque pour $f : K \to X$, lemme 7.197.

(5) Si f est strictement monotone sur un intervalle, son inverse est continue, théorème de la bijection 12.54.

(6) Théorème de la bijection 12.54 (qui contient aussi de la continuité).

(7) Dérivabilité, proposition 12.180.

(8) Une application continue est injective si et seulement si elle est strictement monotone, lemme 12.51.

Thème 35 : applications continues et bornées

(1) Application continue, définition 7.32.

(2) Une application linéaire non continue : exemple 11.63 de $e_k \mapsto ke_k$. Les dérivées partielles sont calculées en (25.156).

(3) La dérivation sur les polynômes (exemple 11.64) donne un autre exemple d'application linéaire non continue.

(4) Une application linéaire est bornée si et seulement si elle est continue, proposition 11.62.

(5) Une forme sesquilinéaire est bornée si et seulement si elle est continue, proposition 25.2.

Thème 36 : suite de Cauchy, espace complet Nous parlons d'espaces topologiques complets. À ne pas confondre avec un espace mesuré complet, définition 14.65.

(1) Corps complet : définition 1.367(5), espace métrique complet : définition 7.239.

(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 17.134.

(3) La définition 7.238 donne la notion de suite de Cauchy dans un espace métrique.

(4) La définition 7.236 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 7.242.

(6) La proposition 7.244 donne l'équivalence entre les suites de Cauchy et les suites τ-Cauchy dans le cas des espaces vectoriels topologiques *normés*.

(7) L'exemple 7.242 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 17.138 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 7.258(2).

(10) Toute suite convergente dans un espace métrique est de Cauchy, proposition 7.245.

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 7.258.

(2) Les complexes $\mathbb{C}$, proposition 7.260.

(3) Un espace vectoriel normé sur un corps complet est complet, proposition 7.264.

(4) La proposition 12.366 donne quelques espaces complets. Soit X un espace topologique métrique, (Y, d) un espace métrique complet. Alors les espaces

(4a) $\left(C_b^0(X,Y), \|.\|_\infty\right)$

(4b) $\left(C_0^0(X,Y), \|.\|_\infty\right)$

(4c) $\left(C_0^k(X,Y), \|.\|_\infty\right)$

sont complets.

(5) Le lemme 12.367 dit que $\left(C^0(A,B), \|.\|_\infty\right)$ 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 que pour la topologie métrique (qui sont les mêmes). C'est la proposition 30.21.

(7) L'espace $\mathscr{S}(\Omega)$ est complet et métrisable par la proposition 30.72.

(8) L'espace $L^p(\Omega, \mathcal{A}, \mu)$ par le théorème 27.43.

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 12.427 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 $\left(C^p(X,Y), \|.\|_\infty\right)$ soit complet en général.

Thème 37 : caractérisations séquentielles Diverses caractérisations séquentielles.

continuité (1) Fonction séquentiellement continue, définition 7.183. Dans un espace métrisable séparé, la continuité séquentielle est équivalente à la continuité, proposition 7.231.

(2) La continuité implique la continuité séquentielle, proposition 7.185 et corolaire 7.127.

(3) Une version spéciale pour $\mathbb{R}^m$ est donnée par le théorème 12.222.

fermeture Fermeture séquentielle, proposition 7.228.

Compacité Un espace topologique séquentiellement compact : toute suite possède une sous-suite convergente, définition 7.83.

Thème 38 : valeurs propres, définie positive

À propos de valeurs propres (1) Définition des valeurs propres d'une forme quadratique : définition 9.246.

(2) Définition de valeur propre et vecteur propre pour un endomorphisme $f : V \to V$, définition 9.80.

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 9.121.

(2) Un opérateur ou une matrice est défini positif si toutes ses valeurs propres sont positives, c'est la définition 9.222.

(3) Pour une matrice symétrique, définie positive si et seulement si $\langle Ax, x\rangle > 0$ pour tout x. C'est le lemme 9.226.

(4) Une application linéaire est définie positive si et seulement si sa matrice associée l'est. C'est la proposition 9.227.

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

Thème 39 : norme matricielle, norme opérateur et rayon spectral Quelques définitions

(1) Définition de la norme opérateur : définition 11.51.

(2) Définition du rayon spectral 11.57.

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 12.120 assure que $\|A\|_2 = \sqrt{\rho(A^tA)}$.

(2) Lien entre valeurs propres et norme opérateur : le lemme 12.121 pour les matrices symétriques strictement définies positives donne $\|A\|_2 = \lambda_{max}$.

(3) Pour une matrice diagonale, $\|D\|_2 = \max\{|\lambda_i|\}$, lemme 12.122.

(4) Pour toute norme algébrique nous avons $\rho(A) \leqslant \|A\|$, proposition 12.114.

(5) Dans le cadre du conditionnement de matrice. Voir en particulier la proposition 34.110 qui utilise le théorème 12.120.

(6) Rayon spectral et convergence de méthode itérative, proposition 34.148.

Pour la norme opérateur nous avons les résultats suivants.

(1) La majoration $\|Au\| \leqslant \|A\|\|u\|$ est le lemme 11.59.

(2) Définition d'une algèbre : 1.340 et pour une norme d'algèbre : 11.56.

(3) La norme opérateur est une norme d'algèbre, lemme 11.61.

(4) Pour des espaces vectoriels normés, être borné est équivalent à être continu : proposition 11.62.

(5) Le lemme à propos d'exponentielle de matrice 15.152 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 11.212.

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 40.

Thème 40 : série de matrices

(1) Rayon spectral et norme opérateur : thème 39.

(2) Exponentielle de matrices : thème 49.

(3) Série entière de matrices : section 15.13.

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

- Pour un espace de Banach : proposition 11.252.
- Pour les matrices nilpotentes : proposition 9.206.
- En lien avec le rayon spectral (si et seulement si $\rho(A) < 1$) dans la proposition 15.148.
- Le lemme 15.47 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 34.168 pour prouver qu'une M-matrice irréductible vérifie $A^{-1} > 0$.

Thème 41 : décomposition de matrices

(1) Décomposition de Bruhat, théorème 13.39.

(2) Décomposition de Dunford, théorème 9.257.

(3) Décomposition polaire 13.32 des matrices symétriques et la proposition 17.60 pour la régularité.

Thème 42 : systèmes d'équations linéaires

— Algorithme des facteurs invariants 4.111.

— 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 17.116 pour l'existence et 17.117 pour la méthode.

Thème 43 : réduction, diagonalisation Des résultats qui parlent diagonalisation

(1) Définition d'un endomorphisme diagonalisable : 9.207.

(2) Conditions équivalentes au fait d'être diagonalisable en termes de polynôme minimal, y compris la décomposition en espaces propres : théorème 9.211.

(3) Diagonalisation simultanée 9.214, pseudo-diagonalisation simultanée 11.37.

(4) Diagonalisation d'exponentielle 15.130 utilisant la décomposition de Dunford.

(5) Décomposition polaire théorème 13.32. $M = SQ$, S est symétrique, réelle, définie positive, Q est orthogonale.

(6) Décomposition de Dunford 9.257. $u = s + n$ où s est diagonalisable et n est nilpotent, $[s, n] = 0$.

(7) Réduction de Jordan (bloc-diagonale) 9.287.

(8) L'algorithme des facteurs invariants 4.111 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 9.219. Via le lemme de Schur complexe 12.100.

(2) Théorème spectral autoadjoint (c'est le même, mais vu sans matrices), théorème 11.6

(3) Théorème spectral hermitien, lemme 11.18.

(4) Théorème spectral, matrice normales, théorème 12.102.

Pour les résultats de décomposition dont une partie est diagonale, voir le thème 41 sur les décompositions. Réduction de quadriques :

(1) Réduction de Gauss, théorème 9.233.

Trigonalisation.

(1) Le lemme de Schur complexe 12.100 dit que toute matrice est unitairement équivalente à une matrice triangulaire suppérieure.

Thème 44 : déterminant

(1) Déterminant d'une matrice : définition 4.76.

(2) Déterminant d'un endomorphisme 9.9.

(3) Le lemme 11.5 donne la formule $\det(f) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} \langle e_{\sigma(i)}, f(e_i) \rangle$.

(4) Principales propriétés algébriques du déterminant : la proposition 9.10.

(5) La formule $\det(AB) = \det(A)\det(B)$ est la proposition 9.241 pour des matrices et la proposition 9.10(1) pour les applications linéaires.

(6) Déterminant et manipulations de lignes et colonnes, section 4.3.10 et les propositions qui précèdent à partir du lemme 4.78 qui dit que $\det(A) = \det(A^t)$.

(7) Les n-formes alternées forment un espace de dimension 1, proposition 9.4.

(8) Déterminant d'une famille de vecteurs 9.5.

(9) Calcul d'un déterminant de taille 2×2 : équation (4.99).

(10) Interprétations géométriques

(10a) À propos d'orthogonalité, le déterminant est très lié au produit vectoriel en dimension 3. Et il le généralise en dimension supérieure.

i. Liaison au produit vectoriel (orthogonalité) dans la proposition 11.34.

ii. En particulier le lemme 11.35 nous dit comment un déterminant donne un vecteur orthogonal à une famille donnée de vecteurs.

(10b) Déterminant et aires, volumes

i. Déterminant et mesure de Lebesgue : théorème 14.289.

ii. Aire du parallélogramme : il y a la formule avec le produit vectoriel dans la proposition 18.55, mais l'aire proprement dite, avec une intégrale est dans la proposition 20.31.

iii. Volume du parallélépipède avec le produit mixte et le déterminant 3×3, 18.56.

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 (20.202) : $dS = \|T_u \times T_v\|$ qui est la norme du produit vectoriel des vecteurs tangents au paramétrage.

Nous voyons dans l'équation (20.199) 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.

(11) Le déterminant de Vandermonde est à la proposition 9.12. Il est utilisé à divers endroits :

(11a) Pour prouver que u est nilpotente si et seulement si $\mathrm{Tr}(u^p) = 0$ pour tout p (lemme 9.203)

(11b) Pour prouver qu'un endomorphisme possédant $\dim(E)$ valeurs propres distinctes est cyclique (proposition 9.293).

Thème 45 : espaces de fonctions En ce qui concerne les densités, voir le thème 33.

(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.

(1) La topologie des seminormes est la définition 7.298.

(2) La définition 30.14 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 30.24.

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 27.76.

(2) Le produit scalaire [14] $\langle f, g\rangle$ est donné en (27.429) et la base trigonométrique est (27.430).

14. Produit scalaire, définition 9.162.

(3) La densité des polynômes trigonométriques dans $L^p(S^2)$ est le théorème 27.74 ou le théorème 28.8, au choix.

(4) Une conséquence de cette densité est que le système trigonométrique est une base hilbertienne[15] de L^2 par le lemme 27.117.

L'espace L^2 est discuté en analyse fonctionnelle, dans la section 27.5 et les suivantes parce que l'étude de L^2 utilise entre autres l'inégalité de Hölder 27.33.

Le fait que L^2 soit un espace de Hilbert est utilisé dans la preuve du théorème de représentation de Riesz 27.163.

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 27.44.

Thème 46 : fonctions Lipschitz

(1) Définition : 12.327.

(2) La notion de Lipschitz est utilisée pour définir la stabilité d'un problème, définition 34.26.

(3) Toute fonction Lipschitz est uniformément continue, proposition 12.332.

Thème 47 : suites et séries

Suites La proposition 10.26 donne une caractérisation de limite de suite dans un espace vectoriel normé.

(1) Les suites adjacentes, c'est la définition 10.37.

(2) Les séries alternées, théorème 11.129. 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 15.99 et ce qui l'entoure.

(4) La définition de la convergence absolue est la définition 11.83.

(5) Une suite réelle croissante et majorée converge, proposition 10.33.

(6) Toute suite dans un compact admet une sous-suite convergente, théorème 7.261.

(7) Pour tout réel, il existe une suite croissante de rationnels qui y converge, proposition 10.17.

Produit de Cauchy (1) Dans une algèbre normée, proposition 11.97,

(2) Dans $\mathbb{C}$, théorème 15.32.

Calcul de suites (1) Somme : $x_n + y_n \to x + y$ est la proposition 10.28.

Série Les séries sont en général dans la section 11.7.

(1) Quelques séries usuelles en 11.9.3 : 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 11.93.

(1b) La série harmonique diverge : $\sum_k \frac{1}{k} = \infty$, exemple 11.122.

(1c) La série géométrique : $\sum_{k=0}^{N} q^k = \frac{1-q^{N+1}}{1-q}$, proposition 11.124.

(1d) Une autre cool série : $\sum_{k=1}^{N} \frac{1}{k(k+1)} = \frac{N}{N+1}$, lemme 11.128.

(2) Critère des séries alternées, théorème 11.129.

(3) Convergence d'une série implique convergence vers zéro du terme général, proposition 11.91.

(4) Dans une algèbre normée : $(\sum_{k=0}^{\infty} a_k)b = \sum_{k=0}^{\infty}(a_k b)$, proposition 11.96.

(5) Produit de Cauchy : théorème 15.32 et proposition 11.97.

15. Définition 25.27.

Sommes infinies En ce qui concerne les sommes finies, la notation $\sum_{i=1}^{N}$ est définie en 1.82. Pour permuter les termes d'une somme avec un élément du groupe symétrique, nous avons la proposition 1.303.

Voici quelques résultats à propos de sommes infinies.

(1) Une somme indexée par un ensemble quelconque est la définition 11.101.

(2) La proposition 11.105 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 11.80.

(4) Une somme de termes positifs indexée par un ensemble indénombrable est toujours infinie par le lemme 11.111.

(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 11.99).

(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 11.116.

Série entières (1) Rayon de convergence, définition 15.12.

(2) Convervence absolue à l'intérieur du rayon de convergence, lemme d'Abel 15.18.

(3) 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 15.42.

(4) 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 15.47.

Thème 48 : suite de fonctions

(1) Une limite uniforme de fonctions continues est continue, proposition 12.365.

(2) Sous certaines hypothèses, si $f_i \to f$, alors $f_i' \to f'$, théorème 12.381.

(3) Si les f_k sont continues et si la convergence $\sum_k f_k$ est uniforme, alors la somme est continue, théorème 12.377.

Thème 49 : 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 15.59.

— Nous démontrons qu'elle vérifie l'équation différentielle $y' = y$, $y(0) = 1$ (théorème 15.75).

— 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 15.81).

— Les fonctions trigonométriques (sinus et cosinus) sont définies par leurs séries. Il est alors montré que $e^{ix} = \cos(x) + i\sin(x)$ (lemme 18.11).

Propriétés

— La formule $a^{-x} = 1/a^x$ est la proposition 12.405(3).

— $\exp(x) = e^x$, proposition 15.78.

— Nous avons l'encadrement $2.5 < e < 3$, lemme 15.79.

— Le nombre e est irrationnel, proposition 15.80.

Complexes (1) La définition de $\exp(a + ib)$ est la définition 15.59.

(2) Les principales propriétés, dont $e^{z+w} = e^z e^w$, sont dans la proposition 18.9.

(3) Nous avons $e^{ix} = e^{iy}$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $y = x + 2k\pi$, corolaire 18.24.

(4) Le fait que $e^{i\theta}$ donne tous les nombres complexes de norme 1 est la proposition 18.61.

(5) Le groupe des racines de l'unité est donné par l'équation (19.1).

Algèbre normée commutative Pour la définition c'est la proposition 15.59 et pour la régularité C^∞ c'est la proposition 15.64.

Idem non commutatif Il y a une tentative de théorème 15.65, 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 15.69.

(2) Si A est une matrice, alors $(e^tA)'(u) = Ae^{uA}$, proposition 15.71.

(3) Les sections 11.14 et 15.5.3 parlent d'exponentielle de matrices.

(4) L'exponentielle donne lieu à une fonction de classe C^∞, proposition 15.149.

(5) Le lemme à propos d'exponentielle de matrice 15.152 donne :

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

(6) La proposition 15.130 : 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 15.13.3 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 32.6.1.

(9) La proposition 15.129 dit que l'exponentielle est surjective sur $\mathrm{GL}(n, \mathbb{C})$.

(10) La proposition 11.255 : si u est un endomorphisme, alors $\exp(u)$ est un polynôme en u.

(11) Calcul effectif : sous-section 15.13.4.

(12) Proposition 13.23 : 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 15.146.

Paramétrisation du cercle (1) La proposition 18.63 dit que

$$\begin{aligned} \varphi\colon [0, 2\pi[&\to S^1 \\ t &\mapsto e^{it} \end{aligned} \tag{-2.2}$$

est un C^∞-difféomorphisme.

Thème 50 : logarithme

(1) Le logarithme pour les réels strictement positifs $\ln\colon]0, \infty[\to \mathbb{R}$ est donné en la définition 15.81 ; c'est l'application réciproque de exp.

(2) Les principales propriétés sont dans la proposition 15.84 : $\ln(xy) = \ln(x) + \ln(y)$ etc.

(3) Dérivée : $\ln'(x) = \frac{1}{x}$, proposition 15.83.

(4) La proposition 15.100 donne la série

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k. \tag{-2.3}$$

(5) L'exemple 20.153 donne l'encadrement $0.644 \leqslant \ln(2) \leqslant 0.846$.

(6) La proposition 15.129 dit que toute matrice complexe admet un logarithme. En particulier une série explicite est donnée pour le logarithme d'un bloc de Jordan [16].

(7) Sur les complexes, le logarithme $\ln\colon \mathbb{C}^* \to \mathbb{C}$ est la définition 26.29. 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 15.118.

(9) Détermination du logarithme le long d'un chemin dans $\mathbb{C}$, définition 26.45.

(10) Un logarithme continu d'une fonction, définition 26.44.

(11) Théorème de Borsuk 26.47 : 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 26.42.

(13) La proposition 26.58 dit qu'une application f a un logarithme continu si et seulement si $\mathrm{Ind}(f \circ \gamma, 0) = 0$.

Thème 51 : 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 1.200.

(2) a^n pour $n \in \mathbb{Z}$ en la définition 12.385.

(3) $a^{1/n}$ pour $n \in \mathbb{Z}$ en la définition 12.388.

(4) a^q pour $q \in \mathbb{Q}$ en la définition 12.388.

(5) $\sqrt[y]{x}$ en la définition 12.390.

(6) La fonction g_a est Cauchy-continue sur $\mathbb{Q}$, c'est la proposition 12.402.

(7) a^x pour $a > 0$ et $x \in \mathbb{R}$ en la définition 12.404.

(8) a^z pour $a > 0$ et $z \in \mathbb{C}$ en la définition 18.5.

Quelques propriétés (1) Pour tout $q \in \mathbb{Q}$, il y a un $\sqrt{q}$ dans $\mathbb{R}$, proposition 1.455.

(2) Pour $a > 0$ et $x, y \in \mathbb{R}$ nous avons $a^x a^y = a^{x+y}$, proposition 12.405.

(3) Si $a > 0$ et $x, y \in \mathbb{R}$ nous avons $(a^x)^y = (a^y)^x = a^{xy}$ par la proposition 12.415.

(4) Si $\alpha > 0$, alors $x \mapsto x^\alpha$ est strictement croissante pour $x \geqslant 0$, proposition 12.410.

(5) La formule $a^{-x} = 1/a^x$ est la proposition 12.405(3).

(6) La fonction puissance $g_a(x) = a^x$ est continue, proposition 12.405.

Croissance (1) La fonction puissance $f_\alpha(x) = x^\alpha$ est strictement croissante pour les $x > 0$, proposition 12.410

(2) La fonction puissance $g_a(x) = a^x$ est strictement croissante, proposition 12.405.

(3) $\lim_{x\to\infty} x^\alpha = \infty$, proposition 12.416.

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 12.414.

(2) La fonction a^x est dérivable et sa dérivée vérifie $g'_a(x) = g_a(x) g'_a(0)$, proposition 12.432.

16. Jordan, théorème 9.287.

(3) La formule de dérivation pour $x \mapsto x^q$ avec $q \in \mathbb{Q}$ est la proposition 12.442.

(4) La dérivation de $x \mapsto x^\alpha$ avec $\alpha \in \mathbb{R}$ est la proposition 14.280. 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 15.93).

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

$$f(x+y) = f(x)f(y) \tag{-2.4}$$

en la définition 12.434.

(1) L'équivalence entre l'équation fonctionnelle et l'équation différentielle est donnée par la proposition 12.440.

(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 12.434 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 12.444.

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 15.78).

— Définir $e = \exp(1)$.

— Définir, pour x irrationnel, $a^x = \exp(x\ln(a))$.

— Prouver que $e^x = \exp(x)$ pour tout x.

Thème 52 : 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 1.82.

(2) Si I est fini et si est à valeur dans un groupe commutatif, $\sum_{i\in I} f(i)$ est 1.302.

(3) Enfin si I est un ensemble quelconque, la définition 11.101 introduit la notion de famille sommable dans un espace vectoriel normé.

(4) 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 11.80.

(5) La somme au sens de Cesàro est la somme des moyennes partielles, définition 11.130.

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 supersomme[2].

Thème 53 : 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 12.452.
(2) Une majoration du reste est dans le théorème 15.53
(3) De classe C^2 sur $\mathbb{R}^n$, proposition 12.459.
(4) Avec un reste donné par un point dans $]x, a[$, proposition 12.463.
(5) Avec reste intégral, proposition 20.154 et théorème 20.151 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 12.172.
(7) Pour les fonctions holomorphes, il y a le théorème 26.76 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 (34.95).
(2) On utilise pas mal de Taylor dans les résultats liant extrémum et différentielle/hessienne. Par exemple la proposition 17.73.

Quelques développements Voici quelques développements limités à savoir. Ils sont calculables en utilisant la formule de Taylor-Young (proposition 12.468).

$$e^x = \sum_{k=0}^{n} \frac{x^k}{k!} + x^n\alpha(x) \qquad \text{ordre } n, \text{proposition 15.95}$$

$$\cos(x) = \sum_{k=0}^{p} \frac{(-1)^k x^{2k}}{(2k)!} + x^{2p+1}\alpha(x) \qquad \text{ordre } 2p+1, \text{proposition 18.77}$$

$$\sin(x) = \sum_{k=0}^{p} \frac{(-1)^k x^{2k+1}}{(2k+1)!} + x^{2p+2}\alpha(x) \qquad \text{ordre } 2p+1, \text{proposition 18.77}$$

$$\ln(1+x) = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k} x^k + \alpha(x)x^n \qquad \text{ordre } n, \text{proposition 15.98}$$

$$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k \qquad \text{exact proposition 15.100}$$

$$\ln(2) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} \qquad \text{exact proposition 15.100}$$

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

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

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.

Thème 54 : 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 12.325. 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 12.250. Pour rappel, la définition de la dérivation partielle est 12.231.

(3) La formule $f(a+\epsilon e_i) = f(a) + \epsilon(\partial_i f)(a) + \epsilon\alpha(\epsilon)$, proposition 12.251.

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

$$f'(c) = \frac{f(b)-f(a)}{b-a} \tag{-2.6}$$

est le théorème des accroissements finis proprement dit. C'est le théorème 12.195.

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

$$f(b) = f(a) + (b-a)(\partial_\beta f)(c) \tag{-2.7}$$

où $\beta = b-a$ est la proposition 12.249.

(6) La formule $f(a+h) = f(a) + hf'(a) + \alpha(h)$ pour une fonction $\mathbb{R} \to \mathbb{R}$ en le théorème 12.172.

(7) Une généralisation pour les intervalles non bornés : théorème 12.196.

(8) Espaces vectoriels normés, théorème 11.245

Thème 55 : dérivation

(1) Définition de la dérivée, définition 12.164.

(2) Dérivée de fonction composée, proposition 12.184 dans le cas réel.

(3) Dérivée partielle de fonction composée, théorème 12.313.

(4) $f(\lambda x)' = \lambda f'(x)$, lemme 12.178.

Thème 56 : différentiabilité

Généralités (1) La différentielle est définie en général pour des espaces vectoriels normés par la proposition 11.219

(2) Différentielle d'une application linéaire, lemme 11.227.

(3) Nous parlons de différentielle en dimension finie et donnons une interprétation géométrique en 12.22.1.

(4) La recherche d'extrémums d'une fonction sur $\mathbb{R}^n$ passe par la seconde différentielle, proposition 17.73.

(5) Lien entre différentielle seconde (hessienne) et convexité en la proposition 17.100 et le corolaire 17.101.

(6) La différentielle est liée aux dérivées partielles par les formules données au lemme 12.268

$$df_a(u) = \frac{\partial f}{\partial u}(a) = \frac{d}{dt}\Big[f(a+tu)\Big]_{t=0} = \sum_{i=1}^{m} u_i \frac{\partial f}{\partial x_i}(a) = \nabla f(a) \cdot u. \tag{-2.8}$$

Je ne vous cache pas que cette suite d'égalités est une de mes préférées.

Différentielle et dérivées partielles À propos de fonctions de classe C^k, définition 11.220.

(1) Une fonction est de classe C^1 si et seulement si ses dérivées partielles sont continues, théorème 12.306.

(2) Une fonction est C^n si et seulement si ses dérivées partielles sont C^{n-1}, c'est le théorème 12.341.

(3) Différentiabilité en un seul point si les dérivées partielles sont continues en ce point : proposition 12.304.

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 11.234 insiste sur des hypothèses locales.

(2) Le théorème 11.235 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.

Thème 57 : 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 Schauder a pour conséquence le théorème de Cauchy-Arzela 20.38 pour les équations différentielles.
(2) Le théorème de Schauder 20.37 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 17.42) sans la condition Lipschitz
(3) Le théorème de Cauchy-Lipschitz 17.42 est utilisé à plusieurs endroits :
   — Pour calculer la transformée de Fourier de $e^{-x^2/2}$ dans le lemme 29.22.
(4) Théorème de stabilité de Lyapunov 32.40.
(5) Le système proie-prédateur de Lotka-Volterra 32.41
(6) Équation de Schrödinger, théorème 32.48.
(7) L'équation $(x-x_0)^\alpha u = 0$ pour $u \in \mathscr{D}'(\mathbb{R})$, théorème 30.44.
(8) La proposition 32.43 donne un résultat sur $y''+qy=0$ à partir d'une hypothèse de croissance.
(9) Équation de Hill $y''+qy=0$, proposition 32.45.

Thème 58 : convexité

Fonctions convexes L'essentiel des résultats sur les fonctions convexes sont dans la section 17.11. On a surtout :

(1) Définition des fonctions convexes : 17.79 et 17.97 en dimension supérieure.
(2) En termes de différentielles, 17.98 pour la différentielle première et 17.101 pour la hessienne.
(3) Une courbe paramétrée convexe est la définition 21.91.
(4) L'enveloppe convexe d'une courbe fermée simple et convexe : 21.93.
(5) Courbure et convexité d'une courbe paramétrée : section 21.13.4.
(6) Une courbe paramétrée convexe est localement le graphe d'une fonction convexe par le lemme 21.92.
(7) La convexité est utilisée dans la méthode du gradient à pas optimal de la proposition 17.117.
(8) La fonction $t \mapsto t^p$ est strictement convexe sur les positifs dans le lemme 17.90.
(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 27.126.

En termes de parties convexes, on a :

Parties convexes (1) Définition 7.144 d'une partie convexe d'un espace vectoriel.
(2) Une boule est convexe, proposition 8.28.
(3) Un polygone convexe est défini en 18.170, et les racines de l'unité forment un polygone convexe par la proposition 18.171.

Thème 59 : espaces de Hilbert, base hilbertienne Beacoup de choses concerant les espaces L^2, et en particulier la base trigonométrique sont dans le thème 45.

(1) Toute partie orthonormale d'un espace de Hilbert est libre, proposition 25.24.
(2) Tout espace de Hilbert possède une base hilbertienne, proposition 25.37.
(3) Unicité de la décomposition dans une base hilbertienne, proposition 25.38.

Thème 60 : analyse complexe, fonctions holomorphes

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

$$df_{z_0}(z) = f'(z_0)z = (\partial_z f)(z_0)z \tag{-2.9}$$

par (12.856) et la proposition 26.4. Cela se résume par la formulation lapidaire $f' = \partial_z f$.
(2) Série de Laurent $f(z) = \sum_{n\in\mathbb{Z}} a_n z^n$, théorème 28.26.

Thème 61 : permuter des limites

Permuter des dérivées partielles Si une fonction est de classe C^2, le théorème de Schwarz 12.350 dit que

$$\partial_k \partial_l f = \partial_l \partial_k f. \tag{-2.10}$$

Fonctions définies par une intégrale Les théorèmes sur les fonctions définies par une intégrale, section 17.4. Nous avons entre autres

(1) $\partial_i \int_B f = \int_B \partial_i f$, avec B compact, proposition 17.27.

(2) Si f est majorée par une fonction ne dépendant pas de x, nous avons le théorème 17.15 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 Leibnitz

$$F'(a) = \int_\Omega \frac{\partial f}{\partial x}(a,\omega)d\mu(\omega) \tag{-2.11}$$

démontrée en le théorème 17.19.

Des variations avec des dérivées partielles et des différentielles sont dans 17.27 et dans 17.28.

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

$$F'(z) = \int_\Omega \frac{\partial f}{\partial z}(z,\omega)d\mu(\omega). \tag{-2.12}$$

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

$$(\partial^\alpha F)(x) = \int_\Omega (\partial^\alpha f_\omega)(a)d\mu(\omega) \tag{-2.13}$$

dans la proposition 17.21.

(6) Si l'intégrale est uniformément convergente, nous avons le théorème 17.16 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 26.64.

(8) En ce qui concerne le x dans la borne, le théorème 14.271 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 14.272 en est une conséquence.

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

$$T\big(x \mapsto (\partial_y^\alpha \phi)(x,y_0)\big) = \partial_y^\alpha \Big(T\big(x \mapsto \phi(x,y)\big)\Big)_{y=y_0}. \tag{-2.14}$$

C'est la proposition 30.48.

Limite et intégrale (1) Théorème de la convergence monotone, théorème 14.173.

(2) $\int \sum_n f_n = \sum_n \int f_n$ dans le corolaire 14.176.

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 [17]. Nous utilisons cette technique pour permuter une somme et une intégrale dans l'équation (26.297).

L'utilisation de Fubini pour permuter des intégrales (sur deux variables différentes) ou deux sommes est expliquée dans 14.298.

C'est par exemple utilisé pour permuter deux sommes dans le cadre des chaines de Markov en 38.8.

17. Mesure de comptage, définition 14.264.

— le théorème de Fubini-Tonelli 14.294 demande que la fonction soit mesurable et positive ;

— le théorème de Fubini 14.297 demande que la fonction soit intégrable (mais pas spécialement positive) ;

— le corolaire 14.296 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 12.381.

(2) Permuter limite et dérivées partielles, théorème 12.384.

(3) Permuter limite et différentielle, théorème 15.9.

Quelques remarques sur les techniques de démonstration.

(1) Le résultat fondamental 12.381 est démontré sans recourir à des intégrales. Une preuve alternative, plus courte, avec des intégrales est donnée en 14.279.

(2) Permuter limite et dérivée partielle, théorème 12.384.

(3) Permuter série et différentielle, théorème 15.9.

Somme et dérivée Permuter somme et différentielle, théorème 15.9.

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 14.18(2).

Thème 62 : 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 14.192 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 27.63.

(3) Et encore un pour L^p dans la proposition 27.168.

(4) Si $\int f\chi = 0$ pour tout χ à support compact alors $f = 0$ presque partout, proposition 30.1.

(5) 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 27.168.

(6) La proposition 27.21 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 17.2.

Dans le même ordre d'idées, si $f > 0$ et si $\mu(X) > 0$ alors $\int_X f > 0$ par le lemme 14.194.

Thème 63 : inversion locale, fonction implicite

(1) Théorème d'inversion locale dans un Banach : théorème 17.50.

(2) Fonction implicite dans un Banach : théorème 17.51.

(3) Utilisé pour montrer que le flot d'une équation différentielle est un C^p-difféomorphisme local, voir 32.36.

(4) Pour le théorème de Von Neumann 17.64.

Thème 64 : points fixes

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

Théorème de Picard 17.37 donne un point fixe comme limite d'itérés d'une fonction Lipschitz. Il aura pour conséquence le théorème de Cauchy-Lipschitz 17.42, l'équation de Fredholm, théorème 17.41 et le théorème d'inversion locale dans le cas des espaces de Banach 17.50.

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 20.35.

(1b) Dans $\mathbb{R}^n$ en version continue, en s'appuyant sur le cas C^∞ et en faisant un passage à la limite, théorème 20.36.

(1c) Dans $\mathbb{R}^2$ via l'homotopie, théorème 26.66. 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 [18].

Théorème de Markov-Kakutani 20.40 qui donne un point fixe à une application 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 20.37

(2) Pour les équations différentielles

(2a) Le théorème de Schauder a pour conséquence le théorème de Cauchy-Arzela 20.38 pour les équations différentielles.

(2b) Le théorème de Schauder 20.37 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 17.42) sans la condition 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 34.48.

— La convergence quadratique de la méthode de Newton est donnée par le théorème 34.54.

— En calcul numérique, section 34.5

— Méthode de Newton comme méthode de point fixe, sous-section 34.6.2.

(4) D'autres utilisations de points fixes.

— Processus de Galton-Watson, théorème 38.59.

— Dans le théorème de Max-Milgram 25.61, le théorème de Picard est utilisé.

Thème 65 : changement de variables Il n'existe rien en mathémaitque 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 14.290.

(2) Dans des limites, le lemme 7.163 donne $\lim_{x\to a} f(x) = \lim_{x\to b} f(x+a-b)$ si la limite existe.

(3) Dans une équation aux dérivées partielles, exemple 33.132.

(4) Limite de fonction composée $\lim_{x\to a}(f\circ g)$, propositions 7.164 et 7.165.

Thème 66 : techniques de calcul Il y en a pour tous les gouts.

Primitives et intégrales Toute la section 18.2 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 18.229) ou autres fonctions trigonométriques. Ils sont donc placés beaucoup plus bas que la théorie.

— Méthode du développement asymptotique, sous-section 18.14.2.

— Méthode des coordonnées polaires, sous-section 18.14.1.

— Utilisation du théorème de la fonction implicite, dans l'exemple 18.231.

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

Thème 67 : méthodes de calcul

(1) Théorème de Rothstein-Trager 20.101.
(2) Algorithme des facteurs invariants 4.111.
(3) Méthode de Newton, théorème 34.63
(4) Calcul d'intégrale par suite équirépartie 28.10.

Thème 68 : méthode de Newton

(1) Nous parlons un petit peu de méthode de Newton en dimension 1 dans 34.6.
(2) La méthode de Newton fonctionne bien avec les fonctions convexes par la proposition 34.56.
(3) La méthode de Newton en dimension n est le théorème 34.63.
(4) Un intervalle de convergence autour de α s'obtient par majoration de $|g'|$, proposition 34.48.
(5) Un intervalle de convergence quadratique s'obtient par majoration de $|g''|$, théorème 34.54.
(6) En calcul numérique, section 34.6.
(7) Méthode de Newton pour calculer $\sqrt{A}$, exemple 34.57.

Thème 69 : prolongement d'applications

(1) Prolongement de fonction définie sur une partie dense, théorème 17.131
(2) Lemme de Borel 15.165.
(3) Prolongement méromorphe de la fonction Γ d'Euler.
(4) Le théorème de Tietze prolonge des fonction continues définies sur un fermé. Prolongement continu dans le cas métrique, théorème 27.157. Dans le cas d'un espace normal, théorème 26.21.

Thème 70 : opérations sur les distributions

(1) Convolution d'une distribution par une fonction, définition par l'équation (30.185).
(2) Dérivation d'une distribution, proposition-définition 30.30.
(3) Produit d'une distribution par une fonction, définition 30.29.

Thème 71 : convolution

(1) Définition 27.55, et principales propriétés sur $L^1(\mathbb{R})$ dans le théorème 27.56.
(2) Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leqslant \|f\|_p \|g\|_1$, proposition 27.60.
(3) $\varphi \in L^1(\mathbb{R})$ et $\psi \in \mathscr{S}(\mathbb{R})$, alors $\varphi * \psi \in \mathscr{S}(\mathbb{R})$, proposition 27.224.
(4) Les suites régularisantes : $\lim_{n\to\infty} \rho_n * f = f$ dans la proposition 29.18.
(5) Convolution d'une distribution par une fonction, définition par l'équation (30.185).

Thème 72 : séries de Fourier

— Le système trigonométrique est donné en la définition 27.69.
— Les coefficients de Fourier de $c_n(f)$ sont donnés par 27.71.
— Formule sommatoire de Poisson, proposition 29.15.
— Inégalité isopérimétrique, théorème 28.23.
— Fonction continue et périodique dont la série de Fourier ne converge pas, proposition 28.21.
— 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 28.7.
  (2) Convergence au sens $L^2\Big([0,2\pi]\Big)$ dans le théorème 27.118.

(3) Si f est continue, périodique et si sa série de Fourier converge uniformément, théorème 28.15.

(4) Si f est périodique et la série des coefficients converge absolument pour tout x, proposition 28.16.

(5) Si f est périodique et de classe C^1, théorème 28.17.

(6) Unicité des coefficients de Fourier, corolaire 28.18.

Il est cependant faux de croire que la continuité et la périodicité suffisent à obtenir une convergence, comme le montre la proposition 28.21.

Thème 73 : transformée de Fourier

(1) Définition sur L^1, définition 29.1.

(2) La transformée de Fourier d'une fonction $L^1(\mathbb{R}^d)$ est continue, proposition 29.11.

(3) L'espace de Schwartz [19] 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 29.20

(4) L'application $\mathcal{F}\colon \mathscr{S}(\mathbb{R}^d) \to \mathscr{S}(\mathbb{R}^d)$ est une bijection. Formule d'inversion, proposition 29.26.

Thème 74 : gaussienne

(1) Le calcul de l'intégrale

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$$

est fait de deux façons dans l'exemple 14.300. Dans les deux cas, le théorème de Fubini 14.297 est utilisé.

(2) Le lemme 29.22 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 29.23 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 29.26

Thème 75 : 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 29.19 sur $\mathscr{S}(\mathbb{R}^d)$

(2) Lemme 31.10 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 14.45. Celui-ci est d'ailleurs plutôt nommé « lemme de transport ».

Il existe aussi un théorème de transfert 36.83 qui parle de variables aléatoires :

$$E(f \circ X) = \int_\Omega f\big(X(\omega)\big) dP(\omega) = \int_{\mathbb{R}^d} f(x) dP_X(x) \tag{-2.15}$$

Thème 76 : invariants de similitude

(1) Théorème 9.284.

(2) Pour prouver que la similitude d'applications linéaires résiste à l'extension du corps de base, théorème 9.298.

(3) Pour prouver que la dimension du commutant d'un endomorphisme de E est de dimension au moins $\dim(E)$, lemme 9.295.

(4) Nous verrons dans la remarque 9.285 à propos des invariants de similitude que toute matrice est semblable [20] à la matrice bloc-diagonale constituées des matrices compagnon (définition 9.279) de la suite des polynômes minimaux.

19. Définition 27.212.
20. Définition 4.108.

Thème 77 : 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 [21]. Les isométries d'un espace euclidien préservent le produit scalaire et fixent donc l'origine (lemme 11.15). Les isométries des espaces affines par contre conservent les distances (définition 8.64) 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).

Général Quelques résultats généraux et en vrac à propos d'isométries.

(1) Définition d'une isométrie pour une forme bilinéaire, 9.150. Pour une forme quadratique : définition 9.149.

(2) Définition du groupe orthogonal 9.38, et le spécial orthogonal $\mathrm{SO}(n)$ en la définition 9.41. Le groupe $\mathrm{SO}(2)$ est le groupe des rotations, par corolaire 18.140.

(3) La rotation $R_A(\theta)$ d'un angle θ autour du point $A \in \mathbb{R}^2$ est donnée par la définition 18.129.

(4) La proposition 18.141 donne à toute rotation $R_0(\theta)$ une matrice de la forme connue. C'est autour de cela que nous définissons les angles, définition 18.159.

(5) Le groupe orthogonal est le groupe des isométries de $\mathbb{R}^n$, proposition 9.40.

(6) Les isométries de l'espace euclidien sont affines, 9.152.

(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 18.81.

(8) Isométries du cube, section 5.7.

(9) Nous parlons des isométries affines du tétraèdre régulier dans la proposition 18.197.

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 18.177.

(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 18.202.

(3) Le théorème 18.204 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 réflexion dans $\mathbb{R}^2$ 18.123.

(2) La caractérisation en termes de projection orthogonale est le lemme 18.108 ; en termes de médiatrice c'est le lemme 18.114.

(3) Définition d'un hyperplan 9.299.

(4) En dimension 2, une rotation est définie comme composée de deux réflexions en la définition 18.120.

(5) En dimension 2, les réflexions ont un déterminant -1 par le lemme 18.133.

(6) Les isométries du plan $(\mathbb{R}^2, d)$ sont données dans le théorème 18.193, et sont au plus 3 réflexions par le théorème 18.191.

(7) Décomposition des isométries de $\mathbb{R}^n$ en réflexions par le lemme 18.89.

21. Définition 9.166.

(8) En particulier, les éléments de SO(3) sont des compositions de deux réflexions par le corolaire 18.91.

(9) 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 18.97.

Sous-groupe fini (1) Les sous-groupes finis des isométries de $(\mathbb{R}^2, d)$ sont cycliques, théorème 18.202.

(2) Les sous-groupes finis de SO(3) sont listés dans 18.226.

(3) Les sous-groupes finis de SO(2) sont cycliques, lemme 18.144.

Thème 78 : enveloppes

(1) L'ellipse de John-Loewner donne un ellipsoïde de volume minimum autour d'un compact dans $\mathbb{R}^n$, théorème 17.125.

(2) Le cercle circonscrit à une courbe donne un cercle de rayon minimal contenant une courbe fermée simple, proposition 21.90.

(3) Enveloppe convexe du groupe orthogonal 13.38.

(4) Enveloppe convexe d'une courbe fermée plane comme intersection des demi-plans tangents, proposition 21.96.

Thème 79 : intégration sur des variétés

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 9.23.

(2) Orientation sur une surface, définition 20.64.

(3) Variété orientable, définition 20.16.

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 20.75.

(2) Rotationnel et circulation, théorème 24.8.

Le théorème de Stokes peut être utilisé pour montrer le théorème de Brouwer, proposition 20.35.

Thème 80 : dénombrements

— Coloriage de roulette (18.10.15.1) et composition de colliers (18.10.15.2).

— Nombres de Bell, théorème 15.167.

— 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 [22], théorème 26.99.

Thème 81 : caractérisation de distributions en probabilités

(1) La probabilité conjointe est la définition 36.19.

(2) La fonction de répartition est la définition 36.73.

(3) La fonction caractéristique est la définition 36.76.

Thème 82 : théorème central limite

(1) Pour les processus de Poisson [23], théorème 40.13.

22. Éléments simples, lemme 19.13.
23. Définition 40.9.

Thème 83 : indépendance d'événements et de variables aléatoires

(1) Événements indépendants, définition 36.6.
(2) Variables aléatoires indépendantes, définition 36.10.
(3) Espérance de variables aléatoires indépendantes : $E(X_1 \cdots X_n) = E(X_1) \dots E(X_n)$, proposition 36.23.
(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 36.21.

Thème 84 : 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 36.49.

Les autres sont listées ci-dessous.

Probabilité conditionnelle .

Plusieurs probabilités conditionnelles.

— D'un événement en sachant un autre : la définition 36.41 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 36.67 qui définit la variable aléatoire

$$P(A|X)(\omega) = P(A|X = X(\omega)).$$

Dans le cas continu, c'est la définition 36.68 :

$$P(A|X) = P(A|\sigma(X)) = E(\mathbb{1}_A|\sigma(X)).$$

— 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 36.61 :

$$E(X|A) = \frac{E(X\mathbb{1}_A)}{P(A)}. \tag{-2.16}$$

— 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 36.49). Cela au sens des projections orthogonales.

— d'une variable aléatoire par rapport à une autre. La définition 36.51 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 36.62.
(2) La probabilité conditionnelle se factorise par rapport à l'union disjointe par le lemme 36.45 : $P\big(\bigcup_{i=0}^{\infty} A_i|B\big) = \sum_{i=0}^{\infty} P(A_i|B)$.

Thème 85 : chaine de Markov

(1) Construction d'une chaine de Markov dont la matrice de transition est donnée, lemme 38.42.

(2) Principales propriétés d'une chaine de Markov homogène, proposition 38.39.

(3) Si la chaine de Markov est irréductible, alors il y a unicité de l'état stationnaire, proposition 38.16. 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 38.37.

(5) État absorbant, définition 38.44.

-2.1 Conventions sur les matrices et changement de bases

-2.1.1 Matrices et applications linéaires

Le lien entre matrice et application linéaire est donné par la définition 4.67. L'application d'une matrice à un vecteur est (4.82). Le lien le plus simple entre l'application linéaire et les éléments de matrice est donné par la proposition 4.70. Voici les relations :

$$T_{\alpha i} = T(e_i)_\alpha \tag{-2.17a}$$
$$T(e_i) = \sum_\alpha T_{\alpha i} f_\alpha \tag{-2.17b}$$
$$T(x) = \sum_{i\alpha} T_{\alpha i} x_i f_\alpha \tag{-2.17c}$$
$$T(x)_\alpha = \sum_i T_{\alpha i} x_i. \tag{-2.17d}$$

De la même manière nous utiliserons (rarement) la notation suivante (définition 10.102) si $x \in \mathbb{R}^n$ et $T \in \mathbb{M}(n \times n)$:

$$xT = \sum_{ij} x_i T_{ij} e_j. \tag{-2.18}$$

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 4.70(4).

(2) C'est un isomorphisme d'algèbre, proposition 4.73.

(3) C'est un isomorphisme d'espaces vectoriels, proposition 4.71.

(4) Isomorphisme d'algèbres et d'anneaux, proposition 4.73.

(5) Isomorphisme d'espaces topologiques, proposition 4.73.

Lorsque nous avons une base orthonormée[24] nous avons aussi les propositions 9.178 et 9.178 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 $\mathbb{R}^n$.

-2.1.2 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 4.112 donne le lien entre les vecteurs de base :

(1) $f_\alpha = \sum_i Q_{i\alpha} e_i$

24. Définition 9.164.

(2) $e_i = \sum_\alpha Q^{-1}_{\alpha i} f_\alpha$

La proposition 4.113 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 4.116. Soit une application linéaire $T : V \to V$ 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

$$B = Q^{-1} A Q. \tag{-2.19}$$

-2.1.3 Changement de base : matrice d'une forme bilinéaire

La proposition 9.146 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

$$B = Q^t A Q. \tag{-2.20}$$

Pour comparaison avec la loi de transformation des matrices des applications linéaires, voir la remarque 9.147.

Plus généralement, si ϕ est une application linéaire, la matrice de $q \circ \phi$ est $\phi^t q \phi$, proposition 9.145.

-2.2 Multiindice et liste d'indices

-2.1.
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** [3] est une vecteur d'entiers positifs à n composantes. Si $\alpha = (2, 1)$ alors nous avons la notation

$$\partial^\alpha f = \frac{\partial^2}{\partial x_1} \frac{\partial}{\partial x_2} f \tag{-2.21}$$

Cette notation pose problème lorsque, par exemple, $\partial_1^2 \partial_2 f \neq \partial_1 \partial_2 \partial_1 f$.

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

$$\partial^\alpha f = \partial_1 \partial_3 \partial_1 \partial_5 f. \tag{-2.22}$$

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 $(\alpha_{p-k+1}, \alpha_{p-k+2}, \dots, \alpha_p)$.

-2.3 Anglicismes

Voici quelques anglicismes dont je ne me souviens jamais.

(1) Une σ-algèbre est une tribu, définition 14.1.
(2) Le « uniform boundedness principle » est le théorème de Banach-Steinhaus 11.140.
(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.

Table des matières

Thématique **1**
-2.1 Conventions sur les matrices et changement de bases . . . 38
-2.1.1 Matrices et applications linéaires . . . 38
-2.1.2 Le changement de base . . . 38
-2.1.3 Changement de base : matrice d'une forme bilinéaire . . . 39
-2.2 Multiindice et liste d'indices . . . 39
-2.3 Anglicismes . . . 39

Table des matières **40**

Index **72**

Liste des notations **97**

0 Introduction **101**
0.1 Auteurs, contributeurs, sources et remerciements . . . 101
0.1.1 Ceux qui ont travaillé sur le Frido . . . 101
0.1.2 Aide directe, mais pas volontairement sur le Frido . . . 102
0.1.3 Des gens qui ont fait un travail qui m'a bien servi . . . 103
0.2 Originalité . . . 103
0.3 Les choses qui doivent vous faire tiquer . . . 104
0.4 Quelques choix qui peuvent provoquer des quiproquos . . . 104
0.5 Autres choix pas spécialement standards . . . 105
0.5.1 Mathématique intéressante . . . 105
0.6 Sage est là pour vous aider . . . 105
0.6.1 Lancez-vous dans Sage . . . 106
0.6.2 Exemples de ce que Sage peut faire pour vous . . . 106
0.7 Comment contribuer et aider ? . . . 107
0.7.1 Des preuves qui manquent . . . 107
0.7.2 Du texte qui manque . . . 107
0.7.3 Des exemples qui manquent . . . 107
0.7.4 Trucs de programmation et de LaTeX . . . 107
0.8 Les politiques éditoriales . . . 108
0.8.1 Licence libre . . . 108
0.8.2 pdflatex . . . 108
0.8.3 utf8 . . . 108
0.8.4 Notations . . . 108
0.8.5 De la bibliographie . . . 108
0.8.6 Faire des références à tout . . . 108
0.8.7 Des listes de liens internes . . . 108
0.8.8 Pas de références vers le futur . . . 108

1 Construction des ensembles de nombres **109**
1.1 Quelques éléments sur les ensembles . . . 109
1.1.1 Petit mot d'introduction . . . 109

1.1.2 Injection, surjection, bijection . . . 110
1.1.3 Ensemble ordonné . . . 110
1.1.4 Lemme de Zorn . . . 112
1.1.5 Complémentaire . . . 113
1.1.6 Quelques relations ensemblistes . . . 113
1.1.7 Relations d'équivalence . . . 115
1.2 Quelques structures algébriques . . . 116
1.3 Les naturels . . . 118
1.3.1 Applications définies par récurrence . . . 118
1.3.2 Addition sur les naturels . . . 121
1.3.3 Ordre sur les naturels . . . 123
1.3.4 Multiplication dans les naturels . . . 128
1.3.5 Presque unicité des triplets naturels . . . 131
1.3.6 Écriture d'un naturel dans une base . . . 135
1.4 Les entiers . . . 140
1.4.1 Opposé . . . 142
1.4.2 Ordre sur $\mathbb{Z}$ . . . 143
1.5 Quelques résultats de cardinalité . . . 143
1.5.1 Équipotence, surpotence, subpotence . . . 143
1.5.2 Un peu d'infinité . . . 144
1.5.3 Dénombrabilité et ensemble des naturels . . . 150
1.5.4 Théorème de Cantor-Schröder-Bernstein . . . 155
1.5.5 Comparabilité cardinale . . . 158
1.5.6 Théorème de Cantor, ensemble des ensembles . . . 159
1.5.7 Ajouter ou soustraire des cardinalités . . . 160
1.6 Groupes . . . 164
1.6.1 Définition, unicité du neutre . . . 164
1.6.2 Groupe ordonné . . . 165
1.6.3 Classes de conjugaison . . . 166
1.7 Anneaux . . . 167
1.7.1 Élément irréductible et premier . . . 170
1.7.2 Anneau intègre . . . 170
1.7.3 Fonction puissance . . . 174
1.8 Idéal dans un anneau . . . 174
1.8.1 Division euclidienne . . . 176
1.9 Anneau principal et idéal premier . . . 178
1.10 Anneau intègre . . . 180
1.10.1 Sous-groupes de $(\mathbb{Z}, +)$ . . . 180
1.10.2 Théorème de Bézout . . . 181
1.11 Anneau euclidien . . . 184
1.12 Le groupe et anneau des entiers . . . 186
1.12.1 PGCD, PPCM et Bézout . . . 186
1.13 Sous-groupe normal . . . 188
1.13.1 Permutations, groupe symétrique . . . 192
1.13.2 Décomposition en cycles . . . 192
1.13.3 Permutation un peu ordonnées . . . 199
1.14 Corps . . . 201
1.14.1 Définitions, morphismes . . . 201
1.15 Symbole de sommation . . . 202
1.15.1 Somme à valeurs dans un groupe commutatif . . . 202
1.16 Symbole de produit . . . 205
1.16.1 Sous-groupe engendré . . . 206
1.17 Module sur un anneau . . . 208

1.17.1 Module produit . . . 209
1.17.2 Sous-module . . . 211
1.18 Caractéristique d'un anneau . . . 213
1.18.1 Caractéristique deux . . . 214
1.19 Polynômes . . . 214
1.19.1 Polynômes d'une variable . . . 214
1.19.2 La notation $A[X]$ . . . 217
1.19.3 Action du groupe symétrique . . . 218
1.19.4 Corps des fractions . . . 219
1.19.5 Corps totalement ordonné . . . 221
1.20 Les rationnels . . . 223
1.20.1 Relation d'ordre . . . 224
1.20.2 Caractéristique . . . 224
1.21 Suite de Cauchy dans un corps totalement ordonné . . . 224
1.21.1 Suites de Cauchy dans les rationnels . . . 227
1.22 Insuffisance des rationnels . . . 228
1.23 Les réels . . . 232
1.23.1 L'ensemble . . . 232
1.23.2 Relation d'ordre . . . 234
1.23.3 Complétude . . . 241
1.23.4 Intervalles . . . 244
1.23.5 Maximum, supremum et compagnie . . . 244
1.23.6 Racines . . . 249
1.23.7 Corps valué . . . 250
1.23.8 Partie entière, partie fractionnaire . . . 250
1.24 Les complexes . . . 251

2 Théorie des groupes **253**
2.1 Groupes . . . 253
2.2 Groupe dérivé . . . 253
2.3 Théorèmes d'isomorphismes . . . 254
2.4 Indice d'un sous-groupe et ordre des éléments . . . 256
2.5 Suite de composition . . . 257
2.6 Groupes résolubles . . . 260
2.7 Action de groupes . . . 262
2.8 Produit semi-direct de groupes . . . 268
2.9 Groupe de torsion . . . 270
2.10 Famille presque nulle . . . 270

3 Anneaux **271**
3.1 Inversibles et nilpotents . . . 271
3.2 PGCD, PPCM et éléments inversibles . . . 272
3.2.1 Calcul effectif du PGCD et théorème de Bézout . . . 272
3.2.2 Générateurs . . . 274
3.2.3 Décomposition en facteurs premiers . . . 276
3.2.4 Ordre d'un élément dans un groupe fini . . . 280
3.2.5 Écriture des fractions . . . 282
3.2.6 Équation diophantienne linéaire à deux inconnues . . . 283
3.2.7 Quotients . . . 284
3.3 Binôme de Newton et morphisme de Frobenius . . . 285
3.4 Polynômes de plusieurs variables . . . 287
3.4.1 Divisibilité et classes d'association . . . 288
3.4.2 PGCD et PPCM . . . 288
3.4.3 Anneaux intègres et corps . . . 289

3.5 Anneau factoriel . . . 290
3.5.1 Autour du théorème de Bézout . . . 291
3.5.2 Idéal premier . . . 293
3.5.3 Anneau noethérien . . . 294
3.6 Anneau $\mathbb{Z}/6\mathbb{Z}$ . . . 296
3.6.1 Équations diophantiennes . . . 299
3.6.2 Triplets pythagoriciens et équation de Fermat pour $n = 4$ . . . 300
3.7 Polynômes à coefficients dans un anneau commutatif . . . 303
3.7.1 Monômes . . . 303
3.7.2 Évaluation . . . 303
3.7.3 Polynômes sur un anneau intègre . . . 304
3.7.4 Division euclidienne . . . 304
3.7.5 Polynôme primitif . . . 305
3.7.6 Racines des polynômes . . . 308
3.7.7 Quelques identités . . . 311
3.7.8 Générateurs pour le groupe multiplicatif . . . 311

4 Espaces vectoriels (début) 313
4.1 Parties libres, génératrices, bases et dimension . . . 313
4.1.1 Et en dimension infinie . . . 319
4.1.2 Espace librement engendré . . . 321
4.2 Applications linéaires . . . 322
4.2.1 Définition . . . 322
4.2.2 Linéarité et bases . . . 325
4.2.3 Rang . . . 326
4.3 Matrices . . . 330
4.3.1 Définitions . . . 330
4.3.2 Identifier matrices et applications linéaires . . . 332
4.3.3 Déterminant . . . 336
4.3.4 Déterminant en petite dimension . . . 336
4.3.5 Manipulations de lignes et de colonnes . . . 337
4.3.6 Réduction de Gauss . . . 342
4.3.7 Matrices inversibles . . . 344
4.3.8 Inversibilité et déterminant . . . 346
4.3.9 Quelques ensembles de matrices particuliers . . . 346
4.3.10 Déterminant et combinaisons de lignes et colonnes . . . 346
4.3.11 Transvections . . . 347
4.3.12 Mineur, rang . . . 348
4.3.13 Matrices équivalentes et semblables . . . 349
4.3.14 Algorithme des facteurs invariants . . . 351
4.4 Changement de base . . . 352
4.4.1 Changement de base : vecteurs de base . . . 353
4.4.2 Changement de base : coordonnées . . . 353
4.4.3 Changement de base : matrice d'une application linéaire . . . 354
4.5 Espaces de polynômes . . . 355
4.6 Projection et orthogonalité . . . 356
4.7 Dualité . . . 357
4.7.1 Orthogonal . . . 359
4.8 Représentation de groupe . . . 360
4.9 Somme directe d'espaces vectoriels . . . 360
4.9.1 Structure réelle . . . 362

5 Classification de certains groupes 365
5.1 Théorèmes de Sylow . . . 365

5.2 Groupe monogène . . . 369
5.3 Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$ . . . 370
5.4 Groupes abéliens finis . . . 372
5.5 Groupes d'ordre pq . . . 374
5.5.1 Fonction indicatrice d'Euler . . . 377
5.5.2 Générateurs . . . 380
5.5.3 Fonction indicatrice d'Euler (propriétés) . . . 381
5.6 Groupe symétrique, groupe alterné . . . 381
5.6.1 Le groupe alterné . . . 381
5.6.2 Sous-groupes normaux . . . 386
5.6.3 Indice . . . 388
5.7 Isométries du cube . . . 389

6 Corps **393**
6.1 Généralités . . . 393
6.1.1 Corps ordonnés . . . 393
6.1.2 Automorphismes de $\mathbb{R}$ et $\mathbb{C}$ . . . 393
6.1.3 Corps premier . . . 395
6.1.4 Petit théorème de Fermat . . . 396
6.1.5 Nombres de Sophie Germain . . . 397
6.2 Théorème des deux carrés . . . 400
6.2.1 Un peu de structure dans $\mathbb{Z}[i]$ . . . 400
6.2.2 Résultats chinois . . . 403
6.3 Polynômes à coefficients dans un corps . . . 406
6.3.1 Irréductibilité . . . 410
6.3.2 Idéaux . . . 411
6.3.3 Identité de Bézout . . . 414
6.3.4 Lemme et théorème de Gauss . . . 414
6.3.5 Polynômes sur un corps et pgcd . . . 415
6.4 Extension de corps . . . 417
6.4.1 Extension et polynôme minimal . . . 419
6.4.2 Extensions algébriques et éléments transcendants . . . 420
6.4.3 Extension algébrique et polynôme minimal . . . 423
6.4.4 Extensions et polynômes . . . 424
6.4.5 Racines de polynômes . . . 434
6.4.6 Corps de rupture . . . 435
6.4.7 Pile d'extensions . . . 437
6.4.8 Clôture algébrique . . . 438
6.4.9 Polynômes à plusieurs variables . . . 444
6.4.10 Corps de décomposition . . . 445
6.4.11 Non irréductible ou pas corps ? . . . 449
6.4.12 Clôture algébrique . . . 449
6.4.13 Dérivée de polynômes . . . 450
6.4.14 Extensions séparables . . . 451
6.5 Idéal maximum . . . 457
6.5.1 Idéal maximum . . . 457
6.6 Polynômes symétriques et alternés . . . 459
6.6.1 Polynômes symétriques, alternés ou semi-symétriques . . . 459
6.6.2 Polynôme symétrique élémentaire . . . 459
6.6.3 Relations coefficients racines . . . 461
6.7 Minuscule morceau sur la théorie de Galois . . . 462

7 Topologie générale **465**
7.1 Éléments généraux de topologie . . . 465

7.1.1 Définitions et propriétés de base . . . 465
7.1.2 Base de topologie . . . 465
7.1.3 Fermés . . . 466
7.1.4 Quelques exemples . . . 467
7.1.5 Topologie produit . . . 468
7.1.6 Adhérence, fermeture, intérieur, point d'accumulation et point isolé . . . 469
7.2 Topologie rendant continue . . . 474
7.2.1 Topologie quotient . . . 475
7.3 Suites et convergence . . . 476
7.3.1 Convergence dans un fermé . . . 477
7.3.2 Pour des limites uniques : séparabilité . . . 477
7.3.3 Fonctions équivalentes . . . 479
7.4 Connexité . . . 480
7.5 Compacité . . . 483
7.5.1 Définition et notions connexes . . . 483
7.5.2 Espace localement compact . . . 484
7.5.3 Autres compacité . . . 485
7.5.4 Quelques propriétés . . . 486
7.5.5 Compactifié d'Alexandrov . . . 488
7.5.6 Propriété d'intersection finie . . . 490
7.6 Limite de fonction . . . 490
7.7 Topologie, distances et normes . . . 492
7.7.1 Distance et topologie métrique . . . 492
7.7.2 Topologie métrique et induite . . . 493
7.7.3 Intérieur, adhérence et frontière . . . 493
7.7.4 Boules ouvertes, fermées, sphères . . . 495
7.7.5 Continuité séquentielle . . . 495
7.7.6 Continuité et compacité . . . 496
7.7.7 Distance à un ensemble . . . 499
7.7.8 Convexité . . . 499
7.7.9 Norme . . . 500
7.8 Espaces vectoriels topologiques . . . 503
7.8.1 Corps topologique . . . 505
7.8.2 Voisinage symétrique et équilibré . . . 506
7.8.3 Limite de suites . . . 508
7.9 Applications continues . . . 509
7.9.1 Continuité . . . 509
7.9.2 Continuité et topologie induite . . . 511
7.9.3 Continuité et connexité . . . 512
7.9.4 Continuité et compacité . . . 514
7.9.5 Continuité de la réciproque sur un compact . . . 514
7.9.6 Topologie et matrices . . . 515
7.10 Produit fini d'espaces vectoriels normés . . . 515
7.10.1 Distance et norme produit . . . 515
7.11 Topologie réelle en dimension n . . . 518
7.11.1 Ouverts et fermés . . . 518
7.11.2 Point d'accumulation, point isolé . . . 519
7.11.3 Limite de suite . . . 519
7.12 Topologie et distance . . . 520
7.12.1 Suites et espaces métriques . . . 521
7.12.2 Espace métrisable . . . 523
7.13 Suites de Cauchy, métrique et espaces complets . . . 524
7.13.1 Généralités . . . 524

7.13.2 Espace topologique métrique . . . 526
7.13.3 Compacts, fermés . . . 527
7.13.4 Équivalence entre Cauchy et $\tau-$Cauchy . . . 533
7.14 Norme, espace vectoriel normé . . . 535
7.15 Espaces métriques . . . 538
7.15.1 Espaces métrisables . . . 538
7.15.2 Fonctions continues . . . 538
7.15.3 Ensembles enchainés . . . 545
7.15.4 Produit fini d'espaces métriques . . . 546
7.15.5 Équicontinuité . . . 547
7.15.6 Continuité uniforme . . . 548
7.16 Ensembles nulle part denses . . . 548
7.17 Topologie des seminormes . . . 549
7.17.1 Seminorme . . . 549
7.17.2 Topologie des seminormes . . . 550
7.17.3 Espace dual . . . 556
7.17.4 Espace $C^k(\mathbb{R}, E')$ . . . 556
7.18 Espaces de Baire . . . 557

8 Espaces affines **559**
8.1 Vecteurs agissant sur un espace . . . 559
8.2 Repères cartésiens affines . . . 560
8.3 Classification affine des coniques . . . 560
8.4 Applications affines . . . 563
8.4.1 Autres propriétés . . . 564
8.5 Isomorphismes . . . 565
8.6 Sous espaces affines . . . 566
8.7 Barycentre . . . 568
8.7.1 Sous-espaces affines . . . 568
8.7.2 Enveloppe convexe . . . 570
8.7.3 Applications affines et barycentre . . . 573
8.8 Repères, coordonnées cartésiennes et barycentriques . . . 574
8.8.1 Équation de droite . . . 577
8.8.2 Associativité, coordonnées barycentriques dans un triangle . . . 578
8.9 Applications affines sur $\mathbb{R}^n$ . . . 579
8.9.1 Structure de groupe pour les applications affines . . . 580
8.10 Isométries . . . 581

9 Espaces vectoriels (encore) **583**
9.1 Déterminants . . . 583
9.1.1 Formes multilinéaires alternées . . . 583
9.1.2 Déterminant d'une famille de vecteurs . . . 584
9.1.3 Déterminant d'un endomorphisme . . . 587
9.1.4 Déterminant de Vandermonde . . . 589
9.1.5 Déterminant de Gram . . . 592
9.1.6 Déterminant de Cauchy . . . 592
9.1.7 Matrice de Sylvester . . . 592
9.1.8 Théorème de Kronecker . . . 595
9.2 Orientation . . . 597
9.2.1 Cas vectoriel . . . 597
9.2.2 Cas affine . . . 598
9.3 Hermitien, orthogonal, adjoint . . . 599
9.3.1 Opérateur orthogonal, matrice orthogonale . . . 601
9.4 Topologie . . . 602

9.4.1 Boules et sphères . . . 602
9.4.2 Ouverts, fermés, intérieur et adhérence . . . 603
9.4.3 Point isolé, point d'accumulation . . . 610
9.4.4 Des exemples . . . 611
9.5 Valeur propre et vecteur propre . . . 613
9.5.1 Généralités . . . 613
9.5.2 Dans le vif du sujet . . . 614
9.6 Polynômes d'endomorphismes . . . 615
9.6.1 Polynômes d'endomorphismes . . . 615
9.6.2 Polynôme minimal et minimal ponctuel . . . 618
9.6.3 Polynôme caractéristique . . . 625
9.7 Formes bilinéaires et quadratiques . . . 628
9.7.1 Dégénérescence d'une forme bilinéaire . . . 629
9.7.2 Orthogonal pour une forme bilinéaire . . . 630
9.7.3 Formes quadratiques . . . 632
9.7.4 Isotropie . . . 634
9.8 Formes bilinéaires et quadratiques . . . 635
9.8.1 Matrice associée à une forme bilinéaire . . . 635
9.8.2 Changement de base : matrice d'une forme bilinéaire . . . 636
9.8.3 Isométrie, forme quadratique et bilinéaire . . . 637
9.8.4 Isométries . . . 638
9.9 Signature, théorème de Sylvester . . . 640
9.10 Produit scalaire, produit hermitien . . . 641
9.10.1 Hermitien, unitaire, etc. . . . 643
9.10.2 Éléments de matrice . . . 644
9.10.3 Transposée : pas d'approche naïve . . . 645
9.10.4 Transposée : la bonne approche . . . 646
9.10.5 Polynômes de Lagrange . . . 649
9.10.6 Dual de $\mathbb{M}(n, \mathbb{K})$ . . . 649
9.11 Diagonalisation et trigonalisation . . . 650
9.11.1 Matrices semblables . . . 651
9.11.2 Trace de matrices semblables . . . 651
9.11.3 Endomorphismes nilpotents . . . 652
9.11.4 Endomorphismes diagonalisables . . . 654
9.11.5 Diagonalisation : cas complexe, pas toujours . . . 658
9.11.6 Diagonalisation : cas réel . . . 658
9.11.7 Matrice définie positive . . . 660
9.11.8 Réduction de Gauss . . . 663
9.11.9 Orthogonalité pour une forme bilinéaire . . . 666
9.11.10 Équivalence de formes quadratiques . . . 671
9.11.11 Diagonalisation . . . 671
9.12 Fonctions . . . 673
9.13 Sous espaces caractéristiques . . . 673
9.13.1 Théorèmes de décomposition . . . 675
9.13.2 Valeurs singulières . . . 678
9.14 Extension du corps de base . . . 679
9.14.1 Extension des applications linéaires . . . 679
9.14.2 Projections . . . 681
9.14.3 Rang, polynôme minimal, polynôme caractéristique . . . 684
9.15 Frobenius et Jordan . . . 685
9.15.1 Matrice compagnon . . . 685
9.15.2 Réduction de Frobenius . . . 686
9.15.3 Forme normale de Jordan . . . 689

9.16 Commutant et endomorphismes cycliques . . . 690
9.16.1 Endomorphisme cyclique . . . 690
9.16.2 Commutant : cas diagonalisable . . . 691
9.16.3 Commutant : cas général . . . 693
9.17 Hyperplans et formes linéaires . . . 696
9.17.1 Trouver la matrice d'une symétrie donnée . . . 697
9.18 Théorème de Burnside . . . 699
9.19 Ellipsoïde . . . 701
9.20 Système d'équations linéaires : méthode de Gauss . . . 702

10 Analyse réelle : topologie et continuité **705**
10.1 Intervalles . . . 705
10.2 Application réciproque . . . 706
10.2.1 Définitions . . . 706
10.2.2 Graphe de la fonction réciproque . . . 707
10.3 Topologie sur l'ensemble des réels . . . 707
10.3.1 Compacité pour les réels . . . 708
10.3.2 Conséquence : les fermés bornés sont compacts . . . 711
10.3.3 Suites et limites dans les réels . . . 712
10.3.4 Opérations sur les limites . . . 712
10.3.5 Exemples . . . 713
10.3.6 Limites infinies . . . 713
10.3.7 Suites croissantes et bornées . . . 714
10.3.8 Suites adjacentes . . . 715
10.3.9 Limite supérieure et inférieure . . . 716
10.3.10 Ouverts, voisinage, topologie . . . 718
10.3.11 Intervalles et connexité . . . 718
10.3.12 Recouvrement par des intervalles ouverts . . . 723
10.4 Connexité par arcs . . . 725
10.4.1 Des exemples . . . 726
10.4.2 Quelques mots à propos de la droite réelle achevée . . . 728
10.5 Continuité . . . 729
10.5.1 Opération sur la continuité . . . 730
10.5.2 La fonction la moins continue du monde . . . 731
10.5.3 Approche topologique . . . 732
10.5.4 Module sur les nombres complexes . . . 734
10.5.5 Théorème de Perron-Frobenius . . . 737
10.6 Norme à partir d'un produit scalaire . . . 740
10.6.1 Continuité de la racine carrée, invitation à la topologie induite . . . 741
10.6.2 Second degré . . . 742

11 Espaces vectoriels normés **745**
11.0.1 Norme, produit scalaire et Cauchy-Schwarz (cas réel) . . . 745
11.1 Théorème spectral autoadjoint . . . 748
11.1.1 Inégalité de Minkowski . . . 750
11.1.2 Cauchy-Schwarz etc. cas complexe . . . 752
11.1.3 Diagonalisation : cas complexe, ce qu'on a . . . 753
11.1.4 Projection et orthogonalité . . . 754
11.1.5 Théorème de Pythagore . . . 755
11.1.6 Produit vectoriel . . . 756
11.1.7 Produit mixte . . . 759
11.1.8 Procédé de Gram-Schmidt . . . 760
11.1.9 Pseudo-réduction simultanée . . . 761
11.2 Approximations . . . 762

11.2.1 Quelques exemples de normes sur $\mathbb{R}^n$ . . . 763
11.3 Équivalence des normes . . . 764
11.3.1 En dimension finie . . . 765
11.3.2 Contre-exemple en dimension infinie . . . 768
11.4 Norme opérateur . . . 769
11.4.1 Norme d'algèbre . . . 771
11.5 Application linéaire continue et bornée . . . 772
11.5.1 Suites . . . 775
11.5.2 Continuité du produit de matrices . . . 777
11.6 Applications multilinéaires . . . 778
11.7 Séries . . . 780
11.7.1 Les trois types de convergence . . . 781
11.7.2 Séries dans une algèbre normée . . . 784
11.8 Sommes de familles infinies . . . 786
11.8.1 Convergence commutative . . . 786
11.8.2 Somme non dénombrables . . . 789
11.8.3 Sommes dénombrables . . . 790
11.9 Série réelle . . . 793
11.9.1 Critères de convergence absolue . . . 793
11.9.2 Critères de convergence simple . . . 795
11.9.3 Quelques séries usuelles . . . 796
11.9.4 Séries alternées . . . 798
11.9.5 Moyenne de Cesàro . . . 799
11.9.6 Écriture décimale d'un réel . . . 800
11.9.7 Théorème de Banach-Steinhaus . . . 803
11.9.8 Convergence forte . . . 806
11.10 Application ouverte . . . 807
11.11 Produit tensoriel d'espaces vectoriels . . . 810
11.12 Produit tensoriel . . . 811
11.12.1 Définition générale . . . 811
11.12.2 Construction abstraite . . . 812
11.12.3 Bases . . . 816
11.12.4 Construction par les formes multilinéaires . . . 818
11.12.5 Décomposabilité . . . 821
11.12.6 Contraction . . . 822
11.12.7 Tenseurs symétriques et alternés . . . 823
11.12.8 Règle de Leibnitz pour le produit extérieur . . . 829
11.12.9 Produit intérieur . . . 836
11.12.10 Pull back . . . 838
11.12.11 Norme . . . 839
11.12.12 Applications bilinéaires, matrices et produit tensoriel . . . 840
11.12.13 Application d'opérateurs . . . 840
11.12.14 Convergence en norme et par composante . . . 841
11.13 Calcul différentiel dans un espace vectoriel normé . . . 841
11.13.1 Définition de la différentielle . . . 842
11.13.2 Quelques mots à propos des différentielles d'ordre supérieur . . . 842
11.13.3 Différentielle d'applications linéaires . . . 844
11.13.4 Accroissements finis . . . 845
11.13.5 Notations pour les applications linéaires . . . 845
11.13.6 (non ?) Différentiabilité des applications linéaires . . . 845
11.13.7 Dérivation en chaine et formule de Leibnitz . . . 846
11.13.8 Différentiation de produit . . . 851
11.13.9 Formule des accroissements finis . . . 854

11.13.10 Applications multilinéaires . . . 857
11.13.11 Différentielle partielle . . . 858
11.13.12 L'inverse, sa différentielle . . . 859
11.14 Exponentielle de matrice . . . 862
11.15 Espace dual . . . 863
11.15.1 Topologies . . . 863
11.15.2 Module de continuité . . . 865
11.16 Mini introduction aux nombres p-adiques . . . 866
11.16.1 La flèche d'Achille . . . 866
11.16.2 La tortue et Achille . . . 867
11.16.3 Dans les nombres p-adiques, c'est vrai . . . 867

12 Analyse réelle : limites et dérivation **869**
12.1 Limite de fonctions . . . 869
12.1.1 Définition . . . 869
12.1.2 Quelques règles de calcul . . . 871
12.2 Limites pointées et épointées . . . 875
12.2.1 Théorèmes de composition de limites . . . 877
12.2.2 Discussion pointée Vs épointée . . . 881
12.3 Limites en l'infini . . . 884
12.3.1 Limite en des nombres . . . 886
12.3.2 Limites quand tout va bien . . . 886
12.3.3 Limites de fonctions . . . 887
12.3.4 Limite à gauche et à droite . . . 888
12.4 Limite en compactifié d'Alexandrov . . . 889
12.4.1 Prolongement par continuité . . . 890
12.4.2 Prolongement par continuité . . . 891
12.4.3 Théorème de la bijection . . . 892
12.5 Limite et continuité . . . 895
12.5.1 Prolongement des rationnels vers les réels . . . 898
12.6 Espace des fonctions continues . . . 900
12.7 Uniforme continuité . . . 905
12.8 Fonctions sur un compact . . . 907
12.9 Polynômes, théorème de d'Alembert . . . 908
12.9.1 Polynômes sur les réels . . . 908
12.9.2 Polynômes sur les complexes . . . 908
12.10 Trigonalisation . . . 914
12.10.1 Trigonalisation : généralités . . . 914
12.10.2 Trigonalisation : cas complexe . . . 915
12.11 Matrices, spectre et norme . . . 921
12.11.1 Rayon spectral . . . 922
12.11.2 Normes de matrices et d'applications linéaires . . . 926
12.12 Géométrie dans l'espace . . . 931
12.12.1 Droites dans l'espace . . . 931
12.12.2 Projection orthogonale . . . 933
12.12.3 Plan médiateur . . . 936
12.12.4 Tétraèdre . . . 937
12.13 Géométrie dans le plan . . . 937
12.14 Dérivée : exemples introductifs . . . 941
12.14.1 La vitesse . . . 941
12.14.2 La tangente à une courbe . . . 942
12.14.3 L'aire en dessous d'une courbe . . . 942
12.15 Dérivation de fonctions réelles . . . 944
12.15.1 Exemples . . . 945

12.15.2 Interprétation géométrique : tangente . . . 946
12.15.3 Interprétation géométrique : approximation affine . . . 947
12.15.4 Développement limité au premier ordre . . . 948
12.16 Règles de calcul . . . 949
12.16.1 Dérivée de la réciproque . . . 953
12.16.2 Dérivée de fonction composée . . . 954
12.16.3 Dérivée de fonction périodique . . . 955
12.17 Dérivation et croissance . . . 956
12.17.1 Théorèmes de Rolle et des accroissements finis . . . 958
12.17.2 Règle de l'Hospital . . . 960
12.17.3 Dérivée et primitive . . . 962
12.18 Fonctions de plusieurs variables . . . 963
12.18.1 Graphes de fonctions à plusieurs variables . . . 966
12.18.2 Courbes de niveau . . . 966
12.19 Limites à plusieurs variables . . . 971
12.19.1 Caractérisation de la limite par les suites . . . 973
12.19.2 Règle de l'étau . . . 974
12.19.3 Méthode des chemins . . . 975
12.20 Dérivée directionnelle . . . 977
12.20.1 Dérivée partielle et directionnelles . . . 978
12.20.2 Gradient : direction de plus grande pente . . . 982
12.20.3 Gradient : orthogonal au plan tangent . . . 983
12.20.4 Mise en bouche en dimension 2 . . . 983
12.20.5 Accroissements finis et dérivées partielles . . . 985
12.21 Formes différentielles . . . 986
12.21.1 Décomposition dans la base duale . . . 986
12.21.2 L'isomorphisme musical . . . 987
12.22 Différentielle . . . 987
12.22.1 Exemples introductifs . . . 988
12.22.2 Différentielle . . . 989
12.22.3 Matrice de la différentielle . . . 989
12.22.4 Différentielle, dual et forme différentielle . . . 991
12.22.5 Ce n'est pas la différentielle extérieure . . . 992
12.22.6 Continuité, dérivabilité et différentiabilité . . . 992
12.22.7 Calcul de valeurs approchées . . . 995
12.22.8 Différentielle et tangente . . . 997
12.22.9 Prouver qu'une fonction n'est pas différentiable . . . 998
12.22.10 Gradient . . . 1002
12.22.11 Linéarité . . . 1002
12.23 Produit . . . 1003
12.23.1 Difficulté d'ordre supérieur . . . 1004
12.23.2 Solution : produit tensoriel . . . 1005
12.23.3 Formes bilinéaires . . . 1005
12.24 Différentielle de fonction composée . . . 1006
12.24.1 Fonctions composées . . . 1008
12.25 Autres trucs sur la différentielle . . . 1009
12.25.1 Différentielle et dérivées partielles . . . 1009
12.25.2 Plan tangent . . . 1009
12.25.3 Notes idéologiques quant au concept de plan tangent . . . 1010
12.25.4 Gradient et recherche du plan tangent . . . 1010
12.26 Jacobienne . . . 1014
12.26.1 Rappels et définitions . . . 1014
12.27 Fonctions de classe C^1 . . . 1015

12.28 Différentielle et dérivée complexe . . . 1024
12.28.1 Quelques règles de calcul . . . 1027
12.29 Théorèmes des accroissements finis . . . 1028
12.30 Fonctions Lipschitziennes . . . 1028
12.31 Différentielles d'ordre supérieur . . . 1030
12.31.1 Différentielle et dérivées partielles . . . 1030
12.31.2 Espaces d'applications multilinéaires et identifications . . . 1034
12.31.3 Fonctions différentiables plusieurs fois . . . 1038
12.31.4 Différentielle seconde, fonction de classe C^2 . . . 1039
12.31.5 Ordre supérieur . . . 1042
12.32 Suites et séries : généralités . . . 1045
12.32.1 Norme suprémum . . . 1045
12.32.2 Convergence uniforme . . . 1046
12.32.3 Série de fonctions . . . 1049
12.33 Permuter limite et dérivée . . . 1051
12.34 La fonction puissance . . . 1058
12.34.1 Sur les naturels . . . 1058
12.34.2 Sur les rationnels, racines . . . 1060
12.35 Densité des polynômes . . . 1075
12.35.1 Théorème de Stone-Weierstrass . . . 1075
12.36 Primitive de fonction continue . . . 1080
12.36.1 Dérivation de la fonction puissance (première) . . . 1081
12.36.2 Équation fonctionnelle . . . 1083
12.36.3 Dérivation de la fonction puissance (seconde) . . . 1085
12.36.4 Vers les complexes . . . 1086
12.37 Polynômes de Taylor . . . 1088
12.37.1 Fonctions « petit o » . . . 1092
12.37.2 Autres formulations . . . 1094
12.37.3 Formule et reste . . . 1094
12.37.4 Reste intégral . . . 1095
12.38 Développement limité autour de zéro . . . 1095
12.38.1 Généralités . . . 1095
12.38.2 Formule de Taylor-Young . . . 1096
12.38.3 Règles de calcul . . . 1098
12.39 Développement ailleurs qu'à l'origine . . . 1100
12.40 Développement au voisinage de l'infini . . . 1100
12.40.1 La fonction puissance : remarques pour la suite . . . 1100
12.41 Fonctions réelles de deux variables réelles . . . 1100
12.41.1 Limites de fonctions à deux variables . . . 1101
12.41.2 Dérivées partielles . . . 1102
12.41.3 Différentielle et accroissement . . . 1102
12.42 Les fonctions à valeurs vectorielles . . . 1103
12.43 Fonctions vectorielles de plusieurs variables . . . 1103
12.44 Limites à plusieurs variables . . . 1104
12.45 Champs de vecteurs . . . 1107
12.45.1 Matrice jacobienne . . . 1108
12.46 Divergence, rotationnel et l'opérateur nabla . . . 1108
12.47 Interprétation de la divergence . . . 1110
12.48 Quelques formules de Leibnitz . . . 1112

13 Analyse sur des groupes **1113**
13.1 Action de groupe et connexité . . . 1113
13.2 Espaces de matrices . . . 1115
13.2.1 Dilatations et transvections . . . 1115

13.2.2 Connexité de certains groupes . . . 1121
13.2.3 Densité . . . 1123
13.2.4 Racine carrée d'une matrice hermitienne positive . . . 1125
13.2.5 Racine carrée d'une matrice symétrique positive . . . 1126
13.2.6 Décomposition polaires : cas réel . . . 1127
13.2.7 Enveloppe convexe . . . 1129
13.2.8 Décomposition de Bruhat . . . 1131
13.3 Sous-groupes du groupe linéaire . . . 1133

14 Tribus, théorie de la mesure, intégration 1137
14.1 Tribus . . . 1137
14.1.1 Généralités . . . 1137
14.1.2 Tribu engendrée . . . 1138
14.1.3 Tribu induite et engendrée . . . 1139
14.2 Théorie de la mesure . . . 1139
14.2.1 Mesure sur un ensemble de parties . . . 1139
14.2.2 Mesure sur une algèbre de parties . . . 1140
14.2.3 Mesure sur une tribu, espace mesuré . . . 1142
14.2.4 Mesures sigma-finies . . . 1142
14.2.5 Suite du texte . . . 1143
14.2.6 Mesure extérieure . . . 1149
14.3 Applications mesurables . . . 1152
14.3.1 Propriétés . . . 1152
14.3.2 D'une tribu à l'autre . . . 1152
14.4 Tribu borélienne . . . 1153
14.4.1 Applications continues et boréliennes . . . 1155
14.4.2 Tribu de Baire . . . 1157
14.5 Espace mesuré complet . . . 1159
14.5.1 Partie négligeable . . . 1159
14.5.2 Prolongement . . . 1168
14.5.3 Mesure image . . . 1170
14.5.4 Régularité d'une mesure . . . 1171
14.5.5 Théorème de récurrence . . . 1178
14.6 Mesurabilité des fonctions à valeurs réelles . . . 1178
14.6.1 Fonctions à valeurs réelles sur un espace mesurable . . . 1179
14.6.2 Fonction étagée . . . 1185
14.6.3 Fonctions réelles à variables réelles . . . 1189
14.7 Tribu produit . . . 1190
14.7.1 Produit d'espaces mesurables . . . 1190
14.7.2 Le cas des boréliens . . . 1191
14.8 Mesure de Lebesgue sur $\mathbb{R}$ . . . 1192
14.8.1 Mesure et tribu de Lebesgue . . . 1197
14.8.2 Propriétés de la mesure de Lebesgue . . . 1198
14.8.3 Fonctions mesurables . . . 1202
14.8.4 Ensemble de Vitali (non mesurable) . . . 1203
14.8.5 Ensemble de Cantor . . . 1203
14.8.6 Mesure positive sans intervalle . . . 1206
14.9 Intégrale par rapport à une mesure . . . 1206
14.9.1 Définition pour les fonctions à valeurs positives . . . 1207
14.9.2 Premières propriétés . . . 1208
14.9.3 Propriétés plus avancées . . . 1211
14.9.4 Fonctions à valeurs réelles . . . 1215
14.9.5 Additivité de l'intégrale . . . 1216
14.9.6 Fonctions à valeurs vectorielles (dimension finie) . . . 1217

14.9.7 Quelques propriétés . . . 1220
14.9.8 Permuter limite et intégrale . . . 1221
14.9.9 Additivité de l'intégrale de Lebesgque . . . 1223
14.9.10 Produit d'une mesure par une fonction (mesure à densité) . . . 1225
14.9.11 Mesure et topologie . . . 1227
14.10 Mesure à densité . . . 1230
14.10.1 Théorème de Radon-Nikodym . . . 1230
14.10.2 Mesure complexe . . . 1244
14.10.3 Théorème d'approximation . . . 1245
14.11 Produit de mesures . . . 1246
14.12 Tribu et mesure de Lebesgue sur $\mathbb{R}^d$ . . . 1251
14.12.1 Ensembles négligeables . . . 1252
14.12.2 Parties et fonctions mesurables . . . 1253
14.12.3 Propriétés d'unicité . . . 1254
14.12.4 Régularité . . . 1256
14.13 Propriétés de l'intégrale de Lebesgue . . . 1256
14.13.1 Quelques limites dans les bornes . . . 1257
14.13.2 Mesure de comptage et série . . . 1259
14.13.3 Théorème de la moyenne . . . 1262
14.13.4 Primitives et intégrales . . . 1262
14.13.5 Exemples et applications . . . 1264
14.13.6 Permuter limite et dérivée . . . 1265
14.13.7 Intégrales impropres . . . 1267
14.14 Changement de variables dans une intégrale multiple . . . 1269
14.14.1 Des lemmes . . . 1270
14.14.2 Déterminant et mesure de Lebesgue . . . 1270
14.14.3 Le théorème et sa démonstration . . . 1272
14.14.4 Exemples . . . 1277
14.15 Changement d'espace mesuré . . . 1277
14.16 Théorème de Fubini-Tonelli et de Fubini . . . 1278

15 Suites et séries de fonctions **1287**
15.1 Séries de fonctions . . . 1287
15.1.1 Intégration de séries de fonctions . . . 1287
15.1.2 Différentiabilité . . . 1288
15.2 Séries entières . . . 1295
15.2.1 Disque de convergence . . . 1295
15.2.2 Somme et produit de séries . . . 1300
15.2.3 Convergence normale . . . 1306
15.2.4 Dérivation . . . 1308
15.2.5 Intégration . . . 1311
15.3 Séries de Taylor . . . 1312
15.3.1 Polynôme de Taylor d'une série entière . . . 1312
15.3.2 Une majoration pour le reste . . . 1312
15.3.3 Fonctions analytiques . . . 1314
15.4 Algèbre engendrée par une matrice . . . 1315
15.5 Exponentielle sur une algèbre normée . . . 1315
15.5.1 Définition . . . 1315
15.5.2 Différentielles . . . 1317
15.5.3 Exponentielle de matrice . . . 1320
15.6 Exponentielle et logarithme dans les réels . . . 1323
15.6.1 L'équation différentielle . . . 1323
15.6.2 Existence . . . 1324
15.6.3 Le nombre de Neper e . . . 1325

15.6.4 Application réciproque : logarithme . . . 1327
15.6.5 Approximations numériques de e . . . 1329
15.6.6 Résumé des propriétés de l'exponentielle . . . 1330
15.6.7 Dérivée de la fonction puissance . . . 1332
15.6.8 Dérivée du logarithme . . . 1332
15.6.9 Taylor pour l'exponentielle . . . 1333
15.6.10 Analycité . . . 1333
15.6.11 Autres propriétés et petits calculs . . . 1333
15.6.12 Taylor pour le logarithme . . . 1333
15.6.13 Développements et calcul de limites . . . 1337
15.6.14 Une petite intégrale . . . 1338
15.7 Vitesses des puissances, de l'exponentielle et du logarithme . . . 1338
15.7.1 Un peu de théorie . . . 1338
15.7.2 Nombres premiers . . . 1344
15.7.3 Quelques limites . . . 1345
15.8 Trigonométrie hyperbolique . . . 1347
15.9 Séries entières de matrices . . . 1348
15.9.1 Différentiabilité . . . 1348
15.10 Exponentielle de matrices . . . 1351
15.10.1 Diagonalisabilité d'exponentielle . . . 1352
15.11 Étude d'asymptote . . . 1353
15.12 Développement en série . . . 1354
15.12.1 Série génératrice d'une suite . . . 1354
15.12.2 Développement en série et Taylor . . . 1354
15.12.3 Resommer une série . . . 1356
15.13 Séries entières de matrices . . . 1361
15.13.1 Rayon de convergence . . . 1361
15.13.2 Convergence et rayon spectral . . . 1362
15.13.3 Exponentielle et logarithme de matrice . . . 1364
15.13.4 Calcul effectif de l'exponentielle d'une matrice . . . 1367
15.14 Lemme de Borel . . . 1368
15.14.1 Fonctions plateaux, Urysohn, partition de l'unité . . . 1368
15.14.2 Lemme de Urysohn . . . 1371
15.14.3 Partition de l'unité . . . 1372
15.14.4 Le lemme de Borel . . . 1373
15.15 Nombres de Bell . . . 1374

16 Représentations et caractères **1379**
16.1 Représentations et caractères . . . 1379
16.1.1 Crochet de dualité et transformée de Fourier . . . 1381
16.1.2 Groupes non abéliens . . . 1382
16.1.3 Représentations linéaires des groupes finis . . . 1382
16.1.4 Module . . . 1384
16.1.5 Structure hermitienne . . . 1385
16.1.6 Caractères . . . 1386
16.2 Équivalence de représentations et caractères . . . 1386
16.2.1 Représentation régulière . . . 1389
16.2.2 Caractères et représentations : suite et fin . . . 1390
16.3 Représentation produit tensoriel . . . 1392
16.4 Exemple sur le groupe symétrique . . . 1393
16.5 Table des caractères du groupe symétrique S_4 . . . 1393
16.5.1 Calculs à partir de rien ou presque . . . 1393
16.5.2 À propos de la représentation ρ_s . . . 1395
16.5.3 À propos de la représentation ρ_u . . . 1396

17 Encore de l'analyse (et c'est pas fini) 1399
17.1 Densité des polynômes . . . 1399
17.2 Primitive et intégrale . . . 1399
17.2.1 Théorème taubérien de Hardy-Littlewood . . . 1400
17.2.2 Théorème de Müntz . . . 1403
17.3 Intégrales convergeant uniformément . . . 1406
17.3.1 Définition et propriété . . . 1406
17.3.2 Critères de convergence uniforme . . . 1407
17.4 Fonctions définies par une intégrale . . . 1407
17.4.1 Continuité sous l'intégrale . . . 1408
17.4.2 Le coup du compact . . . 1409
17.4.3 Dérivabilité sous l'intégrale . . . 1409
17.4.4 Absolue continuité . . . 1412
17.4.5 Différentiabilité sous l'intégrale . . . 1414
17.5 Deux théorèmes de point fixe . . . 1417
17.5.1 Points fixes attractifs et répulsifs . . . 1417
17.5.2 Picard . . . 1418
17.6 Théorèmes de point fixes et équations différentielles . . . 1421
17.6.1 Théorème de Cauchy-Lipschitz . . . 1421
17.7 Théorèmes d'inversion locale et de la fonction implicite . . . 1429
17.7.1 Mise en situation . . . 1429
17.7.2 Théorème d'inversion locale . . . 1430
17.7.3 Théorème de la fonction implicite . . . 1433
17.7.4 Exemple . . . 1435
17.8 Décomposition polaire (régularité) . . . 1436
17.9 Théorème de Von Neumann . . . 1438
17.10 Recherche d'extrémums . . . 1441
17.10.1 Extrema à une variable . . . 1441
17.10.2 Extrema libre . . . 1442
17.10.3 Extremums et Hessienne . . . 1443
17.10.4 Un peu de recettes de cuisine . . . 1445
17.10.5 Extrema liés . . . 1446
17.11 Fonctions convexes . . . 1448
17.11.1 Inégalité des pentes . . . 1449
17.11.2 Convexité et régularité . . . 1450
17.11.3 Dérivées d'une fonction convexe . . . 1450
17.11.4 Graphe d'une fonction convexe . . . 1452
17.11.5 Convexité et hessienne . . . 1458
17.11.6 Quelques inégalités . . . 1463
17.11.7 Norme l^p . . . 1465
17.11.8 Hölder . . . 1466
17.12 Algorithme du gradient à pas optimal . . . 1471
17.13 Formes quadratiques, signature, et lemme de Morse . . . 1475
17.14 Ellipsoïde de John-Loewner . . . 1479
17.15 Prolongement de fonctions . . . 1485
17.15.1 Encore du prolongement . . . 1487
17.16 Complétion d'un espace métrique . . . 1489
17.16.1 Principe des zéros isolés . . . 1493
17.17 Un petit extra . . . 1494

18 Trigonométrie, isométries 1497
18.1 Trigonométrie . . . 1497
18.1.1 Définitions, périodicité et quelques valeurs remarquables . . . 1497
18.1.2 Fonction puissance (pour les complexes) . . . 1498

18.1.3 Formules de trigonométrie . . . 1500
18.2 Trucs et astuces de calcul d'intégrales . . . 1510
18.2.1 Quelques intégrales « usuelles » . . . 1510
18.2.2 Reformer un carré au dénominateur . . . 1513
18.2.3 Décomposition en fractions simples . . . 1513
18.3 Très modeste approximation de π . . . 1514
18.3.1 Les fonctions tangente et arc tangente . . . 1515
18.3.2 La fonction arc sinus . . . 1517
18.3.3 La fonction arc cosinus . . . 1519
18.3.4 Une meilleure approximation de π . . . 1521
18.3.5 Angle entre deux vecteurs . . . 1521
18.3.6 Aire du parallélogramme . . . 1522
18.4 Paramétrisation du cercle . . . 1524
18.5 Cercle trigonométriques . . . 1524
18.5.1 Bijection continue . . . 1525
18.5.2 Inverse . . . 1527
18.5.3 Cercle trigonométrique . . . 1528
18.5.4 Du point de vue de la tribu, mesure et co. . . . 1529
18.6 Exemples trigonométriques . . . 1532
18.6.1 Quelques équations trigonométriques . . . 1532
18.6.2 Développements en série . . . 1533
18.7 Isométries de l'espace euclidien . . . 1534
18.7.1 Structure du groupe $\mathrm{Isom}(\mathbb{R}^n)$ . . . 1534
18.8 Isométries dans $\mathbb{R}^n$ . . . 1536
18.8.1 Préserver l'orientation . . . 1541
18.9 Groupes finis d'isométries . . . 1542
18.9.1 Points fixés par une affinité . . . 1544
18.10 Classification des isométries dans $\mathbb{R}^2$ . . . 1545
18.10.1 Projection orthogonale . . . 1545
18.10.2 Réflexions . . . 1545
18.10.3 Segment, plan médiateur et équidistance . . . 1547
18.10.4 Translations et réflexions . . . 1549
18.10.5 Rotations . . . 1549
18.10.6 Rotation d'un angle donné . . . 1553
18.10.7 Rotations vectorielles . . . 1554
18.10.8 Matrice des transformations orthogonales . . . 1556
18.10.9 Rotations, SO(2) et matrice de rotation . . . 1558
18.10.10 Rotation et application affine . . . 1559
18.10.11 Angle orienté . . . 1560
18.10.12 Angles et nombres complexes . . . 1564
18.10.13 Polygone convexe . . . 1569
18.10.14 Groupe diédral . . . 1570
18.10.15 Applications : du dénombrement . . . 1577
18.10.16 Classification . . . 1578
18.10.17 Classification des isométries de $\mathbb{R}$ . . . 1581
18.10.18 Isométries du tétraèdre régulier . . . 1582
18.10.19 Représentation de S_4 via les isométries du tétraèdre . . . 1583
18.11 Transformations de Lorentz . . . 1585
18.11.1 Sous-groupe fini d'isométries du plan . . . 1587
18.11.2 Relations trigonométriques dans un triangle rectangle . . . 1591
18.11.3 Pavages du plan . . . 1593
18.12 Un peu de structure de $\mathrm{O}(n)$ . . . 1609
18.12.1 Valeurs propres dans $\mathrm{O}(n)$ . . . 1609

18.12.2 Sous-groupes finis de SO(3) . . . 1611
18.13 Systèmes de coordonnées . . . 1620
18.13.1 Coordonnées polaires . . . 1620
18.13.2 Coordonnées cylindriques . . . 1628
18.13.3 Coordonnées sphériques . . . 1629
18.14 Calcul de limites . . . 1630
18.14.1 Méthode des coordonnées polaires . . . 1632
18.14.2 Méthode du développement asymptotique . . . 1634
18.15 Quelques intégrales avec de la trigonométrie . . . 1635
18.15.1 Changement de variables . . . 1636
18.15.2 Coordonnées polaires . . . 1636
18.15.3 Coordonnées cylindriques . . . 1637
18.15.4 Un autre système utile . . . 1639
18.16 Aire d'une surface de révolution . . . 1640
18.17 Table de caractères du groupe diédral . . . 1642
18.17.1 Représentations de dimension un . . . 1642
18.17.2 Représentations de dimension deux . . . 1643
18.17.3 Le compte pour n pair . . . 1644
18.17.4 Le compte pour n impair . . . 1645

19 Corps finis, racines de l'unité **1647**
19.1 Le groupe des racines de l'unité dans les nombres complexes . . . 1647
19.1.1 Le groupe . . . 1647
19.1.2 Fonction indicatrice d'Euler . . . 1649
19.1.3 Décomposition en éléments simples . . . 1651
19.2 Chiffrement RSA . . . 1652
19.2.1 Mise en place par Bob . . . 1652
19.2.2 Chiffrement . . . 1652
19.2.3 Déchiffrement . . . 1653
19.2.4 Une imprudence à ne pas commettre . . . 1653
19.2.5 Problèmes calculatoires . . . 1654
19.2.6 La solidité de RSA . . . 1654
19.2.7 Note non mathématique pour doucher l'enthousiasme . . . 1654
19.3 Polynômes cyclotomiques . . . 1654
19.3.1 Définitions et propriétés . . . 1654
19.3.2 Nombres premiers . . . 1659
19.4 Corps finis . . . 1660
19.4.1 Théorème de Wedderburn . . . 1660
19.4.2 Existence, unicité . . . 1662
19.4.3 Symboles de Legendre et carrés . . . 1665
19.4.4 Théorème de Chevalley-Warning . . . 1670
19.4.5 Contenu d'un polynôme . . . 1673
19.4.6 Théorème de l'élément primitif . . . 1673
19.4.7 Construction de $\mathbb{F}_{p^n}$ . . . 1678
19.4.8 Exemple : étude de $\mathbb{F}_{16}$ . . . 1680
19.4.9 Polynômes irréductibles sur $\mathbb{F}_q$ . . . 1682
19.4.10 Matrices . . . 1685
19.5 Constructions à la règle et au compas . . . 1686
19.5.1 Quelques constructions . . . 1686
19.5.2 Nombres constructibles . . . 1688
19.5.3 Polygones constructibles . . . 1690

20 Intégration sur des variétés **1697**
20.1 Variétés . . . 1697

20.1.1 Introduction . . . 1697
20.1.2 Définition, carte . . . 1697
20.1.3 Ancienne définition . . . 1698
20.1.4 Espace tangent . . . 1700
20.2 Intégration . . . 1700
20.2.1 Le problème pour une intégration globale . . . 1700
20.2.2 Intégrale sur une carte . . . 1700
20.2.3 Quelques expressions pour l'élément de volume . . . 1703
20.3 Intégrale sur une variété . . . 1704
20.3.1 Mesure sur une carte . . . 1704
20.3.2 Intégrale sur une carte . . . 1705
20.3.3 Exemples . . . 1706
20.3.4 Orientation . . . 1706
20.3.5 Formes différentielles . . . 1708
20.3.6 Intégrale d'une fonction sur une sous-variété . . . 1709
20.4 Longueur, aire, volumes etc. . . . 1710
20.4.1 Quelques aires faciles . . . 1710
20.5 Autres théorèmes de points fixes . . . 1712
20.5.1 Brouwer . . . 1712
20.5.2 Théorème de Schauder . . . 1714
20.5.3 Théorème de Cauchy-Arzella . . . 1715
20.5.4 Théorème de Markov-Kakutani . . . 1716
20.6 Intégrales curvilignes . . . 1717
20.6.1 Chemins de classe C^1 . . . 1717
20.6.2 Intégrer une fonction . . . 1718
20.6.3 Intégrer un champ de vecteurs . . . 1719
20.6.4 Intégrer une forme différentielle sur un chemin . . . 1720
20.6.5 Intégration d'une forme différentielle sur un chemin . . . 1720
20.6.6 Interprétation physique : travail . . . 1722
20.6.7 Intégrer un champ de vecteurs sur un bord en $2D$ . . . 1723
20.6.8 Intégrer une forme différentielle sur un bord en $2D$ . . . 1723
20.6.9 Intégrer une forme différentielle sur un bord en $3D$ . . . 1723
20.6.10 Intégrer un champ de vecteurs sur un bord en $3D$ . . . 1723
20.6.11 Dérivées croisées et forme différentielle exacte . . . 1724
20.7 Surfaces paramétrées . . . 1725
20.7.1 Graphe d'une fonction . . . 1726
20.7.2 Intégrale sur une partie de $\mathbb{R}^m$ . . . 1727
20.8 Intégrales de surface . . . 1728
20.8.1 Intégrale d'un champ de vecteurs . . . 1728
20.9 Aires et intégrales . . . 1728
20.9.1 Aire d'une surface paramétrée . . . 1728
20.9.2 Intégrale d'une fonction sur une surface . . . 1730
20.9.3 Intégrale d'une 2-forme . . . 1730
20.10 Flux d'un champ de vecteurs à travers une surface . . . 1731
20.11 Divergence, Green, Stokes . . . 1733
20.11.1 Théorème de la divergence . . . 1734
20.11.2 Lacets et homotopie . . . 1735
20.11.3 Formule de Green . . . 1735
20.11.4 Formule de Stokes . . . 1737
20.12 Résumé des intégrales vues . . . 1738
20.12.1 L'intégrale d'une fonction sur les réels . . . 1738
20.12.2 Intégrale d'une fonction sur un chemin . . . 1739
20.12.3 Intégrale d'une fonction sur une surface . . . 1739

20.12.4 Intégrale d'une fonction sur un volume . . . 1739
20.12.5 Conclusion pour les fonctions . . . 1740
20.12.6 Circulation d'un champ de vecteurs . . . 1740
20.12.7 Flux d'un champ de vecteurs . . . 1740
20.12.8 Conclusion pour les champs de vecteurs . . . 1741
20.12.9 Attention pour les surfaces fermées ! . . . 1741
20.13 Formes différentielles exactes et fermées . . . 1743
20.14 Théorème d'Abel angulaire . . . 1745
20.15 Passage à la limite sous le signe intégral . . . 1748
20.15.1 Intégrale en dimension un . . . 1748
20.15.2 Intégrales convergentes . . . 1749
20.15.3 La méthode de Rothstein-Trager . . . 1749
20.16 Rappel sur les intégrales usuelles . . . 1755
20.17 Intégrales le long de chemins . . . 1755
20.17.1 Circulation d'un champ de vecteur . . . 1755
20.18 Circulation d'un champ conservatif . . . 1757
20.19 Intégration de fonction à deux variables . . . 1759
20.19.1 Intégration sur un domaine rectangulaire . . . 1759
20.19.2 Intégration sur un domaine non rectangulaire . . . 1760
20.19.3 Changement de variables . . . 1762
20.20 Les intégrales triples . . . 1762
20.20.1 Volume . . . 1764
20.21 Un petit peu plus formel . . . 1765
20.21.1 Intégration sur un domaine non rectangulaire . . . 1765
20.22 Aire et primitive . . . 1767
20.22.1 Longueur d'arc de courbe . . . 1767
20.22.2 Aire de révolution . . . 1768
20.23 L'aire en dessous d'une courbe . . . 1768
20.24 Propriétés des intégrales . . . 1769
20.25 Techniques d'intégration . . . 1770
20.25.1 Intégration par parties . . . 1771
20.25.2 Changement de variables – pour trouver des primitives . . . 1772
20.25.3 Changement de variables – pour calculer des intégrales . . . 1774
20.25.4 Intégrations des fractions rationnelles réduites . . . 1776
20.25.5 Quelques formules à connaitre . . . 1776
20.25.6 Approximation de ln(2) . . . 1777
20.26 Constructions plus naïves de l'intégrale dans le cas réel . . . 1780
20.26.1 Mesure de Lebesgue, version rapide . . . 1780
20.26.2 Pavés et subdivisions . . . 1781
20.26.3 Intégrale d'une fonction en escalier . . . 1784
20.26.4 Intégrales partielles . . . 1784
20.26.5 Réduction d'une intégrale multiple . . . 1785
20.26.6 Propriétés de l'intégrale . . . 1786
20.26.7 Intégrales multiples, cas général . . . 1787
20.26.8 Réduction d'une intégrale multiple . . . 1788
20.26.9 Intégrales sur des parties de $\mathbb{R}^2$ . . . 1789
20.26.10 Intégrales sur des parties de $\mathbb{R}^3$ . . . 1792
20.26.11 Fonctions et ensembles non bornés . . . 1794
20.26.12 Lemme de Morse . . . 1795
20.27 Autres intégrales sympathiques . . . 1797
20.27.1 Intégrale de Wallis . . . 1797
20.27.2 Formule de Stirling . . . 1801
20.27.3 La fonction sinus cardinal, intégrale de Dirichlet . . . 1804

21 Arcs paramétrés **1815**
21.1 Définitions . . . 1815
21.2 Longueur d'arc . . . 1815
21.3 Abscisse curviligne . . . 1818
21.3.1 Formule intégrale de la longueur . . . 1819
21.4 Suite du chapitre . . . 1825
21.5 Autres exemples . . . 1826
21.6 Élément de longueur . . . 1827
21.6.1 Élément de longueur : cartésiennes . . . 1827
21.6.2 Élément de longueur : polaires (1) . . . 1827
21.6.3 Élément de longueur : polaires (2) . . . 1828
21.6.4 Approximation de la longueur par des cordes . . . 1830
21.7 Arc géométrique . . . 1831
21.7.1 Abscisse curviligne et paramétrage normal . . . 1833
21.7.2 Tangente à une courbe paramétrée . . . 1838
21.8 Un peu de topologie . . . 1839
21.9 Repère de Frenet . . . 1842
21.9.1 Torsion . . . 1844
21.10 Hors des coordonnées normales . . . 1845
21.11 Tracer des courbes paramétriques dans $\mathbb{R}^2$ . . . 1848
21.12 Courbes planes . . . 1849
21.12.1 Angle . . . 1849
21.12.2 Courbure signée . . . 1850
21.12.3 Degré, indice et homotopie . . . 1853
21.13 Courbes fermées planes . . . 1860
21.13.1 Cercle circonscrit . . . 1860
21.13.2 Description locale . . . 1862
21.13.3 Enveloppe convexe . . . 1863
21.13.4 Courbure et convexité . . . 1867
21.13.5 Théorème des quatre sommets . . . 1868
21.13.6 Espace topologique normal . . . 1870
21.13.7 Théorème d'Urysohn . . . 1870

22 Géométrie hyperbolique **1875**
22.1 Inversion . . . 1875
22.1.1 Cercles perpendiculaires . . . 1875
22.1.2 Inversion . . . 1876

23 Espaces projectifs **1881**
23.1 Sous espaces projectifs . . . 1881
23.2 Espace projectifs comme « complétés » d'espaces affines . . . 1883
23.3 Théorème de Pappus . . . 1886
23.4 Homographies . . . 1887
23.4.1 Homographies . . . 1887
23.4.2 Le groupe projectif . . . 1888
23.4.3 Repères projectifs . . . 1889
23.4.4 Identifications $P(\mathbb{K}^2)$ vers $\mathbb{K} \cup \{\infty\}$ . . . 1893
23.4.5 Birapport . . . 1894
23.5 Coordonnées homogènes . . . 1900
23.5.1 Curiosité : matrice de translation . . . 1900
23.5.2 Dualité . . . 1901
23.5.3 Polynômes . . . 1903
23.6 La sphère de Riemann $P_1(\mathbb{C})$ . . . 1904
23.6.1 Éléments de géométrie dans $P_1(\mathbb{C})$ . . . 1905

23.6.2 Homographies . . . 1908
23.6.3 Birapport . . . 1914
23.6.4 Division harmonique . . . 1917
23.6.5 Groupe circulaire . . . 1921
23.6.6 Action du groupe modulaire . . . 1923

24 Analyse vectorielle **1929**
24.1 Le théorème de Green . . . 1929
24.2 Théorème de la divergence dans le plan . . . 1933
24.2.1 La convention de sens de parcours . . . 1933
24.2.2 Théorème de la divergence . . . 1934
24.3 Théorème de Stokes . . . 1934
24.4 Théorème de Gauss . . . 1936
24.5 Coordonnées curvilignes . . . 1938
24.5.1 Base locale . . . 1938
24.5.2 Importance de l'orthogonalité . . . 1938
24.5.3 Coordonnées polaires . . . 1940
24.5.4 Coordonnées cylindriques . . . 1940
24.5.5 Coordonnées sphériques . . . 1941
24.5.6 Gradient en coordonnées curvilignes . . . 1941
24.5.7 Divergence en coordonnées curvilignes . . . 1942
24.5.8 Laplacien en coordonnées curvilignes orthogonales . . . 1945
24.5.9 Rotationnel en coordonnées curvilignes orthogonales . . . 1945
24.6 Les formules . . . 1946
24.6.1 Coordonnées polaires . . . 1946
24.6.2 Coordonnées cylindriques . . . 1946
24.6.3 Coordonnées sphériques . . . 1947

25 Espaces de Hilbert **1949**
25.1 Espaces de Hilbert . . . 1949
25.1.1 Sous-espace vectoriel fermé ? ? ? . . . 1952
25.2 Théorème de la projection . . . 1953
25.3 Systèmes orthogonaux et bases . . . 1956
25.3.1 Orthogonal d'une partie . . . 1956
25.3.2 Dual, théorème de représentation de Riesz . . . 1957
25.3.3 Séparabilité . . . 1958
25.3.4 Base hilbertienne . . . 1960
25.3.5 Décomposition dans une base hilbertienne . . . 1965
25.3.6 Digression sur les normes opérateurs . . . 1970
25.3.7 Applications linéaires et continuité . . . 1971
25.4 Théorème de Kochen-Specker . . . 1973
25.5 Théorème de Lax-Milgram . . . 1974

26 Analyse complexe **1979**
26.1 Fonctions holomorphes . . . 1979
26.1.1 Équations de Cauchy-Riemann . . . 1979
26.1.2 Intégrale sur un chemin dans $\mathbb{C}$ . . . 1982
26.1.3 Intégrales sur des chemins fermés . . . 1982
26.1.4 Homotopie entre applications . . . 1984
26.1.5 Intégrale et homotopie . . . 1986
26.1.6 Thérorème de Tietze (espace normal) . . . 1988
26.2 Logarithme complexe . . . 1990
26.2.1 La fonction argument . . . 1990
26.2.2 Une définition possible du logarithme . . . 1993

26.2.3 Pas plus de continuité . . . 1995
26.2.4 Pas d'unicité : autres déterminations de l'argument . . . 1996
26.2.5 Pas d'unicité : développement en série . . . 1998
26.2.6 Pas d'unicité : laquelle choisir ? . . . 1998
26.2.7 Logarithme comme primitive . . . 1998
26.2.8 Logarithme sur un chemin . . . 2000
26.2.9 Lacets, indice et homotopie . . . 2002
26.2.10 Théorème de Cauchy et analycité . . . 2008
26.2.11 Théorème de Brouwer en dimension 2 . . . 2012
26.2.12 Principe des zéros isolés . . . 2013
26.2.13 Prolongement de fonctions holomorphes . . . 2015
26.2.14 Théorème de Runge . . . 2015
26.3 Intégrales de fonctions holomorphes . . . 2017
26.3.1 Holomorphie sous l'intégrale . . . 2018
26.3.2 Mesure de Radon . . . 2022
26.4 Conditions équivalentes à l'holomorphie . . . 2024
26.5 Singularités, pôles et méromorphe . . . 2025
26.6 Dénombrement des solutions d'une équation diophantienne . . . 2028
26.7 Fonctions d'Euler . . . 2034
26.7.1 Euler et factorielle . . . 2037
26.8 Exponentielle et logarithme complexe . . . 2038
26.8.1 Propriétés de l'exponentielle . . . 2038
26.8.2 Intégrale de Fresnel . . . 2039
26.9 Théorème de Weierstrass . . . 2041
26.10 Analyse complexe en plusieurs variables . . . 2042
26.10.1 Inverse de fonctions analytiques . . . 2043

27 Analyse fonctionnelle **2045**
27.1 Théorème d'isomorphisme de Banach . . . 2045
27.2 Théorème d'Ascoli . . . 2045
27.3 Espaces de Lebesgue L^p . . . 2050
27.3.1 Généralités . . . 2050
27.3.2 Un peu de convergence de suites . . . 2053
27.3.3 L'espace L^∞ . . . 2055
27.3.4 Quelques identifications . . . 2056
27.3.5 Inégalité de Young, Jensen, Hölder et de Minkowski . . . 2057
27.3.6 Ni inclusions ni inégalités . . . 2068
27.3.7 Complétude . . . 2070
27.3.8 Théorèmes d'approximation . . . 2075
27.3.9 Densité des fonctions infiniment dérivables à support compact . . . 2076
27.3.10 Approximation . . . 2079
27.4 Convolution . . . 2080
27.4.1 Approximation de l'unité . . . 2083
27.4.2 Densité des polynômes trigonométriques . . . 2086
27.5 Espaces L^2, généralités . . . 2087
27.6 L'espace $L^2(\mathbb{R}^d)$ . . . 2089
27.7 L'espace $L^2(S^1)$ . . . 2090
27.7.1 Espace mesuré . . . 2090
27.7.2 Topologie . . . 2091
27.7.3 Système trigonométrique . . . 2097
27.7.4 Convolution . . . 2098
27.7.5 Approximation de l'unité . . . 2100
27.7.6 Base hilbertienne (suite des polynômes trigonométriques) . . . 2105
27.7.7 Convolution, bis . . . 2106

27.8 L'espace $L^2([a,b])$ . . . 2106
27.9 Sur $[0,2\pi[$ . . . 2109
27.10 Sur $[-T,T[$ . . . 2110
27.10.1 Le cas dans $[0,2\pi]$ . . . 2110
27.11 Théorème de la projection normale . . . 2112
27.11.1 Espace uniformément convexe . . . 2112
27.11.2 Des inégalités . . . 2114
27.11.3 Inégalités de Clarkson . . . 2121
27.11.4 Uniforme convexité des espaces de Lebesgue . . . 2125
27.11.5 Théorème de la projection normale . . . 2125
27.12 Théorèmes de Hahn-Banach . . . 2127
27.12.1 Applications $\mathbb{R}$-linéaires et $\mathbb{C}$-linéaires . . . 2127
27.12.2 Hahn-Banach, théorème d'extension dominée . . . 2130
27.12.3 Hyperplan séparateur . . . 2132
27.12.4 Prolongement de fonctionnelles (dimension finie) . . . 2134
27.12.5 Prolongement de fonctionnelles (dimension infinie) . . . 2136
27.13 Théorème de Tietze . . . 2138
27.13.1 Pas de bicontinues entre dimensions différentes . . . 2141
27.14 Dualité, réflexivité et théorème de représentation de Riesz . . . 2144
27.14.1 Le théorème de Jordan . . . 2158
27.14.2 Théorème de Jordan . . . 2171
27.15 Topologie faible . . . 2171
27.15.1 Espace de Banach réflexif . . . 2176
27.15.2 Espaces L^∞ . . . 2176
27.16 Espace de Schwartz . . . 2177
27.16.1 Topologie . . . 2178
27.16.2 Produit de convolution . . . 2181
27.17 Théorème de Montel . . . 2181
27.18 Espaces de Bergman . . . 2182

28 Séries de Fourier **2187**
28.1 Densité des polynômes trigonométriques . . . 2187
28.1.1 Convergence pour les fonctions continues (via Weierstrass) . . . 2187
28.1.2 Convergence pour les fonctions continues (via Fejér) . . . 2187
28.1.3 Densité dans L^p . . . 2191
28.1.4 Suite équirépartie, critère de Weyl . . . 2191
28.2 Fonctions de Dirichlet . . . 2194
28.3 Coefficients et série de Fourier . . . 2195
28.3.1 Le contre-exemple que nous attendions tous . . . 2198
28.3.2 Inégalité isopérimétrique . . . 2201
28.3.3 À propos des coefficients . . . 2202
28.4 Série de Laurent . . . 2204

29 Transformation de Fourier **2211**
29.1 Transformée de Fourier sur $L^1(\mathbb{R}^d)$ . . . 2212
29.1.1 Formule sommatoire de Poisson . . . 2215
29.2 Suite régularisante . . . 2218
29.3 Transformée de Fourier dans l'espace de Schwartz . . . 2220
29.3.1 Quelques transformées de Fourier . . . 2222
29.3.2 Formule d'inversion . . . 2224
29.4 Transformée de Fourier sur $L^2(\mathbb{R}^d)$ . . . 2228
29.4.1 Le problème . . . 2228
29.4.2 Extension de $L^1 \cap L^2$ vers L^2 . . . 2229
29.4.3 Une formule de Leibnitz . . . 2231

30 Distributions **2233**
30.1 Dérivée faible . . . 2234
30.1.1 Dérivée partielle au sens faible . . . 2234
30.1.2 Dérivée faible partielle . . . 2236
30.2 Topologie et convergence sur des espaces de fonctions . . . 2237
30.2.1 Limite inductive . . . 2237
30.2.2 Les espaces classiques . . . 2237
30.3 Distributions . . . 2240
30.3.1 Multiplication d'une distribution par une fonction . . . 2241
30.3.2 Dérivée de distribution . . . 2242
30.3.3 Ordre et support d'une distribution . . . 2243
30.4 L'espace $C^\infty(\mathbb{R}, \mathscr{D}'(\mathbb{R}^d))$ . . . 2246
30.4.1 Dérivation . . . 2248
30.5 Une équation de distribution . . . 2249
30.6 Localisation, principe de recollement . . . 2250
30.7 Permuter distributions, dérivées et intégrales . . . 2254
30.8 Distributions tempérées . . . 2259
30.8.1 Topologie . . . 2261
30.8.2 Distributions associées à des fonctions . . . 2261
30.8.3 Composition avec une fonction . . . 2261
30.8.4 Transformée de Fourier d'une distribution tempérée . . . 2262
30.8.5 Convolution d'une distribution par une fonction . . . 2262
30.8.6 Approximation de la distribution de Dirac . . . 2263
30.8.7 Peigne de Dirac . . . 2266
30.9 L'espace $C^\infty(\mathbb{R}, \mathscr{S}'(\mathbb{R}^d))$ . . . 2267
30.9.1 Propriétés générales . . . 2267
30.9.2 Dérivation . . . 2269

31 Espaces de Sobolev, équations elliptiques **2273**
31.1 Espaces de Sobolev . . . 2273
31.1.1 Sur un intervalle de $\mathbb{R}$ . . . 2273
31.1.2 Sur un ouvert de $\mathbb{R}^n$ . . . 2278
31.1.3 Espace de Sobolev fractionnaire . . . 2280
31.2 Trace . . . 2282
31.3 Théorème de plongement . . . 2285

32 Équations différentielles ordinaires **2291**
32.1 Équation homogène, solution particulière . . . 2292
32.2 Que faire avec $f(z)dz = g(t)dt$? . . . 2293
32.3 Équations linéaires du premier ordre . . . 2294
32.3.1 Pourquoi la variation des constantes fonctionne toujours ? . . . 2295
32.4 Équations à variables séparées . . . 2296
32.4.1 La méthode rapide . . . 2296
32.4.2 La méthode plus propre . . . 2297
32.4.3 Les théorèmes . . . 2297
32.5 Équations linéaires d'ordre supérieur . . . 2299
32.5.1 Équations et systèmes linéaires à coefficients constants . . . 2299
32.5.2 Si les coefficients ne sont pas constants ? . . . 2300
32.6 Système d'équations linéaires . . . 2300
32.6.1 La magie de l'exponentielle. . . . 2300
32.6.2 . . .mais la difficulté . . . 2301
32.6.3 La recette . . . 2301
32.6.4 Système d'équations linéaires avec matrice constante . . . 2302
32.6.5 Système d'équations linéaires avec matrice non constante . . . 2302

32.7 Réduction de l'ordre . . . 2302
32.8 Autour de Cauchy-Lipschitz . . . 2304
32.8.1 Fuite des compacts et explosion en temps fini . . . 2305
32.8.2 Écart entre deux conditions initiales . . . 2306
32.8.3 Flot d'un champ de vecteurs . . . 2308
32.8.4 Stabilité de Lyapunov . . . 2321
32.8.5 Système proies-prédateurs de Lotka-Volterra . . . 2325
32.9 Équation du second ordre . . . 2328
32.9.1 Wronskien . . . 2328
32.9.2 Avec second membre . . . 2329
32.9.3 Équation $y'' + q(t)y = 0$ . . . 2329
32.9.4 Équation de Hill . . . 2331
32.10 Différents types d'équations différentielles . . . 2334
32.10.1 Équation homogène . . . 2334
32.10.2 Équation de Bernoulli . . . 2334
32.10.3 Équation de Riccati . . . 2335
32.10.4 Équation différentielle exacte . . . 2335
32.11 Distributions pour les équations différentielles . . . 2336
32.11.1 Équation de Schrödinger . . . 2336
32.12 Équations différentielles du premier ordre . . . 2340
32.13 Premier ordre, variables séparables . . . 2342
32.14 Équations différentielles linéaires du premier ordre . . . 2345
32.14.1 Méthode de variation de la constante . . . 2346
32.15 Équations différentielles linéaires du second ordre . . . 2347
32.15.1 Équations différentielles linéaires du second ordre homogènes à coefficients constants . . . 2348
32.15.2 Linéaires du second ordre à coefficients constants, non homogènes . . . 2349
32.16 Fonction de Green . . . 2351

33 Équations aux dérivées partielles **2353**
33.1 Symbole principal, équation des caractéristiques . . . 2353
33.2 Méthode des caractéristiques pour l'ordre 1 . . . 2353
33.2.1 Un exemple complet un peu minimal . . . 2354
33.2.2 Un théorème d'existence et d'unicité . . . 2356
33.3 Méthode des caractéristiques pour l'ordre 2 . . . 2360
33.3.1 Principe général . . . 2360
33.3.2 Exemple : l'équation d'onde . . . 2361
33.4 Classification des équations du second ordre . . . 2362
33.4.1 Problème au limite . . . 2363
33.5 Principe du maximum . . . 2364
33.6 Quelques exemples . . . 2368
33.6.1 Un changement de variables . . . 2368

34 Numérique **2371**
34.1 Introduction . . . 2371
34.2 Représentations numériques . . . 2371
34.2.1 Entier relatif en complément à deux (binaire) . . . 2371
34.2.2 Représentation en virgule flottante . . . 2373
34.2.3 Simple précision, IEEE-754 . . . 2373
34.3 Problèmes pour écrire des nombres . . . 2376
34.3.1 Troncature : la base . . . 2376
34.3.2 Troncature : le drift . . . 2377
34.3.3 Quelques bonnes règles . . . 2378
34.3.4 Erreur de "cancellation" . . . 2378

34.3.5 Calcul d'une dérivée . . . 2380
34.3.6 Erreur d'absorption . . . 2380
34.4 Conditionnement et stabilité . . . 2381
34.4.1 Comment choisir et penser le K ? . . . 2384
34.5 Un peu de points fixes . . . 2385
34.5.1 Choix de la fonction à point fixe . . . 2385
34.5.2 Convergence quadratique . . . 2386
34.5.3 Convergence . . . 2388
34.6 Méthode de Newton . . . 2389
34.6.1 « Justification » par la formule de Taylor . . . 2389
34.6.2 « Justification » par points fixes . . . 2390
34.6.3 Convergence de la méthode de Newton . . . 2390
34.6.4 Racine carrée par la méthode de Newton . . . 2392
34.6.5 Formalisation de l'algorithme . . . 2392
34.6.6 Caractéristiques . . . 2393
34.6.7 Exemple de la racine carrée . . . 2394
34.6.8 Si multiplicité . . . 2395
34.6.9 Et la dérivée ? . . . 2395
34.6.10 Méthode de Newton : le cas général . . . 2395
34.7 Estimation de l'ordre de convergence . . . 2397
34.8 Autres méthodes . . . 2398
34.8.1 Méthode de Schröder . . . 2398
34.8.2 Halley . . . 2398
34.9 Méthode des sécantes variables . . . 2398
34.9.1 Aitken . . . 2399
34.10 Équations algébrique . . . 2400
34.10.1 Résoudre un système linéaire . . . 2400
34.10.2 Caractéristiques . . . 2400
34.10.3 Définitions . . . 2401
34.11 Équations non linéaires . . . 2401
34.11.1 Méthode de bisection . . . 2403
34.12 Efficacité . . . 2405
34.13 Exemples sous forme d'exercices . . . 2405
34.14 Approximations de fonctions . . . 2409
34.14.1 Critère d'interpolation . . . 2409
34.14.2 Base de Newton . . . 2410
34.14.3 Méthode des minimums quadratiques . . . 2411
34.14.4 Notre espace de Hilbert . . . 2412
34.14.5 Droite de régression . . . 2413
34.15 Conditionnement d'une matrice . . . 2414
34.15.1 Perturbation du vecteur . . . 2416
34.15.2 Perturbation de la matrice . . . 2418
34.16 Système linéaires (généralités) . . . 2419
34.16.1 Les méthodes directes . . . 2419
34.16.2 Méthodes itératives . . . 2420
34.17 Système linéaires (méthodes directes) . . . 2420
34.17.1 Inversion de matrice triangulaire . . . 2420
34.17.2 Transformation gaussienne . . . 2421
34.17.3 Méthode de Gauss pour résoudre des systèmes d'équations linéaires . . . 2422
34.17.4 Méthode de Gauss sans pivot (décomposition LU) . . . 2423
34.17.5 Matrice de permutation élémentaire . . . 2427
34.18 Méthode de Gauss avec pivot partiel (décomposition PLU) . . . 2428
34.18.1 L'idée . . . 2428

34.18.2 Le théorème . . . 2429
34.18.3 D'un point de vue algorithmique . . . 2432
34.18.4 Exemples . . . 2434
34.19 Résolution de systèmes linéaires (suite) . . . 2437
34.19.1 Déterminant . . . 2437
34.19.2 Plusieurs termes indépendants . . . 2437
34.19.3 Cholesky . . . 2438
34.20 Système linéaire (méthodes itératives) . . . 2441
34.20.1 La méthode générale . . . 2442
34.20.2 Jacobi . . . 2442
34.20.3 Gauss-Seidel . . . 2442
34.20.4 Autres . . . 2442
34.21 Indices connectés, matrice irréductible . . . 2442
34.22 Localisation des valeurs propres . . . 2444
34.22.1 Matrices à diagonale dominante . . . 2446
34.22.2 M-matrice . . . 2449

35 Méthode des différences finies 2453
35.1 Problèmes de dimension un . . . 2453
35.1.1 Un schéma à cinq points . . . 2454
35.1.2 Exemple . . . 2459
35.2 Problèmes de dimension deux . . . 2459
35.2.1 Discrétisation en croix . . . 2460
35.2.2 Discrétisation en carré . . . 2461
35.2.3 Résolution de la discrétisation en croix . . . 2462
35.3 Consistance, convergence . . . 2464
35.3.1 Définitions, mise en place . . . 2464
35.3.2 Exemple . . . 2465
35.3.3 Consistance, stabilité et convergence . . . 2467
35.3.4 Exemple : schéma à cinq points, laplacien en croix . . . 2468
35.4 Autres laplaciens . . . 2469
35.4.1 Travail avec le laplacien à 9 points . . . 2472

36 Variables aléatoires et théorie des probabilités 2473
36.1 Espace de probabilité . . . 2473
36.2 Variables aléatoires . . . 2474
36.2.1 Indépendance . . . 2474
36.2.2 Lois conjointes et indépendance . . . 2477
36.2.3 Espérance . . . 2478
36.2.4 Espérance . . . 2479
36.2.5 Somme et produit de variables aléatoires indépendantes . . . 2479
36.2.6 Variance . . . 2482
36.2.7 Covariance . . . 2483
36.2.8 Probabilité conditionnelle : événements . . . 2483
36.2.9 Espérance conditionnelle . . . 2486
36.2.10 Probabilité conditionnelle : tribu . . . 2494
36.2.11 Variables de Rademacher indépendantes . . . 2496
36.2.12 Un petit paradoxe . . . 2498
36.2.13 Inégalité de Jensen . . . 2504
36.2.14 Fonction de répartition . . . 2505
36.2.15 Fonction caractéristique . . . 2505
36.2.16 Fonction génératrice des moments, transformée de Laplace . . . 2507
36.2.17 Loi d'une variable aléatoire . . . 2508
36.2.18 Changement de variables . . . 2510

36.3 Convergence . . . 2511
36.4 Loi des grands nombres, théorème central limite . . . 2516
36.4.1 Loi des grands nombres . . . 2516
36.4.2 Théorème central limite . . . 2518
36.4.3 Marche aléatoire . . . 2521
36.5 Les lois usuelles . . . 2522
36.5.1 Loi de Bernoulli . . . 2522
36.5.2 Loi binomiale . . . 2523
36.5.3 Loi multinomiale . . . 2524
36.5.4 Loi géométrique . . . 2524
36.5.5 Loi de Poisson . . . 2525
36.5.6 Loi exponentielle . . . 2525
36.5.7 Approximation de la binomiale par une Poisson . . . 2528
36.5.8 Loi de Poisson et loi exponentielle . . . 2529
36.5.9 Loi normale . . . 2530
36.5.10 Vecteurs gaussiens . . . 2532
36.5.11 Variable aléatoire de Rademacher . . . 2536
36.5.12 Loi de Student . . . 2538
36.5.13 Indépendance, covariance et variance de somme . . . 2538
36.6 Estimation des grands écarts . . . 2539
36.7 Simulations de réalisations de variables aléatoires . . . 2542
36.7.1 Générateur uniforme . . . 2543
36.7.2 Simulation par inversion . . . 2543
36.7.3 Algorithme de Box-Muller . . . 2544
36.7.4 Méthode du rejet . . . 2545
36.7.5 Simuler une loi géométrique à l'ordinateur . . . 2547
36.7.6 Simuler une loi exponentielle à l'ordinateur . . . 2547
36.7.7 Simuler une loi de Poisson à l'ordinateur . . . 2547
36.8 Sage . . . 2548
36.8.1 Loi exponentielle . . . 2548
36.8.2 Inverser des lois . . . 2548
36.9 Monte-Carlo . . . 2549
36.9.1 Intervalle de confiance . . . 2550
36.10 Résultats qui se démontrent avec des variables aléatoires . . . 2552
36.10.1 Nombres normaux . . . 2552
36.10.2 Théorème de Bernstein . . . 2554

37 Statistiques **2559**
37.1 Notations et hypothèses . . . 2559
37.2 Modèle statistique . . . 2559
37.3 Modèles d'échantillonnages . . . 2562
37.4 Estimation ponctuelle . . . 2565
37.5 Statistiques et estimateurs . . . 2567
37.5.1 Qualité des estimateurs . . . 2567
37.5.2 Méthode des moments . . . 2568
37.5.3 Méthode de substitution . . . 2569
37.5.4 Méthode du maximum de vraisemblance . . . 2570
37.5.5 Exemples sous forme d'exercices . . . 2570
37.5.6 Estimation d'une fonction de répartition . . . 2572
37.5.7 Exemples sous forme d'exercices . . . 2573
37.5.8 Espérance et variance d'un estimateur . . . 2574
37.6 Estimation par intervalle de confiance . . . 2575
37.6.1 Région de confiance . . . 2578
37.6.2 Fonction pivotale . . . 2578

37.6.3 Sondage de proportion . . . 2581
37.7 Estimer une densité lorsqu'on ne sait rien . . . 2582
37.7.1 Distance entre des mesures . . . 2583
37.7.2 Estimateur par fenêtres glissantes . . . 2584
37.8 Test d'hypothèses, prise de décision . . . 2586
37.8.1 Exemple : qualité des pièces d'usine . . . 2586
37.8.2 Exemple : la résistance d'un fil . . . 2586
37.8.3 Vocabulaire et théorie . . . 2587
37.8.4 Risque de première et seconde espèce . . . 2588
37.8.5 Modèle paramétrique de loi gaussienne . . . 2589
37.9 Tests paramétriques . . . 2590
37.10 Tests d'adéquation . . . 2591

38 Chaînes de Markov à temps discret **2597**
38.1 Généralités . . . 2597
38.1.1 Matrice stochastique . . . 2599
38.2 Chaînes de Markov sur un ensemble fini . . . 2600
38.2.1 Graphe de transition . . . 2602
38.2.2 Nombre de visites . . . 2602
38.2.3 Récurrent et transient . . . 2604
38.2.4 Chaînes irréductibles . . . 2605
38.2.5 Périodique et irréductible . . . 2610
38.3 Marche aléatoire sur $\mathbb{Z}$ . . . 2612
38.3.1 Chaînes de Markov homogènes . . . 2614
38.3.2 Chaîne de Markov définie par récurrence . . . 2616
38.4 Classification des états . . . 2620
38.5 Mesure invariante . . . 2622
38.6 Convergence vers l'équilibre . . . 2624
38.7 Processus de Galton-Watson . . . 2624

39 Martingales **2629**
39.1 Convergence de martingales . . . 2629
39.2 Temps d'arrêt et martingale terminée . . . 2632
39.3 Décomposition de martingales . . . 2634
39.4 Problème de la ruine du joueur . . . 2636
39.4.1 Le cas où la pièce est truquée . . . 2637
39.4.2 Le cas où la pièce est non truquée . . . 2640
39.4.3 Un petit complément . . . 2642

40 Processus de Poisson **2645**
40.1 Processus de Poisson . . . 2645
40.2 Quelques trucs sur la simulation . . . 2656
40.2.1 Le théorème central limite pour Markov . . . 2656
40.2.2 Feuille 5 . . . 2657
40.2.3 Feuille 6 . . . 2657
40.2.4 Feuille 7 . . . 2657
40.2.5 Simuler des lois conditionnelles . . . 2658

41 Langages **2659**
41.1 Alphabets et mots . . . 2659
41.2 Langages . . . 2660

42 Utilisation dans les autres sciences **2663**
42.1 Démystification du MRUA . . . 2663

42.1.1 Preuve de la formule . . . 2663
42.1.2 Interprétation graphique . . . 2664
42.2 Relativité en mécanique newtonienne . . . 2664
42.2.1 Relativité du mouvement . . . 2664
42.2.2 Bob et Alice . . . 2664
42.3 Invariance de la vitesse de la lumière . . . 2665
42.3.1 Champ de gravitation et électrique . . . 2665
42.3.2 Support du champ : pas d'éther . . . 2665
42.3.3 Le problème . . . 2666
42.4 Conséquences . . . 2666
42.4.1 Ligne d'univers . . . 2666
42.4.2 Transformations de Lorentz . . . 2667
42.4.3 Conditions d'existence . . . 2670
42.4.4 La notion d'intervalle . . . 2671
42.4.5 Le cône de lumière d'un point . . . 2671
42.4.6 Contraction des longueurs . . . 2672
42.4.7 Dilatation des intervalles de temps . . . 2672
42.4.8 Invariance de l'intervalle . . . 2673
42.4.9 Vitesse limite . . . 2677
42.5 Applications . . . 2677
42.5.1 Le GPS . . . 2678
42.5.2 Les ondes électromagnétiques . . . 2678
42.6 Mécanique relativiste . . . 2678
42.6.1 Des problèmes, toujours des problèmes . . . 2678
42.6.2 Loi d'addition des vitesses . . . 2679
42.6.3 L'action d'une force . . . 2679
42.6.4 Équivalence entre la masse et l'énergie . . . 2681
42.7 Principe de correspondance . . . 2681

43 Exemples avec Sage **2683**
43.1 Graphiques . . . 2683
43.1.1 Autres . . . 2683

44 Épilogue : la constante de Weiner **2703**

45 Développements possibles **2705**
45.1 Algèbre et géométrie . . . 2705
45.2 Analyse . . . 2709
45.3 Anciennes leçons . . . 2712

46 GNU Free Documentation License **2721**

Bibliographie **2729**

Index

λ-système, 1146
p-groupe, 365
p-Sylow, 366
q-orthogonal, 635

Abel
    angulaire, 1745
    convergence radiale, 1306
Abel
    angulaire, 1745
    convergence radiale, 1306
abélianisé, 254
abscisse
    curviligne, 1833
absolument continue, 1412
absorbant, 2620
accélération d'un chemin, 1815
accroissement, 1102
accroissements finie
    dérivée partielle, 981
action, 218
    adjointe, 262
    de groupe
        Wedderburn, 1660
    domaine fondamental, 265
    fidèle, 262
    libre, 268
    transitive, 268
action de groupe, 590
    sur des matrices, 1795
action fidèle, 262
action transitive, 268
adjoint, 599
affine
    application, 563
    espace, 559
    sous-espace, 566
aire, 1791
aire dans $\mathbb{R}^2$, 1710
algèbre, 212
    de parties, 1140
    engendrée, 212
algèbre de Banach, 525
algèbre engendrée, 1315
algébrique, 421
algébriquement
    indépendant, 463
algorithme, 2401
    consistant, 2401
    facteurs invariants, 351
    fortement consistant, 2401
    stable, 2401
algorithme convergent, 2401
alignement
    dans un espace projectif, 1882
alphabet, 2659
alterné
    groupe, 381
    polynôme, 459
analytique
    au sens complexe, 1088
angle
    d'une courbe, 1852
    entre deux droites, 1566
    orienté de vecteurs, 1561
angle entre deux vecteurs, 1521
anneau, 117
    $\mathbb{Z}/n\mathbb{Z}$, 375, 1652, 1660, 1664
    à division, 393
    de séries formelles, 1375
    euclidien
        facteurs invariants, 351
    factoriel, 290
    noethérien, 294
    principal, 292, 401, 623
        utilisation, 402
    quotient par un idéal, 169
Anneau
    $\mathbb{Z}/n\mathbb{Z}$
        polynôme cyclotomique, 1656
anneau commutatif, 117
anneau intègre, 171
anneau topologique, 505
apériodique
    état d'une chaine de Markov, 2611
application
    de classe C^k, 843
    définie positive, 629

différentiable, 842, 843, 993, 1028, 1431, 1795
extrémums lié, 1446
en escalier, 1783
linéaire
théorème de Banach-Steinhaus, 805
mesurable, 1145
multilinéaire, 778
ouverte, 517
semi-définie positive, 629
tangente, 997
application affine, 638
application bilinéaire, 628
application multilinéaire
décomposable, 821
application ouverte, 807
application quotient, 476
application réciproque, 511
applications homotopes, 1984
applications linéaires semblables, 651
approximation
de fonctions
par des polynômes, 2554
de l'unité, 2083
par polynômes, 1401
polynomiale, 2015
arc
géométriques, 1832
paramétré, 1815
arc cosinus, 1520
arc sinus, 1518
arc tangente, 1516
archimédien, 128
associée
subdivision, 1783
associés
éléments d'un anneau, 288
asymptotiquement pivotale, 2578
attractif
point fixe, 1417
automorphisme, 474
d'espace vectoriel, 323
automorphisme de groupes, 116
axiome
du choix, 110

Baire
espace, 557
théorème, 558
tribu, 1157
Baire
espace, 557
théorème, 558
tribu, 1157
barycentre
cas affine, 568
cas vectoriel, 1542
enveloppe convexe, 572
base, 314
d'un module, 211
de Newton, 2410
de topologie
dénombrable, 495
espace métrique, 495
duale, 357
espace préhilbertien, 1960
hilbertienne, 1960
utilisation, 2201
locale, 1938
base associée à un repère cartésien, 560
base canonique de $\mathbb{R}^m$, 318
base de topologie, 465
base de topologie et continuité, 473
base de voisinages, 466
base orthonormée, 641
base préduale, 358
Bergman (espace), 2182
Bernoulli, 2522
somme, 2540
Berry-Esséen (borne), 2521
Bessel
inégalité, 1959
Bézout
anneau principal, 292
calcul effectif, 274
nombres entiers, 181
polynômes, 414
biais
d'estimateur, 2568
bien
conditionné, 2382
enchainé, 545
biholomorphe, 2043
bijection, 110, 511
bilinéaire, 778
binormale, 1843
birapport, 1895
birapport dans $\mathbb{C} \cup \{\infty\}$, 1914
birégulier
point sur une courbe, 1830
Bolzano-Weierstrass
espaces métriques, 497
bon
ordre, 112
bord, 493
borélienne
fonction, 1155
tribu, 1153

boréliens, 1153
borné, 496
    partie de V, 602
    temps d'arrêt, 2632
bornée
    différentielle, 1015
    partie de $\mathbb{R}^m$, 905
    suite, 714
boule
    avec seminormes, 550
    ouverte, 492
boule dans un corps, 221
boule fermée, 495
Bruhat (décomposition), 1131
Burnisde
    formule, 265

canonique
    base, 318
    décomposition, 116
    espace affine, 560
canonique
    base, 318
    décomposition, 116
    espace affine, 560
Cantor
    ensemble, 1203
caractère, 1386
    abélien, 1379
    de S_4, 1393
    groupe diédral, 1642
    irréductible, 1386
caractéristique
    d'un anneau, 213
    d'une équation différentielle, 2353
    polynôme, 625
    sous-groupe, 166
cardinal, 148
cardioïde, 1829
carré
    dans un corps fini, 1665
carrée
    matrice, 330
carte, 1698
catégorie
    ensemble de première, 548
Cauchy
    critère
        uniforme, 1046
    déterminant, 592
    formule, 2009
    suite, 534
    théorème, 365
Cauchy-continue, 898
Cauchy-Riemann, 1979
Cauchy-Schwarz, 745, 1951
Cayley
    théorème, 365
cellule d'un pavage, 1783
centrale (application), 1386
centralisateur, 166, 168
centre
    d'un anneau, 168
    d'un groupe, 166
    d'une rotation, 1550
cercle
    circonscrit à une courbe, 1860
    dans la sphère de Riemann, 1906
cercle-droite, 1906
cercles
    perpendiculaires, 1875
Cesàro
    moyenne, 799
chaine, 545
    de Markov, 2597
        convergence, 2624
        finie, 2600
        homogène, 2597
        irréductible, 2600
        récurrente positive, 2608
chaine de Markov apériodique, 2611
chaine de Markov régulière, 2600
champ
    conservatif, 1757
    de vecteurs, 1719
champ de vecteur conservatif, 1722
champ dérivant d'un potentiel, 1757
changement de variable, 1832
Chasles, 559
chemin, 1735
    dans $\mathbb{R}^p$, 1815
chemin C^1 par morceaux, 1717
chemin de Jordan, 1735
chemin régulier, 1735
circulation, 1755
classe
    d'association, 288
    de conjugaison, 166
classe d'association, 288
classe de conjugaison
    dans S_4 , 198
clôture algébrique, 422
codimension, 319
coefficient binomial, 285
coefficients
    de Fourier, 2086
coefficients binomiaux, 285

coefficients de Fourier, 2098
coercion, 1974
coercive, 1471
colinéarité, 1881
combinaison
convexe, 568
combinatoire, 1577
commutant, 690
commutateur
dans un groupe, 253
compacité, 497, 541, 546, 2019, 2041
sous-groupes du groupe linéaire, 1134
théorème de Dini, 1048
utilisation, 1481
théorème de Montel, 2181
compact, 483, 604
arc paramétré, 1815
boule unité, 711
et fonction continue, 497, 722
fermé et borné, 711
intervalle $[a, b]$, 710
le coup du, 1409
localement, 484
opérateur, 2045
produit dénombrable, 547
produit fini, 546
quasi, 483
séquentiellement, 485
suite exhaustive, 543
compacts et fermés, 486
complément
à deux, 2372
complémentaire, 113
complet
$\mathbb{R}$
corps, 243
espace métrique, 534
corps, 221
espace mesuré, 1159
espace topologique, 524
métrique, 525
complété
d'un espace métrique, 1491
complète
famille de projecteurs, 211
complétion
projective, 1884
complétion d'espace métrique, 1490
complétude, 1487, 1491, 2070
espaces L^p, 2071
complexe conjugué, 252
composante, 1103
composante connexe, 481
composition
suite de, 257
concaténation
de langages, 2660
de mots, 2659
concave, 1448
log-concave, 1455
condition initiale, 2341
conditionnement
absolu, 2381
d'une matrice inversible, 2415
relatif asymptotique, 2401
Cône de lumière, 2671
conjugué hermitien, 643
conjugués
éléments d'une extension, 420
connectés
indices d'une matrice, 2442, 2443
connexe par arc, 725
connexité, 546
définition, 480
et intervalles, 719
fonction holomorphe, 1494
indice d'une courbe, 2003
le groupe $\mathrm{GL}^+(n, \mathbb{R})$, 1122
par arc
fonction différentiable, 1028
points d'accumulation, 541
prolongement analytique, 1494
signature d'une forme quadratique, 1476
théorème de Runge, 2015
théorème des valeurs intermédiaires, 733
utilisation
Brouwer, 2012
consistance
estimateur, 2567
ordre, 2464
constructible
angle, 1690
point, 1686
réel, 1686
construction
des réels, 233
contenu, 305
continue
fonction entre espaces métriques, 539
fonction entre espaces topologiques, 473
forme différentielle, 987
continuité
fonction définie par une intégrale, 1408
séquentielle, 510
contraction, 822, 1418
convergence

commutative, 786
dans un espace vectoriel normé, 712
de martingales, 2633
en loi, 2511
en probabilité, 2511
ordre, 2397
presque surement, 2511
quadratique, 2386
rapidité, 1344, 2216, 2217, 2396, 2540
suite
dans un corps, 221
suite dans $\mathbb{R}^m$, 519
suite numérique, 712, 1401, 2191
Abel angulaire, 1745
uniforme, 1045
intégrale, 1406
théorème de Dini, 1048
convergence absolue, 781
convergence de suite, 468
convergence forte, 806
convergence normale, 781
convergence uniforme
série de fonctions, 782
convexe
courbe plane, 1862
fonction sur $\mathbb{R}^n$, 1458
convexité
barycentre, 570
enveloppe de $O(n)$, 1130
fonction, 1448
inégalité de Jensen, 1463
locale, 2132
méthode de Newton, 2392
utilisation, 1481
convolution, 2480, 2626
convolution sur S^1, 2098
coordonnées
cartésiennes
dans un espace affine, 575
curvilignes, 1938
cylindrique, 1628
dans un espace affine, 560
homogène, 1900
sphériques, 1630
coordonnées barycentrique, 576
coordonnées polaires, 1623
corps, 174
complet, 221
de décomposition, 445
de rupture, 435
polynôme cyclotomique, 1656
des fractions, 219, 220
extension, 452, 460
fini, 1664, 1668, 1671
Wedderburn, 1660
formellement réel, 393
ordonné, 221
premier, 395
corps algébriquement clos, 421
corps valué, 250
cosinus, 1497
hyperbolique, 1347
courbe, 1815
efficacité, 2588
étude métrique, 2201
fermée, 1849
simple, 1849
courbe de Jordan, 1735
courbe de niveau, 964, 966
courbe simple, 1735
courbure, 1843
signée, 1850
totale, 1851
covariance, 2483
critère
Abel, 1296
Abel pour intégrales, 1407
Cauchy
uniforme, 1046
de Cauchy, 243, 534
Weierstrass, 1407
série de fonctions, 1051
critère du quotient, 794
critique
Galton-Watson, 2626
point, 1442
point d'un arc, 1830
région, 2587
valeur, 2588
cycle, 192
cyclique
endomorphisme, 621
matrice, 621
cycloïde
coordonnées normales, 1835
longueur, 1829

décalage, 2373
décalage, 2373
décomposition
Bruhat, 1131
canonique, 116
corps, 445
Dunford, 677
application, 1352
exponentielle de matrice, 1074
Jordan

et exponentielle de matrice, 1351
polaire, 1128
primaire, 675
sous-espaces caractéristiques, 675
spectrale, 675
décomposition de Hahn, 1234
décomposition de Jordan, 1236, 1237
décomposition décimale, 802
degré
application $S^1 \to S^1$, 1853
d'une représentation, 360
extension de corps, 418
degré d'un polynôme, 215
demi-plan, 938
dénombrable, 150
à l'infini, 485
dénombrement, 1577
partitions de $\{1, \dots, n\}$, 1375
dense, 470
nulle part, 548
densité, 1491
d'une variable aléatoire, 2474
dans un espace de fonction
critère de Weyl, 2191
de $\mathbb{Q}$ dans $\mathbb{R}$, 708
utilisation, 1454
de $\mathrm{GL}(n, \mathbb{R})$ dans $\mathbb{M}(n, \mathbb{R})$, 1123
de $\mathscr{D}(\mathbb{R}^n)$ dans $L^1(\mathbb{R}^n)$, 2179
de $C_c^\infty(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$, 2077
de $L^2\big([0,1]\big)$ dans $L^p\big([0,1]\big)$, 2078
de $S^+(n, \mathbb{R})$ dans $S^{++}(n, \mathbb{R})$, 1127
des fonctions étagées dans L^p, 2077
des polynômes
dans $C_c^0[0,1]$, 2554
matrices diagonalisables dans $\mathbb{M}(n, \mathbb{C})$, 1123
mesure, 1225
points extrémaux dans $\mathcal{L}$, 1129
prolongement, 1487
densité conjointe, 2478
densité d'une mesure, 1226
déplacement, 1593
dérivabilité
fonction définie par une intégrale, 1409
lemme de Borel, 1373
dérivable, 944
au sens complexe, 1024
fonction, 2291
dérivation
au sens des distribution
Sobolev, 2276
dérivé
groupe, 253
dérivée
dans Sobolev $H^1(I)$, 2273
directionnelle, 978, 981
distributionnelle, 2242
faible, 2236
fonction à valeurs dans E', 557
partielle, 977, 1102
seconde, 945
dérivée directionnelle, 978
dérivée faible, 2234
dérivée partielle, 978
déterminant, 583
Cauchy, 1404
d'un endomorphisme, 587
d'une famille de vecteurs, 584
de Cauchy, 592
et inversibilité, 588
forme linéaire alternée, 583
Gram, 592, 1404
interprétation géométrique, 1271
matrice, 336
résultant, 594, 1750
utilisation, 1481
Vandermonde, 589
détermination
logarithme, 1997
principale, 1997
détermination du logarithme, 2000
développable
en série entière, 1354
développement
asymptotique, 1100
limité
en zéro, 1095
fonction holomorphe, 1979
premier ordre, 948
Taylor, 1795
diagonale
dominante, 2446
fortement dominante, 2447
strictement dominante, 2447
diagonalisable, 654
et polynôme minimum scindé, 655
exponentielle, 1352
diagonalisation
cas complexe, 915
cas réel, 659
endomorphisme autoadjoint, 748
simultanée, 657
diamètre, 905
diédral, 1578
difféomorphisme, 843
de classe C^k, 1038
différence

centrée, 2453
divisée, 2410
progressive, 2453
régressive, 2453
différentiabilité, 1028
différentielle, 842
de $u \mapsto u^{-1}$, 860
partielle, 858
totale, 1102
dilatation, 1116
dilatation (matrice), 347
dimension, 318
n-formes multilinéaires alternées, 583
définition, 318
sous espace affine, 566
utilisation, 572
direction, 978, 1838
sous-espace affine, 566
Dirichlet
noyau, 2188
théorème, 2188
théorème (sur les nombres premiers), 1660
disque de convergence, 1295
distance, 492
associée à une norme, 502
compatible, 528
entre deux mesures de probabilités, 2583
invariante, 529
point et ensemble, 521
distance discrète, 521
distance produit, 515
distingué
sous-groupe, 166
distribution, 2240
de Dirac, 2260
équation de Schrödinger, 2336
produit par une fonction, 2242
tempérée, 2259
divergence, 1108
diviseur
dans un anneau, 170
de zéro, 171
de zéro à droite, 171
polynôme, 305
diviseur de zéro, 171
divisible, 134
division
euclidienne, 176, 304
harmonique, 1917
domaine, 705
fondamental d'une action, 265
dominé
modèle statistique, 2566
dominée
convergence (Lebesgue), 1222
mesure, 1230
dominée par le dessus, 550
dominée par une seminorme, 550
droite
dans la sphère de Riemann, 1905
projective, 1881
droite affine, 577, 931
droite réelle achevée, 728
droite vectorielle, 931
droites parallèles, 931
droites perpendiculaires, 931
dual
d'un espace de Hilbert, 1957
de $\mathbb{M}(n, \mathbb{K})$, 649
de $L^p(\Omega)$, 2154
de L^p, 2149
dual algébrique, 357
dual topologique, 863, 1949
Dunford
décomposition, 677
dyadique, 1252
développement, 240
écart-type, 2482
échantillon, 2560, 2562

effectif
empirique, 2592
effectif
empirique, 2592
efficacité
courbe, 2588
d'une méthode itérative, 2405
élément
inversible
dans un anneau, 171
élément
de surface, 1730
de torsion, 270
élément de surface, 1704
élément maximal, 111
élément minimal, 111
élément premier, 170
élément régulier, 121
élément régulier à gauche, 121
élémentaire
polynôme symétrique, 459
ellipsoïde, 701
elliptique
équation aux dérivées partielles, 2363
endomorphisme, 323
cyclique, 621
décomposition

polaire, 1128
diagonalisable, 700, 1125, 2332
Dunford, 677
diagonalisation, 659
nilpotent
Dunford, 677
préservant une forme quadratique, 1136
sous-espace stable, 677, 2332
endomorphisme direct, 598
endomorphisme préserve l'orientation, 598
engendré, 175
λ-système, 1146
corps, extension, 427
idéal dans un anneau, 175
sous-espace affine, 566
sous-groupe, 206
ensemble
archimédien, 128
de Cantor, 1203
différence symétrique, 114
infini, 144
ensemble connexe, 480
ensemble des mots, 2659
ensemble fini, 144
ensemble ordonné, 111
ensemble quotient, 115
ensembles
disjoints, 109
entier, 140
entrelacement, 1386
enveloppe
convexe, 570
équation
différentielle
linéaire, 2294
ordinaire d'ordre 1, 2291
variables séparées, 2296
générale de degré n, 463
équation
aux variations, 2314
de Riccati, 2335
des classes, 265
des orbites, 264
différentielle
étude qualitative, 2332
Hill, 2331
homogène, 2334
système, 2332
diophantienne, 283, 299, 302
Fredholm, 1420
orbite-stabilisateur, 263
équation de droite, 937
équation différentielle
linéaire du premier ordre, 2345
linéaire du premier ordre, homogène, 2345
linéaire du second ordre, 2347
linéaire du second ordre, homogène, 2348
premier ordre, 2340
second ordre, 2340
variables séparables, 2342
équation exponentielle, 1082
équation fonctionnelle, 1082
équation homogène associée, 2345
équi-intégrable, 2633
équicontinu, 547
équipotent, 143
équivalence
arcs paramétrés, 1831
chemin, 1824
classe de fonctions, 2050
de représentations, 1386
de suites, 714
homotopie, 2005
suite de composition, 259
équivalence de forme quadratiques, 671
équivalence de normes, 765
erreur, 2411, 2441
assignation, 2376
de consistance, 2464
discrétisation, 2465
quadratique, 2414
troncature, 2376
erreur relative, 2376
escalier, 1186
espace
L^2
Sobolev, 2276
L^p, 2053
de Baire, 557
de Bergman, 2182
de fonctions
L^p, 2071
Sobolev H^1, 2276
de Hilbert
espace de Sobolev H^1, 2276
de probabilité, 2473
de Schwartz, 2177, 2259
de Sobolev, 2273, 2280
euclidien, 760
mesurable, 1137
mesuré, 1142
complété, 1161
métrique, 492
base de topologie, 495
projectif, 1881
propre, 614

séparé, 477
tangent, 1700
topologique
métrisable, 538
vectoriel, 208
dimension, 583
vectoriel topologique
métrisable, 523
espace de Banach, 525
espace de Sobolev, 2278
espace topologique, 465
espace topologique normal, 1870
espace vectoriel
topologique, 503
espace vectoriel normé, 500
espérance, 2478
conditionnelle, 2487, 2488
événement, 2488
variable aléatoire, 2493
estimateur, 2567
biais, 2568
consistant, 2567
de fonction de répartition, 2572
maximum de vraisemblance, 2570
estimateur convergeant, 2567
estimation
des grands écarts, 2540
étagée
fonction, 1185
état
apériodique, 2611
récurrent, 2604
récurrent positif, 2604
transitoire, 2604
Éther, 2666
étoile de Kleene, 2661
étranger
dans leur ensemble, 305
étrangers
polynômes, 305
Euclide
algorithme étendu, 272
lemme, 276
euclidien
anneau, 184
espace, 642
évaluation
polynôme plusieurs variables, 287
événement, 2473
Événement, 2671
exact
intervalle de confiance, 2576
excès
intervalle de confiance, 2576
exhaustive (suite de compacts), 543
exponentielle, 1331
convergence, 797
de matrice, 862, 1351, 1352, 1364
utilisation, 1440
existence, 1324
rapide, 1654
unicité, 1082
exposant, 372, 700
d'un groupe, 191
extension
corps de base, 679
de corps, 418, 460
algébrique, 431
finie, 1673
simple, 427
utilisation, 1691
isométrie, 1488
séparable, 455
extension algébrique, 421
extension algébriquement clos, 422
extrapolation, 2410
extrémité
d'un intervalle, 719
extrémum, 1795
lié, 1446
local
relatif, 1446
extrémum local, 1441
extrémums, 1443
volume d'un ellipsoïde, 1481

facteur
intégrant, 2336
facteur
intégrant, 2336
factoriel
anneau, 290
factorisation
de polynôme, 310, 434
faisceau de droites, 1903
famille
sommable, 787
famille trigonométrique
sur S^1, 2097
Fatou, 1213
Fejér
noyau, 2188
fermé, 466, 604
fermeture séquentielle, 522
filtration, 2629
fine
subdivision, 1815

fixateur, 262
flot, 2308, 2354
flux
  d'un champ de vecteur, 1734
flux d'un champ de vecteurs, 1732
fonction, 705
  Γ d'Euler, 2034
  à décroissance rapide, 2177
  borélienne, 1155
  caractéristique, 1785
    d'une variable aléatoire, 2505
  continue
    égales, 523
  convexe, 1448, 1454
  croissante, 706
  de Dirichlet, 2194
  de Möbius, 1682
  de répartition, 2505
  décroissante, 706
  définie par une intégrale, 1369, 1407, 1413, 1414, 2041
    Γ d'Euler, 2034
    utilisation, 2527
  en escalier intégrable, 1784
  étagée, 2076
  génératrice, 2507
  holomorphe, 1024, 2041
    théorème de Montel, 2181
  image, 705
  méromorphe
    Γ d'Euler, 2034
  monotone, 706
  valeurs vectorielles, 1103
fonction continue en un point, 473
fonction dérivée, 944
fonction périodique, 955
fonctionnelle
  énergie, 1977
fonctions équivalentes, 479
fondamental
  domaine d'une action, 265
forme
  bilinéaire, 628
    non dégénérée, 629
  différentielle, 986
    exacte, 1743
    fermée, 1743
  linéaire
    différentielle, 1446
  quadratique, 1476, 1478, 1795
    groupe orthogonal, 1136
forme bilinéaire symétrique, 628
forme canonique
  fonction simple, 1186
  matrice de transition, 2621
forme linéaire, 357
forme multilinéaire, 778
forme multilinéaire alternée, 583
forme quadratique, 628
formle multilinéaire antisymétrique, 583
formule
  Bayes, 2484
  Burnside, 265
  d'expulsion (produit vectoriel), 758
  de Cauchy, 2009
  Hadamard, 1299
  inversion Möbius, 1683
  probabilité totales, 2484
  sommatoire de Poisson, 2216
  Taylor
    reste intégral, 1779
    utilisation, 2396
Formule de Leibnitz, 2236
formule de Stirling, 1801
formule des classes, 263
Fourier, 2216
  série
    utilisation, 2201
  transformée
    groupe abélien fini, 1381
fraction
  rationnelle
    intégration, 1750
fraction dyadique, 240, 1873
fraction rationnelle, 1776
fractions
  rationnelles, 219
fractions (corps), 220
Fredholm
  équation, 1420
Frenet
  formules, 1844
fréquence
  empirique, 2592, 2602
Fresnel
  intégrale, 2039
Frobenius
  morphisme, 214
frontière, 471, 493, 609
Fubini
  théorème
    dans $\mathbb{R}^n$, 1286

Galton-Watson
  sous-critique, 2626
  sur-critique, 2626
Galton-Watson

sous-critique, 2626
sur-critique, 2626
Gauss
lemme
polynômes, 414
somme de, 1666
générateur, 207
génératrice
partie d'un module, 211
géométrie
avec des groupes, 1571, 1924
avec nombres complexes, 1571, 1924
géométrique
avec des nombres complexes, 2201
Gershgorin
disque, 2444
gradient, 994, 1002, 1015
Gram (déterminant), 592
Gram-Schmidt, 760
graphe, 706, 946
de transition (chaine de Markov), 2602
fonction, 963
fonction de deux variables, 966
Grönwall (lemme), 2291, 2292
groupe, 116
$\mathrm{GL}(n,\mathbb{R})$, 1478
p-groupe, 365
action, 1924
utilisation, 1136
agissant sur un ensemble
diédral, 1570
alterné, 381
circulaire, 1921
de Galois, 462
de permutation, 1642
de permutations, 1577
caractères de S_4, 1393
de torsion, 270
dérivé, 253
de $\mathrm{GL}(n,\mathbb{K})$, 1121
de $\mathrm{SL}(n,\mathbb{K})$, 1121
du groupe alterné, 384
du groupe symétrique, 382
des isométries
espace métrique, 521
des symétries, 1590
diédral, 1570, 1578
générateurs (preuve), 1571
générateurs (utilisation), 1642
en géométrie, 1570
et géométrie, 583, 1577, 1924
isométries du cube, 389
fini, 367, 375, 1577, 1652, 1660, 1664
alterné, 383
diédral, 1570
Wedderburn, 1660
linéaire, 1131
décomposition polaire, 1128
enveloppe convexe de $\Omega(n)$, 1130
hyperplan, 650
sous-groupes compacts, 1134
modulaire, 1923
orthogonal, 601
d'une forme quadratique, 1136
partie génératrice, 383, 1652, 1924
permutation, 583, 590, 1131, 1652
diédral, 1570
projectif, 1888
quotient, 257
simple, 166
spécial orthogonal, 602
symétrique, 192
action sur un triangle, 1383
groupe abélien, 116
groupe commutatif, 116
groupe cyclique, 207
groupe de pavage, 1593
groupe dérivé
de $\mathrm{GL}(n,\mathbb{C})$, 1115
groupe ordonné, 165
groupe résoluble, 260
groupe simple, 166

Hadamard
conditions, 2364
formule, 1299
Hadamard
conditions, 2364
formule, 1299
Hardy-Littlewood (théorème), 1401
Hausdorff, 477
Heine (théorème), 905
hermitienne, 643
hessienne, 1039
Hilbert
espace, 1951
holomorphe, 1024, 2043
sur un compact, 1024
homéomorphisme, 473
homogène
chaine de Markov, 2597
homographie, 1887, 1924
sur $\mathbb{C}\cup\{\infty\}$, 1910
homotopie, 1735
homotopie à extrémité fixées, 1735
hyperbolique
équation aux dérivées partielles, 2363

hyperplan, 696, 1536
de $\mathbb{M}(n, \mathbb{K})$, 650
sépare
au sens strict, 2133
séparer
au sens large, 2133
hypothèse
alternative, 2587
composite, 2587
multiple, 2587
nulle, 2587
simple, 2587

idéal
bilatère, 168
dans un anneau, 168
principal
à droite, 178
à gauche, 178
idéal
bilatère, 168
dans un anneau, 168
principal
à droite, 178
à gauche, 178
idéal à droite, 168
idéal maximal, 176
identifiable, 2566
identité de polarisation, 633
image, 705
incompressible
champ de vecteur, 1110
indécomposable
module, 212
indépendance
affine, 574
algébrique, 463
événements, 2474
utilisation, 2552, 2636
projective, 1889
sous tribus, 2474
variables aléatoires, 2475
indicatrice d'Euler, 377
indice, 256
d'une courbe dans $\mathbb{C}$, 2002
de rotation, 1854
indice d'inertie, 640
inductif, 112
induite
topologie, 606
tribu, 1139
inégalité
arithmético-géométrique, 1464
Bessel, 1959
Cauchy-Schwarz, 745, 1951
de Khintchine, 2536
de la moyenne, 1028
des pentes, 1449
Hölder, 2058
utilisation, 2481, 2555
isopérimétrique, 2201
Jensen, 1463
espérance conditionnelle, 2504
pour une somme, 1463
version intégrale, 2058
Kantorovitch, 1464
Markov, 2516
Minkowski, 2061
triangulaire, 492, 500
inférence statistique, 2559
infimum, 245
injection, 110, 511
intégrable, 1215
fonction à valeurs vectorielles, 1218
fonction non en escalier, 1790
fonction positive, 1794
intégrale
calcul, 2191
convergente, 1268, 1749
d'une fonction sur une carte, 1705
d'une fonction sur une variété, 1709
d'une forme différentielle, 1720
fonction en escalier, 1784
Fresnel, 2039
impropre, 1267, 1268
sur un chemin, 1718
intégrale d'une fonction, 1207
intégrale d'une forme différentielle, 1720
intégrale de Dirichlet, 1812
intégrale sur une carte, 1701
intégration
fraction rationnelle, 1750
intéressante, 105
intérieur, 469
d'un ensemble, 603
point, 603
interpolation, 2410
intervalle, 112, 705, 724
longueur, 1193
Intervalle, 2671
intervalle de confiance
asymptotique, 2580
invariance cyclique
trace, 332
invariant
de similitude, 687
invariante

mesure
pour une chaine de Markov, 2622
inverse
dans un groupe, 165
inverse généralisé, 2543
inversion, 1876
dans le groupe symétrique, 198
inversion dans $\mathbb{C} \cup \{\infty\}$, 1908
involution, 657
irrationalité
$\sqrt{2}$, 228
irréductible
chaine de Markov, 2600
dans un anneau, 170
module, 212
représentation, 1384
isobarycentre, 568
isométrie
de forme quadratique, 637
de l'espace euclidien $\mathbb{R}^2$, 1571
espace euclidien
isométries du cube, 389
groupe, 521
isométrie (forme bilinéaire), 637
isométrie d'espaces métriques, 520
isométrie positive, 1541
isomorphisme, 811
$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, 1664
d'anneaux, 167
de corps, 201
espace affine, 565
espace vectoriel normé, 845
espaces vectoriels, 323
isomorphisme d'espace topologique, 473
isotrope
cône, 634
sous espace, 634
totalement, 634
vecteur, 634

jacobien, 1015, 1108
jacobien, 1015, 1108
Jordan
réduction, 689
Jordan-Hölder, 258

Kronecker
symbole, 318
Kronecker
symbole, 318

lacet, 1735
lacet, 1735
lacet de Jordan, 1735

Lagrange
multiplicateur, 1446
polynôme, 649
théorème, 257
lagrangien, 1446
langage, 2660
itéré, 2661
itéré strict, 2661
unité, 2660
vide, 2660
Laplace
transformée, 2507
laplacien, 1945
Legendre
symbole, 1665
Leibnitz, 949
applications entre espaces vectoriels normés, 858
lemme
Borel, 1373
d'Euclide, 276
de Borel-Cantelli, 2514
de Gauss
contenu de polynôme, 1673
pour des entiers, 276
de Morse, 1795
de Schreider, 259
de Slutsky, 2513
de transport, 1152
de Zorn, 112
des noyaux, 616
Fatou, 1213
Gauss
dans un anneau principal, 292
polynômes, 414
Grönwall, 2291, 2292
Hadamard, 1416
Schur complexe, 915
Schur réel, 658
lemme de regroupement, 2477
lettres, 2659
Levi-Civita, 1940
libre
action, 268
partie, 313
partie d'un module, 211
librement engendré, 321
Ligne d'univers, 2666
limite, 673
d'ensembles, 1145
d'une fonction, 490, 491
de fonctions holomorphes, 2041
de suite

espace topologique, 468
inférieure, 716
inversion, 1375, 1401, 2041, 2053
permutation
utilisation, 2507
suite dans $\mathbb{R}^m$, 519
suite numérique, 712
supérieure, 716
unicité, 491
limite à droite, 888
limite épointée, 876
limite inductive, 2237
limite inférieure, 716
limite pointée, 876
linéaire
application, 322
linéairement indépendant
module, 209
Lipschitz, 1418
localement, 1029
Lipschitzienne, 1029
liste d'indices, 39
localement
intégrable, 1267
log-concave, 1455
logarithme
complexe, 1993
dans $\mathbb{C}$, 1990
de matrice, 1364
sur les réels positifs, 1327
logarithme d'une application, 2000
loi
χ^2, 2538
binomiale
comportement asymptotique, 2540
conjointe, 2477
de Poisson, 2525
des grands nombres
forte, 2517
pour les chaines de Markov, 2624
processus de Poisson, 2653
utilisation, 2540, 2552
marginale, 2477
normale
vecteur gaussien, 2532
parente, 2559, 2560
parente d'un échantillon, 2562
réciprocité quadratique, 1668
sans mémoire, 2527
Student, 2538
loi d'une variable aléatoire, 2508
loi exponentielle, 2525
loi stationnaire, 2600
longueur
arc géométrique, 1832
d'un arc paramétré compact, 1816
d'un intervalle, 1193
d'une arrête, 1781
élément de, 1827
longueur d'arc, 1818
Lotka-Volterra, 2325

M-matrice, 2449
M-matrice, 2449
maigre, 1157
maigre (ensemble), 548
majorant, 111, 244
essentiel, 2055
Markov
inégalité, 2516, 2565
martingale, 2629
bornée dans $L^2(\Omega)$, 2630
matrice, 330, 1131, 1924
compagnon, 685
creuse, 2419
cyclique, 621
d'une application linéaire, 333
de dilatation, 347
de permutation, 347
de similitude, 1024
de Sylvester, 592
de transvection, 347
dense, 2419
équivalence, 349
dans le groupe linéaire, 1136
hermitienne
racine carrée, 1125
jacobienne, 1002, 1014
normale, 915
orthogonale, 346, 601
permutation
élémentaire, 2427
racine carrée, 1125
réductible, 2443
semblable, 1125
semblables, 1478
symétrique, 1478
réelle, 1476
trigonalisable, 914
matrice d'une forme bilinéaire, 635
matrice de transition, 2598
matrice positive, 737
matrice primitive, 737
matrice stochastique, 2599
matrice-colonne, 331
matrice-ligne, 331
matrices

similitude, 349
matrices équivalentes, 651
matrices semblables, 651
maximale
partie orthonormale, 1961
maximum, 111, 126
global, 1441
local, 1441
maximum local, 1441
méromorphe, 2027
mesurable
application, 1145
au sens de m^*, 1151
ensemble, 1143
fonction, 1152
Lebesgue, 1780
mesure
σ-finie, 1142
angle entre vecteurs, 1562
complexe, 1244
dans une carte, 1704
de Borel, 1176
de comptage, 1259, 1285
de Lebesgue, 1197
de Radon, 1176, 2022
extérieure, 1139
externe, 1780
finie, 1142
image, 1170
positive, 1142
probabilité, 2473
produit, 1249
régulière, 1176
extérieure, 1176
intérieure, 1176
sur un ensemble de parties, 1139
mesure σ-finie, 1140
mesure à densité, 1226
mesure absolument continue, 1230
mesure finie, 1140
mesure signée, 1142
mesures mutuellement singulières, 1230
méthode
des chemins, 975
Newton, 2396
cas convexe, 2392
Méthode
de Newton, 2390
métrisable
espace vectoriel topologique, 523
minimum, 126
ensemble ordonné, 111
minimum local, 1441
minorant, 111, 244
modèle
échantillonnage, 2560, 2562
paramétrique, 2560
modèle statistique, 2559
modulaire (groupe), 1923
module
à gauche, 208
de continuité, 865
indécomposable, 212
irréductible, 212
simple, 212
module d'un nombre complexe, 734
module produit, 209
moment, 2479
fonction génératrice, 2507
monogène, 207
extension de corps, 427
monoïde, 400
monôme, 303
monotone par morceaux, 1190
monotonie, 2330
morphisme
d'algèbres, 212
d'anneaux, 117
de corps, 201
espace vectoriel normé, 845
Frobenius, 214
morphisme de groupes, 116
morphisme de modules, 208
morphisme de produits tensoriels, 811
mot, 2659
longueur d'un mot, 2659
mot vide, 2659
nombre d'occurrences, 2659
mot non vide, 2659
moyenne
de Cesàro, 799
empirique, 2482
empirique d'un échantillon, 2562
quadratique, 2482
multiindice, 39
multiplicateur
de Lagrange, 1446
multiplication, 128
multiplicité
racine d'un polynôme, 308
racine de $f(x) = 0$, 2389
valeur propre
algébrique, 913
géométrique, 913

nabla, 1010
nabla, 1010

négatif, 236
négligeable
partie d'un espace mesuré, 1159
neutre
dans un groupe, 165
Newton
méthode, 2396
nilpotent, 170
niveau de confiance, 2576
nombre
complexe
norme 1, 1660
de Fermat, 1691
dénormalisé, 2374
normal, 2552
normalisé, 2374
premier, 375, 401, 1344, 1652, 1660, 1664
dans leur ensemble, 187
théorème des deux carrés, 402
tours d'une courbe plane, 1853
nombre premier
décomposition, 276
polynôme cyclotomique, 1656
nombres complexes, 251
non dénombrable, 150
normal
arc paramétré, 1833
endomorphisme, 915
nombre, 2552
sous-groupe, 166
normal extérieur
vecteur, 1734
normale
loi réduite, 2531
principale, 1843
normalisateur, 166
norme, 500
d'algèbre, 771
d'application linéaire, 769
d'une application linéaire, 769
euclidienne
dans $\mathbb{R}^m$, 749
supremum, 763
sur $\mathbb{Z}[i\sqrt{5}]$, 296
normé
espace vectoriel, 501
norme maximum, 515
norme quotient, 554
norme suprémum, 1045
normes équivalentes, 765
noyau
application vers un groupe, 254
d'une forme bilinéaire, 635
Dirichlet, 2188
Fejér, 2188
vers un espace vectoriel, 324
noyau d'une forme bilinéaire, 630
nulle part dense, 548

observation, 2473
observation, 2473
opérateur
défini positif, 660
opérateur hermitien, 643
opérateur unitaire, 644
opérateurs
compatibles, 1973
opposés
chemins, 1824
orbite
d'un point sous une action, 262
orbite d'un élément sous une permutation, 192
ordre, 110
bon ordre, 112
d'un élément, 189
d'un polynôme, 308
d'une matrice carrée, 331
dans un corps, 221
de convergence d'un schéma, 2465
distribution, 2243
partiel, 111
sur un anneau factoriel, 291
total, 111
ordre d'un groupe, 189
orientation, 597, 1706, 1728
orientation affine, 598
origine
abscisse curviligne, 1833
repère affine, 575
orthogonal, 641, 1956
coordonnées curviligne, 1938
famille de projecteurs, 211
matrice, 601
opérateur, 601
sous-espace, 359
orthogonal pour une forme bilinéaire, 630
orthonormé, 749
système, 1958
oscillation
d'une fonction, 900
d'une fonction en un point, 900
osculateur (cercle), 1848
ouvert, 465, 604

parabolique
équation aux dérivées partielles, 2363
parabolique

équation aux dérivées partielles, 2363
parallèle
sous-espaces affines, 566
parallélogramme, 1711
paramétrage, 1824
normale, 1833
paramétrages
admissible, 1832
Parseval, 1966
partie
génératrice, 207, 313
régulière, 1095
totale, 1958
partie convexe, 499
partie entière, 250
partie équilibrée, 506
partie fractionnaire, 250
partie inductive, 710
partie libre
module, 209
partie linéaire, 563
partie négative, 1232
partie nulle, 1232
partie positive, 1232
partie symétrique, 506
partition
dénombrable mesurable, 1181
partition de l'unité, 1372
passage aux classes, 476
pavable, 1781
pavage du plan, 1593
pavé, 1780, 1781
Pearson
théorème, 2592
peigne de Dirac, 2266
période, 955
permutation, 192
matrice, 347
permutation impaire, 198
permutation paire, 198
permuter
dérivée et intégrale
$\mathbb{R}^n$, 1414
dans $\mathbb{R}$, 1410
dans $\mathbb{R}$ avec les bornes, 1413
dérivée et limite, 1055
différentielle et intégrale
$\mathbb{R}^n$, 1415
intégrale
et série, 1285
limite et intégrale
convergence dominée, 1222
convergence monotone, 1211
espace mesuré, 1408, 1409
série entière et dérivation, 1309
série entière et intégration, 1311
somme et intégrale, 1212, 1287
permuter limite et intégrale, 1407
petit théorème de Fermat, 396
pgcd
calcul effectif, 273
dans un anneau intègre, 169
polynômes, 416
pivotale, 2578
plan
projectif, 1881
tangent, 1014, 1102
plan affine, 931
plan médiateur, 936
plan vectoriel, 931
Plancherel, 1966
plongement, 1487
Poincaré (demi-plan), 1923
point
d'équilibre
stable, 2321
pondéré, 568
point adhérent, 470
point critique
définition, 1797
point d'accumulation, 472
point d'équilibre, 2321
point extrémal dans un convexe, 1129
point fixe, 2626
attractif, 1417
Brouwer, 1712
Picard, 1419
Schauder, 1714
point intérieur, 469
point isolé, 472
Poisson
formule sommatoire, 2216
processus, 2652
polaire
nombre complexes, 1526
pôle, 1612, 2025
polydisque, 2042
polygone, 1569
polygone convexe, 1569
polynôme
à plusieurs indéterminées, 595, 1671
alterné, 459
annulateur, 615, 619
caractéristique, 625, 920
contenu, 305
cyclotomique, 1654

irréductibilité, 1656
propriétés, 1656
d'endomorphisme, 1125
décomposition de Dunford, 677
de Bernstein, 2554
irréductible
sur $\mathbb{F}_q$, 1683
minimal, 423
d'un élément d'une extension, 419
ponctuel, 619
racines, 460
semi-symétrique, 459
symétrique, 459, 460, 590, 595, 1671
élémentaire, 459, 461
trigonométrique, 2086
polynôme de Lagrange, 649
polynôme de plusieurs variables, 287
polynôme de Taylor, 1088
polynôme dérivé, 450
polynôme irréductible, 170
polynôme primitif, 306
polynôme scindé, 411
polynôme séparable, 454
polynôme trigonométrique, 2097
polynômes, 215
portée
mesure, 1232
positif, 236
potentiel, 1725, 1757
ppcm
dans un anneau intègre, 169
prébase, 467
précision
simple, 2373, 2374
préhilbertien, 1951
premier
corps, 395
deux éléments d'un anneau principal, 186
deux polynômes entre eux, 305
idéal, 179
premier type
région solide, 1792
préserve l'orientation, 598, 1541
presque
nulle, 270
partout, 1145
surjective, 2138
primitif
élément d'un corps, 1664
élément d'une extension de corps, 427
racine, 1677
triplet pythagoricien, 300
primitive, 943, 1755
de fonction continue, 1080
et intégrale, 1269
fonction, 962
primitive et intégrale, 1262
principal
anneau, 178
idéal, 178
principe
prolongement analytique, 1494
zéros isolés, 1493
Principe de correspondance, 2681
probabilité
conditionnelle, 2483
problème
aux limites d'évolution, 2364
aux limites stationnaires, 2363
bien posé, 2364
limite de Dirichlet, 2363
limite de Von Neumann, 2363
problème de Cauchy, 2342
processus
adapté à une filtration, 2629
arrêté, 2634
croissant prévisible, 2634
Galton-Watson, 2624
Poisson, 2652
sans mémoire, 2527
processus de comptage, 2645
processus de Poisson, 2645
produit, 128
d'une mesure par une fonction, 1225
de convolution, 2080
et Fourier, 2213
de langages, 2660
de mots, 2659
distribution et fonction, 2242
espaces mesurés, 1251
espaces topologiques, 468
mixte, 757, 759
scalaire
en général, 641
sur $\mathbb{M}(n, \mathbb{R})$, 927
semi-direct, 268
tensoriel
de représentations, 1392
vectoriel, 756
produit de Cauchy, 1303, 1305
produit extérieur, 826
produit hermitien, 643
produit intérieur, 836
produit pseudo-scalaire, 641
produit remarquable, 2017
produit scalaire sur $\mathbb{R}^n$, 642

produit tensoriel, 811, 812
projecteur
dans un module, 211
projectif
complétion, 1884
droite, 1881, 1882
espace, 1881
groupe, 1888
hyperplan, 1882
plan, 1881
repère, 1889
sous-espace, 1881
projection
orthogonale, 1955
projection normale, 2113
projection orthogonale, 1545
prolongement
analytique, 1494
utilisation, 2182
de fonctions, 1487
lemme de Borel, 1373
méromorphe de la fonction Γ, 2034
par continuité, 891
dans $H^1(I)$, 2276
par densité, 1487
théorème de Hahn, 1168
prolongement de fonctionnelle linéaire, 2136
propriété d'intersection finie, 490
propriété d'intersection non vide, 485
propriété universelle, 811
pseudo-dimension, 2169
puissance
d'un langage, 2661
d'un mot, 2660
d'un point, 1875
d'un test, 2588
d'une inversion, 1908
pull back, 838

quasi-compact, 483
quasi-compact, 483
quaternion, 457
queue de liste d'indices, 39
quotient, 176, 305
dans une suite de composition, 258
de groupe, 257
de groupes, 374
quotient d'un chemin, 2158
quotient d'un espace vectoriel, 810

racine
carré
de matrice hermitienne, 1125
carré de matrice
hermitienne positive, 1125
d'un polynôme, 308
de l'unité, 700, 1571, 1656, 1660, 1924
primitive, 1649
utilisation, 1656
de polynôme, 434
multiple, 2389
primitive, 1677
simple, 2389
racine
carré
de matrice hermitienne, 1125
carré de matrice
hermitienne positive, 1125
d'un polynôme, 308
de l'unité, 700, 1571, 1656, 1660, 1924
primitive, 1649
utilisation, 1656
de polynôme, 434
multiple, 2389
primitive, 1677
simple, 2389
racine carrée, 733
racine de l'unité, 1647
racine multiple, 308
racine simple, 308
raffinement, 1815
subdivision d'un pavé, 1782
rang, 326, 583, 670
classe d'équivalence, 350
diagonalisation, 659
différentielle, 1446
utilisation, 1957
rang d'une forme quadratique, 640
rang d'une matrice, 348
rare, 1157
rationnels, 223
rayon
de convergence, 1295
de courbure, 1843
de torsion, 1844
spectral, 771, 1074
réciproque
dérivabilité, 957
recouvrement, 483
rectangle
produit de tribus, 1190
rectifiable, 1816
arc géométrique, 1832
récurrent
état, 2604
nul, 2604
point d'un système dynamique, 1178

positif, 2604
réduction
d'endomorphisme, 677
Jordan, 689
réduction de Frobenius, 687
réel, 233
réflexif, 2144
réflexion, 1581
dans $\mathbb{R}^2$, 1545
glissée, 1579
par rapport à un hyperplan, 1536
région
critique, 2587
de confiance exacte, 2578
de rejet, 2587
règle du produit nul, 171
régularité
d'une mesure, 1176
extérieure de la mesure de Lebesgue, 1200
intérieure de la mesure de Lebesgue, 1202
régulier
arc, 1830
point d'un arc, 1830
régulier à droite, 170
régulière
surface, 1726
rejet
région dans une prise de décision, 2587
relation anormale, 2406
relation binaire, 110
relation d'équivalence, 115
relations
coefficient-racines, 461
de Chasles, 559, 1769
relativement compact, 484
relèvement, 1853
repère
affine, 575
cartésien
espace affine, 560
de Frenet, 1843
projectif, 1889
représentation, 360
de groupe fini
caractères de S_4, 1393
fidèle, 360
groupe diédral, 1642
irréductible, 1384
produit tensoriel, 1392
régulière gauche, 1389
virgule fixe, 2373
Représentation
virgule flottante normalisée, 2373
répulsif
point fixe, 1417
résidu
méthode itérative, 2441
résolvante, 2302
reste, 176, 305
d'un développement limité, 1095
restriction d'une distribution, 2250
résultant, 593
utilisation, 595, 1750
Riemann
fonction, 1341
risque
première espèce, 2588
quadratique, 2567
seconde espèce, 2588
rotation
en dimension 2, 1549
rotation d'angle θ, 1553
rotation-homothétie, 1907
rupture
corps, 435

schéma
consistant, 2464
schéma
consistant, 2464
schéma discret convergent, 2465
schéma numérique, 2464
Schrödinger, 2336
Schur (théorème), 1387
section, 978
de graphe, 964
propriété des, 1246
segment
dans $\mathbb{R}^p$, 719
dans un espace affine, 568
semi-défini positif, 660
semi-simple
endomorphisme, 622
semi-symétrique
polynôme, 459
seminorme, 549
seminorme quotient, 554
séparable, 1958
élément d'une extension, 455
espace topologique, 477
extension de corps, 455
polynôme non constant, 454
sépare
les points, 1076
séquentiellement fermé, 522
série
dans un espace vectoriel normé, 780

de Fourier, 2195, 2216
utilisation, 2201
de puissance, 1295
donnant $(1-A)^{-1}$, 860
entière, 1295, 1375, 2216
Abel angulaire, 1745
processus de Markov, 2626
utilisation, 2507
fonctions, 1401, 2216
génératrice d'une suite, 1354
géométrique, 796
nombres, 1401
numérique, 1344, 1375
Riemann, 797
Taylor, 1355
série convergente, 780
série de Laurent, 2205
série de Taylor, 1088
série divergente, 780
série entière
fonctions holomorphes, 2009
série harmonique, 796
sesquilinéaire, 643
signature, 198
forme quadratique, 640
similitude, 1024
simple
extension de corps, 427
fonction, 1185
module, 212
singularité, 2025
singularité effaçable, 2025
singularité isolée, 2025
sinus, 1497
hyperbolique, 1347
sinus cardinal, 1512, 1804
solfège, 1648
solution
générale, 2340
particulière, 2340
somme
inférieure, 1787
partielle, 780
supérieure, 1787
somme directe, 360
somme directe (de représentations), 1383
somme directe topologique, 503
somme partielles
Abel angulaire, 1745
sommet, 1868
Sophie Germain, 397
sous arc, 1815
sous-additivité
sur algèbre de parties, 1140
sous-anneau, 175
sous-corps premier, 395
sous-espace
affine engendré par une partie, 566
caractéristique, 674
sous-groupe
caractéristique, 166
distingué, 375
dans le groupe alterné, 383
engendré, 206
normal, 257, 374
sous-groupe distingué, 166
sous-martingale, 2629
sous-module, 211
sous-module engendré, 209
spectre
matrice hermitienne, 753
matrice symétrique réelle, 659
spectre d'un endomorphisme, 614
sphère, 495
de Riemann, 1904
stabilisateur, 262
stabilité
d'un point d'équilibre, 2321
Lyapunov, 2321
stable, 2381
schéma numérique, 2467
stathme
sur $\mathbb{Z}[i]$, 400
stathme euclidien, 184
stationnaire
chaine de Markov, 2622
statistique, 2567
statistiques
descriptives, 2559
strictement
convexe
sur $\mathbb{R}^n$, 1458
strictement convexe, 1448
structure
complexe, 1850
structure d'anneau canonique, 168
structure réelle, 362
Student, 2538, 2580
subdivision, 1782
associée à une fonction, 1783
d'un intervalle, 1815
subordonnée
norme, 769
subpotent, 143
suite, 270
arithmético-géométrique, 797

de Cauchy, 524
dans un corps, 221
de fonctions, 2053
théorème de Montel, 2181
de fonctions intégrables, 1407, 2041
de Jordan-Hölder, 258
définie par itération, 2396
équirépartie, 2191
critère de Weyl, 2191
exacte, 268
régularisante, 2218
suite de composition, 257
suite de variables aléatoires de Bernoulli, 2624
suites adjacentes, 715
support, 1784
d'une permutation, 192
distribution, 2243
famille d'éléments, 270
supremum, 245
d'une suite d'ensembles, 1137
sur-martingale, 2629
surface paramétrée, 1725
surjection, 110, 511
surpotent, 143
Sylow
p-Sylow, 366
Sylvester (matrice), 592
symbole
de Legendre, 1665
symbole principal, 2353
symétrique
polynôme, 459
système
fondamental, 2299
orthonormé, 1958
trigonométrique, 1959, 2086
système trigonométrique, 2108

tangent
vecteur unitaire, 1843
tangent
vecteur unitaire, 1843
tangente, 1515, 1838
tangente à un chemin, 1700
Tangente hyperbolique, 2675
tangente hyperbolique, 1348
taubérien, 1400
taux d'accroissement, 1449
Taylor
série entière, 1355
Taylor avec reste intégral, 1779
temps d'arrêt, 2632
temps de première atteinte, 2603
temps de retour, 2603
tenseur, 817
tenseur alterné, 823
tenseur symétrique, 823
terminée
martingale, 2633
test, 2587
bilatéral, 2588
unilatéral, 2588
tétraèdre régulier, 937
théorème
accroissements finis, 855
dans $\mathbb{R}$, 959
forme générale, 1028
Ascoli, 2046
Banach-Steinhaus, 805
avec seminormes, 2046
base incomplète, 318
Beppo-Levi, 1211
Bézout
polynômes, 414
utilisation, 593
Bolzano-Weierstrass, 497
Borel-Cantelli, 2473
Borel-Lebesgue, 711
Brouwer, 1713
dimension 2, 2012
Carathéodory, 572
Cauchy
groupe, 280
Cauchy-Arzela, 1715
Cauchy-Lipschitz, 1421
Cayley-Hamilton, 627, 1124
central limite, 2518
processus de Poisson, 2655
Chevalley-Warning, 1671
chinois, 405
anneau principal, 184
Cochran, 2564
Cochrane, 2565
convergence
dominée de Lebesgue, 1222
monotone, 1211
de Baire, 558
de Jordan, 2171
de représentation de Riesz, 1957
décomposition des noyaux
et exponentielle de matrice, 1367
des deux carrés, 402
version faible, 401
Dini, 1048
Dirichlet, 2188
forme faible, 1660
Doob, 2633

du rang, 326
élément primitif, 1673
élément primitif, 456, 1674
extension d'isométrie, 1488
Fejér, 2189
fonction implicite dans $\mathbb{R}^n$, 1434
fonction implicite dans Banach, 1433
Fubini
dans $\mathbb{R}^n$, 1286
espace mesuré, 1281
version compacte dans $\mathbb{R}^2$, 1759
Fubini-Tonelli, 1279
fuite des compacts, 2305
Gauss
polynômes, 414
Gauss-Wantzel, 1691
Glivenko-Cantelli, 2572
Hahn-Banach, 2130
Hardy-Littlewood, 1401
Heine, 905
incidence, 1882
inversion locale, 1431
utilisation, 1446, 1795
isomorphisme
second, 254
troisième, 255
isomorphisme de Banach, 2045
Kronecker, 595
Lagrange, 257
Lie-Kolchin, 918
Lotka-Volterra, 2326
Markov-Takutani, 1716
Montel, 2181
Pappus
affine, 1886
projectif, 1886
Pearson, 2592
petit de Fermat, 396
Picard, 1419
point fixe
Brouwer, 2012
projection
cas vectoriel, 1955
partie fermée convexe, 1953
prolongement de Hahn, 1168
prolongement de Riemann, 2026
Radon-Nikodym, 1238
complexe, 1245
Rolle, 958
Rothstein-Trager, 1750
Runge, 2015
Schauder, 1714
Schur, 1387
spectral, 675
autoadjoint, 748
matrice symétrique, 659
matrices normales, 915
stabilité de Lyapunov, 2321
Stone-Weierstrass, 1076, 1079
Sylvester, 670
taubérien, 1400
taubérien faible, 1747
transfert, 2509
Tykhonov, 545
dénombrable, 547
fini, 546
valeurs intermédiaires, 733
Von Neumann, 1440
Wedderburn, 1660
Weierstrass, 497
théorème de Baire, 549
théorème de Cartan-Dieudonné, 1538
théorème des extrémums liés, 1446
théorème fondamental du calcul intégral, 1263
topologie, 465, 606
$*$-faible, 556, 2240
p-adique, 868
discrète, 467
engendrée par une famille, 467
et seminormes, 550
forte, 771
grossière, 467
métrique, 492
produit, 468
sur $\mathscr{D}(\Omega)$, 2237
sur $\mathscr{D}(K)$, 2237
sur $C^\infty(\Omega)$, 2237
sur dual topologique, 556
usuelle sur $\mathbb{R}^n$, 606
topologie faible, 2171
topologie induite, 471
topologie quotient, 475
torsion, 1844
d'un groupe, 270
totale, 1958
trace, 2282
dual de $\mathbb{M}(n,\mathbb{K})$, 649
endomorphisme, 652
matrice, 652
produit scalaire sur $\mathbb{M}(n,\mathbb{R})$, 927
unicité pour la propriété de trace, 650
transcendant, 421
transformation
Fourier, 2216
gaussienne, 2421
transformée

de Cauchy, 2022
de Fourier, 2211, 2506
continuité, 2214
groupe abélien fini, 1381
Fourier
distribution tempérée, 2262
Laplace, 2507
transient
état, 2604
transition
probabilité, 2597
transitoire
état, 2604
transposé, 600
transposée, 646
transposition, 197
transvection, 1116
transvection (matrice), 347
transversale, 265
tribu, 1137
borélienne, 1153
de Baire, 1157
de Lebesgue, 1197
induite, 1139
produit, 1190
tribu de Lebesgue sur S^1, 1531
tribu engendrée, 1138
tribu engendrée par une application, 1138
trigonalisation
et polynôme caractéristique, 914
simultanée, 917, 918
triplet
pythagoricien, 300
triplet naturel, 118
type
fini
en algèbre, 457
espace vectoriel, 316

unicité
des mesures, 1148
unicité
des mesures, 1148
uniformément continue, 548
uniformément convexe, 2112
unipotent, 170
unitaire
normale principale, 1843

valeur
principale (distribution), 2260
propre, 614
valeur
principale (distribution), 2260
propre, 614
valeur absolue, 250
p-adique, 867
valeur principale, 1991
valeur propre
d'une forme quadratique, 672
forme quadratique, 671
valeur singulière, 678
valuation
p-adique, 867
valuation d'un polynôme, 215
Vandermonde (déterminant), 589
variable
de décision, 2588
variable aléatoire, 2474
absolument continue, 2474
Bernoulli
marche aléatoire, 2612
utilisation, 2554
binomiale
utilisation, 2636
centrée, 2481
de Bernoulli
utilisation, 2636
de Rademacher, 2536
variance, 2482
empirique, 2482, 2563
empirique corrigée, 2563
vecteur gaussien, 2532
variation des constantes, 2295, 2300
variété, 1446, 1697
variété
orientée, 1707
variété orientable, 1707
vecteur
cyclique, 621
gaussien, 2532
propre, 614
unitaire normal, 1843
unitaire tangent, 1838
vecteur propre à gauche, 737
Vitali (ensemble), 1203
vitesse d'un chemin, 1815
vitesse de convergence de suites, 1343
voisinage, 466, 606
volume
d'une région solide, 1793
région bornée dans $\mathbb{R}^3$, 1791
volume dans $\mathbb{R}^3$, 1710
vraisemblance, 2570

Weiner
constante, 2703
Weiner

constante, 2703
Wronskien, 2328

Liste des notations

Algèbre

$[\mathbb{L} : \mathbb{K}]$ degré d'une extension de corps, page 418

(p) idéal engendré par p, page 175

$\mathcal{L}(E, F)$ Ensemble des applications linéaires de E dans F, page 322

$\mathbb{F}_p$ lorsque p est premier, page 395

$\mathbb{F}_{p^n}$ corps fini à p^n éléments, page 1662

$\mathbb{K}(A)$ corps contenant $\mathbb{K}$ et A, page 427

$\mathbb{K}[A]$ anneau contenant $\mathbb{K}$ et A, page 427

$\mathrm{Frac}(A)$ Le corps des fractions de l'anneau A, page 220

$\mathrm{Fun}(X, Y)$ les applications de X vers Y, page 168

$\mathrm{S}(E)$ Les opérateurs autoadjoints de E, page 644

∇f gradient de la fonction f, page 1002

$\mathtt{proj}_V$ projection de $V \times W$ sur V, page 517

$\mathrm{res}(P, Q)$ résultant des polynômes P et Q, page 593

$\mathrm{Span}(A)$ l'ensemble des combinaisons linéaires finies d'éléments de A, page 313

$\sqrt{A}$ racine d'une matrice hermitienne positive, page 1125

$\theta_\alpha(P)$ la multiplicité de α par rapport à P, page 308

$A[X]$ tous les polynômes de degré fini à coefficients dans A, page 217

$A_n[X]$ les polynômes à coefficients dans A et de degré inférieur à n, page 303

$C(P)$ matrice compagnon, page 686

$D \mid P$ D divise P, page 305

$df_a(u)$ Application de la différentielle de f sur le vecteur u, page 989

$E_\lambda(T)$ Espace propre de T, page 614

$f^{(n)}$ La n-ième dérivée de la fonction f, page 1090

$mat_{\mathcal{B}}(q)$ matrice de q dans la base $\mathcal{B}$, page 1479

$o(x)$ fonction tendant rapidement vers zéro, page 1092

$U(A)$ ensemble des inversibles, page 171

U_n Le groupe des racines n^{e} de l'unité, page 1647

Ensembles de matrices

$S^+(n, \mathbb{R})$ matrices symétriques définies positives, page 660

$S^{++}(n,\mathbb{R})$ matrices symétriques strictement définies positives, page 660

$\mathrm{Aut}(E)$ automorphisme de l'espace vectoriel E, page 323

$L(E,F)$ applications linéaires bornées (continues), page 845

$\mathrm{End}(E)$ les endomorphismes de E, page 323

$\mathrm{O}(n,\mathbb{R})$ le groupe des matrices orthogonales, page 601

$\Omega(E)$ formes quadratiques non dégénérées, page 1475

$Q(E)$ formes quadratiques réelles sur E, page 628

$Q^{+}(E)$ formes quadratiques positives, page 1475

$Q^{++}(E)$ formes quadratiques strictement définies positives, page 1475

$S_n^{p,q}(\mathbb{R})$ matrices symétriques réelles de signature (p,q), page 1475

$\beta(s)$ Vecteur unitaire de la binormale, page 1843

$\gamma \sim g$ Équivalence d'arcs paramétrés, page 1831

$\nu(s)$ Vecteur unitaire de la normale principale, page 1843

$c(s)$ rayon de courbure, page 1843

$t(s)$ Torsion, page 1844

Géométrie

$P(E)$ l'espace projectif de E, page 1881

$(x_0 : \ldots : x_n)$ coordonnées homogènes dans un espace projectif, page 1900

$\mathcal{C}\mathrm{onv}(A)$ enveloppe convexe, page 570

$\mathrm{PGL}(E)$ groupe projectif, page 1888

B^o orthogonal dans le dual, page 359

$G[\mathbb{C}]$ combinaisons d'éléments de G à coefficients dans $\mathbb{C}$, page 1384

$P_1(\mathbb{C})$ sphère de Riemann, page 1904

Chaînes de Markov

$\pi(x)$ lié au temps de retour, page 2606

Probabilités et statistique

$\sigma(f)$ La tribu engendrée par une variable aléatoire ou une application, page 1138

$a \wedge b$ $\min(a,b)$, page 2632

K_X matrice de covariance d'un vecteur gaussien, page 2532

$m(\mathcal{A})$ Ensemble des fonctions $\mathcal{A}$-mesurables, page 1155

Théorie des groupes

$(G/H)_g$ classes à gauche, page 262

$[a]_p$ ensemble des $a + kp$, page 284

$[G,G]$ groupe dérivé, page 253

$[g,h]$ commutateur dans un groupe, page 253

$\mathrm{Aff}(\mathbb{R}^n)$ Le groupe des applications affines bijectives de $\mathbb{R}^n$., page 580

gr_G groupe engendré, page 206

$\hat{G}$ groupe des caractères de G, page 1379

σ_x réflexion par rapport à x, page 1581

A_n groupe alterné, page 381

$D(G)$ groupe dérivé, page 253

D_n groupe diédral, page 1570

G^{ab} groupe abélianisé de G, page 254

$N \times_\phi H$ produit semi-direct, page 268

S_n le groupe symétrique, page 192

$N \lhd G$ Le sous-groupe N est normal dans G, page 166

Topologie et théorie des ensembles

$\mathrm{Adh}(A)$ adhérence de A, page 470

$\complement A$ Le complémentaire de l'ensemble A, page 113

$\mathrm{Diam}(A)$ Diamètre de la partie A, page 905

∂A La frontière de l'ensemble A, page 609

$A \Delta B$ différence symétrique, page 114

A^c complémentaire de A, page 113

Analyse

$C^\infty(I, \mathscr{D}'(\mathbb{R}^d))$ fonctions à valeurs dans les distributions, page 2246

$(S, \hat{\mathcal{F}}, \hat{\mu})$ complété de l'espace mesuré $(S, \hat{\mathcal{F}}, \hat{\mu})$, page 1161

$\mathcal{L}(E, F)$ Les applications linéaires de E vers F, page 845

$\arg(z)$ La valeur principale de l'argument de $z \in \mathbb{C}$, page 1991

$\mathbb{D}_b$ l'ensemble des écritures décimales en base b, page 800

$\mathbb{R}$ l'ensemble des réels, page 233

$\mathbb{R}^+$ les réels positifs ou nuls, page 236

exp exponentielle, page 1330

$\mathscr{H}'$ dual, page 1957

$\mathrm{Isom}(X)$ Le groupe des isométries de X, page 521

$\liminf a_n$ limite inférieure, page 716

$\limsup a_n$ limite supérieure, page 716

$\mathcal{L}^p$ espace de Lebesgue, sans les classes, page 2051

$\mu \ll \nu$ La mesure μ est absolument continue par rapport à la mesure ν, page 1230

$\mu \perp \nu$ mesures mutuellement singulières, page 1230

μ^* La mesure extérieure associée à la mesure μ, page 1150

∂_z,$\partial_{\bar{z}}$ dérivées partielles d'une fonction complexe, page 1979

$\mathtt{proj}_K(x)$ projection orthogonale de x sur y, page 1955

$\sigma(\mathcal{A})$ tribu engendrée par $\mathcal{D}$, page 1138

$\mathscr{D}(\Omega)$ Les fonctions C^∞ à support compact sur Ω, page 2240

$\mathscr{S}'(\mathbb{R}^d)$ espace des distributions tempérées, page 2259

$A^2(\Omega)$ espace de Bergman, page 2182

$A^\perp$ orthogonal d'une partie., page 1956

$C^\infty\big(\mathbb{R}, \mathscr{S}'(\mathbb{R}^d)\big)$ Fonctions à valeurs dans les distributions., page 2336

$C_c(I)$ fonctions continues à support compact dans I, page 2079

$f \sim g$ fonctions ayant des limites équivalentes, page 975

$H^1(\Omega)$ espace de Sobolev sur Ω, page 2278

$H^1(I)$ espace de Sobolev, page 2273

$H^m(M)$ espace de Sobolev, page 2280

$L^1_{loc}(I)$ fonctions intégrables sur les compacts de I, page 2273

L^p espace de Lebesgue avec les classes, page 2052

$M_i\varphi$ La fonction $x \mapsto x_i\varphi(x)$, page 2177

$S_n f$ somme partielle de série de Fourier, page 2111

Chapitre 0

Introduction

0.1 Auteurs, contributeurs, sources et remerciements

Les remerciements, dans chaque catégorie, sont mis dans l'ordre chronologique approximatif.

0.1.1 Ceux qui ont travaillé sur le Frido

(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 19.8.

(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`.

1. http://linuxfr.org/nodes/110155/comments/1675813

(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 $A \approx A\backslash B$) et pour avoir pointé l'utilité du théorème de comparabilité cardinale.

(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 25.62 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 12.381 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 [4].

0.1.2 Aide directe, mais pas volontairement sur le Frido

(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

(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 9.1 (bien qu'ils ne le savent pas).

(6) Xavier Mauquoy pour l'énoncé et la preuve du théorème 3.36.

(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

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.

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.

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 inclue en la section 0.7. Voir 0.3 pour plus de détails.

0.3 Les choses qui doivent vous faire tiquer

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

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 12.2 ; 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 26.41.

4. Les notes comme celle-ci signifient qu'il y a certaines choses dont je ne suis pas sûr.

(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 -2.3 et la discussion 6.1.

0.5 Autres choix pas spécialement standards

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
$$f(x) = P(x) + o(x^2), \tag{0.1}$$
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

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.*

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. △

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

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

(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 [5].

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

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 43.1 et 43.2.

(2) Tracer des graphes de fonctions, exemple 43.2.

(3) Tracer des courbes en trois dimensions, voir exemple 12.210. 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 43.3.

(5) Résoudre des systèmes d'équations linéaires. Voir les exemples 43.4 et 43.5. Lire aussi la documentation.

(6) Tout savoir d'une forme quadratique, voir exemple 43.6.

(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 43.7 et 43.8.

(8) Indiquer une infinité de solutions à une équation en utilisant des paramètres. L'exemple 43.9 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 43.10.

(10) Calculer des approximations numériques comme dans l'exemple 43.11.

(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 19.62.

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.

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 15.144 pour le logarithme de nombres négatifs. Et aussi ceci :

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.

```
1
2  SageMath version 7.3, Release Date: 2016-08-04
3  Type "notebook()" for the browser-based notebook interface.
4  Type "help()" for help.
5
6 sage: limit(1/x,x=0)
7 Infinity
8 sage: limit(1/x**2,x=0)
9 +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 7.97.

0.7 Comment contribuer et aider ?

0.7.1 Des preuves qui manquent

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.

0.7.2 Du texte qui manque

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 où là, faites le moi savoir.

0.7.3 Des exemples qui manquent

Si vous connaissez de bons exemples, faites-le moi savoir.

0.7.4 Trucs de programmation et de LaTeX

(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) Il y a des problèmes dans la table des matières. « Table des matières », « Index », et « Liste des notations » ne pointent pas vers la bonne page.

(3) 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

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

Je crois que c'est clair.

0.8.2 pdflatex

Tout est compilable avec pdfLaTeX. Pas de pstricks, de psfrag ou de ps<quoiquecesoit>.

0.8.3 utf8

Je crois que c'est clair.

0.8.4 Notations

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

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

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

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

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

Construction des ensembles de nombres

1.1 Quelques éléments sur les ensembles

1.1.1 Petit mot d'introduction

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.

1.1 (On saute la théorie des ensembles)**.**
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.

Bref. Nous supposons avoir une théorie des ensembles qui tient la route. En particulier nous supposons connues les notions suivantes :

(1) ensemble vide,

(2) ensemble, appartenance, intersection, union,

(3) application entre deux ensembles, notation $f(x)$ pour désigner l'image de x par f,

(4) produit cartésien de plusieurs ensembles.

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.

1.2 (On saute la grammaire)**.**
Nous n'allons pas non plus formaliser la grammaire des expressions mathématiques[1]. Nous supposons que vous êtes capables de lire des expressions comme

$$x \in \mathbb{N} \Rightarrow \{a \geqslant x\} \text{ est infini.} \tag{1.1}$$

Tout cela pour dire que le Frido ne traitera que de la partie facile de la mathématique.

Définition 1.3.
*Deux ensembles A et B sont **disjoints** si leur intersection est vide*[2] *; en d'autres termes, si il n'existe aucun élément commun à A et B.*

1. J'utilise ici des mots que je ne comprends pas, juste pour me donner l'air malin.
2. Remarquez que les mots « intersection » et « vide » sont de ceux que nous avons décidé de ne pas définir.

1.4.
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.

1.5.
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.

1.1.2 Injection, surjection, bijection

Définition 1.6.
Soient deux ensembles E et F. Une application $f : E \to F$ 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.*

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 $f(x) = g(x)$ implique une équation faisant intervenir $1/(x - y)$.

Lemme 1.7.
Soient deux ensembles A et B ainsi qu'une application $f : A \to B$. Nous supposons qu'il existe une application $g : B \to A$ telle que $f \circ g = \mathrm{Id}_B$ et $g \circ f = \mathrm{Id}_A$.

Alors f est une bijection.

Démonstration. En deux parties.

(i) **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 $a = b$.

(ii) **Surjection** Soit $x \in B$. Posons $a = g(x)$. Alors, en utilisant le fait que $f \circ g = \mathrm{Id}_B$ nous avons

$$f(a) = (f \circ g)(x) = x. \tag{1.2}$$

Donc x est dans l'image de f et f est surjective.

□

1.1.3 Ensemble ordonné

1.8.
L'**axiome du choix** que nous acceptons peut s'énoncer comme ceci[6] : 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.

Définition 1.9 ([7])**.**
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, nous notons $x\mathcal{R}_G y$ et nous disons que x est en relation avec y.

Définition 1.10.
Une ***relation d'ordre*** *sur un ensemble E est une relation binaire*[3] *(notée $\leqslant$) sur E telle que pour tous $x, y, z \in E$,*

réflexivité *: $x \leqslant x$*

3. Définition 1.9.

antisymétrie : $x \leqslant y$ *et* $y \leqslant x$ *implique* $x = y$

transitivité : $x \leqslant y$ *et* $y \leqslant z$ *implique* $x \leqslant z$.

Pour suivre les notations de la définition 1.9, 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****.*

Définition 1.11.
Un ensemble ordonné est ***totalement ordonné*** *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****.*

Définition 1.12 ([8])**.**
Soit un ensemble ordonné $(E, \leqslant)$. Un élément $M \in E$ est un ***élément maximal*** *de E si pour tout $x \in E$ tel que $M \leqslant x$, nous avons $M \leqslant x \Rightarrow x = M$.*

Nous disons que $m \in E$ est un ***élément minimal*** *si pour tout $x \in E$, nous avons $x \leqslant m \Rightarrow x = m$.*

Définition 1.13.
Soit un ensemble ordonné $(E, \leqslant)$ et une partie A de E. Nous disons que $m \in A$ est un ***minimum*** *de A si pour tout $x \in A$, l'élément m est comparable à x et $m \leqslant x$.*

Un élément $p \in E$ est un ***minorant*** *de A si pour tout $a \in A$, les éléments p et a sont comparables et $p \leqslant a$.*

Les notions de ***maximum*** *et de* ***majorant*** *sont définies de façon analogue.*

Lemme 1.14.
Si E est un ensemble ordonné et si A est une partie finie totalement ordonnée de E, alors A possède un unique minimum et un unique maximum.

1.15.
Notons qu'il n'est pas demandé à un élément maximal [4] 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 [5] 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 4.24 et 4.25.

Lorsqu'une partie possède un minimum, ce dernier est nommé le « 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 $]a, b[$.

4. Définition 1.12
5. Définition 1.13.

Exemple 1.16 ([1]).
Soit un ensemble E ainsi que $a \neq b$ dans E. Nous considérons les parties

$$A = \{P \subset E \text{ tel que } a \in P, b \notin P\} \tag{1.3a}$$
$$B = \{P \subset E \text{ tel que } b \in P, a \notin P\}. \tag{1.3b}$$

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 $E\backslash\{b\}$ est un élément maximal, mais pas un majorant. △

Définition 1.17.
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 $y \in A$.

1.18.
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 1.425 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 $y \leqslant x$.

Exemple 1.19.
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 $Y \subset X$. △

La notion d'ordre permet d'introduire la notion d'intervalle.

Définition 1.20.
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. En language mathématique, la partie I de E est un intervalle si*

$$\forall a, b \in I, (a \leqslant x \leqslant b) \Rightarrow x \in I.$$

1.1.4 Lemme de Zorn

Nous admettons l'axiome du choix qui s'énonce de la façon suivante[9] :

> Pour tout ensemble X d'ensembles non vides, il existe une fonction définie sur X, appelée fonction de choix, qui à chaque ensemble A appartenant à X associe un élément de cet ensemble A.

Définition 1.21 (Ensemble inductif[10]).
Un ensemble est ***inductif*** *si toute partie totalement ordonnée admet un majorant.*

Lemme 1.22 (Lemme de Zorn[11]).
Tout ensemble ordonné inductif non vide admet au moins un élément maximal.

Proposition 1.23 ([12]).
Soient un ensemble inductif $(E, \leqslant)$ et $b \in E$. Il existe un élément maximal[6] *$m \in E$ tel que $b \leqslant m$.*

Démonstration. En plusieurs parties.

6. Définition 1.12.

(i) **Un ensemble** Nous considérons

$$E_b = \{x \in E \text{ tel que } b \leqslant x\}. \tag{1.4}$$

(ii) E_b **est inductif** Soit une partie non vide totalement ordonnée A de E_b. Puisque E est inductif, la partie A admet un majorant $m \in E$.
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

$$b \leqslant x \leqslant m. \tag{1.5}$$

Donc $m \in E_b$. Nous avons prouvé que m est un majorant de A contenu dans E_b. Donc E_b est inductif.

(iii) **Zorn** Puisque $(E_b, \leqslant)$ est inductif, le lemme de Zorn 1.22 nous indique que E_b a un élément maximal. Nous le notons m.

(iv) m **est maximal dans** E Supposons avoir un élément $a \in E$ tel que $m \leqslant a$. Nous avons

$$b \leqslant m \leqslant a, \tag{1.6}$$

et donc $a \in E_b$. Mais m est maximal dans E_b, donc $a = m$.

□

1.1.5 Complémentaire

Définition 1.24.
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 :*

$$\complement A = E \backslash A = \{x \in E \text{ tel que } x \notin A\}. \tag{1.7}$$

Nous allons aussi régulièrement noter le complémentaire de A par A^c.

1.1.6 Quelques relations ensemblistes

Lemme 1.25 (Quelques relations ensemblistes)**.**
Soient $A, B, C \subset X$. Nous avons

(1) $X \backslash (A \cap B) = (X \backslash A) \cup (X \backslash B)$.

(2) $X \backslash (A \cup B) = (X \backslash A) \cap (X \backslash B)$.

(3) $A \cap (B \backslash C) = (A \cap B) \backslash C$.

Lemme 1.26 ([13])**.**
Pour tout ensembles A, B, C nous avons

(1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Lemme 1.27.
Quelques propriétés à propos des complémentaires. Si E est un ensemble et si A et B sont des sous-ensembles de E, nous avons

(1) $\complement\complement A = A$, *en d'autres termes,* $E \backslash (E \backslash A) = A$,

(2) $A \backslash B = A \cap \complement B$.

(3) $(A \backslash B)^c = A^c \cup B$.

(4) $A^c \backslash B^c = B \backslash A$.

Démonstration. Plusieurs points.

(i) **Pour (1)**

(ii) **Pour (2)**

(iii) **Pour (3)** Il faut le faire en deux inclusions.

(i) $(A\backslash B)^c \subset A^c \cup B$ Supposons que $x \in (A\backslash B)^c$. 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 $A\backslash B$, ce qui est contraire à l'hypothèse. Donc $x \in B$.

(ii) $A^c \cup B \subset (A\backslash B)^c$ Supposons d'abord que $x \in A^c$. Comme $A\backslash B \subset A$, si $x \in A^c$, alors $x \in (A\backslash B)^c$.
Si $x \in B$, alors x n'est pas dans $A\backslash B$ et donc x est dans $(A\backslash B)^c$.

(iv) **Pour (4)** 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
$A^c\backslash B^c$	0	0	1	0
$B\backslash A$	0	0	1	0

(1.8)

Les deux dernières lignes étant égales, nous avons l'égalité d'ensembles annoncée.

□

Définition 1.28 (différence symétrique)**.**
Si A et B sont des ensembles, l'ensemble $A\Delta B$ est la ***différence symétrique*** *d'ensembles :*

$$A\Delta B = (A \cup B)\backslash(A \cap B). \tag{1.9}$$

C'est l'ensemble des éléments étant soit dans A soit dans B mais pas dans les deux, ni dans aucun des deux. 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

(1.10)

La deuxième colonne signifie que si $x \in A$ et $x \in B^c$, alors $x \in A\Delta B$.

Lemme 1.29 ([14])**.**
Si A et B sont des parties d'un ensemble, nous avons

$$A\Delta B = (A\backslash B) \cup (B\backslash A), \tag{1.11}$$

et aussi

(1) $A^c\Delta B^c = A\Delta B$.

(2) $(A\Delta B)\Delta B = A$.

(3) $(A\Delta B)^c = (A^c \cap B^c) \cup (A \cap B)$.

(4) Associativité : $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.

Démonstration. Pour (1.11), il suffit de voir que la table de vérité de $(A\backslash B) \cup (B\backslash A)$ est la même que (1.10).

Et pour le reste, c'est parti.

(i) **Pour (1)** Nous rappelons l'égalité $X^c\backslash Y^c = Y\backslash X$ du lemme 1.27(4). De là nous écrivons

$$A^c\Delta B^c = (A^c \cup B^c)\backslash(A^c \cap B^c) = (A^c \cap B^c)^c\backslash(A^c \cup B^c)^c = (A \cup B)\backslash(A \cap B) = A\Delta B. \tag{1.12}$$

(ii) **Pour (2)** Ici, il faut remarquer que $(A\Delta B)\cup B = A\cup B$ et que $(A\Delta B)\cap B = B\backslash A$, donc

$$(A\Delta B)\Delta B = (A\cup B)\backslash(B\backslash A) = A. \tag{1.13}$$

(iii) **Pour (3)** Il s'agit d'utiliser le lemme 1.27(3) :

$$\begin{aligned}(A\Delta B)^c &= \Big((A\cup B)\backslash(A\cap B)\Big)^c && \text{(1.14a)}\\ &= (A\cup B)^c\cup(A\cap B) && \text{(1.14b)}\\ &= (A^c\cap B^c)\cup(A\cap B). && \text{(1.14c)}\end{aligned}$$

(iv) **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

(1.15)

La quatrième ligne s'écrit sur le modèle de (1.10) 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

(1.16)

Puisque les lignes pour $A\Delta(B\Delta C)$ et pour $(A\Delta B)\Delta C$ sont identiques, nous avons égalité.

□

1.1.7 Relations d'équivalence

Définition 1.30.
*Si E est un ensemble, une **relation d'équivalence** sur E est une relation binaire*[7] *$\sim$ 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 $x\sim z$.*

Définition 1.31.
*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*

$$[a] = \{x\in E \text{ tel que } x\sim a\}. \tag{1.17}$$

Lemme 1.32.
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.

7. Définition 1.9.

(i) $\Rightarrow$ 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.

(ii) $\Leftarrow$ Nous supposons que $a \sim b$, et nous démontrons que $[a] \subset [b]$ (pour l'inclusion inverse, vous devriez vous en sortir tout seul). 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 $x \in [b]$.

□

Exemple 1.33.
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 ($P \sim R$).

△

Exemple 1.34.
Soit f une application entre deux ensembles E et F. Nous définissons une relation d'équivalence sur E par

$$x \sim y \Leftrightarrow f(x) = f(y). \tag{1.18}$$

Nous notons par $\pi\colon E \to E/\sim$ la projection canonique. L'application

$$\begin{aligned} g\colon E/\sim &\to F \\ [x] &\mapsto f(x) \end{aligned} \tag{1.19}$$

est bien définie et injective. Elle n'est pas surjective tant que f ne l'est pas. La **décomposition canonique** de f est

$$f = g \circ \pi. \tag{1.20}$$

△

1.2 Quelques structures algébriques

Nous collectons ici les définitions des principales structures algébriques.

Définition 1.35 (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 $g, h \in G$.*

Notons 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.

Définition 1.36 (morphisme, automorphisme)**.**
*Soient deux groupes G et H. Un **morphisme** entre G et H est une application $\alpha\colon G \to H$ telle que pour tout $g, h \in G$ nous ayons $\alpha(gh) = \alpha(g)\alpha(h)$.*

*Comme d'habitude, un isomorphisme est un morphisme bijectif. Un **automorphisme** de G est un isomorphisme de G vers G lui-même.*

Lemme 1.37.
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 :

$$(\alpha\circ\beta)(gh)=\alpha\big(\beta(g)\beta(h)\big)=\alpha\big(\beta(g)\big)\alpha\big(\beta(h)\big)=(\alpha\circ\beta)(g)(\alpha\circ\beta)(h). \tag{1.21}$$

□

Lemme 1.38.
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

$$\begin{aligned}\psi\colon\ \mathrm{Aut}(G)&\to\mathrm{Aut}(H)\\ \alpha&\mapsto f\circ\alpha\circ f^{-1}.\end{aligned} \tag{1.22}$$

(i) 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 :

$$\psi(\alpha\beta)=f\circ\alpha\circ\beta\circ f^{-1}=f\circ\alpha\circ f^{-1}\circ f\circ\beta\circ f^{-1}=\psi(\alpha)\circ\psi(\beta). \tag{1.23}$$

(ii) ψ **est injective** Si $\alpha\beta\in\mathrm{Aut}(G)$ sont tels que $\psi(\alpha)=\psi(\beta)$, alors

$$f\circ\alpha\circ f^{-1}=f\circ\beta\circ f^{-1}. \tag{1.24}$$

Comme f est une bijection, cela implique que $\alpha=\beta$.

(iii) 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 $f^{-1}\circ\sigma\circ f\in\mathrm{Aut}(G)$.

□

Définition 1.39 (Anneau[15])**.**
Un ***anneau***[8] *est un triplet $(A,+,\cdot)$ avec les conditions*

(1) $(A,+)$ est un groupe[9] *commutatif. Nous notons 0 le neutre.*

(2) La multiplication est associative et nous notons 1 le neutre.

(3) La multiplication est distributive par rapport à l'addition.

L'anneau $(A,+,\cdot)$ est ***commutatif*** *si pour tout $a,b\in A$ nous avons $a\cdot b=b\cdot a$.*

Définition 1.40 (Morphisme d'anneaux[16])**.**
Si $(A,+,\cdot)$ et $(B,+,\cdot)$ sont des anneaux, 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.

8. Nous faisons le choix qu'un anneau admet toujours un neutre pour la multiplication. Certains ouvrages parlent dans ce cas d'anneau unitaire.

9. Groupe, définition 1.35.

1.3 Les naturels

Définition 1.41 ([17]).
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,

(2) $s(\mathcal{N}) = \mathcal{N}\backslash\{o\}$

(3) Si $A \subset \mathcal{N}$ est tel que $o \in A$ et $s(A) \subset A$, alors $A = \mathcal{N}$.

Le théorème suivant est typiquement de ceux qui vont demander de gratter la théorie axiomatique des ensembles avec une certaine précision [10].

Théorème 1.42.
Il existe un[11] *triplet naturel.*

1.43 (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 1.80 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.

1.3.1 Applications définies par récurrence

Proposition 1.44 (Récurrence[17]).
Soit un triplet naturel $(\mathcal{N}, o, s)$ et une application $P\colon \mathcal{N} \to \{0,1\}$ vérifiant[12]

(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

$$A = \{x \in \mathcal{N} \text{ tel que } P(x) = 1\}. \tag{1.25}$$

Cet ensemble vérifie la propriété 1.41(3). Donc $A = \mathcal{N}$. □

Théorème 1.45 ([12, 18]).
Soient E un ensemble, g une application de E dans 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 $n \in \mathbb{N}\backslash\{0\}$.

Démonstration. Nous commençons par l'unicité. Soient f_1 et f_2 deux telles applications. Nous posons

$$A = \{n \in \mathbb{N} \text{ tel que } f_1(n) = f_2(n)\}. \tag{1.26}$$

Nous avons $0 \in A$ parce que $f_1(0) = f_2(0) = b$.

10. Ou alors il y a quelque chose qui m'échappe. Écrivez-moi si vous connaissez une construction « simple ».
11. Nous verrons plus tard que toute partie infinie d'un triplet naturel fournit un nouveau triplet naturel ; il en existe donc plusieurs.
12. Les plus pointilleuses 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 certaine que $\mathcal{P}(A) \neq A$?

Supposons que $f_1(k) = f_2(k)$. Alors nous avons

$$f_1\big(s(k)\big) = g\big(f_1(k)\big) = g\big(f_2(k)\big) = f_2\big(s(k)\big). \tag{1.27}$$

Nous en déduisons que $s(k) \in A$. Autrement dit $s(A) \subset A$. La définition 1.41(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.

(i) **L'ensemble est assez grand** Nous considérons l'ensemble $\mathcal{A}$ des parties $A \subset \mathbb{N} \times E$ telles que

(1) $(0, b) \in A$

(2) $(n, x) \in A \Rightarrow \big(s(n), g(x)\big) \in A$.

L'ensemble $\mathcal{A}$ est non vide parce que $\mathbb{N} \times E \in \mathcal{A}$.

(ii) **Le plus petit** Nous posons

$$G = \bigcap_{A \in \mathcal{A}} A, \tag{1.28}$$

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 $\big(s(n), g(x)\big) \in \bigcap_{A \in \mathcal{A}} A = G$.

Pour $n \in \mathbb{N}$ nous posons

$$G_n = \{x \in E \text{ tel que } (n, x) \in G\}. \tag{1.29}$$

Nous avons en particulier que $b \in G_0$ parce que $(0, b) \in G$.

(iii) **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 1.44 en posant

$$\begin{aligned} P\colon \mathbb{N} &\to \{0, 1\} \\ n &\mapsto \begin{cases} 1 & \text{si } G_n \neq \varnothing \\ 0 & \text{sinon.} \end{cases} \end{aligned} \tag{1.30}$$

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 $P\big(s(k)\big) = 1$.

(iv) **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

$$\begin{aligned} P\colon \mathbb{N} &\to \{0, 1\} \\ n &\mapsto \begin{cases} 1 & \text{si } G_n \text{ est un singleton} \\ 0 & \text{sinon.} \end{cases} \end{aligned} \tag{1.31}$$

Nous prouvons par récurrence que $P(n) = 1$ pour tout n.

(i) $P(0) = 1$ 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 $G' = G \backslash \{(0, a)\}$ 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.

(ii) **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

$$G' = G\backslash\{\big(s(k), y\big)\}. \tag{1.32}$$

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 $P\big(s(k)\big) = 1$.

(iii) **Conclusion** Nous avons prouvé que G_n est un singleton pour tout n.

(v) **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

$$\big(s(n), g\big(f(n)\big)\big) \in G. \tag{1.33}$$

Autrement dit, $G_{s(n)} = \{g\big(f(n)\big)\}$. Cela montre que

$$f\big(s(n)\big) = g\big(f(n)\big), \tag{1.34}$$

et donc que f vérifie les propriétés demandées.

□

Remarque 1.46.
Pour faire une récurrence dont chaque élément dépend de tous les précédents (et non seulement du dernier), il faut un peu adapter. Voir 1.96 pour un exemple dans $\mathbb{N}$.

Corolaire 1.47 ([12]).
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 1.45, nous notons $E = \mathrm{Fun}(X, Y)$, $b = \alpha \in E$ et

$$\begin{aligned} g\colon E &\to E \\ s &\mapsto \beta \circ s. \end{aligned} \tag{1.35}$$

Le théorème 1.45 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

$$\begin{aligned} H\colon X \times \mathbb{N} &\to Y \\ (x, n) &\mapsto f(n)x, \end{aligned} \tag{1.36}$$

et nous vérifions qu'elle satisfait aux exigences.

(1) D'abord nous avons

$$H(x, 0) = f(0)x = b(x) = \alpha(x). \tag{1.37}$$

(2) Ensuite, pour $x \in X$ et $n \in \mathbb{N}$ nous avons :

$$\begin{aligned} H(x, n + 1) &= f(x + 1)x && \text{(1.38a)} \\ &= g\big(f(n)\big)x && \text{(1.38b)} \\ &= g\big(f(n)\big)x && \text{(1.38c)} \\ &= \big(\beta \circ f(n)\big)x && \text{(1.38d)} \\ &= \beta\big(f(n)x\big) && \text{(1.38e)} \\ &= \beta\big(H(x, n)\big). && \text{(1.38f)} \end{aligned}$$

Et voilà. □

1.3.2 Addition sur les naturels

Définition 1.48 (élément régulier[19]).
Soit un ensemble E muni d'une opération $*: E\times E\to E$. Un élément $s\in E$ est ***régulier à gauche*** *si pour tout $x,y\in E$ nous avons*

$$s*x=s*y\Rightarrow x=y. \tag{1.39}$$

L'élément s est régulier à droite si pour tout $x,y\in E$ nous avons

$$x*s=y*s\Rightarrow x=y. \tag{1.40}$$

Il est ***régulier*** *si il est régulier à gauche et à droite.*

Proposition-Définition 1.49 ([17, 1]).
Il existe une unique fonction $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ vérifiant

(1) $f(a,0)=a$ pour tout $a\in\mathbb{N}$

(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 $f(a,b)=a+b$.

Lemme 1.50 ([17]).
Pour tout $a\in\mathbb{N}$ nous avons $s(a)=a+1$.

Démonstration. Nous avons :

$$\begin{aligned} s(a)&=s(a+0) && \text{(1.41a)}\\ &=a+s(0) && \text{(1.41b)}\\ &=a+1. && \text{(1.41c)}\end{aligned}$$

Justifications.

(1) Pour (1.41a) c'est dans la définition 1.49(1) de la somme.

(2) Pour (1.41b), c'est dans la définition 1.49(2) de la somme.

(3) Pour (1.41c). Le symbole « 1 » désigne l'élément $s(0)$ dans $\mathbb{N}$.

□

Proposition 1.51 ([17]).
En ce qui concerne la somme dans $\mathbb{N}$.

(1) La somme est associative et commutative.

(2) L'élément 0 est neutre.

(3) Tous les éléments de $\mathbb{N}$ sont réguliers[13] *par rapport à l'addition.*

Démonstration. En plusieurs parties.

(i) **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[14].
Nous vérifions avec $s(c)$:

$$\begin{aligned}(a+b)+s(c)&=s\big((a+b)+c\big) && \text{(1.42a)}\\ &=s\big(a+(b+c)\big) && \text{(1.42b)}\\ &=a+s(b+c) && \text{(1.42c)}\\ &=a+\big(b+s(c)\big). && \text{(1.42d)}\end{aligned}$$

Justifications.

13. Élément régulier pour une opération, définition 1.48.

14. 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.

— Pour (1.42b). 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 1.45.

(ii) **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

$$0+s(a)=s(0+a)=s(a). \tag{1.43}$$

La dernière égalité est l'hypothèse de récurrence.

Nous posons

$$A=\{a\in\mathbb{N}\text{ tel que }0+a=a\}. \tag{1.44}$$

Nous avons prouvé que $0\in A$ et que $s(A)\subset A$. Le théorème 1.45 nous assure alors que $A=\mathbb{N}$.

(iii) **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.

(iv) $a+0=0+a$ Pour $b=0$ c'est correct, car $b+0=0+b=b$ parce que 0 est neutre.

(v) $a+1=1+a$ Nous démontrons par récurrence sur a que $a+1=1+a$. Avec $a=0$ c'est déjà fait. Pour les autres,

$$\begin{aligned}
s(a)+1&=(a+1)+1 && \text{lemme 1.50} && (1.45a)\\
&=(1+a)+1 && \text{hypothèse récurrence} && (1.45b)\\
&=1+(a+1) && \text{associativité} && (1.45c)\\
&=1+s(a). && && (1.45d)
\end{aligned}$$

(vi) $a+b=b+a$ 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,

$$\begin{aligned}
a+s(b)&=a+(b+1) && && (1.46a)\\
&=(a+b)+1 && && (1.46b)\\
&=(b+a)+1 && \text{hypothèse récurrence} && (1.46c)\\
&=b+(a+1) && && (1.46d)\\
&=b+(1+a) && \text{commutativité avec 1} && (1.46e)\\
&=(b+1)+a && \text{associativité} && (1.46f)\\
&=s(b)+a. && && (1.46g)
\end{aligned}$$

Récurrence terminée.

(vii) **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

$$A=\{a\in\mathbb{N}\text{ tel que }\forall x,y\in\mathbb{N},a+x=a+y\Rightarrow x=y\}. \tag{1.47}$$

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 :

$$\begin{aligned}
&s(a)+x=s(a)+y && (1.48a)\\
\Rightarrow\quad &s(a+x)=s(a+y) && (1.48b)\\
\Rightarrow\quad &a+x=a+y && (1.48c)\\
\Rightarrow\quad &x=y && (1.48d)
\end{aligned}$$

Justifications.

— Pour (1.48b). En utilisant la définition de l'addition et la commutativité, nous avons $s(a)+x=s(a+x)$.

— Pour (1.48c). Parce que s est injective ; c'est dans la définition 1.41 d'un triplet naturel.

— Pour (1.48d). Parce que $a\in A$.

Nous avons prouvé que $s(A)\subset A$, et donc que $A=\mathbb{N}$.

□

Lemme 1.52.
Nous avons $0\neq 1$.

Démonstration. Par définition $1=s(0)$. Comme s est à valeurs dans $\mathbb{N}\backslash\{0\}$, nous ne pouvons pas avoir $s(0)=0$. □

Lemme 1.53 ([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 1.41(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 $0=a+b=a+0=a$. □

1.3.3 Ordre sur les naturels

Définition 1.54 ([17])**.**
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* $a\neq b$.

Lemme 1.55.
Nous avons $a\leqslant s(a)$ *pour tout* $a\in\mathbb{N}$.

Démonstration. Cela est une conséquence du lemme 1.50 : $s(a)=a+1$. □

Proposition 1.56.
La relation $\leqslant$ *est une relation d'ordre compatible avec l'addition.*

Démonstration. Plusieurs choses à vérifier.

(i) **Réflexive** Nous avons $a\leqslant a$ parce que $a+0=a$.

(ii) **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

$$b=a+x \tag{1.49a}$$
$$a=b+y. \tag{1.49b}$$

En substituant la seconde équation dans la première, $b=(b+y)+x$ que nous récrivons, en utilisant l'associativité [15],

$$0+b=b+(x+y). \tag{1.50}$$

En utilisant la régularité, $0=x+y$ et donc $x=y=0$ par le lemme 1.53. Cela donne alors $a=b$.

(iii) **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

$$c=(a+n)+p=a+(n+p), \tag{1.51}$$

ce qui signifie que $a\leqslant c$. Notez l'utilisation de l'associativité de la somme, démontrée en la proposition 1.51(1).

15. Proposition 1.51(1).

(iv) **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,

$$b + n = a + x + n = (a + n) + x, \tag{1.52}$$

qui signifie bien que $a + n \leqslant b + n$.

□

Lemme 1.57.
À propos d'ordre et de stricte inégalité.

(1) Si $x \leqslant a$ et $b \neq 0$, alors $x < a + b$.

(2) Si $x \leqslant a$, alors $x < s(a)$.

(3) Si $x < a$, alors $s(x) \leqslant a$.

Démonstration. En plusieurs parties.

(i) **Pour (1)** Si $x \leqslant a$, il existe $d \in \mathbb{N}$ tel que $x + d = a$. Nous avons alors aussi

$$x + d + b = a + b, \tag{1.53}$$

ce qui signifie que $x \leqslant a + b$. Mais si x était égal à $a + b$, nous aurions $d + b = 0$, ce qui impliquerait [16] $d = b = 0$, alors que l'hypothèse stipule que $b \neq 0$. Donc $x \neq a + b$.

(ii) **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 1.50.

(iii) **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

$$x + s(c) = a. \tag{1.54}$$

En utilisant le fait que $s(c) = c + 1$ ainsi que l'associativité et la commutativité de l'addition (proposition 1.51(1)) nous avons

$$a = x + s(c) = s(x) + c, \tag{1.55}$$

ce qui prouve que $s(x) \leqslant a$.

□

Lemme 1.58.
L'élément 0 est l'unique plus petit élément de $\mathbb{N}$.

Démonstration. Puisque 0 est neutre pour l'addition [17], 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 1.52. □

Lemme 1.59.
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 1.56 : $x \leqslant 0$. Nous en déduisons que $x = 0$ parce que zéro est l'unique minimum de $\mathbb{N}$ par le lemme 1.58. □

Proposition 1.60.
Le couple $(\mathbb{N}, \leqslant)$ est totalement ordonné [18].

16. Par le lemme 1.53.
17. Proposition 1.51(2).
18. Définition 1.11.

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

$$A = \{x \in \mathbb{N} \text{ tel que } x \leqslant a\} \tag{1.56a}$$
$$B = \{x \in \mathbb{N} \text{ tel que } a \leqslant x\}, \tag{1.56b}$$

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 1.58.

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 $x \in B$.

(i) **Si $x \in B$** Si $x \in B$, alors $a \leqslant x \leqslant s(x)$ parce que $x \leqslant s(x)$ par le lemme 1.55. Donc $s(x) \in B \subset A \cup B$.

(ii) **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 1.57(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 $A \cup B = \mathbb{N}$. □

Proposition 1.61 ([17, 1])**.**
L'ensemble ordonné $(\mathbb{N}, \leqslant)$ vérifie les propriétés suivantes.

(1) L'élément 0 est l'unique minimum de $\mathbb{N}$.

(2) Toute partie non vide a un unique plus petit élément.

(3) L'ensemble $\mathbb{N}$ n'a pas de plus grand élément.

(4) Toute partie non vide majorée a un unique plus grand élément.

Démonstration. Point par point.

(i) **Pour (1)** C'est le lemme 1.58.

(ii) **Pour (2)** Soit une partie A non vide dans $\mathbb{N}$. Si $0 \in A$, nous avons fini.

(i) **L'ensemble B** Nous supposons donc que A ne contient pas zéro et nous définissons

$$B = \{n \in \mathbb{N} \backslash A \text{ tel que } n \leqslant a, \forall a \in A\}. \tag{1.57}$$

(ii) **Un élément particulier dans B** L'ensemble B vérifie :

— $0 \in B$

— $B \neq \mathbb{N}$ parce que A est non vide.

La contraposée de la condition (3) de la définition 1.41 d'un triplet naturel implique que $s(B) \not\subset B$. Autrement dit, il existe $b \in B$ tel que $s(b) \notin B$.

(iii) **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 $c(a) = d(a) + 1$.

(iv) **$s(b) \in A$** 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 1.60), nous avons

$$a \leqslant s(b). \tag{1.58}$$

Comme $b \in B$ nous avons aussi

$$b \leqslant a. \tag{1.59}$$

Et enfin nous avons

$$b \neq a \tag{1.60}$$

parce que $a \in A$ et $b \in B$.

Les conditions (1.59) et (1.60) se résument en $b < a$. Le lemme 1.57(3) nous indique alors que $s(b) \leqslant a$. Cela mis à côté de (1.58) conclut que $a = s(b)$, et donc que $s(b)$ est dans A. Contradiction. Nous en concluons que $s(b) \in A$.

(v) $s(b)$ **est un minimum de** A En utilisant la commutativité et l'associativité de la somme nous avons, pour tout $a \in A$:

$$a = b + c(a) = b + \big(d(a) + 1\big) = (b + 1) + d(a) = s(b) + d(a). \tag{1.61}$$

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.

(vi) **Unicité** Si a et a' sont des minimums de A, alors $a \leqslant a'$ et $a' \leqslant a$. Nous en déduisons que $a = a'$.

(iii) **Pour (3)** Si $M \in \mathbb{N}$ majore tous les éléments de $\mathbb{N}$, alors en particulier $M \geqslant s(M)$. Mais le lemme 1.55 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 [19], nous trouvons $0 = 1$, ce qui est impossible par le lemme 1.52.

(iv) **Pour (4)** Soit A une partie non vide et majorée de $\mathbb{N}$.

(i) **L'ensemble** B Nous posons

$$B = \{n \in \mathbb{N} \backslash A \text{ tel que } a \leqslant n, \forall a \in A\}. \tag{1.62}$$

(ii) 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 $s(M)$.

(v) **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 $b = s(c)$.

(vi) $a \leqslant c$ **pour tout** $a \in A$ Comme $s(c) \in B$ nous avons $a < s(c)$ pour tout $a \in A$. Donc, par le lemme 1.57(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 $a \in A$.

(vii) $c \in A$ Si c n'est pas dans A, alors il est dans B et il contredit la minimalité de b. Donc c est dans A.

(viii) **Conclusion** L'élément c est dans A tout en étant plus petit que tout élément de A.

(ix) **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 $x = c$.

□

Lemme 1.62.
Toute partie finie non vide de $\mathbb{N}$ *est majorée et minorée.*

Lemme-Définition 1.63.
Si A *est une partie de* $\mathbb{N}$*, il existe un unique élément* $m \in \mathbb{N}$ *tel que*

$$\begin{cases} m \in A & \text{(1.63a)} \\ m \leqslant a \, \forall a \in A. & \text{(1.63b)} \end{cases}$$

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*

$$\begin{cases} M \in A & \text{(1.64a)} \\ M \geqslant a \, \forall a \in A. & \text{(1.64b)} \end{cases}$$

Cet élément est noté $\max(A)$ *et nommé* ***maximum de*** A*.*

19. Dit plus simplement : en simplifiant par M.

Nous verrons dans le lemme 1.71 qu'une partie de $\mathbb{N}$ admet un maximum si et seulement si elle est finie.

Lemme 1.64 ([1]).
Quelques affirmations sur l'ordre dans $\mathbb{N}$.

(1) Il n'existe pas de $n \in \mathbb{N}$ *tel que* $n < 0$.

(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.

(i) **Pour (1)** Nous savons par la proposition 1.61(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 $n \neq 0$.

(ii) **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

$$b + s(y) = a. \tag{1.65}$$

Si de plus il existe $x \in \mathbb{N}$ tel que $a + x = b$ nous aurions

$$a + x + s(y) = a. \tag{1.66}$$

Comme a est régulier pour l'addition [20], nous avons

$$x + s(y) = 0, \tag{1.67}$$

ce qui signifie, par le lemme 1.53 que $x = s(y) = 0$. Puisque s prend ses valeurs dans $\mathbb{N}\backslash\{0\}$, cela est impossible.

□

Définition 1.65.
Soient $a, b \in \mathbb{N}$ *tels que* $a \leqslant b$. *Nous notons par* $\{a, \dots, b\}$ *l'ensemble*

$$\{x \in \mathbb{N} \text{ tel que } a \leqslant x \leqslant b\}. \tag{1.68}$$

Proposition 1.66.
Toute application $\mathbb{N} \to \mathbb{N}$ *strictement croissante est injective.*

Démonstration. Soit une application strictement croissante $f\colon \mathbb{N} \to \mathbb{N}$. Soient $a, b \in \mathbb{N}$ tels que $f(a) = f(b)$. Puisque l'ordre est total [21], 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. □

Lemme 1.67 ([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 :

$$\begin{aligned} g\colon S &\to S \\ n &\mapsto \min\{x \in S \text{ tel que } x > n\}. \end{aligned} \tag{1.69}$$

Cette application est bien définie parce que tout partie non vide de $\mathbb{N}$ a un plus petit élément [22]. Maintenant nous définissons $f\colon \mathbb{N} \to S$ par

$$\begin{cases} f(0) = \min(S) & \text{(1.70a)} \\ f(n+1) = g\big(f(n)\big). & \text{(1.70b)} \end{cases}$$

C'est le théorème 1.45 qui nous permet de le faire. Nous montrons que f est bijective.

20. Proposition 1.51(3).
21. Proposition 1.60.
22. Proposition 1.61(2).

(i) **Injective** Nous avons

$$f(n+1) \in \{x \in S \text{ tel que } x > f(n)\}. \tag{1.71}$$

Donc f est strictement croissante. Elle est donc injective.

(ii) **Surjective** Soit $a \in S$. Nous allons voir que a est dans l'image de f. Pour cela nous posons

$$A = \{x \in \mathbb{N} \text{ tel que } f(x) < a\}. \tag{1.72}$$

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.

(i) **D'abord** Puisque $M \in A$, nous avons $f(M) < a$. Une autre façon de dire cela est de dire que

$$a \in \{x \in S \text{ tel que } x > f(M)\}. \tag{1.73}$$

Or $f(M+1) = \min\{x \in S \text{ tel que } x > f(M)\}$. Donc $f(M+1) \leqslant a$.

(ii) **Ensuite** Puisque M est le maximum de A, $M+1$ majore A, c'est-à-dire que $f(M+1) \geqslant a$.

(iii) **Les deux ensemble** Nous avons prouvé que $f(M+1) \leqslant a$ et $f(M+1) \geqslant a$. Nous en déduisons, par le lemme 1.59, que $f(M+1) = a$.

□

1.68.
Durant la preuve du lemme 1.67, nous n'avons pas été loin de prouver que

$$\big(\min(S), S, g\big) \tag{1.74}$$

est un triplet naturel.

Toute partie non bornée de $\mathbb{N}$ donne lieu à un triplet naturel.

Définition 1.69 ([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

$$\begin{cases} 0 \times a = 0 & \text{(1.75a)} \\ (n+1) \times a = n \times a + a. & \text{(1.75b)} \end{cases}$$

Définition 1.70.
*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 1.69).*

Lemme 1.71.
Une partie de $\mathbb{N}$ admet un maximum si et seulement si elle est finie.

1.3.4 Multiplication dans les naturels

Proposition-Définition 1.72.
Il existe une unique fonction $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ telle que

(1) $f(a,0) = 0$ pour tout $a \in \mathbb{N}$

(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.

(i) **Fonctions définies par récurrence** Soit $a \in \mathbb{N}$. Par le théorème 1.45, il existe une unique application $f_a : \mathbb{N} \to \mathbb{N}$ telle que

$$\begin{cases} f_a(0) = 0 & \text{(1.76a)} \\ f_a\big(s(b)\big) = f_a(b) + a & \text{(1.76b)} \end{cases}$$

(ii) **Existence** Nous considérons, pour chaque $a \in \mathbb{N}$ la fonction f_a définie par les conditions (1.76). En posant $f(a, b) = f_a(b)$, nous avons une application qui vérifie toutes les conditions.

(iii) **Unicité** Soient des applications f et g vérifiant les propriétés demandées. Soit $a \in \mathbb{N}$. Nous pouvons définir $f_a : \mathbb{N} \to \mathbb{N}$ et $g_a : \mathbb{N} \to \mathbb{N}$ 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 (1.76), et sont donc égales : $f_a = g_a$ pour tout a. Donc $f = g$.

□

1.73.
Nous supposons que la lectrice connait déjà la priorité des opérations. Elle 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.

Proposition 1.74 ([17, 1])**.**
La multiplication a les propriétés suivantes.

(1) $n \times 1 = n$ *pour tout* $n \in \mathbb{N}$.

(2) $1 \times n = n$ *pour tout* $n \in \mathbb{N}$.

(3) La multiplication est commutative.

(4) $0 \times n = 0$ *pour tout* $n \in \mathbb{N}$

(5) L'élément 1 *est neutre pour la multiplication.*

(6) La multiplication est distributive par rapport à l'addition.

(7) La multiplication est associative.

Démonstration. Point par point.

(i) **Pour (1)** Nous avons $n \times 1 = n \times s(0) = (n \times 0) + n = 0 + n = n$. Donc $n \times 1 = n$.

(ii) **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 $1 \times s(n) = s(n)$:

$$1 \times s(n) = (1 \times n) + 1 = n + 1 = s(n). \tag{1.77}$$

(iii) **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 $a \times s(b) = s(b) \times a$:

$$\begin{aligned} a \times s(b) &= a \times b + a && && \text{(1.78a)} \\ &= b \times a + a && \text{récurrence} && \text{(1.78b)} \\ &= (b \times a) + (1 \times a) && \text{par (2)} && \text{(1.78c)} \\ &= (b + 1) \times a && \text{distributivité} && \text{(1.78d)} \\ &= s(b) \times a. && && \text{(1.78e)} \end{aligned}$$

(iv) **Pour (4)** C'est vrai pour $n = 0$ par la définition 1.72(1). En ce qui concerne $s(n)$, nous avons

$$0 \times s(n) = (0 \times n) + 0 = 0. \tag{1.79}$$

(v) **Pour (5)** C'est la combinaison de (1) et (2).

(vi) **Pour (6)** Soient $a, b \in \mathbb{N}$. Nous prouvons par récurrence sur $c \in \mathbb{N}$ que [23]

$$(a + b) \times c = a \times c + b \times c. \tag{1.80}$$

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 :

$$\begin{aligned}(a + b) \times s(c) &= (a + b) \times c + (a + b) && \text{(1.81a)}\\ &= a \times c + b \times c + a + b && \text{(1.81b)}\\ &= (a \times c + a) + (b \times c + b) && \text{(1.81c)}\\ &= \big(a \times s(c)\big) + \big(b \times s(c)\big). && \text{(1.81d)}\end{aligned}$$

(vii) **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 $s(c)$:

$$\begin{aligned}(a \times b) \times s(c) &= \big((a \times b) \times c\big) + a \times b && && \text{(1.82a)}\\ &= \big(a \times (b \times c)\big) + a \times b && \text{récurrence} && \text{(1.82b)}\\ &= \big((b \times c) \times a\big) + b \times a && \text{commutativité} && \text{(1.82c)}\\ &= (b \times c + b) \times a && \text{distributivité} && \text{(1.82d)}\\ &= \big(b \times s(c)\big) \times a && \text{définition 1.72(2)} && \text{(1.82e)}\\ &= a \times \big(b \times s(c)\big) && \text{commutativité.} && \text{(1.82f)}\end{aligned}$$

□

Lemme 1.75 ([1])**.**
La multiplication est compatible avec l'ordre :

$$a \leqslant b \Rightarrow a \times n \leqslant b \times n \tag{1.83}$$

pour tout $n \in \mathbb{N}$.

Démonstration. Par la définition 1.54 de l'ordre, si $a \leqslant b$, il existe $c \in \mathbb{N}$ tel que $b = a + c$. En utilisant la distributivité [24], nous avons

$$b \times n = (a + c) \times n = a \times n + c \times n. \tag{1.84}$$

Nous en déduisons que $a \times n \leqslant b \times n$ parce que $c \times n \in \mathbb{N}$. □

Lemme 1.76.
Si $a \times b = 0$*, alors* $a = 0$ *ou* $b = 0$ *(ou les deux).*

23. Nous n'écrivons pas toutes les parenthèses parce que les règles de priorité des opérations sont supposées connues. J'invite cependant le lecteur 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.

24. Proposition 1.74(6).

Démonstration. Supposons que $a \neq 0$. Alors il existe $c \in \mathbb{N}$ tel que $a = s(c)$. Nous avons

$$0 = a \times b = s(c) \times b = c \times b + b. \tag{1.85}$$

Le lemme 1.53 nous dit alors que $c \times b = b = 0$. □

Lemme 1.77 ([1]).
Si $a < b$ et si $n \neq 0$, alors

$$a \times n < b \times n. \tag{1.86}$$

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 [25], nous avons

$$b \times n = (a + c) \times n = (a \times n) + (c \times n). \tag{1.87}$$

Cela prouve que $a \times n \leqslant b \times n$. Et comme c et n ne sont pas nuls, nous avons même [26] $c \times n \neq 0$ et donc $a \times n < b \times n$. □

Une version dans $\mathbb{Z}$ sera le lemme 1.106.

Lemme 1.78 ([1]).
Soient $a \neq 0$ et $b > 1$ dans $\mathbb{N}$. Alors

$$ab > a. \tag{1.88}$$

Démonstration. Il s'agit d'une application du lemme 1.77 en partant de l'inégalité $1 < b$ et en la « multipliant » par a. □

Proposition 1.79 ([1]).
Tous les naturels non nuls sont réguliers par rapport à la multiplication. Autrement dit, si $a \neq 0$, alors nous avons

$$a \times x = a \times y \Rightarrow x = y. \tag{1.89}$$

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 1.60), 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 [27],

$$a \times x = a \times y = a \times (x + d) = (a \times x) + (a \times d). \tag{1.90}$$

Puisque $(a \times x)$ est régulier pour la somme [28] nous en déduisons que

$$0 = a \times d. \tag{1.91}$$

Le lemme 1.76 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 $x = y$. □

1.3.5 Presque unicité des triplets naturels

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 1.68.

Nous voyons maintenant que tous les triplets naturels sont équivalents au moins pour l'ordre.

Théorème 1.80 ([1]).
Soient des triplets naturels $(\mathcal{N}_1, o_1, s_1)$ et $(\mathcal{N}_2, o_2, s_2)$. Alors

25. Proposition 1.74(6).
26. Lemme 1.76.
27. Proposition 1.74(6).
28. Proposition 1.51(3).

(1) il existe une unique application $f\colon \mathcal{N}_1 \to \mathcal{N}_2$ telle que
(1a) $f(o_1) = o_2$
(1b) $f \circ s_1 = s_2 \circ f$.
(2) Une telle application est une bijection croissante.

Démonstration. En plusieurs points.

(i) **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 1.45 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 $f\colon \mathcal{N}_1 \to \mathcal{N}_2$ telle que
(1) $f(o_1) = o_2$
(2) $f\big(s_1(n)\big) = s_2\big(f(n)\big)$
pour tout $n \in \mathcal{N}_1$.

(ii) **Unicité** Le théorème 1.45 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

$$\begin{aligned} P\colon \mathcal{N}_1 &\to \{0,1\} \\ x &\mapsto \begin{cases} 1 & \text{si } g(x) = f(x) \\ 0 & \text{sinon.} \end{cases} \end{aligned} \tag{1.92}$$

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 1.44.
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 succéssivement

$$(s_2 \circ g)(a) = (s_2 \circ f)(a) \tag{1.93a}$$
$$(g \circ s_1)(a) = (f \circ s_1)(a) \tag{1.93b}$$
$$g\big(s_1(a)\big) = f\big(s_1(a)\big). \tag{1.93c}$$

La dernière égalité signifie que $P\big(s_1(a)\big) = 1$. La proposition 1.44 implique que $P(x) = 1$ pour tout $x \in \mathcal{N}_1$.

(iii) **Bijection, définir l'inverse** Nous allons trouver un inverse et le lemme 1.7 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 $g\colon \mathcal{N}_2 \to \mathcal{N}_1$ telle que
(1) $g(o_2) = o_1$
(2) $g \circ s_2 = s_1 \circ g$.
Nous allons prouver que g est un inverse de f.

(iv) $f \circ g = \mathrm{Id}$ Nous posons $A = \{x \in \mathcal{N}_2 \text{ tel que } (f \circ g)(x) = x\}$. Nous avons

$$f\big(g(o_2)\big) = f(o_1) = o_2, \tag{1.94}$$

et donc $o_2 \in A$.
Supposons que $x \in A$. Alors

$$(f \circ g)\big(s_2(x)\big) = (f \circ \underbrace{g \circ s_2}_{s_1 \circ g})(x) \tag{1.95a}$$
$$= (\underbrace{f \circ s_1}_{= s_2 \circ f} \circ g)(x) \tag{1.95b}$$
$$= (s_2 \circ f \circ g)(x) \tag{1.95c}$$
$$= s_2\big((f \circ g)(x)\big) \tag{1.95d}$$
$$= s_2(x) \tag{1.95e}$$

Donc $s_2(x) \in A$. Nous en déduisons que $A = \mathcal{N}_2$ par le point (3) de la définition 1.41 d'un triplet naturel.

(v) $\underline{g \circ f = \mathrm{Id}}$ J'imagine que c'est la même chose que dans l'autre sens (ci-dessus) [29].

□

Proposition 1.81.
L'ensemble structuré $(\mathbb{N}, +, \times, \leqslant)$ est archimédien[30]*. En d'autres termes, pour tout $a, b \in \mathbb{N}\backslash\{0\}$, il existe $n \in \mathbb{N}$ tel que*

$$b < n \times a. \tag{1.96}$$

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

$$X = \{x \in \mathbb{N} \text{ tel que } 1 \leqslant x \times a \leqslant b\} \tag{1.97}$$

et

$$B = \{x \times a \text{ tel que } x \in X\}. \tag{1.98}$$

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 1.61(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

$$x_0 \times a < x_0 \times a + a = s(x_0) \times a = n \times a. \tag{1.99}$$

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

$$1 \leqslant n \times a \leqslant b. \tag{1.100}$$

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 $n \times a > b$. □

Définition 1.82.
Soit A un ensemble muni d'une loi de composition interne[31] *notée $+$. Si nous avons une application $\alpha : \mathbb{N} \to A$, alors nous définissons la notation $\sum_{i=0}^{N} \alpha(i)$ par récurrence de la façon suivante :*

(1) $\sum_{i=0}^{0} \alpha(i) = \alpha(0)$,

(2) $\sum_{i=0}^{k} \alpha(i) = \sum_{i=0}^{k-1} \alpha(i) + \alpha(k)$.

1.83.
Si vous êtes attentive, vous remarquerez que la définition 1.82 a besoin du théorème 1.45 pour s'assurer que $\sum_{i=0}^{N}$ est bien définie pour tout $N \in \mathbb{N}$.

Proposition 1.84 (La multiplication est une somme itérée[17])**.**
Pour tout $a, b \in \mathbb{N}$, nous avons

$$\sum_{i=1}^{n} a = a \times n. \tag{1.101}$$

29. Je n'ai pas fait les calculs ; écrivez-moi si ça pose un problème.
30. Définition 1.70.
31. Peut-être un anneau, mais comme nous avons l'intention, dans les propositions 1.84 et suivantes, de faire des sommes vers $(\mathbb{N}, +)$, plutôt un monoïde.

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 :

$$a \times s(n) = a \times n + a = \sum_{i=1}^{n} a + a = \sum_{i=1}^{n+1} a = \sum_{i=1}^{s(n)} a. \tag{1.102}$$

□

Lemme 1.85.
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 :

$$\begin{aligned}
(n+1)a &= na + a && && \text{(1.103a)}\\
&\leqslant na + na && \text{parce que } a \leqslant na && \text{(1.103b)}\\
&= 2na && && \text{(1.103c)}\\
&\leqslant 2a^n && \text{récurrence} && \text{(1.103d)}\\
&\leqslant aa^n && \text{parce que } a \geqslant 2 && \text{(1.103e)}\\
&= a^{n+1}. && && \text{(1.103f)}
\end{aligned}$$

□

Proposition 1.86 ([17]).
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

$$\begin{aligned}
a^{n+1} &= a^n \times a && && \text{(1.104a)}\\
&> a^n \times 1 && \text{lemme 1.78} && \text{(1.104b)}\\
&= a^n. && && \text{(1.104c)}
\end{aligned}$$

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 [32], nous pouvons considérer N tel que $Na > m$. Le lemme 1.53 nous assure alors que

$$m < Na \leqslant a^N. \tag{1.105}$$

□

Théorème 1.87 (division euclidienne [17]).
Pour tout $a \in \mathbb{N}$, pour tout $b \in \mathbb{N}\backslash\{0\}$, il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ avec $0 \leqslant r < b$.

*Si $r = 0$, nous disons que a est **divisible** par b.*

Démonstration. Existence puis unicité.

(i) **Existence** Nous posons

$$A = \{bx \text{ tel que } x \in \mathbb{N}, bx \leqslant a\}. \tag{1.106}$$

32. Proposition 1.81.

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

$$bq + r = a. \tag{1.107}$$

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 (1.107),

$$bq + b + x = a, \tag{1.108}$$

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.

(ii) **Unicité** Supposons que nous ayons

$$a = bq + r = bq' + r' \tag{1.109}$$

avec $0 \leqslant r < b$ et $0 \leqslant r' < b$. Il y a trois possibilités : $q' < q$, $q' = q$ et $q' > q$.

(i) **Si $q' < q$** Alors il existe $x \in \mathbb{N}$ tel que $q' + x = q$, et nous avons

$$b(q' + x) + r = bq' + bx + r, \tag{1.110}$$

ce qui, après distribution et simplification, donne $r' = bx + r$. Puisque nous avons $x \geqslant 1$, il vient

$$r' = bx + r \geqslant b + r \geqslant b. \tag{1.111}$$

Cela n'est pas possible parce que $r' < b$. Le cas $q' < q$ n'est pas possible.

(ii) **Si $q' = q$** Nous avons alors immédiatement $bq + r = bq + r'$ et donc $r = r'$. Unicité.

(iii) **Si $q' > q$** En posant $q + x = q'$ nous trouvons la même impossibilité que dans le cas $q' < q$.

□

1.3.6 Écriture d'un naturel dans une base

1.88.
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.

Si $b > 1$ et $N \in \mathbb{N}$ sont donnés, nous notons

$$C_{b,N} = \{u \in \{0, \dots, b-1\}^{N+1} \text{ tel que } u_N \neq 0\}. \tag{1.112}$$

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 [33]

$$\begin{aligned} \varphi_{b,N} \colon C_{b,N} &\to \mathbb{N} \\ u &\mapsto \sum_{i=0}^{N} u_i b^i. \end{aligned} \tag{1.113}$$

Cette application $\varphi_{b,N}$ sera encore bien étudiée pour la partie décimale d'un réel. Voir la définition 11.344.

Lemme 1.89 ([17]).
Soient $b > 1$, $N \geqslant 0$ ainsi que $u \in C_{b,N}$. Alors

$$b^N \leqslant \varphi_{b,N}(u) < b^{N+1}. \tag{1.114}$$

33. Le symbole de sommation est défini par 1.82.

Démonstration. En séparant la somme nous avons

$$\varphi_{b,N}(u) = u_N b^N + \sum_{i=0}^{N-1} u_i b^i. \tag{1.115}$$

Puisque $u_N \geqslant 1$ nous avons $b^N \leqslant u_N b^N$, et donc

$$b^N \leqslant u_N b^N \leqslant \varphi_{b,N}(u). \tag{1.116}$$

Voilà qui prouve la première inégalité de (1.114).

Pour prouver que $\varphi_{b,N}(u) < b^{N+1}$, nous faisons une récurrence sur N.

(i) **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 $u_0 \leqslant b - 1 < b$.

(ii) **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 $\varphi_{b,N+1}(v) < b^{N+2}$.

Nous posons $u = (v_0, \dots, v_N)$; nous avons alors

$$\begin{aligned}
\varphi_{b,N+1}(v) &= v_{N+1} b^{N+1} + \sum_{i=0}^{N} v_i b^i && && (1.117a)\\
&= v_{N+1} b^{N+1} + \varphi_{b,N}(u) && && (1.117b)\\
&< v_{N+1} b^{N+1} + b^{N+1} && \text{récurrence} && (1.117c)\\
&= (v_{N+1} + 1) b^{N+1} && && (1.117d)\\
&\leqslant b b^{N+1} && \text{parce que } v_{N+1} \leqslant b - 1 && (1.117e)\\
&= b^{N+2}. && && (1.117f)
\end{aligned}$$

□

Lemme 1.90 ([1]).
Soient $x \in \mathbb{N}$ ainsi que $b \geqslant 2$. Nous posons

$$N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}. \tag{1.118}$$

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.

(i) **Si $n > N$** Nous avons, par définition de $C_{b,n}$ que $u_n \neq 0$, de telle sorte que

$$\varphi_{b,n}(u) \geqslant u_n b^n \geqslant b^n > x. \tag{1.119}$$

La dernière inégalité est due au fait que $n \notin \{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}$.

(ii) **Si $n < N$** Nous avons

$$x \geqslant b^N > \varphi_{b,n}(u). \tag{1.120}$$

Le seconde inégalité est une conséquence du lemme 1.89.

□

Théorème 1.91 ([17]).
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

$$x = \varphi_{b,N}(u). \tag{1.121}$$

Démonstration. Nous commençons par $x < b$. Dans ce cas, $N = 0$ parce que si $u_k \neq 0$ avec $k \neq 0$, nous avons

$$\sum_{i=0}^{N} u_i b^i \geqslant u_k b^k \geqslant b > x. \tag{1.122}$$

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.

(i) $N \geqslant 1$ 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.

(ii) **Unicité, préambule** Le lemme 1.90 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

$$N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}. \tag{1.123}$$

Nous posons

$$X_k = \sum_{i=k}^{N} u_i b^{i-k}, \tag{1.124}$$

et nous allons montrer que le couple (X_{k+1}, u_k) est le résultat de la division euclidienne[34] de X_k par b.
D'abord, $u_k < b$, donc ça a bien la tête d'un reste. Ensuite, pour le quotient,

$$\begin{aligned} bX_{k+1} + u_k &= b \sum_{i=k+1}^{N} u_i b^{i-(k+1)} + u_k && (1.125a)\\ &= \sum_{i=k+1}^{N} u_i b^{i-k} + u_k && (1.125b)\\ &= \sum_{i=k}^{N} u_i b^{i-k} && (1.125c)\\ &= X_k. && (1.125d) \end{aligned}$$

(iii) **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

$$M = N = \max\{k \in \mathbb{N} \text{ tel que } b^k \leqslant x\}. \tag{1.126}$$

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

$$X_0 = Y_0 = x. \tag{1.127}$$

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.

(iv) **Existence** Soit $x \in \mathbb{N}$. Nous posons $y_0 = x$ et

$$y_k = by_{k+1} + u_k \tag{1.128}$$

avec $u_k < b$. Vus l'unicité dans la division euclidienne et le théorème[35] 1.45 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 :

$$\begin{aligned} 2y_{k+1} &\leqslant by_{k+1} && \text{parce que } b \geqslant 2 && (1.129a)\\ &\leqslant y_k && \text{pcq } by_{k+1} + u_k = y_k. && (1.129b) \end{aligned}$$

34. Théorème 1.87.
35. Nous ne citerons pas toujours ce théorème à chaque fois que nous définissons quelque chose par récurrence.

Bref : $2y_{k+1} \leqslant y_k$. Par récurrence[36] nous trouvons que

$$2^k y_k \leqslant x \tag{1.130}$$

parce que $y_0 = x$. Par le lemme 1.85, si k est assez grand,

$$2ky_k \leqslant 2^k y_k \leqslant x. \tag{1.131}$$

Puisque $\mathbb{N}$ est archimédien[37], nous pouvons considérer $s \in \mathbb{N}$ tel que $2s > x$. À ce moment nous avons

$$y_n = 0 \tag{1.132}$$

pour tout $n \geqslant s$. Nous posons

$$N = \max\{k \text{ tel que } y_k \neq 0\}. \tag{1.133}$$

Prouvons par récurrence sur l que

$$y_{N-l} = \sum_{i=N-l}^{N} u_i b^{(i+l)-N}. \tag{1.134}$$

Notez que $i + l \geqslant N - l + l = N$, donc $(i + l) - N$ a un sens.

(i) **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

$$y_N = by_{N+1} + u_N. \tag{1.135}$$

En se rappelant que $y_{N+1} = 0$, nous avons le résultat.

(ii) **Pour $l + 1$** Pour la récurrence nous avons le calcul suivant :

$$\begin{aligned} y_{N-l-1} &= by_{N-l} + u_{N-l-1} && (1.136a)\\ &= b \sum_{i=N-l}^{N} u_i b^{(i+l)-N} + u_{N-l-1} && (1.136b)\\ &= \sum_{i=N-l}^{N} u_i b^{(i+l)-N+1} + u_{N-l-1} && (1.136c)\\ &= \sum_{i=N-l-1}^{N} u_i b^{(i+l+1)-N}. && (1.136d) \end{aligned}$$

La récurrence est prouvée. L'égalité (1.134) est validée pour tout l.

En posant $l = N$ dans (1.134) nous trouvons

$$y_0 = \sum_{i=0}^{N} u_i b^i. \tag{1.137}$$

Mais la définition de la suite (y_k) contient $y_0 = x$. Donc nous avons prouvé que

$$x = \sum_{i=0}^{N} u_i b^i = \varphi_{b,N}(u). \tag{1.138}$$

□

36. Faut-il citer la proposition 1.44 et donner explicitement la fonction P ?
37. Proposition 1.81.

Exemple 1.92.
Comment écrire le nombre b en base b ? Nous devons trouver un N et une suite (u_i) tels que

$$b = \sum_{i=0}^{N} u_i b^i. \tag{1.139}$$

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

$$b = \varphi_{b,1}(1, 0). \tag{1.140}$$

Nous écrivons cela plus sobrement $b = 10$. △

1.93.
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 5.54.

La proposition suivante dit que le nombre qui a le plus de chiffres est le plus grand.

Proposition 1.94 ([17])**.**
Si $u \in C_{b,N}$ et $v \in C_{b,M}$ avec $M > N$ alors $\varphi_{b,N}(u) < \varphi_{b,M}(v)$.

Démonstration. Le lemme 1.89 nous dit que

$$b^N \leqslant \varphi_{b,N}(u) < b^{N+1} \tag{1.141}$$

et

$$b^M \leqslant \varphi_{b,M}(v) < b^{M+1}. \tag{1.142}$$

Puisque $M > N$ nous avons $b^{N+1} \leqslant b^M$ et donc

$$\varphi_{b,N}(u) < b^{N+1} \leqslant b^M \leqslant \varphi_{b,M}(v). \tag{1.143}$$

□

La proposition suivante dit que si deux nombres s'écrivent 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.

Proposition 1.95.
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 $\varphi_{b,N}(u) > \varphi_{b,N}(v)$.

Démonstration. En découpant les sommes nous avons

$$\varphi_{b,N}(u) = \sum_{i=r+1}^{N} u_i b^i + u_r b^r + \sum_{i=0}^{r-1} u_i b^i \tag{1.144}$$

et

$$\varphi_{b,N}(v) = \sum_{i=r+1}^{N} u_i b^i + v_r b^r + \sum_{i=0}^{r-1} v_i b^i. \tag{1.145}$$

Puisque $b^r > \sum_{i=0}^{r-1} u_i b^i$ (lemme 1.89), nous avons aussi

$$b^r + \sum_{i=0}^{r-1} u_i b^i > \sum_{i=0}^{r-1} v_i b^i. \tag{1.146}$$

Et le calcul final :

$$\begin{aligned}
\varphi_{b,N}(v) &< \sum_{i=r+1}^{N} v_i b^i + v_r b^r + b^r + \sum_{i=0}^{r-1} u_i b^i && \text{pcq (1.146)} && \text{(1.147a)}\\
&= \sum_{i=r+1}^{N} u_i b^i + (v_r+1) b^r + \sum_{i=0}^{r-1} u_i b^i && && \text{(1.147b)}\\
&\leqslant \sum_{i=r+1}^{N} u_i b^i + u_r b^r + \sum_{i=0}^{r-1} u_i b^i && \text{pcq } u_r \geqslant v_r + 1 && \text{(1.147c)}\\
&= \sum_{i=0}^{N} u_i b^i && && \text{(1.147d)}\\
&= \varphi_{b,N}(u). && && \text{(1.147e)}
\end{aligned}$$

Et voilà. □

1.96.
Il est aussi possible de définir des choses par récurrence de telle sorte que l'élément x_n soit définit en fonction de tous les x_i $(i < n)$. Voyons comment définir la suite

$$\begin{cases} x_1 = 1 & \text{(1.148a)}\\ x_n = \sum_{k=1}^{n-1} x_n & \text{(1.148b)} \end{cases}$$

en utilisant le théorème 1.45. Il faut prendre $E = \mathbb{N} \cup \mathbb{N} \times \mathbb{N} \cup \dots$ et ensuite $b = 1$ et

$$g(x_1, \dots, x_{n-1}) = (x_1, \dots, x_{n-1}, \sum_{k=1}^{n-1} x_k). \tag{1.149}$$

L'élément x_n de la suite est la projection sur la n^{e}composante de l'élément $f(n)$.

1.4 Les entiers

Proposition-Définition 1.97 ([17])**.**
Soient $a, b, a', b' \in \mathbb{N}$. Nous disons que $(a, b) \sim (a', b')$ si et seulement si

$$a + b' = b + a' \tag{1.150}$$

(1) $\sim$ est une relation d'équivalence sur $\mathbb{N}^2$.

(2) Si $(a, b) \sim (a', b')$ et $(x, y) \sim (x', y')$ alors

$$(a + x, b + y) \sim (a' + x', b' + y'). \tag{1.151}$$

*L'ensemble des **entiers** est*

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim, \tag{1.152}$$

et nous notons $\overline{a, b} \in \mathbb{Z}$ la classe de $(a, b) \in \mathbb{N} \times \mathbb{N}$.

Démonstration. En plusieurs points.

(i) **Symétrie** C'est la commutativité de la somme dans $\mathbb{N}$, proposition 1.51(1).

(ii) **Réflexive** Immédiat.

(iii) **Transitive** Nous supposons que $(a,b)\sim(u,v)$ et que $(u,v)\sim(x,y)$. Alors nous avons

$$a+v=u+b \tag{1.153a}$$
$$u+y=v+x. \tag{1.153b}$$

En additionnant membre à membre,

$$a+v+u+y=u+b+v+x. \tag{1.154}$$

La commutativité nous permet de mettre u et v à droite dans chacun des deux membres. Ensuite la proposition 1.51(3) nous permet de simplifier par $u+v$. Il reste $a+y=b+x$, qui signifie $(a,b)\sim(x,y)$.

(iv) **Pour (2)** L'hypothèse donne les égalités

$$a+b'=b+a' \tag{1.155a}$$
$$x+y'=y+x' \tag{1.155b}$$

En sommant, et en utilisant l'associativité,

$$(a+x)+(b'+y')=(b+y)+(a'+x'). \tag{1.156}$$

Cela signifie bien que $(a+x,b+y)\sim(a'+x',b'+y')$.

□

Lemme 1.98.
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 $a=b$. □

Proposition-Définition 1.99 ([17])**.**
Soient $a,b,x,y\in\mathbb{N}$. L'application

$$\begin{aligned} f\colon \overline{(a,b)}\times\overline{(x,y)} &\to \mathbb{Z} \\ \big((a',b'),(x',y')\big) &\mapsto (a'+x',b'+y') \end{aligned} \tag{1.157}$$

est constante.

Nous nommons sa valeur $\overline{(a,b)}+\overline{(x,y)}$.

Démonstration. Cela est une conséquence de la proposition 1.97(2). □

Proposition 1.100.
La paire $(\mathbb{Z},+)$ est un groupe commutatif.

Démonstration. En plusieurs points.

(i) **Neutre** Le neutre est $e=\overline{(0,0)}$. En effet,

$$\overline{(a,b)}+\overline{(0,0)}=\overline{(a+0,b+0)}=\overline{(a,b)}. \tag{1.158}$$

De même $e+\overline{(a,b)}=\overline{(a,b)}$ par commutativité de la somme dans $\mathbb{N}$.

(ii) **Inverse** Il est facile de vérifier que $\overline{(b,a)}$ est l'inverse de $\overline{(a,b)}$.

(iii) **Associativité** Calcul direct en utilisant l'associativité dans $\mathbb{N}$.

□

Proposition 1.101.
L'application

$$\begin{aligned} \iota\colon \mathbb{N} &\to \mathbb{Z} \\ n &\mapsto \overline{(n,0)} \end{aligned} \tag{1.159}$$

est un morphisme[38] *injectif.*

Démonstration. Le fait que ce soit un morphisme est le calcul

$$\iota(a+b) = \overline{(a+b,0)} = \overline{(a,0)} + \overline{(b,0)} = \iota(a) + \iota(b). \tag{1.160}$$

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 $a = b$. □

1.4.1 Opposé

Lemme 1.102.
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

$$(a,b) \sim (a-b,0) \tag{1.161}$$

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

$$(a,b) \sim (0,b-a). \tag{1.162}$$

Puisque l'ordre sur $\mathbb{N}$ est total[39], tous les cas sont couverts. □

Lemme-Définition 1.103.
Soit $z \in \mathbb{Z}$. L'application[40]

$$\begin{aligned} f\colon z &\to \mathbb{Z} \\ (a,b) &\mapsto \overline{(b,a)} \end{aligned} \tag{1.163}$$

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. □

Lemme 1.104.
Nous avons

(1) $\mathbb{Z} = \iota(\mathbb{N}) \cup -\iota(\mathbb{N})$
(2) $\iota(\mathbb{N}) \cap -\iota(\mathbb{N}) = \{0\}$.

38. Certes $\mathbb{N}$ n'est pas un groupe, donc le mot « morphisme » est un peu abusé, mais vous voyez ce que je veux dire.
39. Proposition 1.60.
40. 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.

Démonstration. Nous avons

$$\iota(\mathbb{N}) = \{\overline{(n,0)} \text{ tel que } n \in \mathbb{N}\} \tag{1.164a}$$
$$-\iota(\mathbb{N}) = \{\overline{(0,n)} \text{ tel que } n \in \mathbb{N}\}. \tag{1.164b}$$

Montrons à présent les deux points.

(i) **Pour (1)** Nous savons par le lemme 1.102 que tous les éléments de $\mathbb{Z}$ sont de la forme (1.164a) ou (1.164b).

(ii) **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 1.53 dit alors que $n = m = 0$.
Nous avons donc $z = \overline{(0,0)} = 0$.

□

1.4.2 Ordre sur $\mathbb{Z}$

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.

Proposition-Définition 1.105 (Relation d'ordre [17])**.**
Nous disons que $x \leqslant y$ si et seulement si $y - x \in \mathbb{N}$.
L'ensemble $(\mathbb{Z}, \leqslant)$ est totalement ordonné.

Une version dans $\mathbb{R}$ sera le lemme 1.418.

Lemme 1.106.
Soient $a > 0$ et $b > 1$ dans $\mathbb{Z}$. Nous avons

$$ab > a. \tag{1.165}$$

Lemme 1.107.
Toute partie bornée de $\mathbb{Z}$ possède un plus grand élément.

Proposition 1.108.
Soit $a, b \in \mathbb{Z}$ tels que a divise b. Alors $|a| \leqslant |b|$.

Lemme 1.109.
L'ensemble $\mathbb{Z}$ est infini dénombrable.

1.5 Quelques résultats de cardinalité

1.5.1 Équipotence, surpotence, subpotence

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 6.134 qui démontre l'existence de clôture algébrique pour tout corps.

Définition 1.110 ([20, 21])**.**
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.

Proposition 1.111 ([1, 12]).
L'ensemble A est subpotent à B si et seulement si B est surpotent à A.

Démonstration. En deux parties.

(i) $\Rightarrow$ 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

$$f(x) = \begin{cases} \varphi^{-1}(x) & \text{si } x \in \varphi(A) \\ a & \text{sinon} \end{cases} \tag{1.166}$$

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.

(ii) $\Leftarrow$ 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

$$\begin{aligned} f\colon A &\to B \\ x &\mapsto b_x. \end{aligned} \tag{1.167}$$

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

$$x = \varphi(b_x) = \varphi(b_y) = y. \tag{1.168}$$

Nous avons prouvé que $x = y$, et donc que f est injective.

□

Vu que l'ensemble des ensembles n'existe pas [41], 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.

1.5.2 Un peu d'infinité

Définition 1.112 (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.*

1.113.
Nous adoptons les notions d'ensembles finis et infinis au sens de Dedekind. De nombreuses sources (dont wikipédia [22, 23]) 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 [42]. 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 1.112) si et seulement si il existe une bijection $\{0, \dots, N\} \to A$ pour un certain $N \in \mathbb{N}$. Ce sera le théorème 1.121.

Lemme 1.114.
Toute partie d'un ensemble fini est finie.

41. Voir le corolaire 1.145.
42. Et même seulement l'axiome du choix dénombrable ; si vous voulez en savoir plus, lisez la page wikipédia [24].

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 1.112, il existe une partie $A' \subsetneq A$ et une bijection $\sigma\colon A' \to A$.

Nous considérons la partie $B' = A' \cup (B\backslash A)$, qui est une partie stricte de B. Puisque $A' \cap (B\backslash A) = \varnothing$, nous pouvons définir

$$\begin{aligned} \varphi\colon B' &\to B \\ x &\mapsto \begin{cases} \sigma(x) & \text{si } x \in A' \\ x & \text{si } x \in B\backslash A. \end{cases} \end{aligned} \tag{1.169}$$

Montrons que φ est une bijection.

(i) **Surjectif** Nous avons $\varphi(A') = A$ et $\varphi(B\backslash A) = B\backslash A$. Donc

$$\varphi(B') = \varphi(A') \cup \varphi(B\backslash A) = A \cup (B\backslash A) = B. \tag{1.170}$$

(ii) **Injectif** Si $\varphi(x) = \varphi(y)$, nous avons 4 possibilités suivant que x et y sont dans A' ou $B\backslash A$.
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 $y \in B\backslash A$ alors $\varphi(x) = \sigma(x) \in A$ et $\varphi(y) = y \in B\backslash A$. Ce cas n'est pas possible. Le cas $x \in B\backslash A$ et $y \in A'$ n'est pas possible non plus.
Si $x, y \in B\backslash A$, 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. □

Proposition 1.115 ([1]).
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.

(i) $\omega \notin B$ Alors $B \subset A$, et il existe $x \in B$ tel que $\sigma(x) = \omega$. Considérons $B' = B\backslash\{x\}$; cela est une partie propre de A. Ensuite nous définissons

$$\begin{aligned} \varphi\colon B\backslash\{x\} &\to A \\ a &\mapsto \sigma(a). \end{aligned} \tag{1.171}$$

C'est injectif parce que σ est injective, et c'est surjectif parce que

$$\varphi\big(B\backslash\{x\}\big) = \sigma(B)\backslash\sigma(\{\omega\}) = \sigma(B)\backslash\{\omega\} = (A \cup \{\omega\})\backslash\{\omega\} = A. \tag{1.172}$$

Pour la dernière égalité nous avons utilisé le fait que ω n'est pas dans A.

(ii) **Si $\omega \in B$** Puisque B est une partie propre de $A \cup \{\omega\}$, il existe $x \in A\backslash B$. Nous considérons $B' = \big(B\backslash\{\omega\}\big) \cup \{x\}$ et nous définissons

$$\begin{aligned} \varphi\colon B' &\to A \\ b &\mapsto \begin{cases} \sigma(b) & \text{si } b \neq x \\ \sigma(\omega) & \text{si } b = x. \end{cases} \end{aligned} \tag{1.173}$$

Nous montrons à présent que φ est une bijection.

(i) **Injectif** Soient u, v 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 $v \neq x$, alors $\varphi(u) = \sigma(\omega)$ et $\varphi(v) = \sigma(v)$. Mais $x \neq \omega$ parce que $x \in A$, donc cette situation n'est pas possible parce que σ est injective.
Si $u \neq x$ et $v \neq x$, alors $\varphi(u) = \sigma(u)$ et $\varphi(v) = \sigma(v)$. Dans ce cas l'injectivité de σ fait que $x = y$.

(ii) **Surjective** Soit $y \in A$. Vu que $\sigma\colon B \to A \cup \{\omega\}$ est surjective, il existe $b \in B$ tel que $\sigma(b) = y$. Si $b \neq \omega$ alors $\varphi(b) = \sigma(b) = y$. 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 $B \subsetneq A \cup \{\omega\}$ et $A \cup \{\omega\}$. □

La proposition suivante est à peu près prise comme définition d'un ensemble fini dans [25] qui donne également une preuve de l'équivalence avec notre définition.

Proposition 1.116.
L'ensemble $\mathbb{N}$ *est infini*[43].

Démonstration. Nous considérons la partie propre[44]

$$A = \{n \in \mathbb{N} \text{ tel que } n \geqslant 1\}. \tag{1.174}$$

Ensuite nous posons

$$\begin{aligned} \sigma\colon \mathbb{N} &\to A \\ x &\mapsto s(x). \end{aligned} \tag{1.175}$$

Le fait que σ prenne ses valeurs dans A est parce que s prend ses valeurs dans $\mathbb{N}\backslash\{0\} = A$.

(i) σ **est injective** Parce que s l'est.

(ii) σ **est surjective** C'est dans la définition 1.41(2)

Nous avons donc une bijection entre $\mathbb{N}$ et un sous-ensemble strict. □

Lemme 1.117.
Soit $N \in \mathbb{N}$. *La partie* $\{0, \dots, N\}$ *est finie*[45].

Démonstration. Par récurrence sur N. Avec $N = 0$, la partie $\{0\}$ est finie parce que son seul sous-ensemble propre est $\varnothing$ qui n'est pas en bijection avec $\{0\}$.

Supposons que $\{0, \dots, N\}$ est fini. Alors $\{0, \dots, N\} \cup \{N+1\}$ est fini par le lemme 1.115. □

Lemme 1.118.
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 1.117), il n'y a pas de bijection avec ses parties strictes. □

Proposition 1.119 ([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

$$\begin{aligned} \varphi_B\colon \sigma(A') &\to \sigma(A) \\ y &\mapsto \sigma\Big(\varphi\big(\sigma^{-1}(y)\big)\Big). \end{aligned} \tag{1.176}$$

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.

43. Définition 1.112.
44. 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 1.55 dit que $0 \leqslant 1$, et d'autre part parce que le lemme 1.53 donne $0 \neq 1$.
45. Pour rappel, la définition de $\{0, \dots, N\}$ est 1.65.

(i) **Injective** Supposons que $\varphi_B(a) = \varphi_B(b)$, c'est-à-dire que

$$(\sigma \circ \varphi_A \circ \sigma^{-1})(a) = (\sigma \circ \varphi_A \circ \sigma^{-1})(b). \tag{1.177}$$

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 $a = b$.

(ii) **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 1.114 conclut que B est infini. □

Lemme 1.120.
À propos d'applications entre ensembles finis.

(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.

(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

$$\mathcal{A} = \{X \subset A \text{ tel que } \sigma\colon X \to \sigma(A) \text{ est injective}\} \tag{1.178}$$

que nous ordonnons (partiellement) par l'inclusion.

(i) **$\mathcal{A}$ 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 [46].

(ii) **Zorn** L'ensemble $\mathcal{A}$ étant inductif et non vide (les singletons dans A sont dans $\mathcal{A}$), il possède un élément maximal [47] par le lemme de Zorn 1.22. Nous nommons A' un élément maximal dans $\mathcal{A}$.

(iii) **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 $y \in \sigma(A)\backslash\sigma(A')$. Alors il existe $a \in A\backslash A'$ 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.

(iv) **Conclusion** L'ensemble A' est fini en tant que partie de l'ensemble fini A (lemme 1.114). L'application σ étant injective, la proposition 1.119 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 $\sigma(A) = B$. □

Proposition-Définition 1.121 (Cardinal d'un ensemble fini[1])**.**
Soit un ensemble non vide I.

(1) L'ensemble I est fini [48] si et seulement si il existe une bijection entre I et $\{0, \dots, N\}$ pour un certain $N \in \mathbb{N}$.

46. Plus précisément c'est l'ensemble ordonné $(\mathcal{A}, \subset)$ qui est inductif.
47. Définition 1.12 ; voir aussi 1.15.
48. Ensemble fini, définition 1.112.

(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* $\mathrm{Card}(I)$. *Pour l'ensemble vide, nous définissons* $\mathrm{Card}(\varnothing) = 0$.

Démonstration. En plusieurs parties.

(i) **(1)⇐** Soit un ensemble A en bijection avec $\{0, \dots, N\}$. Nous avons vu que $\{0, \dots, N\}$ est fini dans le lemme 1.117. Le lemme 1.120(2) conclut que A est fini.

(ii) **(1)⇒** 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

$$\mathcal{A} = \{(N, \varphi) \text{ tel que } \varphi\colon \{0, \dots, N\} \to A \text{ est injective}\}. \tag{1.179}$$

Nous mettons sur $\mathcal{A}$ la relation d'ordre donnée par $(N_1, \varphi_1) \leqslant (N_2, \varphi_2)$ lorsque

(1) $N_1 \leqslant N_2$

(2) φ_2 étend φ_1, c'est-à-dire que $\varphi_2 = \varphi_1$ sur $\{0, \dots, N\}$.

(i) **$\mathcal{A}$ est inductif** Soit une partie $\mathcal{F}$ totalement ordonnée de $\mathcal{A}$. Nous considérons la partie suivante de $\mathbb{N}$:

$$S = \{n \in \mathbb{N} \text{ tel que } \exists (n, \varphi) \in \mathcal{F}\}. \tag{1.180}$$

Si S est majoré, alors il a un maximum (proposition 1.61(4)). Si M est le maximum de S, le (M, φ) de $\mathcal{F}$ qui correspond à ce maximum est un majorant de $\mathcal{F}$.

Supposons –pour l'absurde– que $\mathcal{F}$ n'est pas majoré ; en particulier S n'est pas majoré. Pour chaque $n \in S$, il existe une application φ_n telle que $(n, \varphi_n) \in \mathcal{F}$. Cela nous permet de définir

$$\begin{aligned} \phi\colon S &\to A \\ n &\mapsto \varphi_n(n). \end{aligned} \tag{1.181}$$

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 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[49]. La proposition 1.119 conclut que A est infini, ce qui est contraire aux hypothèses.

Donc $\mathcal{F}$ a un majorant et $\mathcal{A}$ est inductif.

(ii) **Lemme de Zorn** Le lemme de Zorn dit que $\mathcal{A}$ a un élément maximal.

(iii) **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 qu'elle 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

$$\begin{aligned} \phi\colon \{0, \dots, N+1\} &\to A \\ x &\mapsto \begin{cases} \varphi(x) & \text{si } x \neq N+1 \\ a & \text{si } x = N+1, \end{cases} \end{aligned} \tag{1.182}$$

le couple $(N+1, \phi)$ majore strictement (N, φ). Ce qui est une contradiction.

(iii) **(2) existence** L'existence est ce que nous venons de montrer ci-dessus.

(iv) **(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 1.118, cela implique que $M = N$.

49. Le lemme 1.67 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 1.119.

□

Nous ne définissons pas ce qu'est le cardinal d'un ensemble infini ; c'est très compliqué et ça ne nous servira pas.

Lemme 1.122.
Si A est une partie infinie de $\mathbb{N}$, alors pour tout n, la partie $A\backslash\{0,\dots,n\}$ est non vide.

Démonstration. Si $A\backslash\{0,\dots,n\}$ était vide, cela signifierait que A est une partie de $\{0,\dots,n\}$. Or nous savons que $\{0,\dots,n\}$ est fini (lemme 1.117), et que toute partie d'un ensemble fini est finie (lemme 1.114). Donc nous aurions que A est fini, ce qui est contraire à l'hypothèse. □

Lemme 1.123 ([1]).
Union d'ensembles finis.

(1) Si A et B sont des ensembles finis disjoints, alors $A\cup B$ est fini et

$$\text{Card}(A\cup B)=\text{Card}(A)+\text{Card}(B). \tag{1.183}$$

(2) Si A et B sont des ensembles finis, alors $A\cup B$ est fini.

(3) Si A est fini et si $B\subset A$ alors

$$\text{Card}(A\backslash B)=\text{Card}(A)-\text{Card}(B). \tag{1.184}$$

(4) Si A et B sont des ensembles quelconques, alors

$$\text{Card}(A\cup B)=\text{Card}(A)+\text{Card}(B)-\text{Card}(A\cap B). \tag{1.185}$$

(5) Si les $\{A_i\}_{i=1,\dots,n}$ sont des ensembles disjoints, alors

$$\text{Card}\big(\bigcup_{i=1}^{n}A_i\big)=\sum_{i=1}^{n}\text{Card}(A_i). \tag{1.186}$$

(6) Si I ou J est infini, alors $I\cup J$ est infini.

Démonstration. Point par point.

(i) **Pour (1)** Puisque A et B sont finis, la proposition 1.121 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

$$\begin{aligned}\varphi\colon\{0,\dots,M+N+1\}&\to A\cup B\\ n&\mapsto\begin{cases}\varphi_A(n) & \text{si } n\leqslant N\\ \varphi_B(n-N-1) & \text{si } n>N\end{cases}\end{aligned} \tag{1.187}$$

est une bijection. Le fait que A et B soient disjoints est important pour l'injectivité. La proposition 1.121 nous dit qu'alors $A\cup B$ est fini. De plus, par définition le cardinal de $A\cup B$ est $N+M$.

(ii) **Pour (2)** Nous ne supposons plus que A et B sont disjoints. Nous posons $I=A$ et $J=B\backslash A$. Avec ça, I et J sont disjoints et finis (comme parties des ensembles finis, lemme 1.114), et vérifient $I\cup J=A\cup B$. Le point (1) indique que $I\cup J$ est fini.

(iii) **Pour (3)** L'ensemble A peut être écrit sous la forme d'une union disjointe : $A=B\cup(A\backslash B)$. Les ensembles B et $A\backslash B$ étant disjoints, nous avons

$$\text{Card}(A)=\text{Card}(B)+\text{Card}(A\backslash B). \tag{1.188}$$

(iv) **Pour (4)** Nous utilisons quelques égalités d'ensembles pour ramener $A \cup B$ à des cas déjà traités :

$$A \cup B = A \cup (B\backslash A) = A \cup \big(B\backslash(A \cap B)\big). \tag{1.189}$$

Nous avons en particulier utilisé $B\backslash A = B\backslash(A \cap B)$. La chose intéressante dans (1.189) est que l'union est disjointe et que $A \cap B \subset B$. Nous pouvons donc écrire

$$\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}\big(B\backslash(A \cap B)\big) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B). \tag{1.190}$$

(v) **Pour (5)** Récurrence en utilisant le point (4).

(vi) **Pour (6)** Toute partie d'un ensemble fini est finie (lemme 1.114). Donc si $I \cup J$ était fini, I et J devraient l'être.

□

Définition 1.124.
*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 1.112, c'est qu'un ensemble fini n'est ni dénombrable ni non dénombrable [50].

Lemme 1.125.
Si A est dénombrable et si il existe une surjection $f\colon A \to B$, alors B est fini ou dénombrable.

Lemme 1.126.
Si A est un ensemble fini ou dénombrable, alors il existe une surjection $\mathbb{N} \to A$.

1.5.3 Dénombrabilité et ensemble des naturels

Proposition 1.127 ([1, 12])**.**
Toute partie infinie de $\mathbb{N}$ *est dénombrable.*

Démonstration. Soit A, une partie infinie de $\mathbb{N}$.

(i) **Définition de σ** Nous voulons construire une application $\sigma\colon \mathbb{N} \to A$ telle que

$$\begin{cases} \sigma(0) = \min(A) & \text{(1.191a)} \\ \sigma(k+1) = \min\Big(A\backslash\sigma\big(\{0,\dots,k\}\big)\Big) & \text{(1.191b)} \end{cases}$$

Les lâches, par prudence, diront juste que c'est défini par récurrence et n'insisteront pas. Nous, nous insistons.

Nous allons définir $\sigma(n)$ à l'aide du théorème 1.45. Pour cela nous posons $E = \mathcal{P}(A)$, $b = \varnothing$ et

$$\begin{aligned} g\colon E &\to E \\ Z &\mapsto \begin{cases} A & \text{si } Z = A \\ Z \cup \{\min(A\backslash Z)\} & \text{sinon.} \end{cases} \end{aligned} \tag{1.192}$$

Notons que la proposition 1.61(2) nous indique que toute partie non vide de $\mathbb{N}$ possède un minimum ; la définition de g a donc un sens. Le théorème 1.45 donne alors une application $f\colon \mathbb{N} \to E$ telle que

(1) $f(0) = b = \varnothing$

(2) $f(n+1) = g\big(f(n)\big)$ pour tout $n \geqslant 0$.

50. 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[26].

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

$$f(n+1) = g\big(f(n)\big) = f(n) \cup \{\min\big(A\backslash f(n)\big)\}. \tag{1.193}$$

Dans ce cas, $f(n+1)$ est également fini comme union de deux ensembles finis.

Nous posons

$$\sigma(n) = \min\big(A\backslash f(n)\big). \tag{1.194}$$

Avec $n = 0$, nous avons $\sigma(0) = \min\big(A\backslash\varnothing\big) = \min(A)$. La condition (1.191a) est donc déjà satisfaite.

Nous devons encore prouver (1.191b). Pour tout n, la relation entre $f(n)$ et $\sigma(n)$ est donnée par

$$\begin{cases} f(0) = \varnothing & \text{(1.195a)} \\ f(n+1) = f(n) \cup \sigma(n). & \text{(1.195b)} \end{cases}$$

Par récurrence nous avons alors

$$f(n) = \bigcup_{k=0}^{n-1} \{\sigma(k)\} = \sigma\big(\{0, \dots, n-1\}\big) \tag{1.196}$$

pour tout $n \geqslant 1$. Nous avons alors la condition 1.191b en substituant (1.196) dans la définition (1.194) écrite avec $n+1$:

$$\sigma(n+1) = \min\big(A\backslash f(n+1)\big) = \min\Big(A\backslash\sigma\big(\{0, \dots, n\}\big)\Big). \tag{1.197}$$

(ii) **σ est strictement croissante** Vu que $A\backslash\sigma\{0, \dots, k\} \subset A\backslash\sigma\{0, \dots, k-1\}$, le minimum est plus grand ou égal : $\sigma(k+1) \geqslant \sigma(k)$. Mais $\sigma(k+1)$ est sélectionné dans l'ensemble $A\backslash\sigma\{0, \dots, k\}$, qui ne contient justement pas $\sigma(k)$. Donc $\sigma(k+1) \neq \sigma(k)$.

(iii) **σ est définie sur $\mathbb{N}$** Il faut montrer que pour tout k, l'ensemble $A\backslash\sigma\{0, \dots, k\}$ est non vide. Si il l'était, cela signifierait que $A \subset \sigma\{0, \dots, k\}$. Par le lemme 1.120(1), la partie $\sigma\{0, \dots, k\}$ est finie dans $\mathbb{N}$. Le lemme 1.114 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 $\mathbb{N}$.

(iv) **σ est injective** Une application $\mathbb{N} \to \mathbb{N}$ strictement croissante est injective par la proposition 1.66.

(v) **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

$$\min\big(A\backslash\sigma\{0, \dots, a\}\big) > a. \tag{1.198}$$

Si $\sigma\big(\{0, \dots, a\}\big)$ ne contenait pas a, alors $A\backslash\sigma(\{0, \dots, a\})$ le contiendrait et nous n'aurions pas l'inégalité (1.198). Donc $a \in \sigma\big(\{0, \dots, a\}\big)$ et a est bien dans l'image de σ.

□

1.128.

La proposition 1.127 pourrait être prouvée plus facilement en acceptant le théorème de Cantor-Schröder-Bernstein 1.140. 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.

1.129.
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[51]. Son utilité est de pouvoir créer un langage de programmation pouvant traiter des paires d'entiers rien qu'en traitant des entiers.

Proposition 1.130 (Une bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$)**.**
La fonction

$$\begin{aligned} f\colon \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (x,y) &\mapsto \begin{cases} y^2 + x & si\ x < y \\ x^2 + x + y & si\ y \leqslant x. \end{cases} \end{aligned} \tag{1.199}$$

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.

(i) **f est injective** Pour $k \in \mathbb{N}$ donné, nous allons prouver que

(1) l'équation $f(x,y) = k$ possède au maximum une solution avec $x < y$,

(2) l'équation $f(x,y) = k$ possède au maximum une solution avec $y \leqslant x$,

(3) 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.

(1) 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,

$$\begin{aligned} z &= x - 2sy - s^2 && (1.200a)\\ &< x - 2sy && (1.200b)\\ &< x - 2sx && (1.200c)\\ &= x(1-2s) && (1.200d)\\ &< 0. && (1.200e) \end{aligned}$$

Impossible parce que $z \geqslant 0$.

(2) 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.

(3) 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 :

$$(y+s)^2 + x = z^2 + z + t \tag{1.201}$$

qui donne

$$x = z + t - 2zs - s^2 < 2z - 2zs - s^2 = 2z(1-s) - s^2 \leqslant -s < 0 \tag{1.202}$$

parce que $s \geqslant 1$, donc $1 - s \leqslant 0$.

(ii) **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

$$f(1,a), f(2,a), \dots, f(a-1,a) \tag{1.203}$$

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 $a^2 + 2a = (a+1)^2 - 1$.

51. 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.

□

Sachez que cette fonction s'étend aux ordinaux (mais là ce n'est plus pour rigoler).

Corolaire 1.131.
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 1.130, et nous posons

$$\mathbb{N}_i=f^{-1}(i,\mathbb{N}). \tag{1.204}$$

L'application

$$f\colon\mathbb{N}_i\to\{(i,k)\}_{k\in\mathbb{N}} \tag{1.205}$$

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. □

Lemme 1.132 ([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 $\mathbb{N}$.

(i) **Une application** La proposition 1.61(2) nous permet de poser

$$\begin{aligned}\sigma\colon A&\to\mathbb{N}\\ a&\mapsto\min\bigl(f^{-1}(a)\bigr).\end{aligned} \tag{1.206}$$

(ii) **σ est injective** Supposons que $\sigma(a)=\sigma(b)$. Nous appelons x ce nombre :

$$x=\min\bigl(f^{-1}(a)\bigr)=\min\bigl(f^{-1}(b)\bigr). \tag{1.207}$$

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.

(iii) **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 $A\to\mathbb{N}$.

(iv) **$\sigma(A)$ est dénombrable** Puisque $\sigma\colon A\to\mathbb{N}$ est injective et que A est infini, la proposition 1.119 dit que $\sigma(A)$ est infini dans $\mathbb{N}$. La proposition 1.127 nous dit alors que $\sigma(A)$ est dénombrable.
Soit une bijection $\varphi\colon\sigma(A)\to\mathbb{N}$.

(v) **La candidate bijection** Nous posons

$$f=\varphi\circ\sigma\colon A\to\mathbb{N} \tag{1.208}$$

et nous allons prouver que c'est une bijection.

(vi) **Injective** Puisque φ et σ sont injectives, l'égalité $(\varphi\sigma)(a)=(\varphi\sigma)(b)$ implique immédiatement $a=b$.

(vii) **Surjective** Soit $k\in\mathbb{N}$. Puisque φ et σ sont des injections, nous pouvons poser $a=(\overline{\sigma^{-1}\varphi^{-1}})(k)$. Il est alors immédiat que $f(a)=k$.

□

Proposition 1.133 ([1, 26]).
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 1.131. 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

$$\begin{aligned}\varphi\colon \mathbb{N} &\to A\\ n &\mapsto \varphi_{s(n)}(n).\end{aligned} \tag{1.209}$$

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

$$a = \varphi_i(n) = \varphi_{s(n)}(n) = \varphi(n). \tag{1.210}$$

Donc $\varphi\colon \mathbb{N} \to A$ est surjective.

Le lemme 1.132 conclut que A est fini ou dénombrable. □

Lemme 1.134 ([1]).
Si N est un ensemble dénombrable, alors il existe une bijection $g\colon \{1,2\} \times N \to N$.

Démonstration. D'abord nous définissons une bijection $\varphi\colon \{0,1\} \times \mathbb{N} \to \mathbb{N}$ par

$$\begin{aligned}\varphi\colon \{0,1\} \times \mathbb{N} &\to \mathbb{N}\\ (n,k) &\mapsto 2k + n.\end{aligned} \tag{1.211}$$

Ensuite si $f\colon \mathbb{N} \to N$ est une bijection, il suffit de poser $g(n,k) = f\big(\varphi(n,k)\big)$. □

Proposition 1.135 ([26]).
Si N est un ensemble dénombrable, alors pour tout $n \in \mathbb{N}$, l'ensemble N^n est dénombrable.

Les ensembles dénombrables sont les plus petits ensembles infinis possibles, comme en témoigne la proposition suivante.

Proposition 1.136.
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 $\varphi\colon E_0 \to E_1$ une bijection.

Soit $x_0 \in E_0 \backslash E_1$ (axiome du choix et tout ça). Nous définissons

$$\begin{aligned}\psi\colon \mathbb{N} &\to \{\varphi^k(x_0)\}\\ n &\mapsto \varphi^n(x_0)\end{aligned} \tag{1.212}$$

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

$$x_0 = \varphi^{k-l}(x_0) = \varphi\big(\varphi^{k-l-1}(x_0)\big) \tag{1.213}$$

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 $E_0 \backslash E_1$. Donc en réalité $\varphi^k(x_0) \neq \varphi^l(x_0)$ dès que $k \neq l$. □

Proposition 1.137.
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

$$\begin{aligned} \phi: E &\to (E\backslash A) \cup A' \\ x &\mapsto \begin{cases} x & \text{si } x \in E\backslash A \\ \varphi(x) & \text{si } x \in A \end{cases} \end{aligned} \tag{1.214}$$

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 1.127). Dans ce cas A est en bijection avec un ensemble dénombrable. Il est donc dénombrable.

— Si $\varphi(E)$ est fini, alors le lemme 1.120(2) nous dit que A est fini.

□

Lemme 1.138.
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

$$E = \bigcup_{y \in F} f^{-1}(y). \tag{1.215}$$

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 1.133), ce qui est contraire à l'hypothèse. □

1.5.4 Théorème de Cantor-Schröder-Bernstein

Lemme 1.139 ([27])**.**
Soient un ensemble A et une partie B de A. Si il existe une injection $f: A \to B$ alors il existe une bijection $\alpha: A \to B$.

Nous donnons deux preuves de ce lemme.

Première preuve de 1.139. Nous posons $Y = A\backslash B$ et nous décomposons la preuve en étapes.

(i) **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 $Y = A\backslash B$, nous avons

$$f^k(Y) \cap Y = \varnothing \tag{1.216}$$

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 (1.216) :

$$f^{k+m}(Y) \cap f^m(Y) = \varnothing \tag{1.217}$$

pour tout $k, m \in \mathbb{N}$.

(ii) **Une décomposition** Nous posons

$$X = \bigcup_{k \in \mathbb{N}} f^k(Y) = Y \cup \bigcup_{k=1}^{\infty} f^k(Y). \tag{1.218}$$

Vu que $f(X) \subset B$ nous avons l'égalité

$$B = f(X) \cup \big(B\backslash f(X)\big). \tag{1.219}$$

(iii) $A\backslash X = B\backslash f(X)$ Supposons $x \in A\backslash X$. Vu que $Y = A\backslash B$ est dans X, l'élément x n'est pas dans $A\backslash B$ 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 $B\backslash f(X)$.
Dans l'autre sens, nous supposons que $x \in B\backslash f(X)$. 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 $A\backslash B = f^0(Y)$. Donc x est hors de $f^k(Y)$ pour tout $k \geqslant 0$. Donc x est hors de X.

(iv) **La bijection** Nous considérons l'application

$$\begin{aligned} \alpha\colon A &\to B \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in X \\ x & \text{si } x \in A\backslash X. \end{cases} \end{aligned} \tag{1.220}$$

Nous démontrons dans les points suivants que α est bijective.

(v) **Injective** Nous supposons $\alpha(x) = \alpha(y)$. Il y a 4 possibilités suivant que x et y soient dans X ou $A\backslash X$.
Si $x, y \in X$ alors $f(x) = f(y)$ et donc $x = y$ parce que f est injective.
Si $x \in X$ et $y \in A\backslash X$, alors $f(x) = y$. Mais $f(x) \in f(X)$ et $y \in A\backslash X = B\backslash f(X)$. Donc l'élément $f(x) = y$ est dans $f(X) \cap \big(B\backslash f(X)\big) = \varnothing$. Il n'est donc pas possible d'avoir $\alpha(x) = \alpha(y)$ avec $x \in X$ et $y \in A\backslash X$.
Si $x \in A\backslash X$ et $y \in X$, c'est la même chose.
Si $x, y \in A\backslash X$, alors $x = \alpha(x) = \alpha(y) = y$.

(vi) **Surjective** Soit $y \in B$. Il y a deux possibilités : $y \in X$ et $y \in A\backslash X$. La première se divise en deux : $y \in Y$ et $y \in \bigcup_{k=1}^{\infty} f^k(Y)$. On y va.

(i) $y \in Y$ Ce cas n'est pas possible parce que $y \in B$ alors que $Y = A\backslash B$.

(ii) $y \in f^k(Y)$ **avec** $k \geqslant 1$ Nous avons

$$y \in f\big(f^{k-1}(Y)\big) \subset f(X) \subset \alpha(A). \tag{1.221}$$

(iii) $y \in A\backslash X$ Alors $y = \alpha(y)$.

□

Deuxième preuve de 1.139[12]. Nous posons $Y = A\backslash B$ et

$$\mathcal{M} = \{M \subset A \text{ tel que } Y \cup f(M) \subset M\}. \tag{1.222}$$

Nous allons dire de nombreuses choses à propos de ce $\mathcal{M}$.

(i) $\mathcal{M}$ **est non vide** Nous avons $A \in \mathcal{M}$ parce que Y et $f(A)$ sont dans A.

(ii) **Si** $M \in \mathcal{M}$ **alors** $Y \subset M$ C'est dans la définition de $\mathcal{M}$.

(iii) **Encore un ensemble** Vu que $\mathcal{M}$ est non vide, nous pouvons poser

$$X = \bigcap_{M \in \mathcal{M}} M \tag{1.223}$$

sans nous poser trop de questions. Cela étant fait, nous pouvons passer aux choses sérieuses.

(iv) $f(X) \subset M$ **pour tout** $M \in \mathcal{M}$ Soit $M \in \mathcal{M}$. Nous avons

$$\begin{aligned} f(X) &\subset f(M) && \text{(1.224a)} \\ &\subset Y \cup f(M) && \text{(1.224b)} \\ &\subset M && \text{(1.224c)} \end{aligned}$$

Justifications.

— Pour (1.224a). Parce que $X \subset \mathcal{M}$.

— Pour (1.224c). Parce que $M \in \mathcal{M}$.

(v) $\underline{X \in \mathcal{M}}$ 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

$$f(X) \subset \bigcap_{M\in\mathcal{M}} M = X. \tag{1.225}$$

L'ensemble X est le plus petit élément de $\mathcal{M}$ pour l'inclusion.

(vi) $\underline{Y \cup f(X) \subset X}$ 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.

(vii) $\underline{Y \cup f(X) \in \mathcal{M}}$ Vu que $X \in \mathcal{M}$, nous savons déjà que $Y \cup f(X) \subset X$. En appliquant f des deux côtés,

$$f\big(Y \cup f(X)\big) \subset f(X). \tag{1.226}$$

En ajoutant Y des deux côtés,

$$Y \cup f\big(Y \cup f(X)\big) \subset Y \cup f(X), \tag{1.227}$$

et donc $Y \cup f(X) \in \mathcal{M}$.

(viii) $\underline{Y \cup f(X) = X}$ Nous savons déjà que $Y \cup f(X) \in \mathcal{M}$. Vu que X est le plus petit élément de $\mathcal{M}$, nous avons

$$X \subset Y \cup f(X). \tag{1.228}$$

L'inclusion inverse étant déjà faite, nous avons l'égalité.

(ix) $\underline{B\backslash f(X) = A\backslash X}$ Nous avons :

$$\begin{aligned} A\backslash X &= A\backslash\big(Y \cup f(X)\big) && \text{(1.229a)}\\ &= (A\backslash Y) \cap \big(A\backslash f(X)\big) && \text{(1.229b)}\\ &= B \cap \big(A\backslash f(X)\big) && \text{(1.229c)}\\ &= (B \cap A)\backslash f(X) && \text{(1.229d)}\\ &= B\backslash f(X). && \text{(1.229e)} \end{aligned}$$

Justifications :

— Pour (1.229b). Complémentaire de réunion, lemme 1.25(2).

— Pour (1.229c). Parce que $A\backslash Y = B$ du fait que $Y = A\backslash B$.

— Pour (1.229d). Lemme 1.25(3).

— Pour (1.229e). Parce que $B \subset A$.

(x) **Notre bijection** Nous voulons définir

$$\begin{aligned} \alpha\colon A &\to B \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in X \\ x & \text{si } x \in A\backslash X. \end{cases} \end{aligned} \tag{1.230}$$

Pour y parvenir, nous devons prouver que α prend effectivement ses valeurs dans B. Ensuite nous prouverons que α est une bijection.

(xi) $\underline{\alpha \textbf{ prend ses valeurs dans } B}$ Si $x \in X$ nous avons $\alpha(x) = f(x) \in B$. Si au contraire $x \in A\backslash X$ nous avons

$$\alpha(x) = x \in A\backslash X = B\backslash f(X) \subset B. \tag{1.231}$$

(xii) $\underline{\alpha \textbf{ est injective}}$ 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 $A\backslash X$.

(i) $x \in X$, $y \in X$ Alors $f(x) = \alpha(x) = \alpha(y) = f(y)$. Vu que f est injective, nous trouvons que $x = y$.

(ii) $x \in X$, $y \in A\backslash X$ Nous avons $\alpha(x) = f(x) \in f(X)$ et $\alpha(y) = y \in A\backslash X = B\backslash f(X)$. Il n'est donc pas possible d'avoir $\alpha(x) = \alpha(y)$ dans ce cas.

(iii) $x \in A\backslash X$, $y \in X$ Idem.

(iv) $x \in A\backslash X$, $y \in A\backslash X$ Dans ce cas nous avons $\alpha(x) = x$ et $\alpha(y) = y$. Donc $x = y$.

(xiii) α **est surjective** Soit $b \in B$. Il y a deux possibilités : $b \in f(X)$ ou $b \notin f(X)$.

(i) **Si** $b \in f(X)$ Soit $x \in X$ tel que $f(x) = b$. Alors $\alpha(x) = f(x) = b$.

(ii) **Si** $b \notin f(X)$ Alors $b \in B\backslash f(X) = A\backslash X$, et donc $\alpha(b) = b$.

□

Théorème 1.140 (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 1.139 donne alors une bijection $\varphi\colon A \to g(B)$.

Nous montrons que $g^{-1} \circ \varphi\colon A \to B$ est une bijection.

(i) **Injective** Nous supposons $x, y \in A$ tels que

$$g^{-1}\big(\varphi(x)\big) = g^{-1}\big(\varphi(y)\big). \tag{1.232}$$

Nous appliquons g des deux côtés : $\varphi(x) = \varphi(y)$. Puisque φ est une bijection, cela entraîne $x = y$.

(ii) **Surjective** Soit $b \in B$. En posant $a = \varphi^{-1}\big(g(b)\big)$ nous avons bien $(g^{-1} \circ \varphi)(a) = b$.

□

1.5.5 Comparabilité cardinale

Le théorème de comparabilité cardinale énonce que si A et B sont des ensemble, alors nous avons toujours $A \succeq B$ ou $A \preceq B$ (ou les deux ; dans ce cas $A \approx B$ par Cantor-Schröder-Bernstein).

Théorème 1.141 (Théorème de comparabilité cardinale[1, 28, 29])**.**
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 1.22 à l'ensemble [52]

$$\mathcal{A} = \left\{ (X, Y, \varphi) \text{ tel que } \begin{cases} X \subset A \\ Y \subset B \\ \varphi\colon X \to Y \text{ est injective.} \end{cases} \right\} \tag{1.233}$$

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 $\varphi(X) \neq B$.

(i) **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 1.111 conclut que B est subpotent à A.

52. 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.

(ii) **Si $\varphi(X) \neq B$** Nous subdivisons en deux nouveaux cas : soit $X = A$, soit $X \neq A$.

(i) **Si $X = A$** Alors nous avons une injection $\varphi: A \to B$, et c'est bon.

(ii) **Si $X \neq A$** Nous sommes dans le cas $X \neq A$ et $\varphi(X) \neq B$. Soient $a \in A \backslash X$ et $b \in B \backslash \varphi(X)$. Nous considérons l'application

$$\begin{aligned} \psi: X \cup \{a\} &\to Y \cup \{b\} \\ x &\mapsto \begin{cases} \varphi(x) & \text{si } x \in X \\ b & \text{si } x = a. \end{cases} \end{aligned} \tag{1.234}$$

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.

□

1.142.
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 [53]. 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.

1.5.6 Théorème de Cantor, ensemble des ensembles

Théorème 1.143 (Cantor[30])**.**
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 $f: E \to \mathcal{P}(E)$. Nous posons

$$D = \{x \in E \text{ tel que } x \notin f(x)\}. \tag{1.235}$$

Nous prouvons que D ne peut pas être dans l'image de f. Supposons que $y \in E$ soit tel que $f(y) = D$.

(i) **Si $y \in D$** Alors par définition de D, nous avons $y \notin f(y) = D$. Contradiction.

(ii) **Si $y \notin D$** Alors $y \in f(y) = D$, contradiction.

Donc aucune surjection $f: E \to \mathcal{P}(E)$ n'existe. En particulier pas de bijections.

Par ailleurs, l'application $g: \mathcal{P}(E) \to E$ 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. □

1.144.
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 ».

Corolaire 1.145.
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 1.143. □

53. Corolaire 1.145.

1.5.7 Ajouter ou soustraire des cardinalités

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 ».

Lemme 1.146 ([1]).
Si A est infini et B est fini, alors $A \cup B \approx A$.

Démonstration. Nous supposons que A et B sont disjoints[54]. La proposition 1.121 nous permet de considérer une bijection $\psi\colon \{1,\dots,n\} \to B$.

Puisque A est infini, la proposition 1.136 nous permet de considérer $N \subset A$ et une bijection $\varphi\colon \mathbb{N} \to N$.

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

$$\begin{aligned} f\colon A \cup B &\to A \\ x &\mapsto \begin{cases} x & \text{si } x \in A\backslash N \\ \varphi\big(\varphi^{-1}(x)+n\big) & \text{si } x \in N \\ \varphi\big(\psi^{-1}(x)\big) & \text{si } x \in B. \end{cases} \end{aligned} \tag{1.236}$$

□

Lemme 1.147.
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 1.140 nous indique que trouver une injection $A \cup B \to A$ suffira pour la peine.

Nous allons utiliser le lemme de Zorn 1.22 avec l'ensemble

$$\mathcal{A} = \left\{ (X,\varphi_X) \text{ tel que } \begin{cases} X \subset B \\ \varphi_X\colon A \cup X \to A \text{ est injective.} \end{cases} \right\} \tag{1.237}$$

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 $x \in A \cup X$.

(i) **$\mathcal{A}$ 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 $\mathcal{F}$.

(ii) **Un maximum** Le lemme de Zorn nous assure que $\mathcal{A}$ possède (au moins) un élément maximal. Soit un tel élément maximum (X,φ).

(iii) **$X \approx B$** 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

$$b \in B\backslash X \tag{1.238a}$$
$$a \in A\backslash\varphi(X). \tag{1.238b}$$

Nous considérons alors l'élément $(Y,\psi) \in \mathcal{A}$ défini par

$$Y = X \cup \{b\} \tag{1.239a}$$
$$\psi(x) = \begin{cases} a & \text{si } x = b \\ \varphi(x) & \text{sinon .} \end{cases} \tag{1.239b}$$

Cet élément majore (X,φ).

Donc $X \approx B$.

54. Adaptez la démonstration au cas où l'intersection n'est pas vide.

(iv) **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 $\psi\colon B \to X$.

(v) **Conclusion si A est disjoint de B** Si A et B sont disjoints, nous avons une bijection

$$\begin{aligned} l\colon A \cup B &\to A \\ x &\mapsto \begin{cases} \varphi(x) & \text{si } x \in A \\ \varphi\big(\psi(x)\big) & \text{si } x \in B. \end{cases} \end{aligned} \tag{1.240}$$

(vi) **Conclusion si A n'est pas disjoint de B** Il suffit de poser $C = B\backslash A$ et nous avons

$$A \cup B = [A \cup (A \cap B)] \cup C. \tag{1.241}$$

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.

□

La proposition suivante sera utilisée en théorie de la mesure, dans l'exemple 14.70.

Proposition 1.148 ([31, 12])**.**
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 1.146. Mais A est idempotent à S, donc

$$S \approx A \approx A \cup B = \{0,1\} \times S. \tag{1.242}$$

□

Corolaire 1.149.
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 1.148 donne une bijection $\varphi\colon \{1,2\} \times A \to A$. Il suffit de poser $A_1 = \varphi(1, A)$ et $A_2 = \varphi(2, A)$. □

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. C'est en substance ce que signifie la proposition suivante.

Proposition 1.150.
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.

(i) **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 $i \neq j$

(ii) **La construction** Nous commençons à zéro en utilisant le corolaire 1.149 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 1.149 qui fait le travail.

(iii) **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

$$A_j \subset B_{j-1} \subset B_{j-2} \subset \ldots \subset B_i. \tag{1.243}$$

Donc $A_j \cap A_i \subset B_i \cap A_i = \varnothing$.

(iv) **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

$$\begin{aligned} \varphi \colon A \times \mathbb{N} &\to A \\ (a, k) &\mapsto \psi_k(a). \end{aligned} \tag{1.244}$$

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 $A \times \mathbb{N} \preceq A$.

(v) **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 1.140 conclut que $A \times \mathbb{N} \approx A$.

□

Lemme 1.151 ([1])**.**
Sois un ensemble A muni de deux sous-ensembles B et B' équipotents et disjoints. Alors $A\backslash B$ est équipotent à $A\backslash B'$.

Démonstration. Soit une bijection $\psi \colon B' \to B$. L'application

$$\begin{aligned} \varphi \colon A\backslash B &\to A\backslash B' \\ x &\mapsto \begin{cases} x & \text{si } x \notin B' \\ \psi(x) & \text{si } x \in B'. \end{cases} \end{aligned} \tag{1.245}$$

est la bijection cherchée. □

Lemme 1.152 ([32])**.**
Si A est un ensemble infini et si $B \prec A$, alors $A \approx A\backslash B$.

Démonstration. Nous pouvons écrire

$$A = (A\backslash B) \cup B. \tag{1.246}$$

Le théorème de comparabilité cardinale 1.141 nous indique que soit $A\backslash B \preceq B$, soit $A\backslash B \succeq B$. Nous allons étudier les deux cas.

(i) **Si $A\backslash B \succeq B$** Dans ce cas, $(A\backslash B) \cup B \approx A\backslash B$ par le lemme 1.147. Alors, notre résultat est prouvé parce que $A = (A\backslash B) \cup B \approx A\backslash B$.

(ii) **Si $A\backslash B \preceq B$** Dans ce cas, le lemme 1.147 nous indique que $A = (A\backslash B) \cup B \approx B$. Mais $A \approx B$ est exclu par l'hypothèse. Ce cas est donc impossible.

□

Lemme 1.153 ([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 1.152 nous donne une bijection $\varphi\colon A \to A\backslash B$. Il suffit alors de poser $U = \varphi(B)$. Cette partie est disjointe de B parce que φ prend ses valeurs dans $A\backslash B$. □

Lemme 1.154 ([33]).
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 $B \leq B \times B \leq B \leq A$.

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. □

Lemme 1.155 ([33]).
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 1.153, nous considérons une partie $U \subset A$ disjointe de B et équipotente à B. Nous pouvons écrire le développement

$$(B \cup U) \times (B \cup U) = (B \times B) \cup (B \times U) \cup (U \times B) \cup (U \times U). \tag{1.247}$$

Nous savons que B est surpotent à U (il est même équipotent) ; donc le lemme 1.147 nous dit que $B \cup U \approx B$. De plus il existe une bijection $B \to U$, donc

$$U \approx B \approx B \times B \approx B \times U \approx U \times B \approx U \times U. \tag{1.248}$$

Chacun des ensembles $U \times B$, $B \times U$ et $U \times U$ est équipotent à U. Leur union est donc équipotente [55] à U et nous avons une bijection

$$\varphi\colon U \to U \times B \cup (B \times U) \cup (U \times U). \tag{1.249}$$

Et enfin nous définissons

$$\begin{aligned} g\colon B \cup U &\to (B \times U) \times (B \cup U) \\ x &\mapsto \begin{cases} f(x) & \text{si } x \in B \\ \varphi(x) & \text{si } x \in U. \end{cases} \end{aligned} \tag{1.250}$$

Cette définition est bonne parce que U et B sont disjoints, et g est injective. □

Le théorème suivant est une généralisation de la proposition 1.148. 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 1.130 qui donne une bijection explicite et donc sans axiome du choix et sans lemme de Zorn.

Théorème 1.156.
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

$$\mathcal{A} = \left\{ (X, \varphi) \text{ tel que } \begin{cases} X \subset A \\ \varphi\colon X \to X \times X \text{ est surjective.} \end{cases} \right\} \tag{1.251}$$

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 1.130.

55. Lemme 1.147.

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 1.22 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 1.155 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 1.140 nous donne une bijection $\phi\colon B\times B\to B$. Avec ça, l'application

$$\begin{aligned} f\colon A\times A&\to A\\ (a,b)&\mapsto \phi\big(g(a),g(b)\big) \end{aligned} \tag{1.252}$$

est une bijection. Donc les ensembles A et $A\times A$ sont équipotents. □

Lemme 1.157.
Si A est infini, et si pour tout $i\in\mathbb{N}$ nous avons $A_i\approx A$, alors

$$\bigcup_{i\in\mathbb{N}}A_i\approx A. \tag{1.253}$$

Démonstration. Pour chaque $i\in\mathbb{N}$ nous avons une bijection $\varphi_i\colon A_i\to A$. Nous posons

$$\begin{aligned} \varphi\colon A\times\mathbb{N}&\to\bigcup_{i=0}^{\infty}A_i\\ (a,i)&\mapsto\varphi_i(a). \end{aligned} \tag{1.254}$$

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

$$A\approx A\times\mathbb{N} \tag{1.255a}$$
$$\geq\bigcup_{i=0}^{\infty}A_i \tag{1.255b}$$
$$\geq A \tag{1.255c}$$

Justifications :

— Pour (1.255a), c'est la proposition 1.150.
— Pour (1.255b), c'est la surjection (1.254).
— Pour (1.255c), 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 1.140. □

1.6 Groupes

1.6.1 Définition, unicité du neutre

La définition d'un groupe est la définition 1.35.

Lemme-Définition 1.158 (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 $g \in G$,

(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 $k_1 = k_2$.

□

Lemme 1.159.
Soient deux groupes G et H. Si $\alpha : G \to H$ est un morphisme de groupes[56]*, alors*

(1) $\alpha(e_G) = e_H$.

(2) $\alpha(g^{-1}) = \alpha(g)^{-1}$.

Lemme-Définition 1.160.
Soit un groupe G. L'ensemble des automorphismes de G, noté $\mathrm{Aut}(G)$, est un groupe pour la composition.

Lemme 1.161.
Si G est un groupe et si $h \in G$, alors les applications

$$\begin{aligned} L_h : G &\to G \\ g &\mapsto hg \end{aligned} \tag{1.256}$$

et

$$\begin{aligned} R_h : G &\to G \\ g &\mapsto gh \end{aligned} \tag{1.257}$$

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. □

1.6.2 Groupe ordonné

Définition 1.162 ([34])**.**
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.

56. Définition 1.36.

1.6.3 Classes de conjugaison

Définition 1.163 (classe de conjugaison)**.**
*Soit un groupe G et un élément $g \in G$. La **classe de conjugaison** de g est la partie*

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\}. \tag{1.258}$$

Lemme 1.164.
Un groupe est commutatif si et seulement si ses classes de conjugaison sont des singletons.

Démonstration. Supposons que G soit commutatif. Alors

$$C_g = \{kgk^{-1} \text{ tel que } k \in G\} = \{g\}. \tag{1.259}$$

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. □

Définition 1.165 (centralisateur[35])**.**
*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 :*

$$Z_G(h) = \{z \in G \text{ tel que } hz = zh\}. \tag{1.260}$$

Le centralisateur de H dans G est l'ensemble des éléments de G qui commutent avec tous les éléments de H :

$$Z_G(H) = \bigcap_{h \in H} Z_G(h). \tag{1.261}$$

*Le **centre** d'un groupe G est l'ensemble des éléments de G qui commutent avec tous les autres :*

$$Z_G = Z_G(G) = \{z \in G \text{ tel que } gz = zg, \forall g \in G\}. \tag{1.262}$$

Définition 1.166 (normalisateur[35])**.**
*Soient un groupe G et un sous-groupe H. Le **normalisateur** de H dans G est*

$$\mathcal{N}_G(H) = \{g \in G \text{ tel que } gH = Hg\}. \tag{1.263}$$

Définition 1.167 (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 $N \lhd G$.

Définition 1.168.
*Un sous-groupe H de G est un sous-groupe **caractéristique** si $\alpha(H) \subset H$ pour tout automorphisme[57] α de G.*

Lemme 1.169 ([36])**.**
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 :

$$h = \alpha\big(\alpha^{-1}(h)\big) \in \alpha\big(\alpha^{-1}(H)\big) \subset \alpha(H). \tag{1.264}$$

□

Définition 1.170 (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.*

57. Automorphisme de groupe, définition 1.36.

1.7 Anneaux

Définition 1.171.
*Un **isomorphisme d'anneaux** est un morphisme d'anneaux*[58]*, bijectif.*

La distributivité de la partie (3) de la définition 1.39 ne traite que de l'addition ; pas de la soustraction. Voici une lemme qui dit que ça fonctionne quand même.

Lemme 1.172 ([12])**.**
Soient un anneau A ainsi que $a, b, c \in A$. Alors

$$a(b-c) = ab - ac. \tag{1.265}$$

Démonstration. Nous avons le calcul suivant :

$$a(b-c) + ac = a\big((b-c)+c\big) \tag{1.266a}$$
$$= ab. \tag{1.266b}$$

Justifications :

— Pour 1.266a. Distributivité.

— Pour 1.266b. 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. □

Lemme 1.173.
Pour tout élément a d'un anneau nous avons $a \cdot 0 = 0$.

Démonstration. L'élément 0 est le neutre de l'addition. Il peut être écrit $1-1$, et en utilisant la distributivité sous la forme du lemme 1.172,

$$a \cdot 0 = a \cdot (1-1) = a - a = 0. \tag{1.267}$$

Notons que la dernière égalité s'écrit en détail $a-a = a+(-a)$ qui donne le neutre de l'addition. □

Proposition 1.174.
Dans un anneau[59] *non nul, le neutre pour l'addition est distinct du neutre pour la multiplication.*

Démonstration. Supposons par contraposée que dans un anneau A, $1 = 0$. Alors, pour tout $a \in A$, on a $a = 1a = 0a = (1-1)a = a - a = 0$, d'où l'on déduit $-a = 0$ et par suite, $a = 0$. □

Lemme 1.175 ([1])**.**
Un peu d'arithmétique. Soit un anneau A et un élément $a \in A$.

(1) $1 \times 1 = 1$.

(2) $(-1) \times a = -a$.

(3) $-(-a) = a$.

(4) $(-1) \times (-1) = 1$.

Démonstration. En plusieurs parties.

(i) **Pour (1)** La définition de 1 est que $1 \times a = a$ pour tout a. En particulier pour $a = 1$ nous avons le résultat.

(ii) **Pour (2)** Nous avons

$$(-1) \times a + a = a \times \big((-1)+1\big) = a \times 0 = 0. \tag{1.268}$$

Nous avons utilisé le fait que la multiplication était distributive et que le zéro était absorbant (lemme 1.173).

58. Définition 1.40.
59. Définition 1.39.

(iii) **Pour (3)** Nous avons $-a+a=0$ par définition de la notation $-a$. Donc a est bien l'inverse de $-a$ pour l'addition.

(iv) **Pour (4)** En utilisant les points (2) et (3) nous avons

$$(-1)\times(-1)=-(-1)=1. \tag{1.269}$$

□

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

$$(f+g)(x)=f(x)+g(x) \tag{1.270a}$$
$$(fg)(x)=f(x)g(x). \tag{1.270b}$$

C'est la **structure canonique** d'anneau sur $\mathrm{Fun}(X,A)$.

Définition 1.176.
*Le **centralisateur** de $x\in A$ dans A est l'ensemble*

$$\{y\in A \text{ tel que } xy=yx\}, \tag{1.271}$$

*le **centre** de A est*

$$\{y\in A \text{ tel que } xy=yx, \forall x\in A\}. \tag{1.272}$$

Définition 1.177 (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.*

Lemme 1.178.
Les seuls idéaux d'un corps sont $\{0\}$ et le corps lui-même.

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 $x=x\cdot 1\in xI\subset I$. □

Proposition-Définition 1.179.
Soit A, un anneau, I un idéal bilatère[60] de A. Nous considérons la relation d'équivalence $x\sim y$ si et seulement si $x-y\in I$. Sur le quotient[61]

$$A/\sim = A/I, \tag{1.273}$$

nous mettons les opérations

(1) $[x]+[y]=[x+y]$

(2) $[x][y]=[xy]$.

Nous avons alors les résultats suivants :

(1) Les opérations sont bien définies,

60. Définition 1.177.
61. Définition 1.31.

(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 $-[a]$.

(3) la surjection canonique $\pi\colon A\to A/I$ est un morphisme.

Cet anneau est appelé ***anneau quotient****.*

Démonstration. En plusieurs parties.

(i) **Pour (1)** Nous savons que, par définition,

$$\bar{x}=\{x+i \text{ tel que } i\in I\}. \tag{1.274}$$

Calculons le produit de représentants génériques de $\bar{x}$ et de $\bar{y}$:

$$(x+i_1)(y+i_2)=xy+xi_2+yi_1+i_1i_2. \tag{1.275}$$

Puisque I est un idéal, nous avons $xi_2+yi_1+i_1i_2\in I$ et donc bien

$$(x+i_1)(y+i_2)\in\overline{xy}. \tag{1.276}$$

(ii) **Pour (2)** Il s'agit de vérifier les conditions de la définition 1.39.
D'abord A/I est un groupe de neutre $[0]$. En effet, vu que $(A,+)$ est un groupe commutatif de neutre 0, nous avons

(1) Neutre : $[a]+[0]=[a+0]=[a]$.
(2) Associativité : $[a]+([b]+[c])=[a]+[b+c]=[a+b+c]=[a+b]+[c]$.
(3) 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 :

$$[a]+[b]=[a+b]=[b+a]=[b]+[a]. \tag{1.277}$$

Donc $(A/I,+)$ est un groupe commutatif de neutre $[0]$.
L'associativité de A donne l'associativité dans A/I :

$$\big([a][b]\big)[c]=[ab][c]=[abc]=[a][bc]=[a]\big([b][c]\big). \tag{1.278}$$

Et enfin pour la distributivité,

$$[a]\big([b]+[c]\big)=[a][b+c]=[a(b+c)]=[ab+ac]=[ab]+[ac]=[a][b]+[a][c]. \tag{1.279}$$

Nous avons prouvé que A/I est un anneau de neutre $[0]$ et d'unité $[1]$.

(iii) **Pour (3)** Nous devons vérifier les trois conditions de la définition 1.40. Cela est immédiat parce que $\pi(x)=[x]$.

□

Définition 1.180.
Soient A un anneau commutatif et $S\subset A$. Nous disons que $\delta\in A$ est un ***PGCD*** *de S si*

(1) δ divise tous les éléments de S.

(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 6.53.

Remarque 1.181.
Au sens de la définition 1.180, 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 à ce que l'unique pgcd soit effectivement le plus grand pour l'ordre usuel sur $\mathbb{Z}$.

Pour l'unicité dans $\mathbb{Z}$, voir 3.19.

1.7.1 Élément irréductible et premier

Définition 1.182 ([37]).
*Soit un anneau commutatif A. Un élément $p \in A$ est **premier** si il est*

(1) non nul,

(2) non inversible,

(3) si p divise un produit ab, alors il divise soit a soit b (ou le deux).

Définition 1.183 (Élément irréductible[38]).
*Un élément d'un anneau commutatif est **irréductible** si il n'est ni inversible, ni le produit de deux éléments non inversibles.*

1.184.
Nous allons voir dans la section 3.6 que le concept d'élément irréductible n'est vraiment utile que dans le cas des anneaux intègres.

Exemple 1.185.
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 : $0 = 0 \cdot 0$. △

Lemme 1.186 ([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. □

Proposition 1.187.
Les éléments irréductibles de l'anneau $\mathbb{Z}$ sont les nombres premiers[62].

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. □

1.7.2 Anneau intègre

Définition 1.188 (Diviseurs dans un anneau).
*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 $c \in A$.*

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 étudions ces anneaux plus en détail en section 1.10.

Un élément $a \in A$ est **régulier à droite** si $ba = 0$ implique $b = 0$. Il est régulier à gauche si $ab = 0$ implique $b = 0$.

Définition 1.189 (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 $n \in \mathbb{N}$.*

62. Nombre premier, définition 1.182.

Définition 1.190 (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 $A^* = A\backslash\{0\}$.

Conformément à la définition 1.188 de diviseur, nous posons la définition suivante pour les diviseurs de zéro.

Définition 1.191 (diviseur de zéro[39])**.**
*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.*

Proposition-Définition 1.192 (Anneau intègre[1])**.**
Soit A un anneau non réduit à $\{0\}$. Les assertions suivantes sont équivalentes :

(1) A ne possède pas de diviseurs de zéro[63]*.*

(2) La règle du produit nul s'applique dans A : pour tous $a, b \in A$, si $ab = 0$, alors $a = 0$ ou $b = 0$.

(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.

(i) **(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.

(ii) **(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 $b - c = 0$.

(iii) **(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.

□

Lemme 1.193.
Un corps est un anneau intègre[64]*.*

Démonstration. Nous vérifions la définition 1.192, et nous nommons $\mathbb{K}$ le corps considéré.

(i) **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.

(ii) **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.

(iii) **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.

Proposition 1.194 ([40])**.**
Soit un anneau unitaire et intègre A. Soit $p \in A$.

(1) p est premier si et seulement si l'idéal pA est premier.

63. Définition 1.191.
64. Définition 1.192.

(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.

(i) **(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[65], 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

$$a = pk \in pA. \tag{1.280}$$

De même si $p \mid b$ nous avons $b \in pA$.

(ii) **(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 $b \mid p$.

(iii) **(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 $I = pA$.

(iv) **(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 $1 \in A = aA$.

□

Lemme 1.195 ([1]).
Soient un anneau intègre A, et une partie $S \subset A$. Si un des pgcd *de S est inversible*[66]*, alors ils le sont tous.*

Démonstration. Pour rappel, les pgcd d'une partie de A sont définis dans 1.180. 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 $\delta : \delta \mid \delta'$. Réciproquement, $\delta' \mid \delta$.

Soient x et y définis par $\delta = x\delta'$ et $\delta' = y\delta$. Nous avons

$$\delta = x\delta' = xy\delta. \tag{1.281}$$

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. □

Lemme 1.196 ([1, 41]).
Soient un anneau intègre, A, une partie $S \subset A$ et un élément $a \in A$. Nous avons[67]

$$\operatorname{pgcd}(aS) = a \operatorname{pgcd}(S). \tag{1.282}$$

Démonstration. Deux inclusions à prouver.

65. Définition 1.182.
66. Définition 1.190.
67. Définition du pgcd : 1.180.

(i) $\underline{\text{pgcd}(aS) \subset a\,\text{pgcd}(S)}$ Soit un pgcd δ de aS. Nous devons trouver un $\delta' \in \text{pgcd}(S)$ 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

$$\delta x_i = as_i. \tag{1.283}$$

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 $\delta' \in \text{pgcd}(S)$.

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 1.192(3)) :

$$\delta' x_i = s_i. \tag{1.284}$$

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

$$ady = \delta. \tag{1.285}$$

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'.

(ii) $\underline{a\,\text{pgcd}(S) \subset \text{pgcd}(aS)}$ Soit un pgcd δ de S. Nous voulons que $a\delta \in \text{pgcd}(aS)$. Vu que $\delta \in \text{pgcd}(S)$ 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 $d \mid a\delta$.

(i) **Travail préliminaire** Nous considérons $\delta' \in \text{pgcd}(aS)$. 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

$$a\delta \mid \delta'. \tag{1.286}$$

Soit $u \in A$ tel que $\delta' = a\delta u$.

En utilisant la première partie de la preuve, nous avons

$$\delta' \in \text{pgcd}(aS) \subset a\,\text{pgcd}(S). \tag{1.287}$$

Donc il existe $\delta_1 \in \text{pgcd}(S)$ tel que $\delta' = a\delta_1$. En écrivant l'égalité $\delta' = a\delta u$ avec cette valeur de δ', nous trouvons

$$a\delta_1 = a\delta u, \tag{1.288}$$

et donc $\delta_1 = \delta u$ parce que A est intègre. Vu que $\delta_1 \in \text{pgcd}(S)$, nous avons aussi $\delta u \in \text{pgcd}(S)$. 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,

$$\delta' = a\delta u \mid a\delta. \tag{1.289}$$

(ii) **Résumé** Nous avons considéré $\delta \in \text{pgcd}(S)$ et nous sommes en train de prouver que $a\delta \in \text{pgcd}(aS)$. Nous avons déjà prouvé que si $\delta' \in \text{pgcd}(aS)$, alors nous avons $\delta' \mid a\delta$.

Nous posons $y \in A$ tel que $\delta' y = a\delta$.

(iii) **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,

$$dxy = \delta' y = a\delta. \tag{1.290}$$

Nous avons montré que d divise $a\delta$, ce qu'il nous fallait.

□

¡¡ Avertissement/question à la lectrice !! 1.197

Je ne suis pas certain du lemme 1.198. Essayez de le démontrer, et envoyez-moi la preuve pour que je puisse l'ajouter.

Lemme 1.198 ([1]).
Soient un anneau intègre A et une partie $S \subset A$. Si $\delta \in \text{pgcd}(S)$, alors $\text{pgcd}(S/\delta)$ ne contient que des inversibles.

Lemme 1.199 ([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

$$dxu = \delta u, \tag{1.291}$$

de telle sorte que d divise δu. □

1.7.3 Fonction puissance

Voici une première définition de la fonction puissance. Il y en aura d'autres, de plus en plus générales. Voir le thème 51.

Définition 1.200.
Si A est un anneau, si $a \in A$ et si $n \in \mathbb{N}$, nous définissons a^n par récurrence :

(1) $a^0 = 1$ *(l'unité pour la multiplication dans A),*

(2) $a^{k+1} = a \cdot a^k$.

Le lemme suivant dit que le point (2) de la définition 1.200 aurait pu être écrit $a^k \cdot a$ au lieu de $a \cdot a^k$.

Lemme 1.201 ([1]).
Si A est un anneau, si $a \in A$ et si $n \in \mathbb{N}$, alors

$$a^n = a \cdot a^{n-1} = a^{n-1} \cdot a. \tag{1.292}$$

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 $n + 1$:

$$\begin{aligned}
a^{n+1} &= aa^n && \text{Définition de } a^{n+1} && (1.293a)\\
&= a(a^{n-1}a) && \text{hypothèse de récurrence pour } a^n && (1.293b)\\
&= (aa^{n-1})a && \text{associativité} && (1.293c)\\
&= a^n a && \text{Définition de } a^n. && (1.293d)
\end{aligned}$$

□

1.8 Idéal dans un anneau

La définition d'un idéal dans un anneau est la définition 1.177.

Définition 1.202 ([42]).
*Un **corps** est un anneau*[68] *$(A, +, \times)$ 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).*

1.203.
Dans le Frido, nous ne parlons que de corps commutatifs ; nous ne le répéterons pas toujours.

1.204.
Pour savoir ce qu'est un « *ring* » ou « *field* » en anglais, voir -2.3.

68. Définition 1.39.

Définition 1.205 (Idéal engendré par un élément)**.**
*Si p est un élément d'un anneau A alors nous notons (p) l'idéal dans A **engendré** par p, c'est-à-dire pA.*

Définition 1.206.
*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 1.207.
Un idéal n'est pas toujours un anneau parce que l'identité pourrait manquer. Un idéal qui contient l'identité est l'anneau complet.

Lemme 1.208.
L'ensemble $2\mathbb{Z}$ est un idéal[69] *de $\mathbb{Z}$. On peut aussi le noter (2).*

Proposition 1.209 (Premier théorème d'isomorphisme pour les anneaux)**.**
Soient A et B des anneaux et un homomorphisme $f\colon A \to B$. 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

$$\tilde{f}\colon A/\ker f \to f(A) \tag{1.294}$$

tel que $f = j \circ \tilde{f} \circ \phi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\phi}\downarrow & & \uparrow{\scriptstyle j} \\ A/\ker f & \xrightarrow[\tilde{f}]{} & f(A) \subset B \end{array} \tag{1.295}$$

Proposition 1.210.
Soient I un idéal de A et la projection canonique

$$\phi\colon A \to A/I. \tag{1.296}$$

C'est une bijection entre les idéaux de A contenant I et les idéaux de A/I.
Dit de façon imagée :

$$\{\text{idéaux de } A \text{ contenant } I\} \simeq \{\text{idéaux de } A/I\}. \tag{1.297}$$

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

$$\phi(i)\phi(j) = \phi(ij) \in \phi(J). \tag{1.298}$$

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 $I \subset \phi^{-1}(K)$. □

Proposition 1.211 ([1])**.**
Si A est un anneau, nous avons les équivalences

(1) A est un corps[70]*.*

(2) A est non nul et ses seuls[71] *idéaux à gauche sont $\{0\}$ et A.*

69. Idéal, définition 1.177.
70. Définition 1.202.
71. Je vous laisse vous poser de grandes questions sur le fait que le vide est un idéal ou non.

(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.

(i) **(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 $I = A$.

(ii) **(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.

(iii) **(1) implique (3)** Comme pour (1) implique (2).

(iv) **(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. □

Définition 1.212 ([43]).
*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.*

Proposition 1.213 (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 1.210 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 1.211.

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. □

Théorème 1.214 (Théorème de Krull[44]).
Pour tout idéal propre I d'un anneau commutatif A, il existe au moins un idéal maximal de A contenant I.

1.8.1 Division euclidienne

Théorème-Définition 1.215 (Division euclidienne[45]).
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

$$a = bq + r. \tag{1.299}$$

*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.

(i) **Unicité** Nous supposons avoir $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que

$$\begin{cases} 0 \leqslant r < b & \text{(1.300a)} \\ a = qb + r. & \text{(1.300b)} \end{cases}$$

Ce système implique que

$$0 \leqslant a - qb < b. \tag{1.301}$$

En ajoutant qb dans les trois membres de cette inégalité,

$$qb \leqslant a < (q + 1)b. \tag{1.302}$$

Cela implique que

$$q = \max\{k \in \mathbb{Z} \text{ tel que } kb \leqslant a\}. \tag{1.303}$$

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 1.107. Ce maximum vérifie

$$bq \leqslant a < b(q+1). \tag{1.304}$$

Cela donne $0 \leqslant a - bq < b$ et le résultat, en posant $r = a - qb$.

□

Le lemme suivant est souvent pris pour la définition d'un nombre premier lorsqu'on parle de $\mathbb{N}$ ou $\mathbb{Z}$.

Lemme 1.216 ([46, 1])**.**
Dans $\mathbb{N}$, un nombre est premier si et seulement si il admet exactement deux diviseurs entiers distincts.

Démonstration. En deux parties.

(i) $\Rightarrow$ 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

$$1 = nl, \tag{1.305}$$

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.

(ii) $\Leftarrow$ Nous supposons que $p \in \mathbb{N}$ ait exactement deux diviseurs entiers distincts. Nous vérifions que p vérifie les trois conditions de la définition 1.182.

(1) $p \neq 0$ parce que 0 a nettement plus que deux diviseurs distincts.

(2) $p \neq 1$ parce que 1 a exactement un diviseur. Donc p n'est pas inversible dans $\mathbb{N}$.

(3) 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'.

(i) **Un ensemble** Pour cela nous posons

$$E = \{x \in \mathbb{N} \text{ tel que } p \mid ax, p \nmid x\}. \tag{1.306}$$

Nous posons $b = \min(E)$. Nous avons pour hypothèse que E est non vide ; en particulier $0 < b$.

(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 $b < p$.

(iii) **Division euclidienne** Nous effectuons la division euclidienne du théorème 1.215 :

$$p = mb + r. \tag{1.307}$$

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.

(iv) **La contradiction** Nous avons donc $r \in E$, alors que $r < b$. Impossible.

□

Proposition 1.217 ([47]).
Dans un anneau intègre[72] *tout élément premier est irréductible*[73].

Démonstration. Soit p, un élément premier dans un anneau intègre A.

(i) **p n'est pas inversible** Cela fait partie de la définition d'un élément premier.

(ii) **p n'est pas un produit d'inversibles** Soient $a, b \in A$ tels que $p = ab$. Par le point (3) de la définition 1.182, 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 :

$$p = pxb. \tag{1.308}$$

Mais l'anneau est intègre et permet donc des simplifications par tout élément non nul. La relation 1.308 donne donc

$$1 = xb, \tag{1.309}$$

ce qui signifie que b est inversible.

Un travail similaire montre que a est inversible si p divise b.

□

Exemple 1.218.
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 1.217 devient fausse.

Exemple 1.219.
Soit l'anneau $\mathbb{Z}^2$. L'élément $(1,0)$ est premier mais pas irréductible.

(i) **$(1,0)$ 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.

(ii) **$(1,0)$ 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.

△

1.9 Anneau principal et idéal premier

Définition 1.220.
Un idéal[74] *I dans A est **principal à gauche** si il existe $a \in I$ tel que $I = Aa$. Il est **principal à droite** si il existe $a \in I$ tel que $I = aA$. Nous disons qu'il est **principal** si il est principal à gauche et à droite.*

Définition 1.221.
*Un anneau est **principal** si*

(1) il est commutatif et intègre

72. Si pas intègre, voir l'exemple 1.219.
73. Toutes les définitions dans le thème 6.
74. Idéal, définition 1.177.

(2) tous ses idéaux sont principaux[75].

Souvent pour prouver qu'un anneau est principal, nous prouvons qu'il est euclidien (définition 1.244) et nous utilisons la proposition 1.247 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 3.75.

Définition 1.222.
*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 $b \in I$.*

Lemme 1.223.
L'idéal nul (réduit à $\{0\}$) est premier si et seulement si A est intègre.

Démonstration. En deux sens.

(i) **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.

(ii) **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.

□

Proposition 1.224 ([43]).
Soit un anneau commutatif[76] *et un idéal I dans A.*

(1) I est un idéal premier[77] *si et seulement si A/I est un anneau intègre.*

(2) I est un idéal maximal[78] *si et seulement si A/I est un corps.*

(3) Tout idéal maximal propre est premier.

Démonstration. En plein d'étapes.

(i) **(1), $\Rightarrow$** Évacuons le cas trivial pour être sûr. Si $I = \{0\}$ alors A est intègre par le lemme 1.223. 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.

(ii) **(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.

(iii) **(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 $x \in A \backslash I$.

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.

75. Définition 1.220.
76. Tous les anneaux du Frido sont commutatifs
77. Idéal premier, définition 1.222.
78. Idéal maximal, définition 1.212.

(iv) **(2),** $\Leftarrow$ Si $x \in A\backslash I$, 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

$$1 = ax + \underbrace{(1 - ax)}_{\in I}. \tag{1.310}$$

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 1.193 dit que A/I est un anneau intègre. Le point (1) dit alors que I est un idéal premier. □

Remarque 1.225.
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 1.222.

Proposition 1.226 ([48])**.**
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. □

Proposition 1.227.
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.

1.10 Anneau intègre

1.10.1 Sous-groupes de $(\mathbb{Z}, +)$

Proposition 1.228 (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 $H = n\mathbb{Z}$.

(2) Si H est une 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 1.215, 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 $n = m$. □

1.10.2 Théorème de Bézout

Théorème 1.229 (Théorème de Bézout [79][49], thème 3)**.**
Deux entiers non nuls $a, b \in \mathbb{Z}^*$ sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = 1 \tag{1.311}$$

Démonstration. Soit $d = \text{pgcd}(a, b)$ et des nombres u, v tels que $au + bv = 1$. Le PGCD d divise à la fois a et b, et donc divise $au + bv$. Nous en déduisons que d divise 1 et est par conséquent égal à 1.

Nous supposons maintenant que $\text{pgcd}(a, b) = 1$ et nous considérons l'ensemble

$$E = \{au + bv \text{ tel que } u, v \in \mathbb{Z}\} \cap \mathbb{N}^*. \tag{1.312}$$

C'est-à-dire l'ensemble des nombres strictement positifs pouvant s'écrire sous la forme $au+bv$. Cet ensemble est non vide parce qu'il contient par exemple soit a soit $-a$. Soit m le plus petit élément de E et écrivons

$$m = au_1 + bv_1. \tag{1.313}$$

Par le théorème de division euclidienne [80] (avec a et m), il existe des entiers uniques q et r tels que

$$a = mq + r \tag{1.314}$$

avec $0 \leqslant r < m$. En remplaçant m par sa valeur (1.313), $a = (au_1 + bv_1)q + r$ et

$$r = a(1 - u_1q) - bv_1q, \tag{1.315}$$

c'est-à-dire que $r \in \mathbb{Z}a + \mathbb{Z}b$ en même temps que $0 \leqslant r < m$. Si r était strictement positif, il serait dans E. Mais cela est impossible par minimalité de m. Donc $r = 0$ et a est divisible par m.

De la même façon nous prouvons que b est divisible par m. Puisque m divise à la fois a et b nous avons $m = 1$. □

Une généralisation de Bézout 1.229 à plus de 2 variables.

Proposition 1.230.
Si $\{a_i\}_{i=1,\dots,N}$ sont des entiers tels que $\text{pgcd}(a_1, \dots, a_N) = 1$, alors il existe des entiers $\{u_i\}_{i=1,\dots,N}$ tels que

$$\sum_i a_i u_i = 1. \tag{1.316}$$

Corolaire 1.231.
Soient p et q deux entiers premiers entre eux. Alors

$$p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}; \tag{1.317}$$

en particulier, pour tout $x \in \mathbb{Z}$, il existe u_x, v_x entiers tels que $u_xp + v_xq = x$.

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.

Démonstration. Soit $x \in \mathbb{Z}$. Le théorème de Bézout nous donne k et l tels que $kp + lq = 1$. Alors, $(xk)p + (xl)q = x$. □

Corolaire 1.232.
Les quotients de $\mathbb{Z}$ sont $\mathbb{Z}/n\mathbb{Z}$.

79. Il y a une super application ici : https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/mauvais_prix.pdf.
80. Théorème 1.215.

Démonstration. Tous les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$. En effet en vertu de la proposition 1.228, 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[81] : si $a \in n\mathbb{Z}$ et si $k \in \mathbb{Z}$ alors $ak \in n\mathbb{Z}$. □

Proposition 1.233.
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

$$U(\mathbb{Z}/n\mathbb{Z}) = \phi(P_n) = \{\overline{x} \text{ tel que } 0 \leqslant x \leqslant n \text{ tel que } \operatorname{pgcd}(x,n) = 1\}. \tag{1.318}$$

où P_n est l'ensemble $P_n = \{x \in \{0,\dots,n-1\} \text{ tel que } \operatorname{pgcd}(x,n) = 1\}$.

De plus,

$$\operatorname{Card}\big(U(\mathbb{Z}/n\mathbb{Z})\big) = \phi(n). \tag{1.319}$$

Démonstration. Soit $0 \leqslant x \leqslant n$ tel que $\operatorname{pgcd}(x,n) = 1$. Il existe donc[82] $u, v \in \mathbb{Z}$ tels que $ux + vn = 1$. En passant aux classes,

$$\overline{ux} = \overline{1}, \tag{1.320}$$

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[83] que $\operatorname{pgcd}(x,n) = 1$. □

Lemme 1.234.
Un corps[84] *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 1.235.
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 3.99 que l'anneau A est intègre si et seulement si $A[X]$ est intègre.

Corolaire 1.236.
L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

Démonstration. Supposons que n soit premier. La proposition 1.233 donne les inversibles de $\mathbb{Z}/n\mathbb{Z}$ par

$$U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \text{ tel que } 0 \leqslant x \leqslant n \text{ tel que } \operatorname{pgcd}(x,n) = 1\}. \tag{1.321}$$

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

$$[p]_n[q]_n = [pq]_n = [0]_n. \tag{1.322}$$

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. □

Proposition 1.237 (Thème 18, [1])**.**
Soit A un anneau principal[85] *qui n'est pas un corps. Pour un idéal propre I de A, les conditions suivantes sont équivalentes :*

81. Définition 1.177.
82. Théorème de Bézout 1.229
83. À nouveau avec le Théorème de Bézout.
84. Définition 1.202.
85. Définition 1.221.

(1) I est un idéal maximal[86] *;*

(2) I est un idéal premier non nul[87] *;*

(3) il existe p irréductible[88] *dans A tel que $I = (p)$.*

Démonstration. En plusieurs implications.

(i) **(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 1.211). Étant donné que I est un idéal maximal, le quotient A/I est un corps par la proposition 1.213.

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 1.234) 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.

(ii) **(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[89].

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.

(iii) **(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 $I = J$.

□

1.238.
Dans la proposition 1.237, 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.

Proposition 1.239.
Soit A un anneau principal, et soit $p \in A$ un élément irréductible. Alors

(1) (p) est un idéal maximum.

(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 1.213. □

86. Définition 1.212.
87. Définition 1.222.
88. Définition 1.183.
89. ça me semble un peu trop facile. Lisez attentivement, et écrivez-moi pour dire si vous êtes d'accord ou pas.

Exemple 1.240.
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. △

Exemple 1.241 (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.

(i) **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 1.210 dit que $S = \phi(J)$ où J est un idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Mais le corolaire 1.232 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

$$[km]_n = k[m]_n \in ([m]_n). \tag{1.323}$$

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

$$k[m]_n = [km]_n = \phi(km) \in \phi(m\mathbb{Z}). \tag{1.324}$$

(ii) **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 1.236).

(iii) **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 1.242.
Nous verrons dans la proposition 26.68 que l'anneau des fonctions holomorphes sur un compact de $\mathbb{C}$ est principal. △

Théorème 1.243.
Si A est un anneau principal et si p et q sont premiers entre eux dans A, alors on a l'isomorphisme d'anneaux

$$A/pqA \simeq A/pA \times A/qA. \tag{1.325}$$

1.11 Anneau euclidien

Définition 1.244 (Wikipédia)**.**
Soit A un anneau intègre[90]*. Un **stathme euclidien** sur A est une application $\alpha\colon A\backslash\{0\} \to \mathbb{N}$ tel que*

(1) $\forall a, b \in A\backslash\{0\}$, il existe $q, r \in A$ tel que

$$a = qb + r \tag{1.326}$$

et $\alpha(r) < \alpha(b)$.

(2) Pour tout $a, b \in A\backslash\{0\}$, $\alpha(b) \leqslant \alpha(ab)$.

*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.

Lemme 1.245.
L'ensemble $\mathbb{Z}$ avec les opérations usuelles est un anneau intègre[91]*.*

90. Défnition 1.192.
91. Anneau intègre, définition 1.192.

Exemple 1.246.
Le stathme de $\mathbb{N}$ pour la division euclidienne usuelle est $\alpha(n) = n$. Si $a, b \in \mathbb{N}$ nous écrivons

$$a = qb + r \tag{1.327}$$

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

$$r - b = a - b(q + 1) < a - b\frac{a}{b} = 0, \tag{1.328}$$

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.

Proposition 1.247 ([50]).
Tout anneau euclidien[92] *est principal*[93].

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 $a \in I\backslash\{0\}$ qui minimise $\alpha(a)$ va générer[94] 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. □

Proposition 1.248.
L'anneau $\mathbb{Z}$ est principal et euclidien.

Démonstration. Nous allons seulement montrer que $\alpha(x) = |x|$ est un stathme euclidien. Ainsi $\mathbb{Z}$ sera euclidien et donc principal par la proposition 1.247.

D'abord $\mathbb{Z}$ est intègre, c'est le lemme 1.245.

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

$$|a| = q_0|b| + r_0 \tag{1.329}$$

avec $r_0 < |b|$. Cela existe parce que $\alpha(x) = x$ est un stathme sur $\mathbb{N}$ par l'exemple 1.246.

(i) **Si $a > 0$ et $b > 0$** Alors $a = q_0b + r_0$ et le couple (q_0, r_0) vérifie les conditions de la définition 1.244(1).

(ii) **Si $a > 0$ et $b < 0$** Alors $a = -q_0b + r_0$, et le couple $(-q_0, r_0)$ vérifie les conditions de la définition 1.244(1).

(iii) **Si $a < 0$ et $b > 0$** Alors $a = -q_0b - r_0$, et le couple $(-q_0, -r_0)$ vérifie les conditions de la définition 1.244(1) parce que

$$\alpha(-r_0) = r_0 < |b| = \alpha(b). \tag{1.330}$$

(iv) **Si $a < 0$ et $b < 0$** Alors $a = q_0b - r_0$, et le couple $(q_0, -r_0)$ vérifie les conditions de la définition 1.244(1).

□

Nous venons de voir que $\mathbb{Z}$ est principal ; le lemme suivant nous dit que $\mathbb{Z}[X]$ n'est lui, pas principal.

Lemme 1.249 ([51]).
Si A est un anneau intègre[95] *qui n'est pas un corps, alors $A[X]$ n'est pas principal.*

92. Euclidien, définition 1.244.
93. Principal, définition 1.220
94. Un tel élément existe...
95. Définition 1.192.

Démonstration. Soit un élément non nul $a \in A$.

(i) **Un idéal principal contenant a et X est $\mathbf{A[X]}$** 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 :

$$1 = k'k \in k'(P) = (P). \tag{1.331}$$

(ii) **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

$$1 = UX + Va. \tag{1.332}$$

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.

(iii) **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 3.105 que si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est principal.

1.12 Le groupe et anneau des entiers

Certes $(\mathbb{Z}, +)$ est un groupe mais en ajoutant la multiplication, $(\mathbb{Z}, +, \times)$ devient un anneau[96].

1.12.1 PGCD, PPCM et Bézout

Puisque $\mathbb{Z}$ est un anneau intègre, nous avons la définition 1.180 de pgcd et de ppcm.

Proposition 1.250 (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 1.108). □

Lemme 1.251.
Soient $p, q \in \mathbb{Z}^*$. Les entiers $\operatorname{ppcm}(p, q)$ *et* $\operatorname{pgcd}(p, q)$ *fournissent les isomorphismes de groupes suivants :*

$$p\mathbb{Z} \cap q\mathbb{Z} = \operatorname{ppcm}(p, q)\mathbb{Z} \tag{1.333a}$$
$$p\mathbb{Z} + q\mathbb{Z} = \operatorname{pgcd}(p, q)\mathbb{Z}. \tag{1.333b}$$

Définition 1.252.
Nous disons que deux éléments d'un anneau principal[97] *sont* ***premiers entre eux*** *si leurs diviseurs communs sont inversibles.*

96. Définition 1.39.
97. Anneau principal, définition 1.221.

Vu que $\mathbb{Z}$ est un anneau principal (proposition 1.248), la définition 1.252 d'éléments premiers entre eux s'applique.

Lemme 1.253.
Dans $\mathbb{Z}$, les nombres p et q sont premiers entre eux si et seulement si $\operatorname{pgcd}(p,q)=1$.

Définition 1.254.
Si nous avons un ensemble d'entiers a_i, nous disons qu'ils sont premiers ***dans leur ensemble*** *si 1 est le PGCD de tous les a_i ensemble.*

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 38.33 et ce qui suit.

Proposition 1.255.
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.

(i) **Une décomposition pour x** On applique le théorème 1.215 de division euclidienne à x et $a+b$: il existe des entiers p_x, r_x, uniques, tels que

$$\begin{cases} x=(p_x-1)(a+b)+r_x & \text{(1.334a)}\\ 0\leqslant r_x<a+b. & \text{(1.334b)}\end{cases}$$

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

$$ua+vb=p_x(a+b)-x \tag{1.335}$$

par le corolaire 1.231. Ainsi, x peut s'écrire

$$x=(p_x-u)a+(p_x-v)b. \tag{1.336}$$

(ii) **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 1.231, nous considérons les nombres u_i et v_i définis par

$$u_ia+v_ib=i \tag{1.337}$$

pour $i=1,\dots,a+b$. Nous posons $u^*=\max\{u_i\}$, $v^*=\max\{v_i\}$, et $p^*=\max\{u^*,v^*\}$. Nous posons alors $N=p^*(a+b)$, et considérons $x>N$.

(iii) **Nouvelle décomposition pour x** Nous voulons écrire

$$x=(p_x-u_k)a+(p_x-v_k)b \tag{1.338}$$

pour un certain k. Cela demande $u_ka+v_kb=ua+vb=p_x(a+b)-x$ par l'équation (1.335). Vu que $p_x(a+b)-x>0$, les nombres u_k et v_k existent : il suffit de prendre $k=p_x(a+b)-x$.

(iv) **Conclusion** Avec tous ces choix, nous avons d'abord $x>p^*(a+b)$ et donc

$$x=(p_x-1)(a+b)+r_x>p^*(a+b), \tag{1.339}$$

ce qui donne

$$(p_x-1)(a+b)>p^*(a+b)-r_x>(p-1)(a+b). \tag{1.340}$$

ou encore $p_x > p^*$. Nous avons finalement

$$p_x \geqslant p^* \geqslant u^* \geqslant u_k \tag{1.341}$$

et

$$p_x \geqslant p^* \geqslant v^* \geqslant v_k. \tag{1.342}$$

De ce fait, la décomposition (1.338) est celle que nous voulions.

□

1.256.
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 1.257.
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

$$1004 = 72 \cdot 7 + 100 \cdot 5. \tag{1.343}$$

Ensuite $4 = 25 - 21 = -3 \cdot 7 + 5 \cdot 5$. Au final,

$$1000 = 75 \cdot 7 + 95 \cdot 5. \tag{1.344}$$

△

1.13 Sous-groupe normal

Proposition 1.258.
Soit N un sous-groupe de G. Les propriétés suivantes sont équivalentes :

(1) N est normal[98] *dans G.*
(2) N est une union de classes de conjugaison[99] *de G,*
(3) $gNg^{-1} \subseteq N$ pour tout $g \in G$,
(4) $gNg^{-1} = N$ pour tout $g \in G$,
(5) $gN = Ng$ pour tout $g \in G$,
(6) Le normalisateur[100] *de N est G : $\mathcal{N}_G(N) = G$.*

Démonstration. En plusieurs parties.

(i) **(1) implique (3)** C'est la définition de sous-groupe normal.

(ii) **(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

$$N \subset g(g^{-1}Ng)g^{-1} \subset gNg^{-1}. \tag{1.345}$$

Nous avons l'inclusion dans les deux sens. Donc l'égalité.

(iii) **(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

$$n' = gng^{-1} \in gNg^{-1} \subset N. \tag{1.346}$$

Il est immédiat de prouver que $gn = n'g$. Cela prouve que $gN \subset Ng$.
Le même raisonnement donne $Ng \subset gN$.

98. Définition 1.167.
99. Définition 1.163.
100. Définition 1.166.

(iv) **(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,

$$a = gng^{-1} = n'gg^{-1} = n' \in N. \tag{1.347}$$

(v) **(5) implique (2)** Pour chaque $a \in G$ nous notons C_a la classe de conjugaison de a dans G :

$$C_a = \{gag^{-1} \text{ tel que } g \in G\}. \tag{1.348}$$

Comme $a \in C_a$ (prendre $g = e$ dans (1.348).) nous avons forcément

$$N \subset \bigcup_{n \in N} C_n. \tag{1.349}$$

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

$$C_n = \{gng^{-1} \text{ tel que } g \in G\} \subset N. \tag{1.350}$$

Donc il est vrai que $N = \bigcup_{n \in N} C_n$.

(vi) **(2) implique (1)** Nous supposons que $N \subset G$ est un sous-groupe de la forme

$$N = \bigcup_{a \in I} C_a \tag{1.351}$$

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

$$gng^{-1} = g(kak^{-1})g^{-1} = (gk)a(gk)^{-1} \in C_a \subset N. \tag{1.352}$$

Le lecteur attentif aura remarqué l'utilisation de l'axiome du choix. La prudence l'incitera à ne pas le faire remarquer au jury.

(vii) **(6) si et seulement si (5)** C'est la définition du normalisateur.

□

Définition 1.259.
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 $g^n = (g^{-1})^{-n}$.

L'ordre d'un groupe et l'ordre d'un élément d'un groupe sont deux choses différentes.

Définition 1.260 (Ordre d'un groupe)**.**
Soit un groupe G.

*(1) Si G est un ensemble fini, l'**ordre** de G est son cardinal*[101]*, 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 Card(G)*. Au lieu de ça, dans le cas particulier des groupes, il y a une tradition de dire « ordre » et d'écrire $|G|$.*

Définition 1.261 (Ordre d'un élément)**.**
*L'**ordre** d'un élément g de G est le naturel*

$$\min\{n \in \mathbb{N}\backslash\{0\} \text{ tel que } g^n = e\}, \tag{1.353}$$

si il existe ; dans le cas contraire, nous disons que l'ordre de g est infini.

101. Définition 1.121.

1.262.
Nous verrons que le corolaire 2.14 au théorème de Lagrange dira que l'ordre d'un élément divise l'ordre du groupe.

Lemme 1.263 ([52, 12]).
Soient un groupe G et deux sous-groupes normaux[102] *H et K tels que $H \cap K = \{e\}$. Alors :*

(1) Tout élément de H commute avec tout élément de K.

(2) HK est un sous-groupe de G.

(3) L'application

$$\begin{aligned} \varphi\colon H \times K &\to HK \\ (h,k) &\mapsto hk \end{aligned} \tag{1.354}$$

est un isomorphisme de groupes.

Démonstration. Point par point.

(i) **(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

$$kh^{-1}k^{-1} \in H \tag{1.355}$$

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

$$hkh^{-1}k^{-1} = e, \tag{1.356}$$

et donc que $hk = kh$.

(ii) **(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

$$(h_1k_1)(h_2k_2) = h_1h_2k_1k_2 \in HK. \tag{1.357}$$

Donc le produit de deux éléments de HK est dans HK.

(iii) **(3)** En trois sous-parties.

(i) **Morphisme** Soient $h_i \in H$ et $k_i \in K$. En utilisant la commutativité du point (1) nous avons

$$\begin{aligned} \varphi\big((h_1,k_1)(h_2,k_2)\big) &= \varphi(h_1h_2, k_1k_2) && \text{(1.358a)}\\ &= (h_1h_2)(k_1k_2) && \text{(1.358b)}\\ &= (h_1k_1)(h_2k_2) && \text{(1.358c)}\\ &= \varphi(h_1,k_1)\varphi(h_2,k_2). && \text{(1.358d)} \end{aligned}$$

(ii) **Injectif** Si $\varphi(h_1,k_1) = \varphi(h_2,k_2)$ nous avons successivement

$$\begin{aligned} h_1k_1 &= h_2k_2 && \text{(1.359a)}\\ h_1k_1h_2^{-1} &= k_2 && \text{(1.359b)}\\ h_1k_1h_2^{-1}k_1^{-1} &= k_2k_1^{-1} && \text{(1.359c)}\\ h_1h_2^{-1} &= k_2k_1^{-1}. && \text{(1.359d)} \end{aligned}$$

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 $k_1 = k_2$.

102. Sous-groupe normal, définition 1.167.

(iii) **Surjectif** Un élément général de HK est hk avec $h \in H$ et $k \in K$, c'est-à-dire $\varphi(h,k)$.

□

Définition 1.264.
*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.*

Proposition 1.265.
À propos d'exposant de groupe et de ppcm.

(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.

(2) Pour un groupe fini, l'exposant est le ppcm *des ordres des éléments du groupe.*

Démonstration. En deux parties.

(i) **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 1.215, nous avons des entiers u et v tels que $q = ua + v$ avec $v < a$. Nous avons alors

$$g^q = g^{ua}g^v = g^v \neq e \tag{1.360}$$

parce que $v < a$ et que a est le plus petit n tel que $g^n = e$.

(ii) **Pour (2)** Même chose. Pour un groupe fini, le ppcm existe toujours.

□

<++>

Le théorème de Burnside 9.305 nous donnera un bon paquet d'exemples de groupes d'exposant fini dans $\mathrm{GL}(n,\mathbb{C})$.

Proposition 1.266.
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

$$\begin{aligned}
[\psi(g_1)][\psi(g_2)] &= \big[\psi(g_1)\psi(g_2)\big] && (1.361a)\\
&= \big[\psi(g_1g_2)\big] && (1.361b)\\
&= \{\psi(g_1g_2)\psi(h) \text{ tel que } h \in H\} && (1.361c)\\
&= \{\psi(g_1g_2h) \text{ tel que } h \in H\} && (1.361d)\\
&= \psi\Big(\{g_1g_2h \text{ tel que } h \in H\}\Big) && (1.361e)\\
&= \psi\big(\overline{g_1g_2}\big) && (1.361f)\\
&= \psi(\overline{g_2g_1}) && (1.361g)\\
&= \text{refaire à l'envers} && (1.361h)\\
&= [\psi(g_2)][\psi(g_1)]. && (1.361i)
\end{aligned}$$

Par conséquent $\psi(G)/\psi(H)$ est abélien. □

1.13.1 Permutations, groupe symétrique

Nous donnons ici quelques éléments à propos du groupe symétrique. Beaucoup de choses supplémentaires sont reportées à la section 5.6. Voir aussi le thème 8.

Définition 1.267.
*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 $\{1, \dots, n\} \to \{1, \dots, n\}$.*

Définition 1.268.
*Le **support** d'une permutation σ est l'ensemble constitué des éléments modifiés par σ :*

$$\operatorname{supp}\sigma = \{i \in \{1, \dots, n\} \text{ tel que } \sigma(i) \neq i\}.$$

Définition 1.269 ([52]).
*Soient une permutation $\sigma \in E$ ainsi que $a \in E$. La σ-**orbite** de a est l'ensemble*

$$\Omega_\sigma(a) = \{\sigma^i(a)\}_{i \in \mathbb{N}}. \tag{1.362}$$

Lemme 1.270 ([53]).
Le groupe symétrique S_n est un ensemble fini contenant $n!$ éléments :

$$\operatorname{Card}(S_n) = n!. \tag{1.363}$$

Lemme 1.271 ([54]).
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

$$\begin{aligned} \tau_g \colon G &\to G \\ x &\mapsto gx. \end{aligned} \tag{1.364}$$

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 $\tau_g \in S_G$. De plus l'application

$$\begin{aligned} \varphi \colon G &\to S_G \\ g &\mapsto \tau_g \end{aligned} \tag{1.365}$$

est un morphisme de groupe. Il est injectif 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.

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. □

1.13.2 Décomposition en cycles

Définition 1.272 (cycle[52]).
*Soit E un ensemble de cardinal[103] 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[104] non réduite à un élément et qu'elle est de cardinal k.*

103. Définition 1.121.
104. Définition 1.269.

Lemme 1.273 ([1]).
Soient un k-cycle σ et $a \in \Omega$. Alors

$$\Omega_\sigma(a) = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\} \tag{1.366}$$

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

— $\text{Card}(A) = l + 1$

— $A \subset \Omega_\sigma(a)$, et donc $\text{Card}(A) \leqslant \text{Card}(\Omega_\sigma(a)) = k$ par le lemme 1.123(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

$$\Omega_\sigma(a) = \{\sigma^i(a)\}_{0 \leqslant i \leqslant l} = A. \tag{1.367}$$

Le cardinal de $\Omega_\sigma(a)$ étant k par hypothèse nous avons $k = l + 1$, et donc $l = k - 1$. □

Lemme 1.274.
Si σ est une cycle de longueur k, et si $b \in \Omega_\sigma(a)$, alors

$$\Omega_\sigma(a) = \Omega_\sigma(b) = \{\sigma^i(b)\}_{i=0,\dots,k-1}. \tag{1.368}$$

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 1.273 appliqué à b. □

Lemme 1.275 ([1]).
Soient un ensemble fini E, une permutation $\sigma \in S_E$ ainsi que $a \in E$. Si $b \in \Omega_\sigma(a)$, alors $\Omega_\sigma(b) = \Omega_\sigma(a)$.

Lemme 1.276 ([52]).
Tout k-cycle est d'ordre[105] *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. □

Lemme 1.277 ([52, 55]).
Tout élément du groupe symétrique S_n peut être décomposé en un nombre fini de cycles de supports disjoints.

Cette décomposition est unique à l'ordre près de l'écriture des cycles.

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[106] *$\sigma = \prod_{i \in I} \omega_i$.*

Démonstration. Soit $\sigma \in S_E$. Si les éléments $\{a, \sigma(a), \dots \sigma^k(a)\}$ sont distincts, alors soit $\sigma^{k+1}(a)$ est distincts des autres, soit $\sigma^{k+1}(a) = a$. Il n'est en effet pas possible d'avoir $\sigma^{k+1}(a) = \sigma^l(a)$ avec $l < k$ parce que ça contredirait l'injectivité de σ.

Soit donc $a \in E$. Nous considérons le cycle $\big(a, \sigma(a), \dots, \sigma^k(a)\big)$ où k est maximum tel que tous les éléments sont distincts.

105. Définition 1.261.
106. Ici I est un ensemble fini et vu que les supports sont disjoints, le produit est commutatif.

Soit ce cycle contient tous les éléments de E, soit il existe un élément b hors de ce cycle. Dans le second cas, nous considérons le cycle commençant par b.

Et ça continue... □

Lemme 1.278 ([52]).
Deux cycles de support disjoint commutent.

Lemme 1.279 ([56]).
Tout cycle de longueur r est le produit de $r-1$ transpositions.

Démonstration. Il suffit de vérifier que

$$(a_1,\dots,a_r)=(a_1,a_r)(a_1,a_{r-1})\dots(a_1,a_2). \tag{1.369}$$

□

Lemme 1.280 ([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

(1) Si $a\in\text{supp}(\sigma)$, alors pour tout $q\in\mathbb{N}$ nous avons $c^q(a)=\sigma^q(a)$.

(2) Si $a\in\text{supp}(c)$, alors

$$\Omega_\sigma(a)=\Omega_c(a)=\text{supp}(c). \tag{1.370}$$

(3) Si $a\in\text{supp}(c)$, alors

$$c(x)=\begin{cases}\sigma(x) & \text{si } x\in\Omega_\sigma(a)\\ x & \text{sinon.}\end{cases} \tag{1.371}$$

Démonstration. En plusieurs parties.

(i) **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

$$\sigma(a)=(s\circ c)(a)=s\big(c(a)\big)=c(a). \tag{1.372}$$

(ii) $\sigma^q(a)=c^q(a)$ Juste une récurrence sur le point précédent : si $b\in\text{supp}(a)$, alors $\sigma(b)=c(b)\in\text{supp}(a)$.

(iii) **Si $a\in\text{supp}(c)$, alors $\Omega_\sigma(a)=\Omega_c(a)$** Utilisant le point précédent, ainsi que la définition 1.269 d'une orbite,

$$\Omega_\sigma(a)=\{\sigma^q(a)\}=\{c^q(a)\}=\Omega_c(a). \tag{1.373}$$

(iv) $\text{supp}(c)\subset\Omega_c(a)$ 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 $b\in\Omega_c(b)=\Omega_c(a)$.

(v) $\Omega_c(a)\subset\text{supp}(c)$ Soit $b\in\Omega_c(a)$. Le lemme 1.274 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 $b\in\text{supp}(c)$.

(vi) **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 $c(x)=x$.

□

Le lemme suivant permet d'extraire le cycle de σ associé à un élément de E.

Lemme 1.281 ([1]).
Soient un ensemble finie E ainsi que $\sigma \in S_E$, et $a \in E$ tel que $\sigma(a) \neq a$. Nous posons

$$\begin{aligned} c\colon E &\to E \\ x &\mapsto \begin{cases} \sigma(x) & si\ x \in \Omega_\sigma(a) \\ x & sinon \end{cases} \end{aligned} \tag{1.374}$$

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

$$c^q(b) = \sigma^q(b) \in \Omega_\sigma(a) \tag{1.375}$$

pour tout q. Donc nous avons

$$\Omega_c(b) = \{c^q(b) \text{ tel que } q \in \mathbb{N}\} = \{\sigma^q(b) \text{ tel que } q \in \mathbb{N}\} = \Omega_\sigma(b) = \Omega_\sigma(a). \tag{1.376}$$

La dernière égalité est le lemme 1.275.

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. □

Théorème 1.282 ([55]).
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.

Démonstration. Plusieurs points.

(i) **Existence** Nous choisissons des éléments $\{a_i\}_{i=1,\dots,p}$ tels que les $\Omega_\sigma(a_i)$ forment une partition de E en sous-ensembles disjoints. En posant $l_k = \min\{r \text{ tel que } \sigma^r(a_k) = a_k\}$, nous avons

$$\Omega_\sigma(a_k) = \{\sigma^q(a_k)\}_{q=1,\dots,l_k-1} \tag{1.377}$$

et tous les $\sigma^q(a_k)$ sont distincts pour $q = 1, \dots, l_k - 1$.

Posons

$$\begin{aligned} c_k\colon E &\to E \\ x &\mapsto \begin{cases} \sigma(x) & \text{si } x \in \Omega_\sigma(a_k) \\ x & \text{sinon.} \end{cases} \end{aligned} \tag{1.378}$$

Le lemme 1.280 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

$$x \in \Omega_\sigma(a_k) = \Omega_{c_k}(a_k) = \Omega_{c_k}(x), \tag{1.379}$$

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,

$$(c_1 \circ \dots c_p)(x) = c_k(x) = \sigma(x). \tag{1.380}$$

(ii) **Unicité** Nous supposons avoir $\sigma = c_1 \circ \ldots \circ c_p = \gamma_1 \circ \gamma_q$ où les c_i et les γ_j sont deux ensembles de cycles de supports disjoints. Nous avons

$$\operatorname{supp}(\sigma) = \bigcup_{i=1}^{p} \operatorname{supp}(c_i) = \bigcup_{j=1}^{q} \operatorname{supp}(\gamma_j). \tag{1.381}$$

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

$$\operatorname{supp}(c_i) = \Omega_{c_i}(a) = \Omega_\sigma(a) = \Omega_{\gamma_j}(a) = \operatorname{supp}(\gamma_j). \tag{1.382}$$

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

$$\begin{aligned} u\colon \{1,\ldots,p\} &\to \{1,\ldots,q\} \\ i &\mapsto \text{l'unique } j \text{ tel que } \operatorname{supp}(c_i) = \operatorname{supp}(\gamma_j). \end{aligned} \tag{1.383}$$

Autrement dit, l'application u permet d'écrire

$$\operatorname{supp}(c_i) = \operatorname{supp}\big(\gamma_{u(i)}\big). \tag{1.384}$$

L'application u est injective. En effet si $u(i) = u(l)$, nous avons

$$\operatorname{supp}(c_i) = \operatorname{supp}\big(\gamma_{u(i)}\big) \tag{1.385a}$$
$$\operatorname{supp}(c_l) = \operatorname{supp}\big(\gamma_{u(l)}\big) \tag{1.385b}$$
$$u(i) = u(l). \tag{1.385c}$$

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 $j \in \{1,\ldots,q\}$. 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 $u\colon \{1,\ldots,p\} \to \{1,\ldots,q\}$ est bijective. Nous en déduisons que $p = q$. Concluons en montrant que $c_i = \gamma_{u(i)}$. Soit $a \in \operatorname{supp}(c_i) = \operatorname{supp}\big(\gamma_{u(i)}\big)$.
Nous avons

$$c_i(x) = \begin{cases} \sigma(x) & \text{si } x \in \Omega_\sigma(a) \\ x & \text{sinon} \end{cases} \tag{1.386}$$

et

$$\gamma_j(x) = \begin{cases} \sigma(x) & \text{si } x \in \Omega_\sigma(a) \\ x & \text{sinon,} \end{cases} \tag{1.387}$$

et donc $c_i = \gamma_j$.

□

Lemme 1.283 ([57]).
Soit $\sigma = (i_1,\ldots,i_k) \in S_n$, un cycle de longueur k et $\theta \in S_n$. Alors

$$\theta\sigma\theta^{-1} = \big(\theta(i_1),\ldots,\theta(i_k)\big). \tag{1.388}$$

Tous les cycles de longueur k sont conjugués entre eux.

Proposition 1.284 (Classes de conjugaison et structure en cycles[58]).
Une classe de conjugaison[107] *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'.*

107. Définition 1.163.

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

$$\sigma' = \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \dots (\tau c_m \tau^{-1}), \tag{1.389}$$

mais $\tau c_i \tau^{-1}$ est un cycle de même longueur que c_i, puisque le lemme 1.283 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 1.283. Comme les supports des c_i et des c'_i sont disjoints, la permutation $\tau_1 \dots \tau_m$ conjugue σ et σ'. □

Exemple 1.285.
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

$$C_1 = \{\mathrm{Id}\} \tag{1.390a}$$
$$C_2 = \{(1,2), (1,3), (2,3)\} \tag{1.390b}$$
$$C_3 = \{(1,2,3), (2,1,3)\}. \tag{1.390c}$$

△

Définition 1.286 (transposition)**.**
Une ***transposition*** *est une permutation*[108] *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*

$$\sigma(x) = \begin{cases} a & \text{si } x = b \\ b & \text{si } x = a \\ x & \text{sinon.} \end{cases} \tag{1.391}$$

Exemple 1.287.
Les classes de conjugaison de S_4. Nous savons que les classes de conjugaison dans S_4 sont caractérisées par la structure des décompositions en cycles (proposition 1.284). Le groupe symétrique S_4 possède donc les classes de conjugaison suivantes.

(1) Le cycle vide qui représente la classe constituée de l'identité seule.

(2) Les transpositions (de type (a, b)) qui sont au nombre de 6.

(3) Les 3-cycles. 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.

(4) Les 4-cycles. 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.

108. Une permutation est une bijection, définition 1.267.

(5) Les doubles transpositions, du type $(a,b)(c,d)$. 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.

△

Proposition 1.288.
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 lemme 1.277 et chacun des cycles peut être décomposé en un nombre fini de transpositions par le lemme 1.279. □

Cette décomposition n'est pas à confondre avec celle en cycles de support disjoints. Par exemple $(1,2,3) = (1,3)(1,2)$.

Le théorème suivant, qui donne la notion de parité d'une permutation, est la clef pour savoir quelles positions du jeu de taquin sont possibles ou impossibles[59, 60].

Proposition-Définition 1.289 (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).*

Définition 1.290.
*La **signature** est l'application*

$$\begin{aligned}\epsilon\colon S_E &\to \{-1,1\}\\ \sigma &\mapsto \begin{cases}1 & \text{si } \sigma \text{ est paire}\\ -1 & \text{si } \sigma \text{ est impaire.}\end{cases}\end{aligned} \tag{1.392}$$

Lemme 1.291.
*Nous disons qu'un élément $\sigma \in S_n$ est une **inversion** pour les nombres $i<j$ si $\sigma(i)>\sigma(j)$. Soit N_σ le nombre d'inversions que $\sigma \in S_n$ possède (c'est le nombre de couples (i,j) avec $i<j$ tels que $\sigma(i)>\sigma(j)$). Nous avons*

$$\epsilon(\sigma) = (-1)^{N_\sigma} \tag{1.393}$$

où ϵ est la signature[109] *dans S_n.*

Lemme 1.292 ([52])**.**
Un k-cycle est une permutation impaire si k est pair et paire si k est impair.

Proposition 1.293 ([57])**.**
Soit S_n le groupe symétrique.

(1) *L'application $\epsilon\colon S_n \to \{1,-1\}$ est l'unique homomorphisme 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. Soit $\sigma,\theta \in S_n$. Afin de montrer que $\epsilon(\sigma\theta) = \epsilon(\sigma)\epsilon(\theta)$, nous divisons les couples (i,j) tels que $i \leqslant j$ en 4 groupes suivant que $\theta(i) \gtrless \theta(j)$ et $\sigma\big(\theta(i)\big) \gtrless \sigma\big(\theta(j)\big)$. Nous notons N_1, N_2, N_3 et N_4 le nombre de couples dans chacun des quatre groupes :

109. Définition 1.290.

(i,j)	$\sigma\big(\theta(i)\big) < \sigma\big(\theta(j)\big)$	$\sigma\big(\theta(i)\big) > \sigma\big(\theta(j)\big)$
$\theta(i) < \theta(j)$	N_1	N_2
$\theta(i) > \theta(j)$	N_3	N_4

Nous avons immédiatement $N_\theta = N_3 + N_4$ et $N_{\sigma\theta} = N_2 + N_4$. Les éléments qui participent à N_σ sont ceux où $\theta(i)$ et $\theta(j)$ sont dans l'ordre inverse de $\sigma\big(\theta(i)\big)$ et $\sigma\big(\theta(j)\big)$ (parce que θ est une bijection). Donc $N_\sigma = N_2 + N_3$. Par conséquent nous avons

$$\epsilon(\sigma)\epsilon(\theta) = (-1)^{N_2+N_3}(-1)^{N_3+N_4} = (-1)^{N_2+N_4} = (-1)^{N_{\sigma\theta}} = \epsilon(\sigma\theta). \tag{1.394}$$

Nous avons prouvé que ϵ est un homomorphisme. Pour montrer que ϵ est surjectif sur $\{-1,1\}$ nous devons trouver un élément $\tau \in S_n$ tel que $\epsilon(\tau) = -1$. Si τ est la transposition $1 \leftrightarrow 2$ alors le couple $(1,2)$ est le seul à être inversé par τ et nous avons $\epsilon(\tau) = -1$.

Avant de montrer l'unicité, nous montrons que si $\sigma = t_1 \dots t_k$ alors $\epsilon(\sigma) = (-1)^k$. Pour cela il faut montrer que $\epsilon(\tau) = -1$ dès que τ est une transposition. Soit τ_{ij}, la transposition (i,j) et $\theta = (i, i+1, \dots, j-1)$ alors le lemme 1.283 dit que

$$\tau_{ij} = \theta\tau_{j-1,j}\theta^{-1}. \tag{1.395}$$

La signature étant un homomorphisme,

$$\epsilon(\tau_{ij}) = \epsilon(\theta)\epsilon(\tau_{j-1,j})\epsilon(\theta)^{-1} = \epsilon(\tau_{j-1,j}) = -1. \tag{1.396}$$

Nous passons maintenant à la partie unicité de la proposition. 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[110]). Si τ' est une autre transposition, il existe $\sigma \in S_n$ tel que $\tau' = \sigma\tau\sigma^{-1}$ (lemme 1.283). Dans ce cas, $\varphi(\tau') = \varphi(\tau) = -1$, et si $\sigma = (\tau_1 \dots \tau_k)$,

$$\varphi(\sigma) = (-1)^k = \epsilon(\sigma). \tag{1.397}$$

□

Corolaire 1.294.
Si $\sigma \in S_n$, alors

$$\epsilon(\sigma) = \epsilon(\sigma^{-1}). \tag{1.398}$$

Démonstration. Comme énoncé par la proposition 1.293, ϵ est un homomorphisme, donc

$$\epsilon(\sigma)\epsilon(\sigma^{-1}) = \epsilon(\sigma\sigma^{-1}) = \epsilon(\mathrm{Id}) = 1. \tag{1.399}$$

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. □

1.13.3 Permutation un peu ordonnées

Lemme 1.295 ([1]).
Deux énoncés.

(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 $\epsilon(\tau) = \epsilon(\pi)$.

(2) L'application

$$\begin{aligned} \varphi\colon \{\pi \in S_k \text{ tel que } \pi(1) = 1\} &\to S_{k-1} \\ \pi &\mapsto \Big[\tau(i) = \pi(i+1) - 1\Big] \end{aligned} \tag{1.400}$$

est une bijection.

110. Nous utilisons ici le fait que tous les éléments de S_n sont des produits de transpositions, proposition 1.288.

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 1.288) :

$$\pi = \sigma_1 \circ \dots \circ \sigma_n. \tag{1.401}$$

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

$$\begin{aligned} \psi\colon \{2,\dots,k\} &\to \{1,\dots,k-1\} \\ i &\mapsto i-1. \end{aligned} \tag{1.402}$$

En termes de ψ, la définition de τ s'écrit $\psi(\pi) = \psi \circ \pi \circ \psi^{-1}$, et nous avons

$$\tau = \psi \circ \pi \circ \psi^{-1} \tag{1.403a}$$
$$= \psi \circ \sigma_1 \circ \dots \circ \sigma_n \circ \psi^{-1} \tag{1.403b}$$
$$= \psi \circ \sigma_1 \circ \psi^{-1} \circ \psi \circ \sigma_2 \circ \dots \circ \psi \circ \sigma_n \circ \psi^{-1}. \tag{1.403c}$$

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.

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

$$(\psi\sigma\psi^{-1})(i) = \psi\sigma\big(\psi^{-1}(i)\big) = \psi\big(\psi^{-1}(i)\big) = i. \tag{1.404}$$

Donc la décomposition $\tau = \sigma_1' \circ \dots \circ \sigma_n'$ 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).

(i) **Injectif** Supposons que $\varphi(\pi) = \varphi(\sigma)$. Alors pour tout $i = 1,\dots,k-1$ nous avons

$$\pi(i+1) - 1 = \sigma(i+1) - 1, \tag{1.405}$$

c'est-à-dire $\pi(j) = \sigma(j)$ pour tout $j = 2,\dots,k$. Vu que $\pi(1) = \sigma(1)$ nous avons bien $\pi = \sigma$.

(ii) **Surjectif** Soit $\tau \in S_{k-1}$. En posant

$$\pi(i) = \begin{cases} 1 & \text{si } i = 1 \\ \tau(i-1)+1 & \text{sinon,} \end{cases} \tag{1.406}$$

nous avons bien $\tau = \varphi(\pi)$.

□

Définition 1.296 ([1, 61]).
Nous notons

$$S_{(k,l)} = \{\pi \in S_{k+l} \text{ tel que } \pi(1) < \dots \pi(k),\ \pi(k+1) < \dots < \pi(k+l)\}, \tag{1.407}$$

et

$$A_{(k,l)} = \{\pi \in S_{(k,l)} \text{ tel que } \pi(1) = 1\}. \tag{1.408}$$

Lemme 1.297 ([1]).
Deux énoncés.

(1) Soit $\pi \in A_{(k,l)}$. En posant $\tau(i) = \pi(i+1) - 1$ nous avons $\tau \in S_{(k-1,l)}$.

(2) *L'application*

$$\begin{aligned}\varphi\colon A_{(k,l)} &\to S_{(k-1,l)}\\ \pi &\mapsto \Big[\tau(i) = \pi(i+1) - 1\Big]\end{aligned} \tag{1.409}$$

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

$$\tau(i) = \pi(i+1) - 1 < \pi(i+j) - 1 = \tau(j) \tag{1.410}$$

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 1.295. □

1.14 Corps

La définition d'un corps est 1.202.

1.14.1 Définitions, morphismes

La proposition suivante donne une caractérisation d'un corps, en disant un tout petit peu plus que la définition 1.202.

Proposition 1.298.
L'anneau A *est un corps si et seulement si* $U(A) = A^*$.

Démonstration. En deux parties.

(i) **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 1.173 couplé à la proposition 1.174 : $a \cdot 0 = 0 \neq 1$ pour tout a.

(ii) **Sens inverse** Si $U(A) = A^*$, nous avons immédiatement que tous les éléments non nuls sont inversibles et donc que A est un corps.

□

Lemme 1.299.
Si $\mathbb{K}$ *est un corps et si* $a \in \mathbb{K}$ *vérifie* $a^2 = 1$, *alors* $a = \pm 1$.

Définition 1.300 (Morphisme de corps)**.**
Un corps étant un anneau sans plus de structure, un ***morphisme de corps*** *n'est qu'un morphisme des anneaux*[111].

Le lemme suivant montre que définir un morphisme de corps comme étant simplement un morphisme des anneaux est une bonne idée.

Lemme 1.301.
Si $\varphi\colon \mathbb{K} \to \mathbb{K}'$ *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

$$1 = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}). \tag{1.411}$$

111. Définition 1.40.

Donc, par unicité de l'inverse[112], $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Pour l'injectivité nous supposons $\varphi(a) = \varphi(b)$. Étant donné que $\mathbb{K}'$ est un corps, nous pouvons multiplier par $\varphi(b)^{-1}$:

$$\varphi(a)\varphi(b)^{-1} = 1. \tag{1.412}$$

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 $a = b$. □

1.15 Symbole de sommation

1.15.1 Somme à valeurs dans un groupe commutatif

Si S est un ensemble fini, nous savons de la proposition 1.121 qu'il existe un unique $N \in \mathbb{N}$ pour lequel il existe une bijection $\varphi\colon \{0,\dots,N\} \to S$. Cette bijection n'est à priori pas unique.

Lemme-Définition 1.302 ([1]).
Soient un groupe commutatif $(G,+)$ ainsi qu'un ensemble fini I contenant n éléments. Soit une application $f\colon I \to G$. Si $\sigma_1,\sigma_2\colon \{1,\dots,n\} \to I$ sont deux bijections, alors[113]

$$\sum_{i=1}^{n} f\big(\sigma_1(i)\big) = \sum_{i=1}^{n} f\big(\sigma_2(i)\big). \tag{1.413}$$

La valeur commune est notée

$$\sum_{i\in I} f(i) \tag{1.414}$$

Démonstration. Nous commençons par considérer une transposition σ (qui permute k et l avec $k<l$). Nous avons

$$\sum_{i=1}^{n} f(i) = \sum_{i=1}^{k-1} f(i) + f(k) + \sum_{i=k+1}^{l-1} f(i) + f(l) + \sum_{i=l+1}^{n} f(i) \tag{1.415a}$$

$$= \sum_{i=1}^{k-1} f(i) + f(l) + \sum_{i=k+1}^{l-1} f(i) + f(k) + \sum_{i=l+1}^{n} f(i) \tag{1.415b}$$

$$= \sum_{i=1}^{n} f\big(\sigma(i)\big). \tag{1.415c}$$

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 1.288). Donc pour toute permutation σ nous avons

$$\sum_{i=1}^{n} f\big(\sigma(i)\big) = \sum_{i=1}^{n} f(i). \tag{1.416}$$

□

La définition 1.302 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 52.

112. Lemme 1.158 (2).
113. Pour rappel, le symbole $\sum_{i=1}^{n}$ est défini par 1.82.

Proposition 1.303.
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

$$\sum_{i\in I} f(i)=\sum_{i\in I} f\big(\sigma(i)\big). \tag{1.417}$$

Si nous avons une application $L\colon S\to S$, nous notons

$$\sum_{s\in S} f\big(L(s)\big)=\sum_{s\in S}(f\circ L)(s). \tag{1.418}$$

Cette façon d'écrire donne une interprétation pour la notation $\sum_{g\in G} f(hg)$ qui arrive dans la proposition 1.306. Il s'agit de considérer l'application L_h du lemme 1.161, de considérer [114]

$$\sum_{g\in G} f(hg)=\sum_{g\in G}(f\circ L_h)(g) \tag{1.419}$$

et de faire tourner la définition 1.302. La même chose tient pour définir $\sum_{g\in G}(gh)$ à l'aide de R_h.

Lemme 1.304 (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

$$\sum_{i\in I} f(i)=\sum_{j\in J} f\big(\varphi^{-1}(j)\big). \tag{1.420}$$

Lemme 1.305.
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

$$\sum_{a\in A} f(a)=\sum_{k=1}^{n}\sum_{a\in A_k} f(a). \tag{1.421}$$

Démonstration. Le lemme 1.114 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 1.121).

Nous avons $\mathrm{Card}(A)=S_n$ par le lemme 1.123(4). Nous définissons une belle bijection comme il faut :

$$\begin{aligned}\alpha\colon\{1,\dots,S_n\}&\to A\\ i&\mapsto\varphi_{k+1}(i-S_k)\end{aligned} \tag{1.422}$$

pour $i\in\,]S_k,S_{k+1}]$.

(i) 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 $i-S_k$.

(ii) 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

$$\varphi_{k+1}(i-S_k)=\varphi_{k+1}(j-S_k). \tag{1.423}$$

Étant donné que φ_{k+1} est injective, nous avons $i-S_k=j-S_k$, ce qui montre que $i=j$.

(iii) 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 $s+S_k\in\,]S_{k-1},S_k]$.

114. Le fait que L_h soit une bijection n'a pas d'importance ici.

Vu que α est une bijection, nous avons l'égalité

$$\sum_{a\in A} f(a) = \sum_{i=1}^{S_n} (f\circ\alpha)(i). \tag{1.424}$$

Nous avons encore besoin d'introduire une bijection. Nous posons

$$\begin{aligned} \beta_k\colon]S_{k-1}, S_k] &\to A_k \\ i &\mapsto \varphi_k(i-S_{k-1}). \end{aligned} \tag{1.425}$$

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 :

$$\sum_{a\in A} f(a) = \sum_{i=1}^{S_n} (f\circ\alpha)(i) \tag{1.426a}$$

$$= \sum_{k=1}^{n} \left(\sum_{i=S_{k-1}-1}^{S_k} (f\circ\alpha)(i) \right) \tag{1.426b}$$

$$= \sum_{k=1}^{n} \left(\sum_{i\in]S_{k-1},S_k]} f\big(\varphi_k(i-S_{k-1})\big) \right) \tag{1.426c}$$

$$= \sum_{k=1}^{n} \left(\sum_{i\in]S_{k-1},S_k]} f\big(\beta_k(i)\big) \right) \tag{1.426d}$$

$$= \sum_{i=1}^{n} \left(\sum_{a\in A_k} f(a) \right). \tag{1.426e}$$

Justifications :

— Pour (1.426b). Associativité de la somme.

□

Proposition 1.306 ([1])**.**
Soient un groupe fini G et une fonction $f\colon G\to A$ où A est un anneau commutatif. Alors

$$\sum_{g\in G} f(g) = \sum_{g\in G} f(gh) = \sum_{g\in G} f(hg) \tag{1.427}$$

pour tout $h\in G$.

Démonstration. Nous avons une bijection $\varphi\colon\{0,\dots,N\}\to G$ garantie par la proposition 1.121. Sa définition est

$$\sum_{g\in G} f(g) = \sum_{i=0}^{N} f\big(\varphi(i)\big). \tag{1.428}$$

Par ailleurs, le lemme 1.161 donne une bijection $L_h\colon G\to G$ et permet de considérer la composée

$$\begin{aligned} \varphi'\colon \{0,\dots,N\} &\to G \\ \varphi' &= L_h\circ\varphi. \end{aligned} \tag{1.429}$$

La proposition 1.302 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 (1.419) donne

$$\begin{aligned} \sum_{g\in G} f(g) &= \sum_{i=0}^{N} f\big(\varphi(i)\big) = \sum_{i=0}^{N} f\big(\varphi'(i)\big) = \sum_{i=0}^{N} (f\circ L_h\circ\varphi)(i) \\ &= \sum_{i=0}^{N} (f\circ L_h)\big(\varphi(i)\big) = \sum_{g\in G} (f\circ L_h)(g) = \sum_{g\in G} f(hg). \end{aligned} \tag{1.430}$$

En ce qui concerne $\sum_{g\in G} f(gh)$, c'est la même chose, en utilisant R_h au lieu de L_h. □

Lemme 1.307.
Soit un groupe totalement ordonné[115] $(A,+,\leqslant)$. *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*

$$\sum_{i=0}^{n}a_i\leqslant\sum_{i=0}^{n}b_i. \tag{1.431}$$

Tout cela nous permet de définir une somme sympathique et bien connue.

Lemme 1.308.
Soit $n\in\mathbb{N}$. *Nous avons*

$$\sum_{k=0}^{n}k=\frac{n(n+1)}{2}. \tag{1.432}$$

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 1.302 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

$$S=\sum_{k=0}^{n}k=\sum_{k=0}^{n}(n-k). \tag{1.433}$$

Donc

$$2S=\sum_{k=0}^{n}\big(k+(n-k)\big)=\sum_{k=0}^{n}n=n\sum_{k=0}^{n}1=n(n+1). \tag{1.434}$$

En divisant par deux, nous obtenons le résultat annoncé. □

1.16 Symbole de produit

1.309.
Si $(G,\ \cdot\ )$ est un groupe et si $H\subset G$, nous notons le produit des éléments de H par

$$\prod_{g\in H}g=\sum_{g\in H}g \tag{1.435}$$

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 1.82(1) signifie qu'une somme vide vaut zéro : $\sum_{x\in\emptyset}x=0$. Vu que zéro est la façon usuelle de noter le neutre pour une opération notée « + », lorsque l'opération est notée $\cdot$ nous avons

$$\prod_{x\in\emptyset}x=1 \tag{1.436}$$

parce que 1 est la façon usuelle de noter le neutre d'une opération notée « $\cdot$ ».

Notez que (1.436) n'est pas une nouvelle définition ou une nouvelle convention. C'est seulement l'égalité $\sum_{x\in\emptyset x}x=0$, avec des notations adaptées à un groupe dont l'opération est notée multiplicativement.

115. Définition 1.162.

Proposition 1.310.
Si E est un ensemble fini et si G est un groupe commutatif, alors pour toute fonction $f : E \to G$ et pour toute permutation[116] *σ de E,*

$$\prod_{i\in E} f(i) = \prod_{i\in E} f\big(\sigma(i)\big) \tag{1.437}$$

Démonstration. C'est exactement la proposition 1.302, sauf qu'ici la loi de groupe est notée multiplicativement au lieu d'additivement. □

1.16.1 Sous-groupe engendré

Définition 1.311 (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* $\mathrm{gr}_G(A)$.

Lorsque A est fini (disons $A = \{a_1, \dots, a_n\}$), on note aussi le sous-groupe engendré $\langle a_1, \dots, a_n\rangle$.

1.312.
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[117].

1.313.
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 1.314.
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 1.315.
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 $\mathrm{gr}(A)$. □

Lemme 1.316 ([62])**.**
Si A est une partie du groupe G, alors le sous-groupe $\mathrm{gr}(A)$ *engendré*[118] *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*[119]

$$\prod_{i=1}^{n} g_i^{a_i} \tag{1.438}$$

où $a_i \in \mathbb{Z}$ et $g : \mathbb{N} \to A$ n'est pas spécialement injective : il peut arriver que $g_i = g_j$.

116. Une permutation est une bijection, définition 1.267.
117. Demandez-vous si il est possible que $\mathrm{gr}(\varnothing)$ contienne d'autres éléments que e.
118. Définition 1.311.
119. 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.

Démonstration. Puisqu'un produit vide est égal à l'identité [120], le lemme est vrai (un peu trivialement) dans le cas où $A = \emptyset$. À partir de maintenant, nous supposons que A est non vide.

Nous nommons $\text{gr}(A)$ le groupe engendré par A et H, l'ensemble

$$H = \{g_1 \dots g_n \text{ tel que } g_i \in A \cup A^{-1}\}. \tag{1.439}$$

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 [121].

Comme H est un groupe contenant A, nous avons $\text{gr}(A) \subset H$ parce que $\text{gr}(A)$ est une intersection dont un des éléments est H.

Par ailleurs tout groupe contenant A doit contenir les inverses et les produits finis, donc $H \subset \text{gr}(A)$.

Au final, $H = \text{gr}(A)$, ce qu'il fallait. □

Lemme 1.317.
Soit un groupe G et un sous-groupe $H = \text{gr}(h_1, \dots, h_n)$. Si $\alpha \in G$, alors

$$\alpha H \alpha^{-1} = \text{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1}). \tag{1.440}$$

Démonstration. Il s'agit d'une conséquence du lemme 1.316. Un élément de $\text{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1})$ 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

$$\alpha h_i \alpha^{-1} \alpha h_j \alpha^{-1} = \alpha h_i h_j \alpha^{-1} \in \alpha H \alpha^{-1}. \tag{1.441}$$

Donc

$$\text{gr}(\alpha h_1 \alpha^{-1}, \dots, \alpha h_n \alpha^{-1}) \subset \alpha H \alpha^{-1}. \tag{1.442}$$

L'inclusion dans l'autre sens est du même tonneau. □

Définition 1.318 (Partie génératrice, groupe monogène)**.**
Soient un groupe G, et une partie $A \subset G$. Si $\text{gr}(A) = G$, 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.*

Définition 1.319 (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****.*

1.320.
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 1.321.
Soit le groupe $\big(\mathbb{Z}/10\mathbb{Z}, +\big)$. L'élément $[2]_{10}$ n'est pas générateur parce que ses puissances [122] sont

$$\text{gr}([2]_{10}) = \{[2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}, [0]_{10}\}. \tag{1.443}$$

Par contre l'élément $[3]_{10}$ est générateur : ses puissances sont dans l'ordre

$$[3]_{10}, [6]_{10}, [9]_{10}, [2]_{10}, [5]_{10}, [8]_{10}, [1]_{10}, [4]_{10}, [7]_{10}, [0]_{10}. \tag{1.444}$$

△

120. Voir 1.309.
121. Et c'est ici qu'on se rend compte que la décomposition n'est probablement que rarement unique.
122. 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.

Un exemple presque identique, mais un peu masqué sera l'exemple 18.158.

Lemme 1.322 ([1]).
Si $n = dr$, alors

(1) $r\mathbb{Z}/n\mathbb{Z}$ *est un groupe.*

(2) Le groupe $r\mathbb{Z}/n\mathbb{Z}$ *est cyclique*[123].

(3) $\text{Card}(r\mathbb{Z}/n\mathbb{Z}) = d = n/r$.

1.17 Module sur un anneau

Définition 1.323 (module sur un anneau[63]).
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*[124].

(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 $\text{Hom}_A(M, N)$. *Si B st une sous-anneau de A, nous parlons de* $\text{Hom}_B(M, N)$ *pour parler des morphismes de groupes qui ne vérifient $f(a \cdot x) = a \cdot f(x)$ que pour $a \in B$.*

Proposition 1.324.
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 :

$$(1 + 1) \cdot (x + y) = 1 \cdot (x + y) + 1 \cdot (x + y) = x + y + x + y \tag{1.445}$$

d'une part et

$$(1 + 1) \cdot (x + y) = (1 + 1) \cdot x + (1 + 1) \cdot y = x + x + y + y, \tag{1.446}$$

d'autre part. En égalant les deux expressions, il vient

$$x + y + x + y = x + x + y + y, \tag{1.447}$$

qui se simplifie (nous sommes dans un groupe) en $y + x = x + y$. □

Définition 1.325.
Un ***espace vectoriel*** *est un module*[125] *sur un corps commutatif*[126].

123. Définition 1.319.
124. Nous verrons dans la proposition 1.324 qu'il est forcément commutatif.
125. Définition 1.323.
126. La condition de commutativité n'est pas indispensable, mais comme nous ne parlerons que de corps commutatifs...

Définition 1.326 ([64]).
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*

$$\sum_{j\in J} a_j m_j = 0, \tag{1.448}$$

alors $a_j = 0$ pour tout j.

Définition 1.327 ([65]).
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*

$$\sum_{t\in T} a_t t \tag{1.449}$$

où T est fini dans S et $a_t \in A$.

1.17.1 Module produit

Lemme-Définition 1.328 ([64]).
*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 :

$$A^I = \{(a_i)_{i\in I}, a_i \in A\}. \tag{1.450}$$

L'ensemble A^I devient un module par les définitions, pour $x, y \in A^I$ et $a \in A$:

$$ax = (ax_i)_{i\in I} \tag{1.451a}$$
$$x + y = (x_i + y_i)_{i\in I}. \tag{1.451b}$$

En d'autres termes, $A^I = \mathrm{Fun}(I, A)$.

Démonstration. Il faut vérifier toutes les conditions de la définition 1.323. En guise d'exemple, nous vérifions la distributivité. Soient $a \in A$ et $x, y \in A^I$. Nous avons

$$\big[a \cdot (x + y)\big]_i = a(x + y)_i \qquad (1.451a) \tag{1.452a}$$
$$= a(x_i + y_i) \qquad (1.451b) \tag{1.452b}$$
$$= ax_i + ay_i \qquad \text{distrib. dans } A \tag{1.452c}$$
$$= (ax + ay)_i \qquad (1.451b). \tag{1.452d}$$

□

Lemme 1.329.
Pour chaque $i \in I$ nous considérons l'élément $e_i \in A^I$ donné par

$$e_i \colon I \to A$$
$$j \mapsto \begin{cases} 1 & \text{si } j = i \\ 0 & \text{sinon.} \end{cases} \tag{1.453}$$

La famille $\{e_i\}_{i\in I}$ est libre[127] *dans A^I.*

127. Définition 1.326.

Démonstration. Soient J fini dans I ainsi que des éléments $a_j \in A$ ($j \in J$). Nous supposons que[128] $\sum_{j\in J} a_j e_j = 0$. Calculons un peu :

$$\sum_{j\in J} a_j e_j = \sum_{j\in J} (a_j\delta_{ji})_{i\in I} = \left(\sum_{j\in J} a_j\delta_{ji} \right)_{i\in I}. \tag{1.454}$$

Pour que le tout soit nul dans A^I, il faut que

$$\sum_{j\in J} a_j\delta_{ji} \tag{1.455}$$

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 $a_i = 0$. □

Définition 1.330.
Nous notons $A^{(I)}$ le sous-module de A^I engendré[129] *par les e_i.*

Lemme 1.331 ([1])**.**
L'ensemble $A^{(I)}$ est l'ensemble des applications $I \to A$ de support fini.

Démonstration. En deux sens.

(i) **Si $x \in A^{(I)}$** Pour rappel, la définition 1.328 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

$$x = \sum_{j\in J} x_j e_j. \tag{1.456}$$

Pour $i \in I$ nous avons

$$x(i) = \sum_{j\in J} x_j\delta_{ij} = \begin{cases} x_i & \text{si } i \in J \\ 0 & \text{sinon.} \end{cases} \tag{1.457}$$

Donc le support de x est dans J qui est fini. Vu que toute partie d'un ensemble fini est fini (lemme 1.114), le support de x est fini.

(ii) **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

$$x = \sum_{j\in J} x_j e_j. \tag{1.458}$$

□

Théorème 1.332 (Propriété universelle de $A^{(I)}$[64])**.**
Soient un anneau A ainsi qu'un A-module P. Pour $\phi \in \mathrm{Hom}_A(A^{(I)}, P)$, nous considérons

$$\begin{aligned} \phi|_I\colon I &\to P \\ i &\mapsto \phi(e_i). \end{aligned} \tag{1.459}$$

(1) L'application

$$\begin{aligned} f\colon \mathrm{Hom}_A(A^{(I)}, P) &\to \mathrm{Fun}(I, P) \\ \phi &\mapsto \phi|_I \end{aligned} \tag{1.460}$$

est une bijection.

(2) L'application inverse est $g\colon \mathrm{Fun}(I, P) \to \mathrm{Hom}_A(A^{(I)}, P)$ donnée par

$$g(\psi)\big(\sum_{j\in J} a_j e_j\big) = \sum_{j\in J} a_j\psi(j) \tag{1.461}$$

pour tout J fini dans I et choix de $a_j \in A$.

128. Pour rappel, les sommes finies sont définies par 1.302.
129. Définition 1.327.

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 :

$$g\big(f(\phi)\big)\big(\sum_j a_j e_j\big) = \sum_j a_j f(\phi)(j) \tag{1.462a}$$
$$= \sum_j a_j \phi(e_j) \tag{1.462b}$$
$$= \phi(\sum_j a_j e_j). \tag{1.462c}$$

Justifications :

— Pour (1.462b), nous avons utilisé le fait que $f(\phi)(i) = \phi|_I(i) = \phi(e_i)$.

— Pour (1.462c), nous utilisons le fait que ϕ est un morphisme de modules.

Et pour l'autre sens,

$$f\big(g(\psi)\big)(i) = g(\psi)(e_i) = \psi(i). \tag{1.463}$$

Vérifions que cela est suffisant pour que f soit une bijection.

(i) **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.

(ii) **Injectif** Supposons que $f(\phi_1) = f(\phi_2)$. Alors en appliquant g des deux côtés, il vient $\phi_1 = \phi_2$.

□

1.17.2 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

$$\begin{aligned} \mu_x \colon A^{(I)} &\to M \\ (a_i)_{i\in I} &\mapsto \sum_{i\in I} a_i x_i. \end{aligned} \tag{1.464}$$

Ici $A^{(I)}$ désigne l'ensemble de toutes les applications $I \to A$ de support fini (définition 1.330).

Définition 1.333.
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 1.334.
*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 1.335.
Un anneau A est lui-même un A-module et ses sous-modules sont les idéaux. △

Définition 1.336.
*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 $\sum_{i\in I} p_i = \mathbb{1}$.*

Théorème 1.337.
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

$$p_i(x_1 + \dots + x_n) = x_i \tag{1.465}$$

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

$$M = \bigoplus_{i=1}^{n} p_i(M). \tag{1.466}$$

Définition 1.338.
*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 1.339.
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 $\mathcal{E}$. △

Définition 1.340 (Algèbre[66])**.**
Si $\mathbb{K}$ est un corps commutatif[130]*, une $\mathbb{K}$-**algèbre** A est un espace vectoriel*[131] *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 $x \times y$.

Lemme 1.341 ([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. □

Définition 1.342.
*L'**algèbre engendrée** par X est l'intersection de toutes les sous-algèbres de A contenant X (qui est une algèbre par le lemme 1.341).*

130. Définition 1.202
131. Définition 1.325.

1.18 Caractéristique d'un anneau

Lemme-Définition 1.343.
Soit l'application

$$\begin{aligned}\mu\colon \mathbb{Z} &\to A\\ n &\mapsto n\cdot 1_A\end{aligned} \tag{1.467}$$

où $n\cdot 1_A$ signifie $\sum_{k=1}^{n} 1_A$.

(1) C'est un morphisme d'anneaux.

(2) Le noyau est un sous-groupe de $\mathbb{Z}$

(3) Il existe un unique $p\in\mathbb{Z}$ tel que $\ker(\mu)=p\mathbb{Z}$.

*Ce p est la **caractéristique** de A.*

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 9.215.

Lemme 1.344.
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. □

Lemme 1.345.
Soit un anneau A de caractéristique p.

(1) Si $p>0$, alors nous avons l'isomorphisme d'anneaux

$$\mathbb{Z}1_A\simeq\mathbb{Z}/p\mathbb{Z}. \tag{1.468}$$

(2) Si $p=0$, alors nous avons l'isomorphisme d'anneaux

$$\mathbb{Z}1_A\simeq\mathbb{Z} \tag{1.469}$$

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. □

Proposition 1.346.
La caractéristique d'un anneau fini divise son cardinal.

Démonstration. Si A est un anneau, le groupe $\mathbb{Z}$ agit sur A par

$$n\cdot a=a+n1_A. \tag{1.470}$$

Chaque orbite de cette action est de la forme

$$\mathcal{O}_a=\{a+n1_A \text{ tel que } n=0,\dots,p-1\} \tag{1.471}$$

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. □

Lemme 1.347 ([67]).
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 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

Proposition 1.348.
Soit A un anneau commutatif unitaire de caractéristique p. L'application

$$\begin{aligned} \mathrm{Frob}_A\colon A &\to A \\ x &\mapsto x^p \end{aligned} \tag{1.472}$$

est un automorphisme d'anneau unitaire.

Nous le nommons le **morphisme de Frobenius**. Nous utiliserons aussi les itérés du morphisme de Frobenius : $\mathrm{Frob}^k\colon x \mapsto x^{p^k}$.

Exemple 1.349.
Soit à factoriser $X^p - 1$ dans $\mathbb{F}_p$. Grâce au morphisme de Frobenius, nous avons immédiatement

$$X^p - 1 = (X - 1)^p. \tag{1.473}$$

△

Lemme 1.350.
La caractéristique[132] *d'un anneau intègre est zéro ou un élément premier*[133].

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 1.236 dit que $\mathbb{Z}/p\mathbb{Z}$ est intègre si et seulement si p est premier, ce qui conclut la preuve. □

Exemple 1.351.
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 :

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = 0. \tag{1.474}$$

△

1.18.1 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 9.3.

1.19 Polynômes

1.19.1 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[134].

L'ensemble des polynômes sur A sera simplement $A^{(\mathbb{N})}$ (notation 1.330). 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.

132. Définition 1.343.
133. Définition 1.182.
134. Pour les polynômes à plusieurs variables, voir la définition 3.45.

Définition 1.352.
*L'ensemble des **polynômes** en une indéterminée sur l'anneau A est l'anneau*

$$\mathcal{P}(A) = A^{(\mathbb{N})} \tag{1.475}$$

défini en 1.330.

1.353.
En ce qui concerne la notation $A[X]$, voir 1.19.2. Pour $\mathbb{K}(X)$ lorsque $\mathbb{K}$ est un corps, voir 6.83.

Proposition-Définition 1.354 ([68]).
Soit P non nul dans $\mathcal{P}(A)$. Nous notons a_n la valeur[135] *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*

$$\deg(P) = \max\{n \in \mathbb{N} \text{ tel que } a_n \neq 0\}, \tag{1.476}$$

*et la **valuation** de P est*

$$\mathrm{val}(P) = \min\{n \text{ tel que } a_n \neq 0\}. \tag{1.477}$$

Nous notons

$$\mathcal{P}_n(A) = \{P \in \mathcal{P}(A) \text{ tel que } \deg(P) \leqslant n\}, \tag{1.478}$$

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

$$\mathrm{val}(0) = +\infty \tag{1.479a}$$
$$\deg(0) = -\infty. \tag{1.479b}$$

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 1.62), le lemme 1.63 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 $P = \sum_{i=1}^{n} a_i e_i$.

Définition 1.355.
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*

$$P(\alpha) = (\sum_{i=0}^{n} a_i e_i)(\alpha) = \sum_{i=0}^{n} a_i \alpha^i, \tag{1.480}$$

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 (1.480).

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*

$$(PQ)_n = \sum_{k=0}^{n} P_k Q_{n-k}, \tag{1.481}$$

135. 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 formule du type $P(x) = \sum_n a_n x^n$. D'ailleurs nous n'avons pas encore vu cette évaluation.

et donc $PQ = \sum_i (PQ)_i e_i$. *Plus explicitement,*

$$(\sum_{i=0}^{n} a_i e_i)(\sum_{j=0}^{m} b_j e_j) = \sum_{k=0}^{\infty} \Big(\sum_{\substack{(i,j)\in\mathbb{N}^2 \\ i+j=k}} a_i b_j \Big) e_k. \tag{1.482}$$

Notons qu'à droite, la somme sur k *est une somme finie.*

Proposition 1.356.
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

$$\begin{aligned} g\colon A^{(\mathbb{N})} &\to A \\ P &\mapsto P(\alpha) \end{aligned} \tag{1.483}$$

est un morphisme d'anneaux[136]. *En particulier,* $(PQ)(\alpha) = P(\alpha)Q(\alpha)$.

Démonstration. En plusieurs points

(i) **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 (1.482). La distributivité aussi[137].

(ii) **Le morphisme** Nous notons P_k les éléments de la suite définissant P et Q_k ceux de Q. Alors nous avons

$$(P+Q)(\alpha) = \sum_k (P_k + Q_k)\alpha^k = \sum_k P_k\alpha^k + \sum_k Q_k\alpha^k = P(\alpha) + Q(\alpha). \tag{1.484}$$

Vous aurez noté que la première égalité était la définition (1.451b). De même,

$$P(\alpha)Q(\alpha) = \big(\sum_n P_n\alpha^n\big)\big(\sum_k Q_k\alpha^k\big) = \sum_k Q_k\big(\sum_n P_n\alpha^n\big)\alpha^k = \sum_k\sum_n Q_k P_n \alpha^{n+k} \tag{1.485a}$$

$$= \sum_m \big(\sum_{l=0}^{m} P_l Q_{m-l}\big)\alpha^m = \sum_m (PQ)_m\alpha^m = (PQ)(\alpha). \tag{1.485b}$$

□

Lemme 1.357.
Si A *est commutatif, alors* $A^{(\mathbb{N})}$ *est commutatif.*

Démonstration. Soient $P, Q \in A^{(\mathbb{N})}$; pour rappel, le produit est donné par la définition 1.481. L'application

$$\begin{aligned} \varphi\colon \{0,\dots,n\} &\to \{0,\dots,n\} \\ k &\mapsto n-k \end{aligned} \tag{1.486}$$

est une bijection. Voici maintenant le calcul :

$$(PQ)_n = \sum_{k=0}^{n} P_k Q_{n-k} \tag{1.487a}$$

$$= \sum_{k=0}^{n} P_{\varphi(k)} Q_{n-\varphi(k)} \tag{1.487b}$$

$$= \sum_{k=0}^{n} P_{n-k} Q_k \tag{1.487c}$$

$$= \sum_{k=0}^{n} Q_k P_{n-k} \tag{1.487d}$$

$$= (QP)_n. \tag{1.487e}$$

136. Définition 1.40.
137. Je n'ai pas fait les calculs, écrivez-moi pour me dire si ça va facilement.

Justifications

— Pour (1.487b). Lemme 1.302 et le fait que φ soit une bijection.

— Pour (1.487d). Commutativité de A.

□

1.19.2 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 1.356.

Le polynôme donné par la suite $(a_n)_{n\in\mathbb{N}}$ est souvent notée

$$\sum_k a_k X^k. \tag{1.488}$$

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.

1.19.2.1 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.

1.19.2.2 Seconde façon (la bonne)

1.358.
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 1.355 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.

Lemme 1.359.
Nous avons

$$P(X) = P \tag{1.489}$$

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

$$\sum_k a_k X^k, \tag{1.490}$$

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 $P=X^2+2X-3$.

1.19.3 Action du groupe symétrique

Définition 1.360 (Thème 9)**.**
*Une **action de groupe** G sur un ensemble E est la donnée, pour chaque élément $g\in G$, d'une fonction $\phi_g : E\to E$, de telle sorte que :*

$$\begin{aligned}\phi_e(x)&=x, &&\forall x\in E;\\ \phi_{gh}(x)&=\phi_g(\phi_h(x)), &&\forall g,h\in G,\forall x\in E.\end{aligned}$$

*On dit dans ce cas que G **agit** sur E.*

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 1.332 nous donne une application

$$g\colon \operatorname{Fun}\big(\mathbb{N}^n,\mathcal{P}_n(A)\big)\to \operatorname{Hom}_A\big(\mathcal{P}_n(A),\mathcal{P}_n(A)\big) \tag{1.491}$$

Avec cela nous pouvons énoncer et démontrer le lemme qui donne l'action de S_n [138] sur $\mathcal{P}_n(A)$.

Lemme 1.361 ([69])**.**
Pour $\sigma\in S_n$ nous définissons

$$\begin{aligned}\phi_\sigma\colon \mathbb{N}^n&\to\mathcal{P}_n(A)\\ m&\mapsto e_{\sigma(m)}.\end{aligned} \tag{1.492}$$

Alors l'application

$$\begin{aligned}\rho\colon S_n&\to\operatorname{Hom}_A\big(\mathcal{P}_n(A),\mathcal{P}_n(A)\big)\\ \sigma&\mapsto g(\phi\sigma)\end{aligned} \tag{1.493}$$

est une action [139].

Démonstration. Nous commençons par donner une expression à notre ρ. Un élément de $\mathcal{P}_n(A)$ est de la forme $\sum_{m\in\mathbb{N}^n}a_me_m$, et nous avons [140]

$$\rho(\sigma)\Big(\sum_{m\in\mathbb{N}^n}a_me_m\Big)=\sum_m a_m\phi_\sigma(m)=\sum_m a_me_{\sigma(m)}. \tag{1.494}$$

Nous avons tout de suite $\rho(\mathrm{Id})=\mathrm{Id}$.

En ce qui concerne la composition, nous avons d'une part

$$\rho(\sigma_1\sigma_2)\Big(\sum_m a_me_m\Big)=g(\phi_{\sigma_1\sigma_2})\Big(\sum_m a_me_m\Big)=\sum_m a_me_{\sigma_1\sigma_2(m)}, \tag{1.495}$$

et d'autre part,

$$\begin{aligned}\rho(\sigma_1)\rho(\sigma_2)\Big(\sum_m a_me_m\Big)&=\rho(\sigma_1)\Big(\sum_m a_me_{\sigma_2(m)}\Big) &&\text{(1.496a)}\\ &=\rho(\sigma_1)\Big(\sum_m a_{\sigma_2^{-1}(m)}e_m\Big) &&\text{(1.496b)}\\ &=\sum_m a_{\sigma_2^{-1}(m)}e_{\sigma_1(m)} &&\text{(1.496c)}\\ &=\sum_m a_me_{\sigma_1\sigma_2(m)} &&\text{(1.496d)}\end{aligned}$$

La proposition 1.303 est utilisée pour (1.496b) et pour (1.496d). □

138. Définition du groupe symétrique S_n en 1.267.
139. Définition 1.360.
140. La somme est définie par 1.302, 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.

1.19.4 Corps des fractions

Définition 1.362 ([70]).
Soit un anneau commutatif et intègre[141] A. *Nous posons* $E = A \times A\backslash\{0\}$, *et nous définissons les deux opérations suivantes sur* E :

(1) $(a,b) + (c,d) = (ad + cb, bd)$;

(2) $(a,b)(c,d) = (ac, bd)$.

Et aussi la relation d'équivalence $(a,b) \sim (c,d)$ *si et seulement si* $ad = bc$.

Le ***corps des fractions*** *de* A *est le quotient*

$$\mathrm{Frac}(A) = \big(A \times A\backslash\{0\}\big)/\sim . \tag{1.497}$$

Nous notons a/b *la classe de* (a,b).

Lorsque A *est un anneau de polynômes*[142], *alors les éléments de* $\mathrm{Frac}(A)$ *sont des* ***fractions rationnelles****.*

Le fait que A soit intègre est important pour être certain que $bd \neq 0$ sous l'hypothèse que $b, d \neq 0$.

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.

Proposition 1.363 ([12, 1]).
Soit un anneau commutatif A. *Tout corps commutatif contenant un sous-anneau isomorphe*[143] *à* A *contient un sous-corps isomorphe à* $\mathrm{Frac}(A)$.

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.

(i) **Une partie bien choisie** Nous considérons la partie suivante de $\mathbb{K}$:

$$S = \{ab^{-1} \text{ tel que } a, b \in A'\}. \tag{1.498}$$

(ii) **S est un corps** Deux éléments arbitraires de S sont ab^{-1} et xy^{-1}. Nous devons prouver plusieurs choses.

(i) **Neutres** En prenant $a = b = 1$ nous avons $ab^{-1} = 1 \in S$. En prenant $a = 0$ et $b = 1$ nous avons $ab^{-1} = 0 \in S$.

(ii) **Somme** Il faut remarquer que $ab^{-1} + xy^{-1} = (ay + xb)(by)^{-1}$. En effet,

$$\begin{aligned}(ay + xb)(by)^{-1} &= (ay + xb)y^{-1}b^{-1} && \text{(1.499a)}\\ &= ayy^{-1}b^{-1} + xby^{-1}b^{-1} && \text{(1.499b)}\\ &= ab^{-1} + xy^{-1} && \text{(1.499c)}\end{aligned}$$

Justifications :

— Pour (1.499b). Distributivité.

— Pour (1.499c). Commutativité dans A.

(iii) **Produit** Il s'agit du même genre de calculs en utilisant les mêmes propriétés. Nous avons

$$(ab^{-1})(xy^{-1}) = (ax)(by)^{-1}. \tag{1.500}$$

(iii) **Ce qui va être notre isomorphisme** Ensuite nous montrons que l'application

$$\begin{aligned}\varphi : S &\to \mathrm{Frac}(A)\\ ab^{-1} &\mapsto \sigma(a)/\sigma(b)\end{aligned} \tag{1.501}$$

est bien définie et est un isomorphisme de corps.

141. Définition 1.192.
142. Définition 1.352.
143. Morphisme d'anneaux, définition 1.40.

(iv) **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 $\text{Frac}(A)$.

(v) **Morphisme** Deux éléments arbitraires de S sont ab^{-1} et xy^{-1}. Calculons un peu :

$$\begin{aligned}\varphi\big((ab^{-1})(xy^{-1})\big) &= \varphi(axy^{-1}b^{-1}) && (1.502a)\\ &= \varphi\big((ax)(by)^{-1}\big) && (1.502b)\\ &= \sigma(ax)/\sigma(by) && (1.502c)\\ &= \big(\sigma(a)/\sigma(b)\big)\big(\sigma(x)/\sigma(y)\big) && (1.502d)\\ &= \varphi(ab^{-1})\varphi(xy^{-1}). && (1.502e)\end{aligned}$$

Justifications :

— Pour (1.502a). Commutativité dans A.

— Pour (1.502b). Associativité dans A.

— Pour (1.502d). Définition 1.362(2) de la multiplication de fractions.

(vi) **Surjectif** Tout élément de $\text{Frac}(A)$ 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 $ab^{-1} \in S$.

(vii) **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 $ab^{-1} = xy^{-1}$.

□

1.364.
Soit un anneau A et son anneau des polynômes $\mathcal{P}(A)$. Si $\alpha \in A$, nous avons la définition 1.355 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.

Définition 1.365 (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[144]

$$R(\alpha) = (P/Q)(\alpha) = P(\alpha)Q^{-1}(\alpha). \tag{1.503}$$

Dans cette formule, les polynômes, l'inverse et le produit sont calculés dans $\mathbb{K}$ et non dans A.

Théorème-Définition 1.366.
Soit A un anneau commutatif intègre.

(1) Il existe 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

$$\lambda = \epsilon(a)\big(\epsilon(b)\big)^{-1} \tag{1.504}$$

*(2) Si $(\mathbb{K}', \epsilon')$ est un autre couple qui vérifie la propriété, les corps $\mathbb{K}$ et $\mathbb{K}'$ sont isomorphes. Le corps $\mathbb{K}$ associé à l'anneau A est le **corps des fractions** de A, et sera noté* $\text{Frac}(A)$.

(3) Nous posons

$$\begin{aligned}\sigma\colon A \times A^* &\to \mathbb{K}\\ (a, b) &\mapsto \epsilon(a)\big(\epsilon(b)\big)^{-1}.\end{aligned} \tag{1.505}$$

Nous avons

$$\sigma(xa, xb) = \sigma(a, b) \tag{1.506}$$

pour tout $a, b, x \in A$.

144. Les fractions rationnelles, définition 1.362.

1.19.5 Corps totalement ordonné

Définition 1.367.
Ordre et choses reliées dans un corps.

(1) *Un corps $\mathbb{K}$ est* ***totalement ordonné*** *si il existe une relation d'ordre total*[145] *tel que*
   (1a) *$x \leqslant y$ implique $x + z \leqslant y + z$ pour tout $x, y, z \in \mathbb{K}$*
   (1b) *$x \geqslant 0$ et $y \geqslant 0$ implique $xy \geqslant 0$.*

(2) *Si $\mathbb{K}$ est un corps totalement ordonné, nous y définissons la valeur absolue par*

$$|x| = \begin{cases} x & si\ x \geqslant 0 \\ -x & si\ x \leqslant 0. \end{cases} \tag{1.507}$$

(3) *La suite (x_n) dans le corps totalement ordonné $\mathbb{K}$ est* ***de Cauchy*** *si pour tout $\epsilon \in \mathbb{K}^+$, il existe $N \in \mathbb{N}$ tel que si $p, q \geqslant N$ alors $|x_p - x_q| \leqslant \epsilon$.*

(4) *La suite (x_n) dans le corps totalement ordonné $\mathbb{K}$ est* ***convergente*** *si il existe $q \in \mathbb{K}$ tel que pour tout $\epsilon \in \mathbb{K}^+$, il existe N tel que si $k \geqslant N$ alors $|x_k - q| \leqslant \epsilon$.*

(5) *Un corps totalement ordonné est* ***complet*** *si toute suite de Cauchy y est convergente.*

(6) *Si $a, \epsilon \in \mathbb{K}$ avec $\epsilon > 0$ alors nous définissons la* ***boule ouverte*** *de centre a et de rayon ϵ par*

$$B(a, \epsilon) = \{x \in \mathbb{K} \text{ tel que } |a - x| < \epsilon\}, \tag{1.508}$$

et la ***boule fermée*** *par*

$$\overline{B(a, \epsilon)} = \{x \in \mathbb{K} \text{ tel que } |a - x| \leqslant \epsilon\}. \tag{1.509}$$

Lemme 1.368.
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 (4) et (6) de la définition 1.367. □

1.369.
Ces boules prendront une nouvelle force avec le super-théorème 7.108.

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.

Lemme 1.370 (Règle des signes[71])**.**
Soit un corps totalement ordonné $\mathbb{K}$ ainsi que $x, y \in \mathbb{K}$. Nous avons :

(1) *Si $x \leqslant 0$ et $y \leqslant 0$ alors $xy \geqslant 0$.*
(2) *Si $x \leqslant 0$ et $y \geqslant 0$ alors $xy \leqslant 0$.*
(3) *Si $x \geqslant 0$ et $y \leqslant 0$ alors $xy \leqslant 0$.*
(4) $0 \leqslant 1$.
(5) *Si $x \geqslant 0$ alors $x^{-1} \geqslant 0$.*

Lemme 1.371 (Propriétés de la valeur absolue)**.**
Soit $\mathbb{K}$ un corps totalement ordonné. Si $x, y \in \mathbb{K}$ alors[146]

(1) *Si $x \geqslant 0$ alors $-x \leqslant 0$.*

145. Définition 1.11.
146. La « valeur absolue » est définie en (1.367)(2).

(2) *Si* $x \leqslant 0$ *alors* $-x \geqslant 0$.

(3) $|x| \geqslant 0$

(4) $|x| = 0$ *si et seulement si* $x = 0$

(5) $|-x| = |x|$.

(6) $|x + y| \leqslant |x| + |y|$.

(7) $|xy| = |x||y|$

Démonstration. Point par point

(i) **(1)** Nous partons de $x \geqslant 0$ et nous ajoutons $-x$ des deux côtés en profitant de la définition d'un corps totalement ordonné : $x - x \geqslant -x$ et donc $0 \geqslant -x$, c'est-à-dire $-x \leqslant 0$.

(ii) **(2)** Nous partons de $x \leqslant 0$ et nous ajoutons $-x$ des deux côtés.

(iii) **(3)** Si $x \geqslant 0$ alors c'est vrai. Sinon, $x \leqslant 0$ et $|x| = -x \geqslant 0$ par le point (1).

(iv) **(4)** Si $x = 0$ alors $x = -x$ et $|x| = 0$. Au contraire si $x \neq 0$ alors $-x \neq 0$ et que x soit positif ou négatif, nous aurons toujours $\pm x \neq 0$.

(v) **(5)** Il faut décomposer en deux cas selon que $x \geqslant 0$ et $x \leqslant 0$. Supposons $x \geqslant 0$. Alors d'une part $|x| = x$. D'autre part $-x \leqslant 0$ par le point (1), de telle sorte que

$$|-x| = -(-x) = x. \tag{1.510}$$

Nous avons donc $|x| = |-x| = x$.

Le même raisonnement tient avec $x \leqslant 0$.

(vi) **(6)** Nous supposons que $x \leqslant y$ et nous distinguons divers cas suivant la positivité de x et y.

(1) Si $x, y \geqslant 0$. Dans ce cas, $x + y \geqslant y \geqslant 0$, donc $|x + y| = x + y = |x| + |y|$.

(2) Si $x, y \leqslant 0$. Dans ce cas, $x + y \leqslant 0$ et nous avons $|x + y| = -x - y = |x| + |y|$.

(3) 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

$$x \leqslant 0 \tag{1.511a}$$

$$x + y \leqslant y \leqslant y + |x| = |x| + |y| \tag{1.511b}$$

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.

(vii) **Pour (7)** Il suffit de prendre les 4 cas suivant les signes de x et y, et d'utiliser les règles de signes du lemme 1.370 dans la définition 1.507.

□

Remarque 1.372.
La partie (6) est très importante parce que c'est elle qui fera presque toutes les majorations dont nous aurons besoin en analyse. En effet elle donne l'inégalité triangulaire de la façon suivante : si $x, y, z \in \mathbb{K}$ nous avons

$$|x - y| = |(x - z) + (z - y)| \leqslant |x - z| + |z - y|. \tag{1.512}$$

Lemme 1.373 (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 :*

(1) $y \in B(x, \epsilon)$ *si et seulement si* $x - \epsilon < y < x + \epsilon$.

(2) *Si* $y \in \overline{B(x, \epsilon)}$ *alors* $y \in B(x, \epsilon')$ *pour tout* $\epsilon' > \epsilon$.

Démonstration. Pour rappel,

$$|x-y| = \begin{cases} x-y & \text{si } x-y \geqslant 0 \\ y-x & \text{si } x-y \leqslant 0. \end{cases} \tag{1.513}$$

Nous pouvons maintenant démontrer nos assertions.

(i) **(1)** En deux parties.

(i) $\Rightarrow$ 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.

(ii) $\Leftarrow$ 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 $|x-y| < \epsilon$.

(ii) **(2)** C'est immédiat parce que

$$|x-y| \leqslant \epsilon < \epsilon'. \tag{1.514}$$

□

Lemme 1.374.
Tout corps totalement ordonné est de caractéristique nulle.

1.20 Les rationnels

Note : pour l'existence et l'unicité de l'écriture $q = k/d$, il faut voir le théorème 3.33.
Une construction très explicite est faite dans [17]. Ici nous allons prendre plus court :

Définition 1.375.
*Le corps des fractions de $\mathbb{Z}$ (définition 1.362) est noté $\mathbb{Q}$ et ses éléments sont les **rationnels**.*

Proposition 1.376.
L'application

$$\begin{aligned} f\colon \mathbb{Z} &\to \mathbb{Q} \\ z &\mapsto z/1 \end{aligned} \tag{1.515}$$

est une injection.

Démonstration. Supposons que $f(a) = f(b)$, c'est-à-dire que $a/1 = b/1$. En vertu de la relation d'équivalence donnée en 1.362, nous avons $a1 = b1$, c'est-à-dire $a = b$. □

1.377.
À partir de maintenant, nous allons identifier la partie $f(\mathbb{Z})$ à $\mathbb{Z}$. Nous nous autorisons donc à dire que $4 \in \mathbb{Q}$ ou que $-7 \in \mathbb{Q}$, et même que $0 \in \mathbb{Q}$.

Proposition 1.378.
L'ensemble des rationnels est infini dénombrable[147].

Démonstration. L'ensemble $\mathbb{Z}$ est infini[148] et la proposition 1.376 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 1.114.

L'application

$$\begin{aligned} g\colon \mathbb{Z}^2 &\to \mathbb{Q} \\ a,b &\mapsto a/b \end{aligned} \tag{1.516}$$

147. 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.
148. Lemme 1.109.

est surjective alors que $\mathbb{Z}^2$ est dénombrable. Le lemme 1.125 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. □

Lemme 1.379.
Soient $a, b, x, y \in \mathbb{Z}$. Nous avons $ay = xb$ dans $\mathbb{Z}$ si et seulement si nous avons $ab^{-1} = xy^{-1}$ dans $\mathbb{Q}$.

1.20.1 Relation d'ordre

Proposition-Définition 1.380.
Pour $a, b, c, d \in \mathbb{Z}$ nous disons que

$$\frac{a}{b} \geqslant \frac{c}{d} \tag{1.517}$$

si et seulement si $ad \geqslant bc$ dans $\mathbb{Z}$.

Avec cette définition, $(\mathbb{Q}, \geqslant)$ est un ensemble totalement ordonné.

Lemme 1.381.
Tout rationnel est majoré par un naturel.

Proposition 1.382.
Si $q < 1$ dans $\mathbb{Q}$, alors $qx < x$ pour tout $x \in \mathbb{Q}^+$.

Proposition 1.383.
Le corps $\mathbb{Q}$ est archimédien[149].

Lemme 1.384.
Si $q \in \mathbb{Q}$, alors il existe $k \in \mathbb{N}$ tel que $kq \in \mathbb{Z}$.

1.20.2 Caractéristique

Lemme 1.385.
Le corps $\mathbb{Q}$ est de caractéristique[150] *nulle.*

1.21 Suite de Cauchy dans un corps totalement ordonné

Lemme 1.386 ([67, 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 1.343 que

$$\begin{aligned} \mu\colon \mathbb{Z} &\to \mathbb{K} \\ n &\mapsto n1_{\mathbb{K}} \end{aligned} \tag{1.518}$$

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 :

(i) **Morphisme** L'application μ est un morphisme par le lemme 1.343.

(ii) **Surjectif** Par définition les éléments de Z sont dans l'image de $\mathbb{Z}$.

(iii) **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 1.363 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 1.386.

149. Définition 1.70.
150. Définition 1.343.

Proposition 1.387 ([1]).
Soit un corps totalement ordonné $\mathbb{K}$. Nous considérons l'application

$$\begin{aligned}\mu\colon \mathbb{Z} &\to \mathbb{K}\\ n &\mapsto n\cdot 1_{\mathbb{K}}\end{aligned} \tag{1.519}$$

et ensuite

$$\begin{aligned}\sigma\colon \mathbb{Q} &\to \mathbb{K}\\ a/b &\mapsto \mu(a)\mu(b)^{-1}.\end{aligned} \tag{1.520}$$

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.

(i) **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 1.362 du corps des fractions), nous avons $ay=bx$ dans $\mathbb{Q}$. Vu que μ est un morphisme nous avons alors

$$\mu(a)\mu(y)=\mu(b)\mu(x) \tag{1.521}$$

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.

(ii) **Morphisme pour la somme** L'application μ est un morphisme d'anneaux, comme déjà dit depuis le lemme 1.343. Notons aussi que, parce que $\mathbb{K}$ est commutatif,

$$\mu(qy)^{-1}=\mu(q)^{-1}\mu(y)^{-1}. \tag{1.522}$$

En utilisant la définition 1.362(1) de la somme nous avons

$$\begin{aligned}\sigma(p/q+x/y)&=\sigma\big((py+qx)/qy\big) && \text{(1.523a)}\\ &=\big[\mu(py)+\mu(qx)\big]\mu(qy)^{-1} && \text{(1.523b)}\\ &=\mu(py)\mu(qy)^{-1}+\mu(qx)\mu(qy)^{-1} && \text{(1.523c)}\\ &=\mu(p)\mu(q)^{-1}+\mu(x)\mu(y)^{-1} && \text{(1.523d)}\\ &=\sigma(p/q)+\sigma(x/y). && \text{(1.523e)}\end{aligned}$$

(iii) **Morphisme pour le produit** Même genre de calculs que pour la somme.

(iv) **Croissante** Nous savons aussi par le lemme 1.370(4) que $1\geqslant 0$. Puisque μ est un morphisme d'anneaux,

$$\mu(n+1)=\mu(n)+\mu(1)=\mu(n)+1 \tag{1.524}$$

La définition 1.367(1a) 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

$$\sigma(p/q)=\mu(p)\mu(q)^{-1} \tag{1.525}$$

où $\mu(p)\geqslant 0$ et $\mu(q)\geqslant 0$. Ensuite le lemme 1.370(5) nous indique que $\mu(q)^{-1}\geqslant 0$. Enfin la condition 1.367(1b) 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

$$\sigma(q_1)=\sigma(q_2+q_1-q_2)=\sigma(q_2)+\sigma(q_1-q_2)\geqslant\sigma(q_2) \tag{1.526}$$

par la condition 1.367(1a).

□

1.388.
Si $\mathbb{K}$ est un corps totalement ordonné, la proposition 1.387 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

$$qk = \sigma(q)k. \tag{1.527}$$

Nous pourrons donc écrire $\frac{k}{2}$ pour $\sigma(1/2)k$.

Le lemme suivant explique que la notation (1.527) n'est pas complètement idiote.

Lemme 1.389.
Soit un corps commutatif totalement ordonné $\mathbb{K}$. Soit $k \in \mathbb{K}$. Nous avons

$$k + k = 2k. \tag{1.528}$$

Démonstration. Vu que $\sigma\colon \mathbb{Q} \to \mathbb{K}$ est un morphisme, il vérifie $\sigma(1) = 1$, donc

$$\begin{aligned} k + k &= \sigma(1)k + \sigma(1)k && \text{(1.529a)}\\ &= \big(\sigma(1) + \sigma(1)\big)k && \text{(1.529b)}\\ &= \sigma(2)k && \text{(1.529c)}\\ &= 2k. && \text{(1.529d)} \end{aligned}$$

□

Proposition 1.390.
Toute suite convergente dans un corps totalement ordonné est de Cauchy.

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 $k > N$,

$$|x_k - x| < \epsilon. \tag{1.530}$$

Soient $p, q > N$. Alors en utilisant la majoration du lemme 1.371(6),

$$|x_p - x_q| = \big|(x_p - x) + (x - x_q)\big| \leqslant |x_p - x| + |x - x_q| \leqslant 2\epsilon. \tag{1.531}$$

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 (1.531) est en réalité $\epsilon + \epsilon = \sigma(2)\epsilon$ en vertu de ce qui est raconté en 1.388 et en vertu du lemme 1.389.

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

$$|x_p - x_q| \leqslant 2\epsilon' = \sigma(2)\sigma(1/2)\epsilon = \sigma(1)\epsilon = \epsilon. \tag{1.532}$$

Ce dernier ϵ étant bien celui fixé au début de la preuve, nous en déduisons que (x_n) est de Cauchy. □

1.21.1 Suites de Cauchy dans les rationnels

Proposition 1.391 ([17]).
Principales propriétés des suites de Cauchy dans $\mathbb{Q}$.

(1) Toute suite convergente est de Cauchy[151].

(2) Toute suite de Cauchy est bornée.

(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.

(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 1.390.

(2) Soit (x_n) une suite de Cauchy dans $\mathbb{Q}$. Avec $\epsilon = 1$ dans la définition, si $q > N$, nous avons

$$|x_q - x_N| \leqslant 1. \tag{1.533}$$

Et donc pour tout q plus grand que N, $x_N - 1 \leqslant x_q \leqslant x_N + 1$, ou encore, pour tout n :

$$|x_n| \leqslant \max\{|x_1|, |x_2|, \dots, |x_N|, |x_N + 1|\}. \tag{1.534}$$

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 $|x_n y_n| \leqslant M\epsilon$.

(4) En ce qui concerne la somme,

$$|x_p + y_p - x_q - y_q| \leqslant |x_p - x_q| + |y_p - y_q|. \tag{1.535}$$

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 (1.535) 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 :

$$|x_p y_p - x_q y_q| \leqslant |x_p y_p - x_q y_p| + |x_q y_p - x_q y_q| \leqslant |y_p||x_p - x_q| + |x_q||y_p - y_q|. \tag{1.536}$$

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

$$|x_p y_p - x_q y_q| \leqslant M\epsilon + M\epsilon = 2M\epsilon, \tag{1.537}$$

ce qui prouve que $(x_n y_n)$ est de Cauchy.

(5) En ce qui concerne la somme, nous pouvons tout de suite calculer

$$|x_n + y_n - (a + b)| \leqslant |x_n - a| + |y_n - b|. \tag{1.538}$$

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.

151. Et non la réciproque, qui sera justement la grande innovation des nombres réels.

En ce qui concerne le produit,

$$|x_ny_n - ab| \leqslant |x_ny_n - ay_n| + |ay_n - ab| \leqslant |y_n||x_n - a| + |a||y_n - b|. \tag{1.539}$$

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

$$y_n|x_n - a| + a|y_n - b| \to 0. \tag{1.540}$$

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

$$|x_p - x_q| \leqslant \frac{\alpha}{2}. \tag{1.541}$$

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

$$\left|\frac{1}{x_p} - \frac{1}{x_q}\right| \leqslant \frac{|x_q - x_p|}{|x_px_q|} \leqslant \frac{4}{\alpha^2}|x_q - x_p| \leqslant \frac{4}{\alpha^2}\epsilon. \tag{1.542}$$

Donc $\left(\frac{1}{x_n}\right)$ est de Cauchy.

□

1.22 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 $x_n^2 \to 2$.

Lemme 1.392.
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 3.36 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 1.455.

Proposition 1.393 (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 1.392 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 [152]. Il n'y a donc pas de fractions d'entiers dont le carré vaut 2. □

Lemme 1.394 (Série géométrique)**.**
Si $q \neq 1$ dans $\mathbb{Q}$ et $p \in \mathbb{N}$ nous avons

$$\sum_{k=0}^{p} q^k = \frac{1 - q^{p+1}}{1 - q}. \tag{1.543}$$

Démonstration. En posant $S_p = 1 + q + q^2 + \cdots + q^p$, nous avons $S_p - qS_p = 1 - q^{p+1}$ et donc

$$S_p = \sum_{k=0}^{p} q^k = \frac{1 - q^{p+1}}{1 - q}. \tag{1.544}$$

□

Proposition 1.395.
La suite donnée par

$$x_n = 1 + \frac{1}{1!} + \cdots + \frac{1}{n!} \tag{1.545}$$

est de Cauchy et ne converge pas dans $\mathbb{Q}$.

Démonstration. Si $p > q > 0$ nous avons

$$\begin{aligned}
x_p - x_q &= \sum_{k=q+1}^{p} \frac{1}{k!} && \text{(1.546a)}\\
&\leqslant \sum_{k=q+1}^{p} \frac{1}{(q+1)!} \frac{1}{(q+1)^{k-q-1}} && \text{(1.546b)}\\
&\leqslant \frac{1}{(q+1)!} \lim_{p\to\infty} \sum_{k=0}^{p} \frac{1}{(q+1)^k} && \text{(1.546c)}\\
&\leqslant \frac{1}{(q+1)!} \frac{1}{1 - \frac{1}{q+1}} && \text{(1.546d)}\\
&\leqslant \frac{1}{(q+1)!} \frac{q+1}{q} && \text{(1.546e)}\\
&\leqslant \frac{1}{q!q}. && \text{(1.546f)}
\end{aligned}$$

Justifications :

— Pour (1.546b), 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 (1.546c), il y a une inégalité parce que la suite $p \mapsto \sum_{k=0}^{p} 1/(q + 1)^k$ est une suite strictement croissante.

152. Voir [17], et attention : ce n'est pas tout à fait évident.

— Pour (1.546d), le lemme 1.394 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

$$x_p - x_q \leqslant \frac{1}{b!b} < \frac{1}{b} < \frac{a}{b} = \epsilon. \tag{1.547}$$

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

$$0 < x_p - x_q < \frac{1}{qq!}. \tag{1.548}$$

Prenons la limite $p \to \infty$; par stricte croissance de la suite, les inégalités restent strictes :

$$0 < \frac{a}{b} - x_q < \frac{1}{qq!}. \tag{1.549}$$

Si $n > b$ alors nous pouvons écrire

$$\frac{a}{b} - x_n = \frac{\alpha}{n!} \tag{1.550}$$

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 (1.549) nous pouvons écrire

$$0 < \frac{\alpha}{q!} < \frac{1}{qq!}, \tag{1.551}$$

c'est-à-dire $0 < \alpha < \frac{1}{q}$, ce qui est impossible pour $\alpha \in \mathbb{Z}$. □

Lemme 1.396.
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 1.383), il existe $n \in \mathbb{N}$ tel que $1 < nA$. Pour ce n, nous avons

$$\left(\frac{1}{n}\right)^2 < \frac{1}{n} < A. \tag{1.552}$$

□

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 [72] que la suite peut être vue comme une forme de méthode de Newton 34.54 ; voir l'exemple 34.57. Si vous aimez les dessins et les approches géométriques, il y a une explication sur Wikipédia[73].

Proposition 1.397 ([72]).
Soient $A > 0$ dans $\mathbb{Q}$ et $x_0 \in \mathbb{Q}$. La suite (x_k) définie par

$$x_{k+1} = \frac{1}{2}\left(x_k + \frac{A}{x_k}\right) \tag{1.553}$$

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.

(i) **La suite s_k** En posant $y_k = x_k^2$ nous calculons que

$$y_{k+1} - A = \frac{(y_k - A)^2}{4y_k}. \tag{1.554}$$

Autrement dit, la suite $s_k = y_k - A$ vérifie

$$s_{k+1} = \frac{s_k^2}{4(A + s_k)}. \tag{1.555}$$

Quelle que soit la valeur de $s_0 = x_0^2 - A$, nous avons

$$s_1 = \frac{s_0^2}{4(A + s_0)} = \frac{(x_0^2 - A)^2}{4(A + x_0^2 - A)} = \frac{(x_0^2 - A)^2}{4x_0^2} > 0. \tag{1.556}$$

Donc à partir de s_1, tous les éléments sont positifs. Vu que $A > 0$ nous avons aussi

$$s_{k+1} < \frac{s_k^2}{4s_k} = \frac{s_k}{4} \tag{1.557}$$

et donc $s_k < s_0/4^k$. Donc $s_k \to 0$.

(ii) **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 1.391(1).

(iii) **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

$$|x_r^2 - x_s^2| < \epsilon \tag{1.558}$$

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 1.396. 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

$$x_r^2 - x_s^2 = (x_r + x_s)(x_r - x_s) \tag{1.559}$$

et ensuite de prendre la valeur absolue et de diviser par $|x_r + x_s|$:

$$|x_r - x_s| = \frac{|x_r^2 - x_s^2|}{|x_r + x_s|} < \frac{\epsilon}{2q}. \tag{1.560}$$

Donc (x_k) est une suite de Cauchy.

(iv) **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 1.391(5)). Mais nous savons par la proposition 1.393 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 3.36 dira que $\sqrt{n}$ est soit entier, soit irrationnel.

1.398.
Un petit programme en python pour explorer la suite de la proposition 1.397.

```
#!/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

1.23 Les réels

Une construction des réels via les coupures de Dedekind est donnée dans [74].

1.399.
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 7.236) alors que la topologie métrique (celle entre autres de $\mathbb{Q}$) ne sera définie que par le théorème 7.108. Nous avons donc dû définir en la définition 1.367 *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 [153]. Et par conséquent que $\mathbb{R}$ sera un espace métrique complet [154].

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[75].

1.23.1 L'ensemble

Soit $\mathcal{E}$ l'ensemble des suites de Cauchy [155] dans $\mathbb{Q}$. Soit aussi l'ensemble $\mathcal{E}_0$ constituée des suites qui convergent vers zéro [156].

En posant

$$x + y = (x_n + y_n) \tag{1.561}$$

et

$$xy = (x_n y_n), \tag{1.562}$$

l'ensemble $\mathcal{E}$ devient un anneau [157] commutatif dont le neutre de l'addition est la suite constante $x_n = 0$ et le neutre pour la multiplication est la suite constante $x_n = 1$.

Proposition 1.400.
La partie $\mathcal{E}_0$ est un idéal[158] *de l'anneau $\mathcal{E}$.*

Démonstration. Nous savons par la proposition 1.391(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 1.391 (il s'agit du fait que la somme de deux suites convergeant vers zéro est une suite convergente vers zéro).

153. Proposition 7.244.
154. Théorème 1.438 pour la complétude en tant que corps et théorème 1.390 pour la complétude en tant que espace métrique.
155. Définition 1.367(3)
156. Nous rappelons qu'à ce niveau nous n'avons pas encore prouvé que toutes les suites de Cauchy convergent.
157. Définition 1.39.
158. Définition 1.177.

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 1.391(3)). □

Théorème-Définition 1.401 (L'anneau des réels[17])**.**
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.

(i) **Les opérations sont bien définies** La partie $\mathcal{E}_0$ est un idéal par la proposition 1.400. Le quotient est donc bien défini et est un anneau par la proposition 1.179(2).

(ii) **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

$$\bar{x} = \{\text{suites qui convergent vers } q\}. \tag{1.563}$$

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

$$y_n = x_n + (y_n - x_n), \tag{1.564}$$

mais $y_n - x_n \to 0$. Donc la suite $y - x \in \mathcal{E}_0$ ce qui signifie que $y \in \bar{x}$.

(iii) **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.

(iv) **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 [159] alors il existe $y \in \mathcal{E}$ tel que $xy \in \bar{1}$.

Nous savons par la proposition 1.391(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

$$y_n = \begin{cases} 0 & \text{si } n \leqslant n_0 \\ \frac{1}{x_n} & \text{si } n > n_0. \end{cases} \tag{1.565}$$

Nous avons alors

$$(xy)_n = \begin{cases} 0 & \text{si } n \leqslant n_0 \\ 1 & \text{si } n > n_0 \end{cases} \tag{1.566}$$

et donc $xy \in \bar{1}$.

□

1.402 (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.

159. $x \in \mathcal{E}$ peut soit ne pas converger du tout, soit converger vers autre chose que zéro.

D'autre part nous définissons

$$\begin{aligned}\varphi\colon \mathbb{Q} &\to \mathbb{R}\\ q &\mapsto \overline{[k\mapsto q]},\end{aligned} \tag{1.567}$$

c'est-à-dire que $\varphi(q)$ est la classe de la suite constante $x_k = q$.

Proposition 1.403.
Soit l'application

$$\begin{aligned}\varphi\colon \mathbb{Q} &\to \mathbb{R}\\ q &\mapsto \bar{q}.\end{aligned} \tag{1.568}$$

où par $\bar{q}$ nous entendons la classe de la suite constante égale à q (qui est de Cauchy).

(1) C'est un homomorphisme 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

$$\varphi(q) = \{\text{suites de Cauchy qui convergent vers zéro}\} \tag{1.569}$$

Mais nous savons aussi que [160]

$$\varphi(q) = \bar{q} = \{\text{suites de Cauchy qui convergent vers } q\} \tag{1.570}$$

Nous en déduisons que $q = 0$. □

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.

Lemme 1.404.
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

$$x = y + z. \tag{1.571}$$

Pour tout n nous avons donc $x_n = y_n + z_n$, ou encore

$$z_n = q - l \tag{1.572}$$

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 $q = l$. □

1.23.2 Relation d'ordre

Définition 1.405.
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 $\mathcal{E}^{++} = \mathcal{E}^+ \backslash \mathcal{E}_0$.

160. Voir dans la démonstration du théorème 1.401.

Dans le lemme suivant, le point (2) peut sembler perturbant. Il s'agit de dire que si x est la classe de la suite constante 0, alors il est le neutre pour l'addition dans $\mathbb{R}$.

Lemme 1.406 (À propos du zéro)**.**
Nous avons

(1) $\mathcal{E}^+ \cap \mathcal{E}^- = \{\bar{0}\}$.

(2) Si $x = \bar{0}$ *alors* $x = 0$.

Lemme 1.407.
Les parties $\mathcal{E}^+$ *et* $\mathcal{E}^-$ *partitionnent* $\mathcal{E}$ *de la façon suivante :*

(1) $\mathcal{E}^+ \cap \mathcal{E}^- = \mathcal{E}_0$

(2) $\mathcal{E}^+ \cup \mathcal{E}^- = \mathcal{E}$

Démonstration. 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 $x \in \mathcal{E}_0$.

Pour prouver le second point, soit $x \in \mathcal{E}\backslash\mathcal{E}^-$, 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

$$x_n > \frac{\alpha}{2} > 0 \tag{1.573}$$

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. □

Lemme 1.408 ([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

$$|x_p - x_n| < \frac{\delta}{2}. \tag{1.574}$$

Cela implique que $x_p > \delta/2 > 0$ pour tout $p > N_2$. □

La proposition suivante est une version plus précise du lemme 1.408.

Proposition 1.409 ([12])**.**
Soit $x \in \mathcal{E}^{++}$*. Il existe* $r \in \mathbb{Q}^+\backslash\{0\}$ *et* $N \in \mathbb{N}$ *tel que* $x_n \geqslant r$ *pour tout* $n \geqslant N$.

Démonstration. Fixons $\epsilon \in \mathbb{Q}^+\backslash\{0\}$, et procédons par l'absurde. Du coup nous savons trois choses sur la suite (x_n).

(1) Hypothèse absurde : pour tout $q \in \mathbb{Q}^+\backslash\{0\}$ 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

$$x_n < x_p + \frac{\epsilon}{2} < \epsilon, \tag{1.575}$$

et donc $-\epsilon < x_n < \epsilon$.

Au final, nous avons prouvé que pour tout $\epsilon \in \mathbb{Q}^+\backslash\{0\}$, il existe P tel que $n > P$ implique $|x_n| < \epsilon$. Cela signifie que

$$x_n \xrightarrow{\mathbb{Q}} 0, \tag{1.576}$$

c'est-à-dire $x \in \mathcal{E}_0$, ce qui est contraire à l'hypothèse. □

Lemme 1.410 ([17])**.**
Quelques propriétés du partitionnement.

(1) $x \in \mathcal{E}^-$ *si et seulement si* $(-x) \in \mathcal{E}^+$

(2) $x \in \mathcal{E}^+$ *et* $y \in \mathcal{E}^+$ *implique* $x + y \in \mathcal{E}^+$

(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 1.408 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

$$\begin{cases} x_n > -\frac{\epsilon}{2} & \text{(1.577a)} \\ |x_n - y_n| < \frac{\epsilon}{2}. & \text{(1.577b)} \end{cases}$$

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 $y \in \mathcal{E}^-$.

□

Définition 1.411 (Positivité dans $\mathbb{R}$)**.**
Vocabulaire et notations.

(1) Nous notons $\mathbb{R} = \mathcal{E}/\mathcal{E}_0$.

(2) Nous notons $\mathbb{R}^+ = \bar{\mathcal{E}}^+$.

(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* $\mathcal{E}_0$.

1.412.
Avec les conventions de la définition 1.411, 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 $\mathbb{R}^+\backslash\{0\}$.

(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[76].

Définition 1.413 (Ordre sur $\mathbb{R}$)**.**
Si $x, y \in \mathbb{R}$ nous notons $x \leqslant y$ si et seulement si $y - x \in \overline{\mathcal{E}^+}$.

Proposition 1.414.
Le couple $(\mathbb{R}, \leqslant)$ est un corps totalement ordonné[161]

Démonstration. Il s'agit de vérifier, dans l'ordre, les définitions 1.10, 1.11 et 1.367(1). 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 $z = \bar{c}$.

(i) **Réflexivité** Pour savoir si $x \geqslant x$, nous devons nous demander si $x - x \in \overline{\mathcal{E}^+}$. Nous avons $x - x = \bar{a} - \bar{a} = \bar{0} = 0$.

(ii) **antisymétrie** Nous supposons que $x \geqslant y$ et $y \geqslant x$. Du côté des suites de Cauchy, cela signifie que $a - b \in \mathcal{E}^+$ et $b - a \in \mathcal{E}^+$. Le lemme 1.410(1) nous indique alors que $a - b = -(b - a) \in \mathcal{E}^-$. Donc

$$a - b \in \mathcal{E}^+ \cap \mathcal{E}^- = \{\bar{0}\}. \tag{1.578}$$

Donc le réel $x - y$ est la classe de la suite constante 0. Le lemme 1.406(2) dit alors que $x - y = 0$ ou encore que $x = y$.

(iii) **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

$$\begin{aligned} c - a &= c - b + b - a && \text{(1.579a)}\\ &= (c - b) + (b - a) && \text{(1.579b)}\\ &\in \mathcal{E}^+ + \mathcal{E}^+ && \text{(1.579c)}\\ &\subset \mathcal{E}^+ && \text{(1.579d)} \end{aligned}$$

où nous avons utilisé le lemme 1.410(2). Puisque $c - a \in \mathcal{E}^+$, nous avons $z - x = \overline{c - a} \geqslant 0$.

(iv) **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 1.407(2) nous avons $\overline{b - a} \in \mathcal{E}^-$, ce qui donne, par le lemme 1.410(1) que $\overline{a - b} \in \mathcal{E}^+$, c'est-à-dire $y \leqslant x$.

(v) **Corps ordonné** Enfin nous devons vérifier les deux conditions de la définition 1.367(1). Pour la première condition, nous supposons $x \leqslant y$, c'est-à-dire $b - a \in \mathcal{E}^+$. Nous avons donc

$$(b + c) - (a + c) = b + x - a - c = b - a \in \mathcal{E}^+, \tag{1.580}$$

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 1.410(3).

□

Définition 1.415.
Puisque $\mathbb{R}$ est un corps totalement ordonné (proposition 1.414), si $x \in \mathbb{R}$, nous définissons $|x|$ conformément à 1.367(2).

Lemme 1.416.
L'application

$$\begin{aligned} \varphi\colon \mathbb{Q} &\to \mathbb{R} \\ q &\mapsto \bar{q} \end{aligned} \tag{1.581}$$

dont nous avons déjà parlé dans la proposition 1.403 est strictement croissante.

161. Corps totalement ordonné, définition 1.367.

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

$$x_n = l - q > 0 > -\epsilon, \tag{1.582}$$

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 1.404 dit que $\bar{q} = \bar{l}$ uniquement si $q = l$, ce qui est exclu parce que $q < l$. Donc $\bar{q} \neq \bar{l}$. □

Lemme 1.417.
Si $a, b \in \mathbb{R}^+$ satisfont $a + b = 0$, alors $a = b = 0$.

Voici une version dans $\mathbb{R}$ du lemme 1.106.

Lemme 1.418.
Soient $a > 0$ et $b > 1$ dans $\mathbb{R}$. Nous avons

$$ab > a. \tag{1.583}$$

Remarque 1.419.
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.

Lemme 1.420.
Si $x, y, z \in \mathbb{R}$ avec $x > 0$ sont tels que $z > y/x$ alors $zx > y$.

Démonstration. Nous savons que

$$z - \frac{y}{x} \in \mathcal{E}^+ \backslash \{0\} = \mathcal{E}^{++}. \tag{1.584}$$

Puisque $x \in \mathcal{E}^{++}$, multiplier par x fait rester dans $\mathcal{E}^{++}$:

$$zx - x\frac{y}{x} \in \mathcal{E}^{++}. \tag{1.585}$$

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 $zx > y$. □

Lemme 1.421.
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.

(i) **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 1.391(2)). Soit M un naturel strictement plus grand que m/q [162].
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 [163]. Par définition de la relation d'ordre, $M \geqslant a$.

(ii) **Seconde façon** La suite (a_n) est majorée par $\frac{m}{q}$, donc on a dans $\mathbb{Q}$ et pour tout n :

$$a_n \leqslant \frac{m}{q} = M \leqslant qM. \tag{1.586}$$

L'application $\varphi\colon \mathbb{Q} \to \mathbb{R}$ est croissante, donc

$$\varphi\big((a_n)\big) \leqslant \varphi(qM). \tag{1.587}$$

162. Lemme 1.381.
163. Et nous allons d'ailleurs arrêter de toujours préciser « la classe de » lorsque ce n'est pas nécessaire.

□

En corolaire, nous avons

Lemme 1.422.
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 $q = -p$. □

Théorème 1.423 ([17]).
Le corps $\mathbb{R}$ est archimédien[164].

Démonstration. La proposition 1.414 dit que $\mathbb{R}$ est totalement ordonné. Soient $x, y \in \mathbb{R}$ avec $x > 0$; posons $a = \frac{y}{x}$. Le lemme 1.421 nous donne un $p \in \mathbb{N}$ tel que $p > a$. Nous concluons alors avec le lemme 1.420 :

$$px > ax = \frac{y}{x}x = y. \tag{1.588}$$

□

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 $\mathbb{R}$.

Lemme 1.424.
À propos de rationnels entre des réels.

(1) Si $x, y \in \mathbb{R}$ sont tels que $x < y$, alors il existe $s \in \mathbb{Q}$ tel que $x < s < y$.

(2) Si $\epsilon > 0$ dans $\mathbb{R}$, il existe $n \in \mathbb{N}$ tel que $\frac{1}{n} < \epsilon$.

Démonstration. Nous avons par hypothèse que $y - x > 0$ et donc le fait que $\mathbb{R}$ soit archimédien (théorème 1.423) nous donne $q \in \mathbb{N}$ tel que $q(y - x) > 1$. Soit

$$E = \{n \in \mathbb{Z} \text{ tel que } \frac{n}{q} \leqslant x\}. \tag{1.589}$$

Cet ensemble n'est pas vide à cause du lemme 1.422 ; de plus, comme $|x|q \leqslant n_0$ pour un certain n_0 (à cause du lemme 1.421), l'ensemble E est majoré par n_0. Donc E possède un plus grand élément[165] p qui vérifie

$$\frac{p}{q} \leqslant x < \frac{p+1}{q}. \tag{1.590}$$

De plus $(p+1)/q < y$ parce que

$$\frac{p+1}{q} = \frac{p}{q} + \frac{1}{q} \leqslant x + \frac{1}{q} < x + y - x = y \tag{1.591}$$

où nous avons utilisé l'inégalité stricte $y - x > \frac{1}{q}$.

Nous avons donc

$$x < \frac{p+1}{q} < y, \tag{1.592}$$

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

$$0 < \frac{1}{q} \leqslant \frac{p}{q} < \epsilon. \tag{1.593}$$

□

164. Définition 1.70.
165. Lemme 1.107.

Remarque 1.425.
Le lemme 1.424 a également pour conséquence que des ensembles comme $[-1,1]$ ne sont pas bien ordonnés (définition 1.11). 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...

1.426.
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.

Lemme 1.427 ([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

$$E = \{n \in \mathbb{N} \text{ tel que } d_n \neq d'_n\}. \tag{1.594}$$

Comme $q \neq q'$, les développements dyadiques sont différents [166], 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 $a = \sum_{i=1}^{N} d_i 2^i$. □

Corolaire 1.428.
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 $x < d < y$.

La partie

$$D = \{\frac{a}{2^b} \text{ tel que } a \in \mathbb{Z}, b \in \mathbb{N}\} \tag{1.595}$$

est dense dans $\mathbb{R}$.

*Ce D est nommé l'ensemble des **fractions dyadiques**.*

Lemme 1.429 ([1])**.**
Soient des réels a, b, x, y tels que

$$a \leqslant x \leqslant b \tag{1.596}$$

et

$$a \leqslant y \leqslant b, \tag{1.597}$$

alors $|x - y| \leqslant |b - a|$.

Lemme 1.430.
Soient deux réels a, b tels que

(1) $a \geqslant 0$,
(2) $b \geqslant 0$
(3) $a + b = 0$.

Alors $a = 0$ et $b = 0$.

Lemme 1.431.
Si $a \in \mathbb{R}$, alors $a^2 \geqslant 0$ et $a^2 = 0$ si et seulement si $a = 0$.

Lemme 1.432.
Soit un réel strictement positif a. Si $b > 1$, alors $ab > a$.

Lemme 1.433.
Soient $a, b, x \in \mathbb{R}$ tels que $a + x = b + x$. Alors $a = b$.

166. À vérifier tout de même...

1.23.3 Complétude

Le théorème 17.138 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 17.138 utilise le fait que $\mathbb{R}$ est complet.

Lemme 1.434.
Nous avons

$$|\varphi(q)| = \varphi(|q|) \tag{1.598}$$

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

$$|\varphi(q)| = \varphi(q) = \varphi(|q|). \tag{1.599}$$

Supposons au contraire que $q < 0$. Alors $|q| = -q$ dans $\mathbb{Q}$, mais aussi $\varphi(q) \leqslant 0$. Donc

$$|\varphi(q)| = -\varphi(q) = \varphi(-q) = \varphi(|q|). \tag{1.600}$$

□

Lemme 1.435 ([17, 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 1.402, 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 $\lim_{n\to\infty} \varphi(x_n) = \bar{x}$.

(i) **$\varphi(x_k)$ est de Cauchy** Soit $\epsilon > 0$ dans $\mathbb{R}$. Nous considérons $\epsilon' \in \mathbb{Q}$ tel que $0 < \epsilon' < \epsilon$. Plus précisément tel que

$$0 < \varphi(\epsilon') < \epsilon. \tag{1.601}$$

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

$$\begin{aligned} |\varphi(x_p) - \varphi(x_q)| &= |\varphi(x_p - x_q)| && \text{(1.602a)}\\ &= \varphi\big(|x_p - x_q|\big) && \text{(1.602b)}\\ &\leqslant \varphi(\epsilon') && \text{(1.602c)}\\ &\leqslant \epsilon. && \text{(1.602d)} \end{aligned}$$

Justifications :

— Pour (1.602b). C'est le lemme 1.434.

— Pour (1.602c). L'application φ est croissante, lemme 1.416.

Donc la suite $\varphi(x_k)$ est de Cauchy.

(ii) **$\varphi(x_k) \xrightarrow{\mathbb{R}} \bar{x}$** 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 $\epsilon \in \mathbb{R}$.

(i) **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

$$x_p - \epsilon < x_n < x_p + \epsilon. \tag{1.603}$$

Ces inégalités sont dans $\mathbb{Q}$. Nous fixons p et nous commençons par écrire plus en détail la première inéquation :

$$x_p - \epsilon - x_n < 0. \tag{1.604}$$

Autrement dit, pour tout n nous avons

$$(\overline{x_p - \epsilon})_n < x_n. \tag{1.605}$$

Pour rappel, la suite $\overline{x_p - \epsilon}$ est la suite constante dans $\mathbb{Q}$. La suite

$$n \mapsto x_n - (\overline{x_p - \epsilon})_n \tag{1.606}$$

est dans $\mathcal{E}^+$. Donc, en vertu de la définition 1.413 nous avons

$$\bar{x} - \overline{x_p - \epsilon} \geqslant 0. \tag{1.607}$$

Nous pouvons aussi bien écrire

$$\bar{x} \geqslant \varphi(x_p) - \varphi(\epsilon). \tag{1.608}$$

En prenant l'autre inégalité de (1.603) nous trouvons de la même manière que

$$\bar{x} \leqslant \varphi(x_p) + \varphi(\epsilon). \tag{1.609}$$

Ces deux inégalités ensemble montrent que

$$\varphi(x_p) \in B\big(\bar{x}, \varphi(\epsilon)\big). \tag{1.610}$$

(ii) **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

$$\varphi(x_p) \in B\big(\bar{x}, \varphi(\epsilon')\big). \tag{1.611}$$

Étant donné que $\varphi(\epsilon') < \epsilon$ nous avons

$$\varphi(x_p) \in B\big(\bar{x}, \varphi(\epsilon')\big) \subset B\big(\bar{x}, \epsilon\big). \tag{1.612}$$

□

Proposition 1.436.
Soit une suite convergente $x_k \xrightarrow{\mathbb{Q}} q$. Alors

$$\varphi(x_k) \xrightarrow{\mathbb{R}} \varphi(q) \tag{1.613}$$

où φ est la fonction qui à un rationnel fait correspondre la classe de la suite constante correspondante[167].

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 1.391(1).

Le lemme 1.435 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. □

167. Voir les notations en 1.402.

Proposition 1.437 ([1]).
Deux choses à propos de suites de rationnels convergeant vers un réel.

(1) *Soit un réel x. Il existe une suite de rationnels strictement croissante qui converge vers x.*
(2) *Si de plus $x > 0$, alors la suite (toujours strictement croissante) peut être choisie parmi les rationnels strictement positifs.*

Démonstration. Le lemme 1.424 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 $0 < q_0 < x$. □

Théorème 1.438 (Complétude de $\mathbb{R}$, critère de Cauchy[17]).
Nous avons :

(1) *Le corps $\mathbb{R}$ est un corps complet (définition 1.367(5))*
(2) *Une suite dans $\mathbb{R}$ est convergente (définition 1.367(4)) si et seulement si elle est de Cauchy (définition 1.367(3)).*

Notez la grande similitude entre ce théorème et le théorème 7.258. 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.

Démonstration. Soit (x_n) une suite de Cauchy dans $\mathbb{R}$. Pour chaque n, il existe par le lemme 1.424 un $y_n \in \mathbb{Q}$ tel que

$$x_n - \frac{1}{n} < y_n < x_n + \frac{1}{n}. \tag{1.614}$$

(i) **(y_n) est une suite de Cauchy dans $\mathbb{Q}$** Nous prouvons que (y_n) est une suite de Cauchy dans $\mathbb{Q}$ (définition 1.367(3)). 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 :

$$|y_p - y_q| \leqslant |y_p - x_p| + |x_p - x_q| + |x_q - y_q| < \frac{1}{p} + \epsilon + \frac{1}{q}. \tag{1.615}$$

En choisissant $N_\epsilon > \max\{n_\epsilon, \frac{1}{\epsilon}\}$ (ce qui est possible par le lemme 1.421), et en prenant $p, q > N_\epsilon$, nous avons

$$|y_p - y_q| \leqslant 3\epsilon, \tag{1.616}$$

ce qui prouve que (y_p) est une suite de Cauchy dans $\mathbb{Q}$, pour la notion de suite de Cauchy dans $\mathbb{Q}$.

(ii) **Le réel représenté** Puisque (y_p) est de Cauchy dans $\mathbb{Q}$, elle représente un réel que nous notons $\bar{y}$.

(iii) **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 1.435). 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

$$|\bar{y} - x_p| \leqslant |\bar{y} - y_p| + |y_p - x_p| \leqslant \epsilon + \frac{1}{p}. \tag{1.617}$$

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 1.390.
□

Nous avons terminé avec la construction des réels. Les propriétés topologiques arrivent en la section 10.3. En particulier le théorème 7.258 pour la complétude de $\mathbb{R}$ en tant qu'espace métrique.

1.23.4 Intervalles

Nous avons déjà défini la notion d'intervalle pour un espace totalement ordonné en 1.20. Nous posons quelques notations dans $\mathbb{R}$.

Définition 1.439.
Soient $a \neq b$ dans $\mathbb{R}$. Nous définissons les parties suivantes de $\mathbb{R}$:

(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) $]-\infty,\infty[= \mathbb{R}$.

La proposition 1.447 nous dira que tous les intervalles de $\mathbb{R}$ sont d'une de ces formes.

1.23.5 Maximum, supremum et compagnie

Ce n'est un secret pour personne que $\mathbb{R}$ est un ensemble totalement ordonné[168] : 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 $\mathbb{R}$.

Définition 1.440.
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 1.441.
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.

△

Proposition-Définition 1.442 (Least-upper-bound property[77])**.**
Soit A une partie majorée de $\mathbb{R}$. Il existe un unique élément $M \in \mathbb{R}$ tel que

168. Proposition 1.414.

(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) $m \leqslant x$ *pour tout* $x \in A$,

(2) *pour tout* $\epsilon > 0$, *le nombre* $m + \epsilon$ *n'est pas un minorant.*

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.

(i) **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 1.424). Cela prouve que $m_2 + \epsilon$ est un minorant de A et donc que m_2 n'est pas un infimum.

(ii) **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) :

$$\begin{aligned} &x_0 \text{ est un élément de } A,\\ &x_1 \text{ est un minorant de } A,\\ &a_0 = x_0\\ &b_0 = x_1\\ &b_1 = x_1. \end{aligned} \tag{1.618}$$

Ensuite, nous faisons la récurrence suivante :

$$\begin{aligned} x_{n+1} &= \frac{a_n + b_n}{2},\\ a_{n+1} &= \begin{cases} a_n & \text{si } x_{n+1} \text{ minore } A\\ x_{n+1} & \text{sinon,} \end{cases}\\ b_{n+1} &= \begin{cases} x_{n+1} & \text{si } x_{n+1} \text{ minore } A\\ b_n & \text{sinon.} \end{cases} \end{aligned} \tag{1.619}$$

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

$$\begin{aligned} |a_n - b_n| &= |a_{n-1} - x_n|\\ &= \left|a_{n-1} - \frac{a_{n-1} + b_{n-1}}{2}\right|\\ &= \frac{1}{2}|a_{n-1} - b_{n-1}|, \end{aligned} \tag{1.620}$$

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

$$|a_n - a_{n-1}| = \begin{cases} 0\\ \left|\frac{a_n - b_n}{2}\right| \end{cases} \leqslant \frac{1}{2n}. \tag{1.621}$$

Il en est de même pour la suite (b_n). Ce sont deux suites de Cauchy (donc convergentes par la proposition 1.390) 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. □

Lemme 1.443.
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. □

Lemme 1.444.
Si A est une partie de $\mathbb{R}$, alors

$$\sup(A) = -\inf(-A). \tag{1.622}$$

Lemme 1.445.
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 $\sup(A)$.

1.23.5.1 Intervalles

Lemme 1.446 ([1])**.**
Soit une partie A de $\mathbb{R}$.

(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 1.442 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 :

$$x < \sup(A) - \epsilon < y < \sup(A). \tag{1.623}$$

□

Proposition 1.447 ([1])**.**
Tous les intervalles[169] *de $\mathbb{R}$ sont d'une des formes listées dans la définition 1.439.*

Démonstration. Il y a beaucoup de cas, et nous ne les feront pas tous[170].

(i) **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.

(ii) **Si $\inf(I) \in I$ et $\sup(I) \in I$** Nous prouvons que $I = [\inf(I), \sup(I)]$.

(i) **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 $x \in [\inf(I), \sup(I)]$.

(ii) **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 $x \in I$.

(iii) **$\inf(I) \in I$ et $\sup(I) \notin I$** Nous allons démontrer que $I = [\inf(I), \sup(I)[$.

169. Définition 1.20.
170. Si vous avez un doute, écrivez-moi.

(i) **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

$$\inf(I) \leqslant x < \sup(I), \tag{1.624}$$

ce qui montre que $I \subset [\inf(I), \sup(I)[$.

(ii) **Dans l'autre sens** Soit $x \in [\inf(I), \sup(I)[$. Nous utilisons le lemme 1.446(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 $I \subset [\inf(I), \sup(I)[$.

(iv) $\inf(I) \notin I$ **et** $\sup(I) \in I$ C'est le même raisonnement, mais en utilisant l'autre partie du lemme.

(v) $\inf(I) \notin I$ **et** $\sup(I) \notin I$ Nous prouvons que $I =]\inf(I), \sup(I)[$.

(i) **Dans un sens** Nous avons

$$I \subset \{x \in \mathbb{R} \text{ tel que } \inf(I) \leqslant x \leqslant \sup(I)\}. \tag{1.625}$$

Mais comme $\inf(I)$ et $\sup(I)$ ne sont pas dans I, nous pouvons les enlever dans le membre de droite :

$$I \subset \{x \in \mathbb{R} \text{ tel que } \inf(I) < x < \sup(I)\} =]\inf(I), \sup(I)[. \tag{1.626}$$

(ii) **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

$$\inf(I) < y_1 < x < y_2 < \sup(I). \tag{1.627}$$

Vu que I est un intervalle, nous en déduisons que $x \in I$.

(vi) $\inf(I) = -\infty$, $\sup(I) \in I$ Nous prouvons que $I =]-\infty, \sup(I)]$.

(i) **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.

(ii) **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. □

1.23.5.2 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 1.448.
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 :

$$10 = \max[0, 10] = \sup[0, 10] \quad 10 = \sup[0, 10[\tag{1.628}$$

Exemple 1.449.
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 1.450.
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. △

Lemme 1.451.
À propos de bornes d'un intervalle dans $\mathbb{R}$.

(1) *La borne inférieure*[171] *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, $a = \inf(I)$ en vérifiant les deux conditions de la définition 1.442. 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

$$a < a + \epsilon < b. \tag{1.629}$$

Dans ce cas, le lemme 1.424 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 1.452.
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.
(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 1.453.
Prenons $E = \{\frac{1}{n}$ tel que $n \in \mathbb{N}_0\}$, dont les premiers points sont indiqués sur la figure 1.1. 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. △

L'exemple suivant est une source classique d'erreurs en ce qui concerne l'infimum.

Exemple 1.454.
Les premiers points de l'ensemble $F = \{\frac{(-1)^n}{n}$ tel que $n \in \mathbb{N}_0\}$ sont représentés à la figure 1.2. 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. △

171. Ici par « borne inférieure » nous entendons le a dans les intervalles du type $]a,b]$, $[a,b]$, etc.

FIGURE 1.1 – Les premiers points du type $x_n = 1/n$.

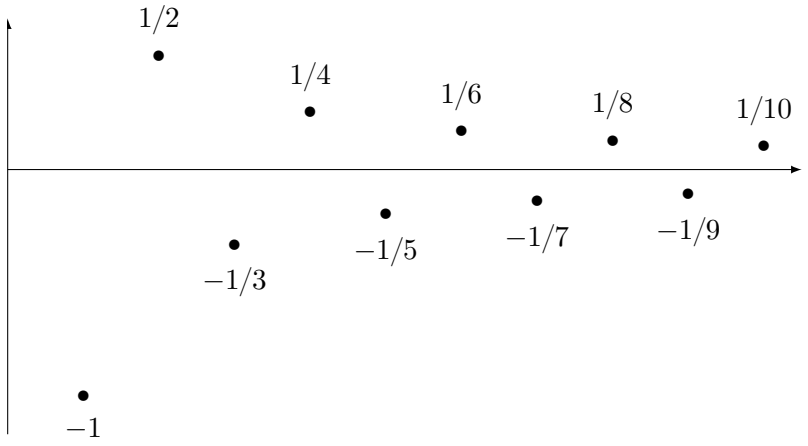


FIGURE 1.2 – Les quelques premiers points du type $(-1)^n/n$.

1.23.6 Racines

Dans cette section, nous définissons $\sqrt{x}$ pour $x \in \mathbb{Q}^+$. Vous notez que c'est fait de façon assez algébrique [172], 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 12.388). Il est même expliqué dans [72] que la méthode décrite ici permet de définir $\sqrt[n]{x}$ pour tout n entier, et pas seulement pour $n = 2$.

Proposition 1.455.
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 1.402, 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.

(i) **Existence** Si $q = 0$, c'est $r = 0$. Nous supposons $q > 0$. La suite (x_k) de la proposition 1.397 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

$$r = \bar{x}. \tag{1.630}$$

En ce qui concerne r^2, nous avons, par définition du produit dans $\mathbb{R}$,

$$r^2 = \bar{x}^2 = \overline{(x_k^2)}, \tag{1.631}$$

c'est la classe de la suite de Cauchy donnée par les x_k^2. Posons $y_k = x_k^2$; la relation (1.631) s'écrit

$$r^2 = \bar{y}. \tag{1.632}$$

172. Discutable parce que des limites sont utilisées.

La proposition 1.397 nous dit également que y est une suite de Cauchy et que

$$y_k \xrightarrow{\mathbb{Q}} q \tag{1.633}$$

La proposition 1.436 donne alors $\bar{y} = \bar{q}$, et finalement

$$r^2 = \bar{q} = \varphi(q). \tag{1.634}$$

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 : $(-r)^2 = r^2$.

(ii) **Unicité** Supposons $r_1, r_2 \in \mathbb{R}$ tels que $r_1^2 = r_2^2$. La proposition 1.414 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 :

$$r_2^2 = (r_1 + s)^2 = r_1^2 + 2r_1 s + s^2. \tag{1.635}$$

Vu que $r_1^2 = q = r_2^2$, nous avons $2r_1 s + s^2 = 0$ ou encore

$$s(2r_1 + s) = 0. \tag{1.636}$$

Puisque $\mathbb{R}$ est un corps, c'est un anneau intègre [173] 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 $r_1 = r_2$.

□

1.23.7 Corps valué

Définition 1.456 (Valeur absolue, corps valué[78, 79])**.**
*Soit un corps $\mathbb{K}$. Une **valeur absolue** sur $\mathbb{K}$ est une application $|.| : \mathbb{K} \to \mathbb{R}^+$ telle que*

(1) $|x| = 0$ si et seulement si $x = 0$,

(2) $|x + y| \leqslant |x| + |y|$

(3) $|xy| \leqslant |x||y|$.

*Un corps muni d'une valeur absolue est un **corps valué**.*

Un corps valué sera un espace topologique métrique dans la définition 7.168. Dans le cas d'un corps totalement ordonné, nous avons une valeur absolue donnée par 1.367(2) et les principales propriétés dans le lemme 1.371.

1.23.8 Partie entière, partie fractionnaire

Lemme-Définition 1.457 ([80])**.**
Pour tout réel x, il existe un unique entier n vérifiant

$$n \leqslant x < n + 1. \tag{1.637}$$

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 $\mathrm{int}(x)$. Le nombre $x - \mathrm{int}(x)$ est la **partie fractionnaire** de x que nous notons $\mathrm{frac}(x)$.*

Il est toutefois à noter que la partie fractionnaire de x n'est pas garantie d'être une fraction ; cette dénomination est donc un peu trompeuse.

Lemme 1.458.
Si $\lambda \in \mathbb{R}$ n'est pas un entier, alors $\mathrm{int}(\lambda) + 2 > \lambda$.

173. Lemme 1.193.

1.24 Les complexes

La notion de module d'un nombre complexe $|z|$ sera donnée beaucoup plus tard, dans le lemme 10.93. La raison est que le module demande la racine carrée.

Définition 1.459 (Nombres complexes[81]).
L'ensemble des ***nombres complexes*** $\mathbb{C}$ *est l'ensemble* $\mathbb{R}^2$ *muni des opérations suivantes :*

(1)

$$\begin{aligned} \times_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} &\to \mathbb{C} \\ \big((x,y),(x',y')\big) &\mapsto (xx'-yy',xy'+yx') \end{aligned} \tag{1.638}$$

(2)

$$\begin{aligned} +_{\mathbb{C}} : \mathbb{C} \times \mathbb{C} &\to \mathbb{C} \\ \big((x,y),(x',y')\big) &\mapsto (x+x',y+y') \end{aligned} \tag{1.639}$$

(3)

$$\begin{aligned} \cdot : \mathbb{R} \times \mathbb{C} &\to \mathbb{C} \\ \big(\lambda,(x,y)\big) &\mapsto (\lambda x,\lambda y). \end{aligned} \tag{1.640}$$

Lemme 1.460.
Le triplet $(\mathbb{C},+_{\mathbb{C}},\times_{\mathbb{C}})$ *est un anneau*[174] *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 :

$$\big((a,b)(x,y)\big)(s,t) = (ax-by,ay+bx)(s,t) \tag{1.641a}$$
$$= (axs-bys-ayt-bxt,axt-byt+ays+bxs). \tag{1.641b}$$

Nous avons utilisé la distributivité sur $\mathbb{R}$, provenant du fait que $\mathbb{R}$ est un corps par le théorème 1.401. □

Lemme 1.461.
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 1.430 et 1.431 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 $\mathbb{C}$:

$$z = \Big(\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}\Big). \tag{1.642}$$

Prouver que $z(a,b)=(1,0)$ est maintenant juste un calcul. □

Lemme 1.462.
L'application

$$\begin{aligned} \varphi : \mathbb{R} &\to \mathbb{C} \\ x &\mapsto (x,0) \end{aligned} \tag{1.643}$$

est un morphisme d'anneaux[175].

Démonstration. Simples calculs. Par exemple

$$\varphi(xx') = (xx',0) = (x,0)(x',0) = \varphi(x)\varphi(x'). \tag{1.644}$$

□

174. Définition 1.39.
175. Définition 1.40.

1.463.
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.

1.464.
À partir de maintenant, lorsque nous parlons de $\mathbb{R}$, nous parlons en réalité de $\varphi(\mathbb{R}) \subset \mathbb{C}$.

Lemme 1.465.
Nous avons $(0,1)^2 = (-1,0)$. *Nous notons* $i = (0,1)$.

Démonstration. Calcul direct à partir de la définition 1.638. □

La proposition suivante donne la forme cartésienne des nombres complexes. Pour la forme trigonométrique, il faudra attendre la proposition 18.64.

Proposition 1.466 ([1])**.**
L'application

$$\begin{aligned} f\colon \mathbb{R}^2 &\to \mathbb{C} \\ (a,b) &\mapsto a\varphi(1) + bi \end{aligned} \tag{1.645}$$

est un isomorphisme de $\mathbb{R}$*-module*[176].

Cette proposition permet d'écrire tout nombre complexe sous la forme $a + bi$ pour des réels a et b.

Définition 1.467.
Si $z = a + bi$ *est un nombre complexe (avec* $a, b \in \mathbb{R}$*), son* ***complexe conjugué*** *est le nombre* $a - bi$.

L'étude de la série géométrique est reportée à (beaucoup) plus tard, à la proposition 11.124. Dans l'immédiat il nous est possible de calculer la somme partielle.

Lemme 1.468 (Somme partielle de la série géométrique)**.**
Soit $q \in \mathbb{C}$. *Nous avons*

$$\sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}. \tag{1.646}$$

Démonstration. Posons $S_N = 1 + q + \ldots + q^N$. Nous avons évidemment $S_N - qS_N = 1 - q^{N+1}$ et donc

$$S_N = \sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}. \tag{1.647}$$

□

176. Module, définition 1.323.

Chapitre 2

Théorie des groupes

Pour rappel, la notion de groupe est définie en 1.35.

2.1 Groupes

2.2 Groupe dérivé

Définition 2.1.
*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 $g = h$, $[g,g] = ggg^{-1}g^{-1} = e$.

Définition 2.2.
*Le **groupe dérivé** de G est le sous-groupe noté $D(G)$ ou $[G,G]$ engendré*[1] *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 1.316, 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

$$D(G) = \bigcup_{m=1}^{\infty} S_m. \tag{2.1}$$

Lemme 2.3.
Le groupe dérivé est un sous-groupe caractéristique[2]*, et un sous-groupe normal*[3]*.*

Démonstration. Il est évident que si $\alpha \in \mathrm{Aut}(G)$ alors

$$\alpha\big([g,h]\big) = \big[\alpha(g), \alpha(h)\big], \tag{2.2}$$

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,

$$\begin{aligned} x(ghg^{-1}h^{-1})x^{-1} &= (xgx^{-1})(xhx^{-1})(xg^{-1}x^{-1})(xh^{-1}x^{-1}) && \text{(2.3a)}\\ &= (xgx^{-1})(xhx^{-1})(xgx^{-1})^{-1}(xhx^{-1})^{-1}. && \text{(2.3b)} \end{aligned}$$

□

Proposition 2.4.
Le groupe quotient $G/D(G)$ est abélien.

1. Définition 1.311.
2. Définition 1.168.
3. Définition 1.167.

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

$$[g][h] = [gh] = [ghh^{-1}g^{-1}hg] = [hg] = [h][g]. \tag{2.4}$$

□

Le groupe quotient $G/D(G)$ est appelé l'**abélianisé** de G et est parfois noté G^{ab}.

Si $f : G \to A$ 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 $\bar{f} : G/D(G) \to A$ telle que $f = \bar{f} \circ \pi$ où $\pi : G \to G/D(G)$ est la projection canonique.

2.3 Théorèmes d'isomorphismes

Définition 2.5.
*Soient un groupe G, un ensemble X et une application $f : X \to G$. Le **noyau** de f est la partie*

$$\ker(f) = \{x \in X \text{ tel que } f(x) = e\} \tag{2.5}$$

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 $\pi : G \to G/N$ est un morphisme surjectif de noyau N.

Théorème 2.6 (Premier théorème d'isomorphisme)**.**
Soit $\theta : G \to H$ un morphisme de groupe. Alors

(1) $\ker(\theta)$ *est normal dans G,*

(2) $\operatorname{Image}\theta$ *est un sous-groupe de H*

(3) nous avons un isomorphisme

$$\frac{G}{\ker(\theta)} \simeq \operatorname{Image}\theta \tag{2.6}$$

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 $\varphi([g]) = \theta(g)$.

□

Théorème 2.7 (Deuxième théorème d'isomorphisme)**.**
Soient H et N deux sous-groupes de G et supposons que N soit normal[4]*. 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.

(4) Nous avons l'isomorphisme

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}. \tag{2.7}$$

Démonstration. Point par point.

4. Si N n'est pas normal, il y aura la proposition 2.8.

(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,

$$nhn'h' = n\underbrace{hn'h^{-1}}_{\in N}hh' \in NH. \tag{2.8}$$

Cela prouve que NH est un groupe.

De la même façon, nous prouvons que HN est un groupe par

$$hnh'n' = hh'\underbrace{h'^{-1}nh'}_{\in N}n' \in HN \tag{2.9}$$

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.

(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

$$\begin{aligned} j\colon H &\to HN \\ h &\mapsto h \end{aligned} \tag{2.10}$$

et la surjection canonique

$$\sigma\colon HN \to HN/N \tag{2.11}$$

Nous considérons ensuite l'application composée

$$\begin{aligned} f\colon H &\to HN/N \\ h &\mapsto hN. \end{aligned} \tag{2.12}$$

(i) **f est surjective** L'application f est surjective parce que l'élément $hnN \in HN/N$ est l'image de h, étant donné que $hnN = hN$.

(ii) $\ker(f) = H \cap N$ 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[5] implique alors que $H/\ker(f) \simeq \text{Image}\, f$, c'est-à-dire

$$H/N \cap H \simeq HN/N. \tag{2.13}$$

□

Proposition 2.8 (Deuxième théorème d'isomorphisme (suite))**.**
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

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}. \tag{2.14}$$

Théorème 2.9 (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

$$(G/M)/(N/M) \simeq G/N. \tag{2.15}$$

5. Théorème 2.6.

Démonstration. Afin de montrer que N/M est normal dans G/M, nous considérons $g \in G$, $nM \in N/M$ et nous calculons

$$gnMg^{-1} = gng^{-1}\underbrace{gMg^{-1}}_{=M} = \underbrace{gng^{-1}}_{\in N}M \in N/M. \tag{2.16}$$

Pour prouver l'isomorphisme nous considérons le morphisme

$$\begin{aligned}\varphi\colon G/M &\to G/N\\ gM &\mapsto gN.\end{aligned} \tag{2.17}$$

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

$$(G/M)/\ker(\varphi) \simeq \text{Image}\,\varphi, \tag{2.18}$$

c'est-à-dire

$$(G/M)/(N/M) \simeq G/N. \tag{2.19}$$

□

2.4 Indice d'un sous-groupe et ordre des éléments

Lemme 2.10.
Lorsque H est normal dans G, alors la définition

$$[a] \cdot [b] = [ab] \tag{2.20}$$

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 (2.20) est une bonne définition : $[ah] \cdot [bh'] = [ab]$ pour tout $h, h' \in H$. Nous avons :

$$[ah] \cdot [bh'] = [ahbh'] = [ahb]. \tag{2.21}$$

Pour montrer que c'est $[ab]$, l'astuce est d'introduire bb^{-1} à côté du a :

$$[ahb] = [abb^{-1}hb] = [ab] \tag{2.22}$$

parce que $b^{-1}hb \in H$ du fait que H soit normal dans G. □

Exemple 2.11 ([82]).
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 2.

Il n'en est pas moins vrai que l'application

$$\begin{aligned}f\colon G &\to G/H\\ g &\mapsto [g]\end{aligned} \tag{2.23}$$

est un morphisme de groupes. △

Définition 2.12.
*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 6.61).

Théorème 2.13 (Théorème de Lagrange)**.**
Soit H un sous-groupe du groupe fini G. Alors

(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

$$|G/H| = \frac{|G|}{|H|}. \tag{2.24}$$

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

$$\begin{aligned} \varphi\colon H &\to gH \\ h &\mapsto gh. \end{aligned} \tag{2.25}$$

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 :

$$|G| = |H| \cdot \text{ nombre de classes.} \tag{2.26}$$

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. □

Corolaire 2.14.
L'ordre d'un élément[6] *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

$$H = \{g^k \text{ tel que } k \in \mathbb{N}\}. \tag{2.27}$$

Par le théorème de Lagrange 2.13, 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 3.30 et le lemme 3.32. En particulier le théorème de Cauchy 3.26 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.

2.5 Suite de composition

Définition 2.15 (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*

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \dots \subseteq G_1 \subseteq G_0 = G \tag{2.28}$$

et telle que G_{i+1} est normal[7] *dans G_i.*

6. Ordre d'un élément, définition 1.261.
7. Nous rappelons au cas où, que « normal » signifie « distingué ».

(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 2.21).

Lemme 2.16 (du papillon ou de Zassenhaus[83])**.**
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*

$$\frac{A'(A\cap B)}{A'(A\cap B')}\simeq\frac{(A\cap B)B'}{(A'\cap B)B'}\simeq\frac{B'(A\cap B)}{B'(A'\cap B)}. \tag{2.29}$$

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 $x,y\in A\cap B'$,

$$axby=xx^{-1}axbx^{-1}xy \tag{2.30}$$

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

$$x^{-1}a^{-1}=\underbrace{x^{-1}a^{-1}x}_{\in A'}x^{-1}. \tag{2.31}$$

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 $f\in A\cap B$. Alors

$$\begin{aligned}(bf)^{-1}(ax)(bf)&=(bf)^{-1}(a\underbrace{xbx^{-1}}_{=c\in A'}xf) &(2.32a)\\ &=f^{-1}b^{-1}acxf &(2.32b)\\ &=f^{-1}b^{-1}acf\underbrace{f^{-1}xf}_{=y\in A\cap B'} &(2.32c)\\ &=\underbrace{f^{-1}b^{-1}acf}_{\in A'}y &(2.32d)\\ &\in A'(A\cap B'). &(2.32e)\end{aligned}$$

Pour prouver l'isomorphisme

$$\frac{A'(A\cap B)}{A'(A\cap B')}\simeq\frac{(A\cap B)B'}{(A'\cap B)B'}, \tag{2.33}$$

nous allons utiliser le deuxième théorème d'isomorphisme (2.8) 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

$$\frac{A'(A\cap B')(A\cap B)}{A'(A\cap B')}\simeq\frac{A\cap B}{A\cap B\cap A'(A\cap B')}. \tag{2.34}$$

Pour simplifier un peu cette expression nous prouvons d'abord que

$$(A\cap B)\cap A'(A\cap B')=(A'\cap B)(A\cap B'). \tag{2.35}$$

L'inclusion $\supset$ est facile. Pour l'autre sens, étant donné que $A'(A\cap B')\subset A$ nous avons

$$A\cap B\cap A'(A\cap B)=B\cap A'(A\cap B). \tag{2.36}$$

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

$$B\cap A'(A\cap B)\subset (A'\cap B)(A\cap B) \tag{2.37}$$

et nous avons

$$(A\cap B)\cap A'(A\cap B)=B\cap A'(A\cap B)\subset (A'\cap B)(A\cap B'), \tag{2.38}$$

et donc l'égalité (2.35). Toujours dans l'idée de simplifier (2.34) 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

$$\frac{A'(A\cap B)}{A'(A\cap B')}=\frac{A\cap B}{(A'\cap B)(A\cap B')}. \tag{2.39}$$

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

$$\frac{B'(A\cap B)}{B'(A'\cap B)}=\frac{A'(A\cap B)}{A'(A\cap B')}. \tag{2.40}$$

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

$$bx=x\underbrace{x^{-1}bx}_{\in B'}\in (A\cap B)B'. \tag{2.41}$$

□

Proposition 2.17.
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 2.13 s'applique et, à chaque pas de la suite de composition, nous avons :

$$\left|\frac{G_i}{G_{i+1}}\right|=\frac{|G_i|}{|G_{i+1}|}. \tag{2.42}$$

Il suffit maintenant d'écrire $|G|$ de façon télescopique :

$$|G|=\prod_{0\leqslant i\leqslant n-1}\frac{|G_i|}{|G_{i+1}|} \tag{2.43}$$

□

Définition 2.18.
*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*

$$\frac{G_i}{G_{i+1}}\simeq\frac{H_{\sigma(i)}}{H_{\sigma(i)+1}}. \tag{2.44}$$

Proposition 2.19 (Schreider)**.**
Deux suites de composition d'un même groupe admettent des raffinements équivalents.

Démonstration. Soient les suites de composition

$$\{e\} = G_m \subseteq \ldots \subseteq G_1 \subseteq G_0 = G \tag{2.45a}$$
$$\{e\} = H_n \subseteq \ldots \subseteq H_1 \subseteq H_0 = G \tag{2.45b}$$

Nous raffinons la suite (G_i) en ajoutant, entre G_{i+1} et G_i, les sous-groupes

$$G_{i+1} = G_{i+1}(G_i \cap H_n) \subset G_{i+1}(G_i \cap H_{n-1}) \subseteq \ldots \subseteq G_{i+1}(G_i \cap H_0) = G_i, \tag{2.46}$$

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 2.16 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

$$\frac{G_{i+1}(G_i \cap H_k)}{G_{i+1}(G_i \cap H_{k+1})} \simeq \frac{H_{k+1}(H_k \cap G_i)}{H_{k+1}(H_k \cap G_{i+1})} \tag{2.47}$$

en vertu du lemme du papillon (2.16). Le membre de droite de (2.47) est un des quotients du raffinement de (H_j). □

Lemme 2.20 (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. □

Théorème 2.21 (Jordan-Hölder)**.**
À propos de suites de Jordan-Hölder dans un groupe fini.

(1) Tout groupe fini admet une suite de Jordan-Hölder.

(2) Toutes les suites de Jordan-Hölder dans un groupe fini sont équivalentes.

Démonstration. En deux parties.

(i) **Pour (1)**

(ii) **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 2.20. 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.

□

2.6 Groupes résolubles

Définition 2.22 (Groupe résoluble[84, 85])**.**
*Le groupe G est **résoluble** si il existe une suite finie de sous-groupes G_i*

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G \tag{2.48}$$

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[8] dont les quotients sont abéliens.

Lemme 2.23 ([86]).
Soit G un groupe et H un sous-groupe normal. Le groupe G/H est abélien si et seulement si[9] *$D(G) \subset H$.*

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 2.1.
— $D(G) \subset H$.

□

Proposition 2.24 ([86]).
Un groupe est résoluble si et seulement si sa suite dérivée termine sur $\{e\}$.

Démonstration. Grâce au lemme 2.3 et à la proposition 2.4, si la suite dérivée termine sur $\{e\}$ alors la suite dérivée est une suite qui répond aux conditions de la définition 2.22 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

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G \tag{2.49}$$

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 :

$$D^i(G) \subset G_{n-i}. \tag{2.50}$$

Vu que G_{n-i}/G_{n-i-1} est abélien, le lemme 2.23 dit que

$$D(G_{n-i}) \subset G_{n-i-1}. \tag{2.51}$$

En dérivant (2.50) et en tenant compte de (2.51),

$$D^{i+1}(G) \subset D(G_{n-i}) \subset G_{n-i-1}. \tag{2.52}$$

Nous avons donc bien $D^i(G) \subset G_{n-i}$ pour tout i. En particulier pour $i = n$, nous trouvons $D^n(G) \subset G_0 = \{e\}$. □

Proposition 2.25.
Soient des groupes G et H. Nous supposons que G est résoluble[10] *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

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{n-1} \subset G_n = G \tag{2.53}$$

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

$$\{e\} = \psi(G)_0 \subset \psi(G)_1 \subset \ldots \subset \psi(G)_{n-1} \subset \psi(G)_n = \psi(G). \tag{2.54}$$

La proposition 1.266 nous indique que $\psi(G)_i$ est normal dans $\psi(G)_{i+1}$, et que $\psi(G)_{i+1}/\psi(G)_i$ est abélien. □

8. Voir définition 2.15.
9. Ici $D(G)$ est le groupe dérivé de G, voir 2.2.
10. Définition 2.22.

2.7 Action de groupes

Le concept d'action d'un groupe est donné par la définition 1.360

Lemme 2.26.
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

$$(\phi_{g^{-1}}\phi_g)(x) = (\phi_{g^{-1}}\phi_g)(y), \tag{2.55}$$

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 [11] 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.

Définition 2.27 (Orbite)**.**
*Si G agit sur un ensemble E, nous notons $G \cdot x$ l'**orbite** de $x \in E$ sous l'action de G :*

$$G \cdot x = \{gx \text{ tel que } g \in G\}.$$

Définition 2.28 (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 :*

$$\mathrm{Stab}(x) = G_x = \{g \in G \text{ tel que } g \cdot x = x\}. \tag{2.56}$$

Définition 2.29 (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 :*

$$\mathrm{Fix}(g) = \{x \in E \text{ tel que } g \cdot x = x\}. \tag{2.57}$$

Définition 2.30.
*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*

$$(gx = x \quad \forall x \in E) \Rightarrow g = e. \tag{2.58}$$

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 23.95.

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 $g \cdot h = hg^{-1}$.

Définition 2.31.
*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

$$x \sim_g y \Leftrightarrow xh = y \tag{2.59}$$

11. Si vous décidez de dire ça à un jury dans un concours, soyez prêts à préciser les domaines.

pour un certain $h \in H$. Ensuite

$$x \sim_d y \Leftrightarrow hx = y \tag{2.60}$$

pour un certain $h \in H$.

Le lemme suivant est une généralisation du théorème de Lagrange 2.13.

Lemme 2.32.
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

$$\begin{aligned} f\colon (G/H)_g &\to (G/H)_d \\ [x]_g &\mapsto [x^{-1}]_d \end{aligned} \tag{2.61}$$

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

$$f([x]_g) = f([y]_g). \tag{2.62}$$

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

$$\begin{aligned} f\colon [x]_g &\to [y]_g \\ xh &\mapsto yh. \end{aligned} \tag{2.63}$$

(3) Le nombre d'éléments dans une classe est égal à $|H|$ par la bijection

$$\begin{aligned} g\colon [x]_g &\to H \\ xh &\mapsto h. \end{aligned} \tag{2.64}$$

Par conséquent

$$|G| = |H| \cdot \text{nombre de classes} = |H| \cdot \operatorname{Card}\big((G/H)_g\big), \tag{2.65}$$

et nous avons bien

$$\operatorname{Card}\big((G/H)_g\big) = \frac{|G|}{|H|} = |G : H|. \tag{2.66}$$

□

Proposition 2.33 (Orbite-stabilisateur[57])**.**
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.

(2) L'orbite de x est finie si et seulement si $\operatorname{Stab}(x)$ est d'indice fini dans G. Dans ce cas nous avons

$$\operatorname{Card}(G \cdot x) = |G : \operatorname{Stab}(x)|, \tag{2.67}$$

et

$$|G| = |\operatorname{Stab}(x)||\mathcal{O}_x|. \tag{2.68}$$

La formule (2.67) est nommée ***formule des classes****[87].*

Démonstration. En deux points.

(1) Soit l'application

$$\begin{aligned}\psi\colon G\cdot x &\to G/G_x\\ a\cdot x &\mapsto [a].\end{aligned} \tag{2.69}$$

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

$$A_y=s\operatorname{Stab}(x). \tag{2.70}$$

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

$$\bigcup_{y\in\mathcal{O}_x}A_y=G. \tag{2.71}$$

Les ensembles A_y divisent donc G en $|\mathcal{O}_x|$ paquets de $|\operatorname{Stab}(x)|$ éléments. D'où la formule (2.68).

□

Corolaire 2.34.
Soit C_g la classe de conjugaison d'un élément g du groupe fini G. Alors

$$\operatorname{Card}(C_g)=|G:Z_G(g)| \tag{2.72}$$

où $Z_G(g)$ est le centralisateur de g dans G[12] *de G.*

Démonstration. C'est une application de la proposition 2.33 (formule (2.67)) 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 :

$$\begin{aligned}\operatorname{Fix}(g)&=\{h\in G \text{ tel que } h\cdot g=g\} &(2.73a)\\ &=\{h\in G \text{ tel que } hgh^{-1}=g\} &(2.73b)\\ &=\{h\in G \text{ tel que } gh=hg\} &(2.73c)\\ &=Z_G(g). &(2.73d)\end{aligned}$$

Donc la formule $\operatorname{Card}(G\cdot g)=|G:G_g|$ devient, dans le cas de l'action adjointe de G sur lui-même : $\operatorname{Card}(C_g)=|G:Z_G(g)|$. □

Lemme 2.35.
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.

Corolaire 2.36 (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) $\operatorname{Card}(E)=\sum_i\operatorname{Card}(\mathcal{O}_i)$.

12. Définition 1.165.

Définition 2.37.
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 :

$$E = \bigsqcup_{g\in G} g(F) \tag{2.74}$$

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 $g(F) \cap g'(F) = \varnothing$.

Proposition 2.38 (Équation des classes[88])**.**
Soit G, un groupe fini opérant sur un ensemble E. Si E'' est un ensemble contenant exactement un élément de chaque orbite dans $E\backslash \operatorname{Fix}_G(E)$, alors

$$|G| = |\operatorname{Fix}_G(E)| + \sum_{x\in E''} \frac{|G|}{|\operatorname{Fix}_G(x)|}. \tag{2.75}$$

Si de plus G est un p-groupe, alors

$$|E| = |\operatorname{Fix}_G(E)| \mod p. \tag{2.76}$$

Démonstration. Par le corolaire 2.36, 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,

$$|G| = \operatorname{Card}(\operatorname{Fix}_G(E)) + \sum_{x\in E''} \frac{|G|}{|\operatorname{Fix}_G(x)|} \tag{2.77}$$

où nous avons utilisé le fait que $|G| = |\operatorname{Fix}_G(x)||\mathcal{O}_x|$.

Si G est un p-groupe alors si $x \in E''$, $\operatorname{Fix}_G(x)$ est un sous-groupe propre de G et donc $|\operatorname{Fix}_G(x)|$ est un diviseur propre de $|G|$. Du coup la fraction $|G|/|\operatorname{Fix}_G(x)|$ est une puissance non nulle de p et l'équation (2.75) devient immédiatement (2.76). □

Corolaire 2.39 (Équation des classes)**.**
Soient G un groupe, et $C_1,\ldots, C_l$ la liste de ses classes de conjugaison contenant plus d'un élément. Alors

$$\operatorname{Card}(G) = \operatorname{Card}\big(Z(G)\big) + \sum_i |G : Z_{g_i}| = \operatorname{Card}\big(Z(G)\big) + \sum_i \frac{\operatorname{Card}(G)}{\operatorname{Card}\big(\operatorname{Fix}(g_i)\big)} \tag{2.78}$$

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, $\operatorname{Card}(C_{g_i}) = |G : Z_{g_i}|$ par le théorème orbite-stabilisateur (proposition 2.33). □

Théorème 2.40 (Formule de Burnside)**.**
Si G est un groupe fini agissant sur l'ensemble fini E et si Ω est l'ensemble des orbites, alors

$$\operatorname{Card}(\Omega) = \frac{1}{|G|} \sum_{g\in G} \operatorname{Card}\big(\operatorname{Fix}(g)\big). \tag{2.79}$$

Démonstration. Nous considérons l'ensemble

$$A = \{(g, x) \in G \times E \text{ tel que } gx = x\}, \tag{2.80}$$

et nous en calculons le cardinal de deux façons. D'abord

$$\begin{aligned}\operatorname{Card}(A) &= \sum_{x\in E} \operatorname{Card}\{g\in G \text{ tel que } gx=x\} && (2.81a)\\ &= \sum_{x\in E} \operatorname{Card}(\operatorname{Fix}(x)) && (2.81b)\\ &= \sum_{\omega\in\Omega}\sum_{x\in\omega} \operatorname{Card}(\operatorname{Fix}(x)) && (2.81c)\\ &= \sum_{\omega\in\Omega} \frac{|G|}{\operatorname{Card}(\omega)} && (2.81d)\\ &= |G|. && (2.81e)\end{aligned}$$

Pour obtenir (2.81d) nous avons utilisé l'équation des classes (2.68). L'autre façon de calculer $\operatorname{Card}(A)$ est de regrouper ainsi :

$$\operatorname{Card}(A) = \sum_{g\in G} \operatorname{Card}\{x\in E \text{ tel que } gx=x\} = \sum_{g\in G} \operatorname{Card}(\operatorname{Fix}(g)). \tag{2.82}$$

En égalisant les deux expressions de $\operatorname{Card}(A)$ nous trouvons

$$|G|\operatorname{Card}(\Omega) = \sum_{g\in G} \operatorname{Card}(\operatorname{Fix}(g)). \tag{2.83}$$

□

Proposition 2.41.
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.

Proposition 2.42 ([89])**.**
L'indice du centre d'un groupe n'est jamais un nombre premier.

Lemme 2.43 ([90])**.**
Soient un groupe cyclique G et un sous groupe H.

(1) Il existe $r, n\in\mathbb{N}$ tels que $r \mid n$ et $H\simeq r\mathbb{Z}/n\mathbb{Z}$.

(2) $\operatorname{Card}(H) = n/r$

(3) H est cyclique.

En particulier, tout sous-groupe d'un groupe cyclique est cyclique.

Démonstration. En plusieurs parties.

(i) **Pour (1)** Soit un générateur a de G. L'application

$$\begin{aligned} f\colon \mathbb{Z} &\to G\\ k &\mapsto a^k \end{aligned} \tag{2.84}$$

est un morphisme de groupe surjectif.

La partie $f^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$. La proposition 1.228(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

$$n\mathbb{Z} = \ker(f) = f^{-1}(e) \subset f^{-1}(H) = r\mathbb{Z}. \tag{2.85}$$

Étant donné que $n\mathbb{Z}\subset r\mathbb{Z}$, il existe $d\in\mathbb{N}$ tel que $n = dr$.

Nous considérons maintenant

$$\begin{aligned} g\colon r\mathbb{Z} &\to H \\ k &\mapsto a^k, \end{aligned} \tag{2.86}$$

qui est encore un morphisme de groupes. En utilisant le premier théorème d'isomorphismes 2.6(3), nous avons

$$\frac{r\mathbb{Z}}{\ker(g)} \simeq \text{Image}(g). \tag{2.87}$$

Mais $\ker(g) = n\mathbb{Z}$ et $\text{Image}(g) = H$. Donc nous avons bien $H \simeq r\mathbb{Z}/n\mathbb{Z}$.

(ii) **Pour (2)** En ce qui concerne le cardinal, vu que nous avons un isompshisme,

$$\text{Card}(H) = \text{Card}(r\mathbb{Z}/n\mathbb{Z}) = n/r \tag{2.88}$$

par le lemme 1.322(3).

(iii) **Pour (3)** Le fait que H soit cyclique est le lemme 1.322(2).

□

Théorème 2.44 (Sous-groupe d'un groupe cyclique[90])**.**
Soit G un groupe cyclique[13] *d'ordre n. Pour chaque $d \in \mathbb{N}$ nous posons*

$$H_d = \{x \in G \text{ tel que } x^d = e\}. \tag{2.89}$$

(1) Ces H_d sont des sous-groupes de G.

(2) $\text{Card}(H_d) = d$.

(3) L'ensemble des sous-groupes de G est $\{H_d \text{ tel que } d \mid n\}$.

(4) Si g est un générateur de G, alors H_d peut être décrit des façons suivantes :

$$H_d = \{x \in G \text{ tel que } x^d = e\} = \text{gr}(g^{n/d}). \tag{2.90}$$

Démonstration. Point par point.

(i) **H_d est un sous-groupe** Si $g, h \in H_d$, alors $(gh)^d = g^d h^d = ee = e$. De plus $(g^{-1})^d = (g^d)^{-1} = e^{-1} = e$.

(ii) **Tout sous-groupe est un H_d avec $d \mid n$** Soit un sous-groupe H de G. Nous notons $\text{Card}(H) = d$. Le lemme 2.43(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

$$\text{ord}(a) \mid d. \tag{2.91}$$

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[14], nous avons $d \mid n$.

(iii) $\text{Card}(H_d) = d$ C'est contenu dans ce que nous avons fait dans la partie ii.

(iv) **Si $d \mid n$ alors H_d est un sous-groupe de G** C'est un cas particulier de la partie i.

13. Définition 1.319.
14. Théorème de Lagrange 2.13(1).

(v) **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 i), et que tous les sous-groupes de G sont de la forme H_d avec $d \mid n$.

(vi) **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

$$g^{n/d}, g^{2n/d}, \dots, g^{(d-1)n/d}, g^n = e \tag{2.92}$$

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

$$H_d = \{g^{kn/d}\}_{1,\dots,d}. \tag{2.93}$$

□

Définition 2.45.
*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 $g = g'$.*

2.8 Produit semi-direct de groupes

Définition 2.46.
*Une **suite exacte** est une suite d'applications comme suit :*

$$\dots \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots \tag{2.94}$$

où pour chaque i, les applications f_i et f_{i+1} vérifient $\ker(f_{i+1}) = \text{Image}(f_i)$. 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

$$1 \longrightarrow A \xrightarrow{f} G \xrightarrow{g} B \longrightarrow 1 \tag{2.95}$$

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.

Définition 2.47.
*Soient N et H deux groupes et un morphisme de groupes $\phi\colon H \to \text{Aut}(N)$. 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)*

$$(n, h) \cdot (n', h') = (n\phi_h(n'), hh'). \tag{2.96}$$

Attention à l'ordre quelque peu contre-intuitif. Lorsque nous notons $N \times_\phi H$, c'est bien $\phi\colon H \to \text{Aut}(N)$, 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 2.31.

Le théorème suivant permet de reconnaitre un produit semi-direct lorsqu'on en voit un.

Théorème 2.48 ([10]).
Soit une suite exacte de groupes

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{s} H \longrightarrow 1 \tag{2.97}$$

Si il existe un sous-groupe $\tilde{H}$ de G à partir duquel s est un isomorphisme, alors

$$G \simeq i(N) \times_\sigma \tilde{H} \tag{2.98}$$

où σ est l'action adjointe[15] *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.

(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 $G = \tilde{N}\tilde{H}$.

(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 $n = n'$.

(5) L'application

$$\begin{aligned} \phi\colon G &\to \tilde{N} \times \tilde{H} \\ nh &\mapsto (n, h) \end{aligned} \tag{2.99}$$

est une bijection. C'est une conséquence des points (3) et (4).

(6) Si sur $\tilde{N} \times \tilde{H}$ nous mettons le produit

$$(n, h) \cdot (n', h') = (n\sigma_h n', hh') \tag{2.100}$$

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

$$\begin{aligned} \phi(nhn'h') &= \phi(n \underbrace{hn'h^{-1}}_{\in\tilde{N}} hh') && \text{(2.101a)} \\ &= \phi\big((nhn'h^{-1})(hh')\big) && \text{(2.101b)} \\ &= (nhn'h^{-1}, hh') && \text{(2.101c)} \\ &= (n, h) \cdot (n', h') && \text{(2.101d)} \\ &= \phi(nh)\phi(n'h'). && \text{(2.101e)} \end{aligned}$$

□

Corolaire 2.49.
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 $n \in N$[16]*),*

(2) $H \cap N = \{e\}$,

(3) $HN = G$.

15. Le fait que H agisse sur $i(N)$ fait partie du théorème.
16. Ou encore que H agit sur N par automorphismes internes.

Alors l'application

$$\begin{aligned}\psi\colon N \times_\sigma H &\to G\\ (n,h) &\mapsto nh\end{aligned} \tag{2.102}$$

est un isomorphisme de groupes.

Démonstration. En plusieurs parties.

(i) ψ **est un morphisme** Simple calcul en utilisant la formule (2.96) du produit dans $N \times_\sigma H$:

$$\begin{aligned}\psi\big((n,h)(n',h')\big) &= \psi\big(n\sigma_h(n'),hh'\big) && \text{(2.103a)}\\ &= nhn'h^{-1}hh' && \text{(2.103b)}\\ &= nhn'h' && \text{(2.103c)}\\ &= \psi(n,h)\psi(n',h'). && \text{(2.103d)}\end{aligned}$$

(ii) ψ **est injective** Supposons que $\psi(n,h) = \psi(n',h')$. Alors $nh = n'h'$ et

$$n = n'h'h^{-1}. \tag{2.104}$$

En multipliant par $(n')^{-1}$ nous trouvons

$$h'h^{-1} = (n')^{-1}n \in N. \tag{2.105}$$

Donc $h'h^{-1} \in H \cap N = \{e\}$. Nous en déduisons que $h = h'$ et donc que $n = n'$.

(iii) 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

$$g = nh = \psi(n,h). \tag{2.106}$$

□

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.

2.9 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 2.50.
Le groupe additif $\mathbb{Q}/\mathbb{Z}$ est un groupe de torsion parce que si $[x] = [p/q]$, alors $q[x] = [p] = [0]$. △

2.10 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 1.224 où nous parlons d'idéal maximum propre. Comparez par exemple avec [43]. Soyez attentif.

En cas de doutes, nous suivons les conventions de Wikipédia.

3.1 Inversibles et nilpotents

Le concept d'anneau est la définition 1.39.

Lemme 3.1.
Si a et b commutent, nous avons, pour tout $r \in \mathbb{N}$ et $r > 0$, la formule

$$a^{r+1} - b^{r+1} = (a-b)\left(\sum_{k=0}^{r} a^{r-k}b^k\right). \tag{3.1}$$

Démonstration. Démontrons cela par récurrence. Le cas $r = 0$ est évident. Pour un r donné, si (3.1) 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 3.2.
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 (3.1) nous avons

$$1 = 1 - a^n = (1-a)(1 + a + \cdots + a^{n-1}) = (1 + a + \cdots + a^{n-1})(1-a). \tag{3.2}$$

La somme $1 + a + \cdots + a^{n-1}$ est donc un inverse de $(1-a)$. □

3.2 PGCD, PPCM et éléments inversibles

La définition de pgcd et ppcm dans un anneau commutatif est la définition 1.180. 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.

Proposition 3.3.
Dans un anneau intègre[1] *A, on a l'équivalence suivante concernant deux éléments $a, b \in A$:*

$$a \mid b \Leftrightarrow (b) \subset (a). \tag{3.3}$$

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 1.40 de morphisme d'anneaux. Remarquons que si f est un morphisme, nous avons $f(0) = 0$ et $f(x)^{-1} = f(x^{-1})$.

Lemme 3.4 ([91])**.**
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 3.5 ([91])**.**
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. □

3.2.1 Calcul effectif du PGCD et théorème de Bézout

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 (19.2).

Cela se base sur le lemme suivant.

Lemme 3.6.
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

$$\frac{a}{s} = \frac{qb}{s} + \frac{r}{s}$$

1. Définition 1.192.

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. □

Remarque 3.7.
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 :

$$a = q_2 b + r_2 \qquad r_2 < b \tag{3.4a}$$
$$b = q_3 r_2 + r_3 \qquad r_3 < r_2 \tag{3.4b}$$
$$\vdots \tag{3.4c}$$

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 $\text{pgcd}(a, b) = \text{pgcd}(r_{n-1}, r_n) = r_n$.

3.2.1.1 Algorithme d'Euclide pour le PGCD

Écrivons l'algorithme[92] en détail (parce que Bézout, ça va être la même chose en cinq fois plus compliqué). On pose

$$r_0 = a \tag{3.5a}$$
$$r_1 = b \tag{3.5b}$$

(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 :

$$r_2 = r_0 - q_2 r_1. \tag{3.6}$$

Ensuite, sachant r_2 nous pouvons continuer :

$$r_1 = q_3 r_2 + r_3 \tag{3.7}$$

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

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_k &= q_{k+2} r_{k+1} + r_{k+2} \end{aligned} \tag{3.8}$$

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 3.6 et le principe de l'algorithme d'Euclide nous donnent

$$\begin{cases} \text{pgcd}(r_k, r_{k+1}) = \text{pgcd}(r_{k+1}, r_{k+2}) = \text{pgcd}(a, b) & \text{(3.9a)} \\ 0 \leqslant r_{k+1} < r_k. & \text{(3.9b)} \end{cases}$$

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 (3.8) devient :

$$r_{n-1} = q_{n+1} r_n \tag{3.10}$$

avec $\text{pgcd}(a, b) = \text{pgcd}(r_n, r_{n-1}) = r_n$.

Exemple 3.8.
Calculons le PGCD de 18 et 231. Pour cela nous écrivons les divisions euclidiennes en chaine :

$$231 = 18 \cdot 12 + 15 \tag{3.11a}$$
$$18 = 1 \cdot 15 + 3 \tag{3.11b}$$
$$15 = 5 \cdot 5 + 0. \tag{3.11c}$$

Donc le PGCD est 3 (le dernier reste non nul). △

3.2.1.2 Algorithme étendu : calcul effectif des coefficients de Bézout

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

$$r_k = q_{k+2}r_{k+1} + r_{k+2}. \tag{3.12}$$

Nous voulons trouver les couples (u_k, v_k) de telle façon à avoir à chaque étape

$$r_n = u_k r_k + v_k r_{k-1}. \tag{3.13}$$

Notons que c'est à chaque fois r_n que nous construisons. La première équation de type Bézout à résoudre est

$$r_n = u_n r_n + v_n r_{n-1}, \tag{3.14}$$

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 :

$$r_n = u_k r_k + v_k r_{k-1} = u_{k-1}r_{k-1} + v_{k-1}r_{k-2}; \tag{3.15}$$

dans laquelle nous substituons $r_{k-2} = q_k r_{k-1} + r_k$:

$$u_k r_k + v_k r_{k-1} = u_{k-1}r_{k-1} + v_{k-1}(q_k r_{k-1} + r_k) \tag{3.16}$$
$$= (u_{k-1} + q_k v_{k-1})r_{k-1} + v_{k-1}r_k \tag{3.17}$$

et nous égalons les coefficients de r_k et r_{k-1} pour obtenir

$$\begin{cases} v_{k-1} = u_k & \text{(3.18a)} \\ u_{k-1} = v_k - v_{k-1}q_k. & \text{(3.18b)} \end{cases}$$

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

$$r_n = u_1 r_1 + v_1 r_0, \tag{3.19}$$

c'est-à-dire

$$\text{pgcd}(a, b) = u_1 b + v_1 a. \tag{3.20}$$

Nous avons ainsi trouvé des coefficients de Bézout pour a et b.

3.2.2 Générateurs

3.9.
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 :

$$[a]_n = \{a + kn \text{ tel que } k \in \mathbb{Z}\}. \tag{3.21}$$

Pour écrire les éléments de $\mathbb{Z}/n\mathbb{Z}$, nous pouvons écrire

$$\{[i]_n\}_{i=1,\dots,n} \tag{3.22}$$

ou

$$\{[i]_n \text{ tel que } 1 \leqslant i \leqslant n\}. \tag{3.23}$$

Mais attention : l'ensemble

$$\bigcup_{i=1}^{n}[i]_n \tag{3.24}$$

est très différent. Ce dernier ensemble est $\mathbb{Z}$.

Proposition 3.10 ([93]).
Soit $n \geqslant 2$.

(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

$$\begin{aligned}\varphi\colon \{1,\dots,n\} &\to \mathbb{Z}/n\mathbb{Z}\\ k &\mapsto [k]_n\end{aligned} \tag{3.25}$$

est une bijection.

(i) **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

$$l + tn \geqslant 1 + n > n, \tag{3.26}$$

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 $k = l$.

(ii) **Surjective** Soit $l \in \mathbb{Z}$. Nous allons montrer que $[l]_n$ est dans l'image de φ. Par la division euclidienne 1.215, 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. □

Proposition 3.11 ([93]).
Soit $n \geqslant 2$ et $m \in \mathbb{Z}$. Nous avons équivalence entre

(1) $\text{pgcd}(n, m) = 1$,

(2) $[m]_n$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

(3) $[m]_n$ est inversible dans $\big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big)$.

Démonstration. En trois parties.

(i) **(1) implique (2)** Si $\text{pgcd}(m, n) = 1$, le théorème de Bézout 1.229 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

$$[k]_n = uk[m]_n, \tag{3.27}$$

ce qui signifie que $[k]_n$ est bien un multiple de $[m]_n$ qui est donc générateur.

(ii) **(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 $\big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big)$.

(iii) **(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

$$km = 1 + ln. \tag{3.28}$$

Par le théorème de Bézout (pris dans l'autre sens), cela signifie que $\text{pgcd}(m, n) = 1$.

□

3.2.3 Décomposition en facteurs premiers

Lemme 3.12 (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 1.229 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. □

Lemme 3.13 (Lemme d'Euclide[94])**.**
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 3.12 implique que p divise b. □

Lemme 3.14.
Soient $a, b \in \mathbb{N}$ tels que a divise b et b divise a. Alors $a = b$.

Le théorème fondamental de l'arithmétique permet de décomposer des nombres en facteurs premiers.

Théorème 3.15 (Décomposition en facteurs premiers[95])**.**
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 [2].

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 3.13, 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. □

2. Voir 1.309.

Lemme 3.16 ([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

$$a = \prod_{p\in\mathcal{P}} p^{a_p} \quad et \quad b = \prod_{p\in\mathcal{P}} p^{b_p}. \tag{3.29}$$

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 3.15 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,

$$b = as = \prod_{p\in\mathcal{P}} p^{s_p+a_p}. \tag{3.30}$$

Par unicité de la décomposition de b (toujours le théorème 3.15), nous en déduisons que $b_p = s_p + a_p \geqslant a_p$.

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

$$as = \prod_{p\in\mathcal{P}} p^{s_p+a_p} = \prod_{p\in\mathcal{P}} p^{b_p} = b. \tag{3.31}$$

Donc $a \mid b$. □

Lemme 3.17.
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 3.15 nous dit que

$$a = q^{a_1} \prod_{i\neq 1} p_i^{a_i} \tag{3.32}$$

et

$$a^n = q^{na_1} \prod_{i\neq 1} p_i^{na_i} \tag{3.33}$$

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.

□

Corolaire 3.18.
Si $n \in \mathbb{N}$ n'est pas une puissance d'un nombre premier, alors il existe $a, b \in \mathbb{N}$ tels que $\operatorname{pgcd}(a, b) = 1$ *et $n = ab$.*

Démonstration. Si n n'est pas une puissance d'un nombre premier, alors le théorème 3.15 de décomposition en nombres premiers dit que

$$n = \prod_{i=1}^{r} p_i^{k_i} \tag{3.34}$$

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 3.17. Étant donné que q divise $\prod_{i=2}^{r} p_i^{k_i}$, il divise au moins un des facteurs (lemme d'Euclide 3.13). 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. □

Lemme 3.19 ([1])**.**
Dans $\mathbb{N}$, le pgcd[3] 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 3.16 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. □

Lemme 3.20.
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.

Lemme 3.21 ([1])**.**
Soient $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}$ tels que $ab = q^k$ et $\gcd(a, b) = 1$. 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 3.15 :

$$a = \prod_i p_i^{a_i} \tag{3.35a}$$

$$b = \prod_i p_i^{b_i} \tag{3.35b}$$

$$q = \prod_i p_i^{q_i}. \tag{3.35c}$$

D'un part, en utilisant la commutativité et l'associativité du produit,

$$ab = \prod_i p_i^{a_i + b_i}. \tag{3.36}$$

D'autre part, puisque $ab = q^k$, nous avons

$$ab = (\prod_i p_i^{q_i})^k = \prod_i p_i^{kq_i}. \tag{3.37}$$

En vertu de l'unicité de la décomposition en facteurs premiers, pour chaque i nous avons

$$a_i + b_i = kq_i. \tag{3.38}$$

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 (3.35a) :

$$a = \prod_i p_i^{ks_i} = (\prod_i p_i^{s_i})^k, \tag{3.39}$$

de telle sorte que a soit une puissance k^{e}. La même chose tient pour b. □

3. Le pgcd et ppcm sont définis dans 1.180.

Proposition 3.22.
Soient $a, b \in \mathbb{Z}\backslash\{0\}$ décomposés en $a = \prod_{p\in\mathcal{P}} p^{a_p}$ et $b = \prod_{p\in\mathcal{P}} p^{b_p}$. En posant

$$m_p = \min\{a_p, b_p\} \tag{3.40a}$$
$$M_p = \max\{a_p, b_p\}, \tag{3.40b}$$

nous avons

$$\operatorname{pgcd}(a, b) = \prod_{p\in\mathcal{P}} p^{m_p} \tag{3.41a}$$
$$\operatorname{ppcm}(a, b) = \prod_{p\in\mathcal{P}} p^{M_p}. \tag{3.41b}$$

Pour rappel, la définition de pgcd et ppcm sont dans 1.180.

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.

(i) **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 3.16 nous dit alors que $\delta \mid a$ et $\delta \mid b$.

(ii) **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 $\{a, b\}$.

(i) **a et b divisent μ** Pour tout p, nous avons $M_p \geqslant a_p$. Le lemme 3.16 implique que $a \mid \mu$. Idem pour b, donc tous les éléments de $\{a, b\}$ divisent μ.

(ii) **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 3.19), nous avons prouvé que δ et μ sont les nombres recherchés. □

Corolaire 3.23.
Soit un nombre premier p. Un élément $m \in \mathbb{Z}^*$ vérifie $\operatorname{pgcd}(m, p^n) \neq 1$ 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 3.15, 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 3.22 :

$$\operatorname{pgcd}(m, p^n) = \prod_{s\in\mathcal{P}} s^{\min\{a_s, b_s\}}. \tag{3.42}$$

Le minimum est toujours zéro lorsque $s \neq p$, donc $\operatorname{pgcd}(m, p^n) = p^{\min\{a_s, n\}}$.

Nous avons donc $\operatorname{pgcd}(m, p^n) \neq 1$ si et seulement si $a_p \neq 0$. Mais $a_p \neq 0$ si et seulement si m est un multiple de p. □

Lemme 3.24.
Un entier $n \geqslant 1$ 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 $n \geqslant 2$.

En ce qui concerne l'existence, nous décomposons n en facteurs premiers [4] et nous séparons les

4. Théorème 3.15.

puissances paires des puissances impaires :

$$n = \prod_{i=1}^{r} p_i^{2\alpha_i} \prod_{j=1}^{s} q_j^{2\beta_j+1} \tag{3.43a}$$

$$= \underbrace{\left(\prod_{i=1}^{r} p_i^{2\alpha_i} \prod_{j=1}^{s} q^{2\beta_j} \right)}_{m^2} \underbrace{\prod_{j=1}^{s} q_j}_{q}. \tag{3.43b}$$

Nous passons à l'unicité. Supposons que $n = q_1 m_1^2 = q_2 m_2^2$ avec q_1 et q_2 sans facteurs carrés (dans leur décomposition en facteurs premiers). Soit $d = \text{pgcd}(m_1, m_2)$ et k_1, k_2 définis par $m_1 = dk_1$, $m_2 = dk_2$. Par construction, $\text{pgcd}(k_1, k_2) = 1$. Étant donné que

$$n = q_1 d^2 k_1^2 = q_2 d^2 k_2^2, \tag{3.44}$$

nous avons $q_1 k_1^2 = q_2 k_2^2$ et donc k_1^2 divise $q_2 k_2^2$. 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 (3.44) se réduit à $n = q_1 m_1^2 = q_2 l^2 m_1^2$ et donc

$$q_1 = q_2 l^2, \tag{3.45}$$

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 15.118 que la somme des inverses des nombres premiers diverge. Pour comparaison, la somme des inverses des carrés converge par la proposition 11.125. 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.

3.2.4 Ordre d'un élément dans un groupe fini

Voir plus d'informations dans la partie 5.2 sur les groupes monogènes.

Lemme 3.25 ([1]).
Si g est un élément d'ordre s, et si $g^r = e$, alors $s \mid r$.

Théorème 3.26 (Théorème de Cauchy[96, 97]).
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.

(i) **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.

(ii) **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 2.14). Donc

$$g^{kd} = e. \tag{3.46}$$

Le lemme 3.25 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 :

$$h = g^{tn/d} = (g^{n/d})^t \in \text{gr}(g^{n/d}). \tag{3.47}$$

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.

Lemme 3.27 ([98]).
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

$$a^{r_1s_1}b^{r_1s_1} = (ab)^{r_1s_1} = 1, \tag{3.48}$$

que nous élevons à la puissance r_2 où r_2 est défini en posant $r = r_1r_2$:

$$a^{rs_1}b^{rs_1} = 1. \tag{3.49}$$

Et comme $a^{rs_1} = 1$, nous concluons que $b^{rs_1} = 1$. Donc $s \mid rs_1$. Par le lemme de Gauss 3.12, 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 $r_1s_1 = rs$. □

Lemme 3.28 ([57]).
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 2.13) 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 1.258. □

Lemme 3.29 ([99]).
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 $a^m \in H$. □

Proposition 3.30 ([99]).
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 3.29. Étant donné que m et n sont premiers entre eux, par le théorème de Bézout 1.229, il existe $a, b \in \mathbb{Z}$ tels que

$$am + bn = 1. \tag{3.50}$$

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 $|H'| = |H| = |G|/m$. □

3.31.
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.

Lemme 3.32.
L'ensemble des ordres d'un groupe commutatif est stable par PPCM[5].

5. Définition 1.180.

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 $\text{ppcm}(r,s)$.

Démonstration. Soit $m = \text{ppcm}(r,s)$. Afin d'écrire m sous une forme pratique, nous considérons les décompositions en facteurs premiers de r et s :

$$r = \prod_{i=1}^{k} p_i^{\alpha_i} \tag{3.51a}$$

$$s = \prod_{i=1}^{k} p_i^{\beta_i} \tag{3.51b}$$

où $\{p_i\}_{i=1,\dots,k}$ est l'ensemble des nombres premiers arrivant dans les décompositions de r et de s. Si nous posons

$$r' = \prod_{\substack{i=1\\ \alpha_i > \beta_i}}^{k} p_i^{\alpha_i} \tag{3.52a}$$

$$s' = \prod_{\substack{i=1\\ \alpha_i \leqslant \beta_i}}^{k} p_i^{\beta_i}, \tag{3.52b}$$

alors $\text{ppcm}(r,s) = r's'$ 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 3.27 pour conclure que l'ordre de $x^{r/r'}y^{s/s'}$ est $r's' = m$. □

3.2.5 Écriture des fractions

Théorème 3.33 ([100]).
Tout élément de $\mathbb{Q}^+$ s'écrit de façon unique comme quotient de deux entiers premiers entre eux.

Démonstration. En deux parties[6]

(i) **Unicité** Supposons avoir $\frac{a}{b} = \frac{c}{d}$ avec $\text{pgcd}(a,b) = \text{pgcd}(c,d) = 1$. Nous avons

$$ad = bc \tag{3.53}$$

donc

(1) a divise bc mais est premier avec b donc a divise c par le lemme de Gauss 3.12.

(2) c divise ad mais est premier avec d donc c divise a par le lemme de Gauss 3.12.

En conclusion a divise c et c divise a, ergo[7] $a = c$. L'égalité $b = d$ est alors immédiate.

(ii) **Existence** Soit le quotient $\frac{a}{b}$. Nous avons

$$\frac{a}{b} = \frac{a/\text{pgcd}(a,b)}{b/\text{pgcd}(a,b)}, \tag{3.54}$$

qui est encore un quotient d'entiers parce que $\text{pgcd}(a,b)$ divise aussi bien a que b. Il faut montrer que les nombres $a/\text{pgcd}(a,b)$ et $b/\text{pgcd}(a,b)$ sont premiers entre eux. Pour cela nous supposons que k est un diviseur commun. En particulier, les nombres $a/k\,\text{pgcd}(a,b)$ et $b/k\,\text{pgcd}(a,b)$ sont des entiers, ce qui fait que $k\,\text{pgcd}(a,b)$ est un diviseur commun de a et b. Étant donné que $\text{pgcd}(a,b)$ est le plus grand tel diviseur, nous devons avoir $k\,\text{pgcd}(a,b) = \text{pgcd}(a,b)$ c'est-à-dire que $k = 1$. Donc les nombres $a/\text{pgcd}(a,b)$ et $b/\text{pgcd}(a,b)$ sont premiers entre eux.

6. Définitions des pgcd et ppcm en 1.180.
7. Lemme 3.14.

□

Proposition 3.34 ([1]).
Soient $l, l, d_1, d_2 \in \mathbb{N}$ tels que

$$\frac{k}{d_1} = \frac{l}{d_2} \tag{3.55}$$

avec $\text{pgcd}(k, d_1) = 1$.
Alors

(1) $d_1 \leqslant d_2$

(2) $d_1 = \frac{d_2}{\text{pgcd}(l,d_2)}$.

Proposition 3.35.
Les entiers p et q sont premiers entre eux[8] *si et seulement si p^2 et q^2 sont premiers entre eux.*

Démonstration. En deux parties.

(i) $\Rightarrow$ 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 3.17 implique que δ divise p et q. Donc p et q ne sont pas premiers entre eux.

(ii) $\Leftarrow$ Si p^2 et q^2 sont premiers entre eux, par le théorème de Bézout 1.229 il existe $a, b \in \mathbb{Z}$ tels que

$$ap^2 + bq^2 = 1 \tag{3.56}$$

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 3.36.

Nous avons déjà vu dans la proposition 1.393 que $\sqrt{2}$ était irrationnel. En fait le théorème suivant va nous montrer que le nombre $\sqrt{n}$ est soit entier, soit irrationnel.

Théorème 3.36.
Soit $n \in \mathbb{N}$. Le nombre $\sqrt{n}$ est rationnel si et seulement si n est un carré parfait.

Démonstration. Supposons que $\sqrt{n}$ soit rationnel. Le théorème 3.33 nous donne $p, q \in \mathbb{N}$ premiers entre eux tels que $\sqrt{n} = p/q$. La proposition 3.35 nous enseigne de plus que p^2 et q^2 sont premiers entre eux. Nous avons

$$p^2 = nq^2. \tag{3.57}$$

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. □

3.2.6 Équation diophantienne linéaire à deux inconnues

Soient a, b et c des entiers naturels donnés. Nous considérons l'équation

$$ax + by = c \tag{3.58}$$

à résoudre[101] 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

$$d(a'x + b'y) = c, \tag{3.59}$$

8. Premiers entre eux, définition 1.252.

et donc si c n'est pas un multiple de d, il n'y a pas de solution[9]. Si par contre c est un multiple de d alors nous écrivons $c = c'd$ et l'équation devient

$$a'x + b'y = c' \tag{3.60}$$

C'est maintenant que nous utilisons le théorème de Bézout 1.229 : puisque a' et b' sont premiers entre eux, nous avons la relation $a'u + b'v = 1$ pour certains[10] 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 :

$$a'(x - c'u) = b'(c'v - y). \tag{3.61}$$

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[11] diviser $c'v - y$. Disons $c'v - y = ka'$. Alors $a'(x - c'u) = b'ka'$ et donc

$$x = b'k + c'u. \tag{3.62}$$

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

$$\begin{cases} x = b'k + c'u & \text{(3.63a)} \\ y = vc' - a'k & \text{(3.63b)} \end{cases}$$

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 (3.63) sont solutions.

Exemple 3.37.
Résoudre l'équation $2x + 6y = 52$.

Nous pouvons factoriser 2 dans le membre de gauche et simplifier alors toute l'équation par 2 :

$$x + 3y = 26. \tag{3.64}$$

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

$$x + 3y = 26 \times (-5 + 3 \times 2), \tag{3.65}$$

et donc $x + 5 \times 26 = -3(y - 26 \times 2)$, et en posant $k = y - 26 \times 2$ nous avons

$$x = -3k - 130. \tag{3.66}$$

En injectant nous trouvons l'équation $3y - 3k - 130 = 26$ et donc

$$y = 52 + k. \tag{3.67}$$

△

3.2.7 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.

9. Exemple : $8x + 2y = 9$. Le membre de gauche est certainement un nombre pair et il n'y a donc pas de solution.
10. Nous avons décrit un algorithme pour les trouver en démontrant l'équation 3.20.
11. C'est Gauss 3.12 qui le dit, et vous savez que lorsque Gauss dit, c'est *forcément* vrai.

Proposition 3.38.
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 $\mu\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. 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 1.215 donne l'existence de q et r avec $0 \leqslant r < n$ et $q \geqslant 0$ tels que

$$x_0 = nq + r. \tag{3.68}$$

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

$$\mathbb{Z}/n\mathbb{Z} = \mu(\mathbb{Z}) = \mu(\mathbb{N}_{n-1}). \tag{3.69}$$

La restriction $\mu\colon \mathbb{N}_{n-1} \to \mathbb{Z}/n\mathbb{Z}$ 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 3.39 ([102]).
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 1.215, 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

$$q^n = (q^d)^a q^b \in [1]_{q^d-1} q^b = [q^b]_{q^d-1}. \tag{3.70}$$

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

$$q^n \in [1]_{q^d-1}. \tag{3.71}$$

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

$$[1]_{q^d-1} = [q^b]_{q^d-1}, \tag{3.72}$$

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. □

3.3 Binôme de Newton et morphisme de Frobenius

Lemme 3.40 ([1]).
Nous considérons ces deux ensembles :

$$A = \{I = (i_1, \dots, i_k) \text{ tel que } 1 \leqslant i_1 < \dots < i_k \leqslant n\} \tag{3.73a}$$

$$C = \big\{\text{parties de cardinal } k \text{ dans } \{1, \dots, n\}\big\}. \tag{3.73b}$$

Il existe une bijection entre A et C.

Nous avons de plus

$$\text{Card}(C) = \binom{n}{k} \tag{3.74}$$

*où les $\binom{n}{k}$ sont les **coefficients binomiaux** donnés par*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{3.75}$$

Proposition 3.41 ([103]).
Pour tout x, $y \in \mathbb{R}$ et $n \in \mathbb{N}$, nous avons

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \tag{3.76}$$

où les coefficients binomiaux sont donnés dans le lemme 3.40.

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 (3.76) soit vraie pour $n \geqslant 1$, et prouvons la pour $n+1$. Nous avons

$$\begin{aligned}(x+y)^{n+1} &= (x+y) \cdot \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \\ &= \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1} \\ &= x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} + y^{n+1}.\end{aligned} \tag{3.77}$$

La seconde grande somme peut être transformée en posant $i = k+1$:

$$\sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} = \sum_{i=1}^{n} \binom{n}{i-1} x^{n-(i-1)} y^{i-1+1}, \tag{3.78}$$

dans lequel nous pouvons immédiatement renommer i par k. En remplaçant dans la dernière expression de (3.77), nous trouvons

$$(x+y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n-k+1} y^k. \tag{3.79}$$

La thèse découle maintenant de la formule

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \tag{3.80}$$

qui est vraie parce que

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!(n-k+1) + n!k}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n+1-k)!}, \tag{3.81}$$

par simple mise au même dénominateur. □

Lemme 3.42 ([1]).
Si $n \geqslant k$ nous avons

$$\frac{n!}{k!(n-k)!} \leqslant \frac{n^{k-1}}{k!}. \tag{3.82}$$

Démonstration. Nous décomposons le produit définissant $n!$ en les facteurs entre 1 et $n-k$ et ceux entre $n-k+1$ et n :

$$n! = (n-k)! \prod_{i=n-k+1}^{n} i \leqslant n^{k-1}(n-k)!. \tag{3.83}$$

Donc

$$\frac{n!}{k!(n-k)!} \leqslant \frac{n^{k-1}}{k!}. \tag{3.84}$$

□

Tant que nous sommes à démontrer des égalités, en voici une.

Lemme 3.43 ([104]).
Pour $a, b \in \mathbb{R}$ et $n \in \mathbb{N}$ nous avons

$$a^n + (-1)^{n-1}b^n = (a+b)\sum_{k=0}^{n-1}(-1)^k a^{n-1-k}b^k. \tag{3.85}$$

Démonstration. C'est un simple calcul :

$$(a+b)\sum_{k=0}^{n-1}(-1)^k a^{n-1-k}b^k = \sum_{k=0}^{n-1}(-1)^k a^{n-k}b^k + \sum_{k=0}^{n-1}(-1)^k a^{n-k-1}b^{k+1} \tag{3.86a}$$

$$= a^n + \sum_{k=1}^{n-1}(-1)^k a^{n-k}b^k + \sum_{k=0}^{n-2}(-1)^k a^{n-k-1}b^{k+1} + (-1)^{n-1}b^n \tag{3.86b}$$

$$= a^n + (-1)^{n-1}b^n \tag{3.86c}$$

Justifications.

— Pour (3.86b). Dans la première somme, nous avons séparé le terme $k = 0$ et dans la seconde nous avons séparé le terme $k = n - 1$

— Pour (3.86c). 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.

□

Proposition 3.44.
Soit A un anneau commutatif de caractéristique première p. Alors $\sigma(x) = x^p$ est un automorphisme de l'anneau A. Nous avons la formule

$$(a+b)^p = a^p + b^p \tag{3.87}$$

pour tout $a, b \in A$.

Démonstration. Nous utilisons la formule du binôme de la proposition 3.41 et le fait que les coefficients binomiaux non extrêmes sont divisibles par p et donc nuls. □

3.4 Polynômes de plusieurs variables

Définition 3.45.
*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

$$(PQ)(k_1, \dots, k_n) = \sum_{\substack{(l_1,\dots,l_n),(m_1,\dots,m_n)\in\mathbb{N}^n\times\mathbb{N}^n \\ l_i+m_i=k_i}} P_{l_1,\dots,l_n}Q_{m_1,\dots,m_n}. \tag{3.88}$$

3.46.
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.

Définition 3.47.
*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*

$$P(x_1, \dots, x_n) = \sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} P_{k_1,\dots,k_n}x_1^{k_1}\dots x_n^{k_n}. \tag{3.89}$$

Notez que la somme, bien que sur $\mathbb{N}^n$, est une somme finie.

3.48.
Comme dans le cas des polynômes d'une seule variable, les X_i dans la notation $A[X_1, \ldots, X_n]$ 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

$$X_1(k_1, \ldots, k_n) = \begin{cases} 1 & \text{si } (k_1, \ldots, k_n) = (1, 0 \ldots, 0) \\ 0 & \text{sinon.} \end{cases} \tag{3.90}$$

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 $A[X_1, \ldots, X_n]$ sont des indices muets. L'anneau $A[X_1, \ldots, X_n]$ est exactement le même que $A[T_1, \ldots, T_n]$.

3.4.1 Divisibilité et classes d'association

Définition 3.49.
*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.*

Lemme 3.50.
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,

$$b(1 - yx) = 0. \tag{3.91}$$

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. □

Lemme 3.51.
Si A est un anneau et si $a \in A$, la classe d'association de a est $aU(A)$ où $U(A)$ est l'ensemble des éléments inversibles de A.

Exemple 3.52.
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 :

$$(2 + i)(4 + i) = 7 + 6i. \tag{3.92}$$

△

Exemple 3.53.
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. △

¡¡ Avertissement/question à la lectrice !! 3.54
Est-ce que quelqu'un connaît un anneau contenant $\mathbb{Z}$ dans lequel 7 est divisible en 2 ?

Peut-être $\mathbb{Z}$ étendu par tous les $1/2^n$?

3.4.2 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 1.180.

Lemme 3.55.
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 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.

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 3.50), 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 $\delta = \operatorname{pgcd}(S)$.

Remarque 3.56.
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.

3.4.3 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.

Proposition 3.57.
Un anneau fini intègre est un corps.

Démonstration. Soit A un tel anneau. Soit $a \neq 0$. Les applications

$$l_a : x \mapsto ax \tag{3.93a}$$
$$r_a : x \mapsto xa \tag{3.93b}$$

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 [12]

$$b = b(ac) = (ba)c = c. \tag{3.94}$$

Par conséquent b est un inverse de a. □

Proposition 3.58.
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.

12. 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.

Démonstration. L'équivalence entre les deux premiers points est le contenu du corolaire 1.236. Le fait que $\mathbb{Z}/n\mathbb{Z}$ soit un corps lorsque $\mathbb{Z}/n\mathbb{Z}$ est intègre est la proposition 3.57. 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 1.193). □

3.5 Anneau factoriel

Définition 3.59 (Anneau factoriel)**.**
Un anneau commutatif A est ***factoriel*** *si il vérifie les propriétés suivantes.*

(1) L'anneau A est intègre[13]*.*

(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[14]*.*

(3) Si $a = q_1 \dots q_m$ est une autre décomposition de a en irréductibles, alors $m = k$ et il existe une permutation[15] *$\sigma \in S_k$ telle que p_i et $q_{\sigma(i)}$ soient associés*[16]*.*

Un anneau factoriel permet de caractériser le pgcd et le ppcm de nombres.

Lemme 3.60 ([105])**.**
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 3.59(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 :

$$pq_1 \dots q_k = x_1 \dots x_m y_1 \dots y_l. \tag{3.95}$$

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[17]

$$x = pux_1 \dots x_{i-1}x_{i+1} \dots x_m. \tag{3.96}$$

Donc p divise x et fin de l'histoire. □

Proposition 3.61 ([105])**.**
Dans un anneau factoriel, tout élément irréductible est premier[18]*.*

Démonstration. Soit un anneau factoriel A et un élément irréductible p dans A. Nous devons prouver qu'il est premier.

(i) **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.

(ii) **Non inversible** L'élément p est non inversible parce que c'est dans la définition d'un élément irréductible.

(iii) **Si $p \mid xy$** Si p divise xy, alors il divise x ou y ; c'est le lemme 3.60.

□

Lemme 3.62 ([1])**.**
Si A est un anneau factoriel, et si p est irréductible dans A, alors :

(1) L'idéal pA est premier.

13. Anneau intègre, définition 1.192.
14. Élément irréductible, définition 1.183.
15. Définition 1.267.
16. Définition 3.49.
17. Le fait que A soit commutatif est utilisé partout.
18. Élément premier, définition 1.182.

(2) L'anneau A/pA est intègre.

Démonstration. En deux parties.

(i) **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 3.60 dit alors que p divise a ou b. Supposons pour fixer les idées que $p \mid a$. Il existe y tel que $a = py \in pA$.

(ii) **L'anneau A/pA est intègre** C'est la proposition 1.224.

□

Proposition 3.63.
Soit une famille $\{a_n\}$ d'éléments de A qui se décomposent en irréductibles comme

$$a_i = \prod_k p_k^{\alpha_{k,i}}. \tag{3.97}$$

Alors

$$\text{pgcd}\{a_n\} = \prod_k p_k^{\min_i\{\alpha_{k,i}\}}. \tag{3.98}$$

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[19].

De la même manière,

$$\text{ppcm}\{a_n\} = \prod_k p_k^{\max_i\{\alpha_{k,i}\}}. \tag{3.99}$$

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[20] : $a < b$ si et seulement si $(b) \subset (a)$.

Exemple 3.64.
L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel parce que 4 a au moins deux décompositions distinctes en irréductibles :

$$4 = 2 \cdot 2, \tag{3.100}$$

et

$$4 = (1 + i\sqrt{3})(1 - i\sqrt{3}). \tag{3.101}$$

△

Nous allons voir dans l'exemple 3.83 que $\mathbb{Z}[i\sqrt{2}]$ est factoriel parce qu'il sera euclidien.

3.5.1 Autour du théorème de Bézout

Rappel de notations : si A est un anneau et si $p \in A$, nous notons (p) l'idéal engendré par p, c'est-à-dire pA. C'est la définition 1.205.

Lemme 3.65 ([106]).
Soient un anneau principal[21] *A ainsi que $a, b \in A$.*

(1) d est PGCD de $\{a, b\}$ si et seulement si $(d) = (a) + (b)$.

(2) m est PPCM de $\{a, b\}$ si et seulement si $(m) = (a) \cap (b)$.

19. 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.
20. Voir proposition 3.3.
21. Définition 1.221.

Théorème 3.66 ([107, 106]).
Soient un anneau principal et $S \subset A$ non vide.

(1) d est un PGCD de S si et seulement si il génère l'idéal engendré par S.

(2) m est PPCM de S si et seulement si $(m) = \bigcap_{s\in S}(s)$.

Toute partie d'un anneau principal admet un PGCD et un PPCM[22].

¡¡ Avertissement/question au lecteur !! 3.67
La preuve est à revoir.

Démonstration. Puisque l'anneau A est principal, tous ses idéaux sont principaux et donc engendrés par un seul élément. En particulier il existe $\delta, \mu \in A$ tels que

$$(\delta) = \sum_{s\in S}(s) \tag{3.102a}$$

$$(\mu) = \bigcap_{s\in S}(s) \tag{3.102b}$$

(i) **PGCD** Montrons ce que δ est un PGCD de S. Pour tout $x \in S$, nous avons $(x) \subset (\delta)$, et donc $\delta \mid x$. Par ailleurs si $d \mid x$ pour tout $x \in S$, nous avons $(x) \subset (d)$ et donc

$$\sum_{x\in S}(x) \subset (d), \tag{3.103}$$

puis $(\delta) \subset (d)$ et finalement $d \mid \delta$.

(ii) **PPCM** Si $x \in S$ nous avons $(\mu) \subset (x)$ et donc $x \mid \mu$. D'autre part si $x \mid m$ pour tout $x \in S$, alors $(m) \subset (x)$ et donc $(m) \subset (\mu)$, finalement $\mu \mid m$.

□

Corolaire 3.68 (Théorème de Bézout[107]).
Soit un anneau principal A. Deux éléments $a, b \in A$ sont premiers entre eux si et seulement si il existe un couple $(u, v) \in A^2$ tel que

$$ua + vb = 1. \tag{3.104}$$

À la place de 1 on aurait pu écrire n'importe quel inversible.

Démonstration. Pour cette preuve, nous allons écrire $\operatorname{pgcd}(a, b)$ l'ensemble de PGCD de a et b, c'est-à-dire la classe d'association d'un PGCD.

Si a et b sont premiers entre eux, alors

$$1 \in \operatorname{pgcd}(a, b) = \sum_{x=a,b}(x) = (a) + (b). \tag{3.105}$$

À l'inverse, si nous avons $ua + vb = 1$, alors $1 \in (a) + (b)$, mais puisque $(a) + (b)$ est un idéal principal, $(1) = (a) + (b)$ et donc $1 \in \operatorname{pgcd}(a, b)$. □

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 6.51), et une généralisation directe au théorème de Gauss, théorème 6.50.

Lemme 3.69 (Lemme de Gauss[108]).
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.

22. Ce n'est pas aussi trivial que ça parce qu'il faut encore qu'il existe des éléments vérifiant les formules données.

Démonstration. Comme a est premier avec c, nous avons $\text{pgcd}(a,c)=1$ et Bézout (1.229) nous donne donc $s,t\in A$ tels que $sa+tc=1$. En multipliant par b,

$$sab+tbc=b. \tag{3.106}$$

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. □

Lemme 3.70 ([40]).
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 3.68 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,

$$(ua+vb)(xa+yc)=1. \tag{3.107}$$

En développant, nous trouvons

$$(uax+uc+vbx)a+(vy)bc=1. \tag{3.108}$$

Donc le théorème de Bézout (dans l'autre sens) nous indique que $\text{pgcd}(a,bc)=1$. □

3.5.2 Idéal premier

Proposition 3.71 ([109, 1], thème 6).
Soit un anneau principal A et un élément $p\neq 0$ dans A. Nous avons équivalence de :

(1) *(p) est un idéal premier,*

(2) *p est un élément premier,*

(3) *p est un élément irréductible,*

(4) *(p) est un idéal maximum propre*[23].

Démonstration. En plusieurs implications.

(i) **(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.

(ii) **(2) implique (3)** Un anneau principal est intègre ; c'est dans la définition 1.221. Dans un anneau intègre, tout élément premier est irréductible, c'est la proposition 1.217.

(iii) **(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.

(iv) **(4) implique (1)** C'est la proposition 1.224(3).

□

Un exemple d'élément premier non irréductible est $[4]_6$ dans l'anneau non principal $\mathbb{Z}/6\mathbb{Z}$. Voir 3.81 et le lemme 3.82.

23. 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/Discussion:Idéal_premier

3.5.3 Anneau noethérien

Définition 3.72.
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.

Lemme 3.73.
Tout anneau principal[24] *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

$$J \subset J_N \subset J_n \subset J. \tag{3.109}$$

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 3.74.
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 3.82. △

Théorème 3.75 ([110, 40])**.**
Tout anneau principal est factoriel.

Démonstration. Soit un anneau principal A. Nous devons prouver les trois points de la définition 3.59. D'abord A est intègre parce que ça fait partie de la définition 1.221 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 1.214 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 :

$$a \in aA \subsetneq M = pA. \tag{3.110}$$

Comme l'idéal pA est maximal, la proposition 1.194 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 :

$$a_n = p_{n+1}a_{n+1} \tag{3.111}$$

avec p_{n+1} irréductible.

24. Définition 1.221.

Pour tout n assez petit pour que la suite ne soit pas finie, nous avons

$$a = a_0 = p_1 a_1 = p_1 p_2 a_2 = \ldots = p_1 \ldots p_n a_n \tag{3.112}$$

où les p_i sont irréductibles.

Nous montrons à présent que la suite des (a_n) est finie. Considérons les idéaux $I_n = a_n A$, et montrons qu'ils sont croissants en montrant que a_{n+1} n'est pas dans I_n.

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 3.73). 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

$$a = a_0 = p_1 a_1 = p_1 p_2 a_2 = \ldots = p_1 \ldots p_N a_N. \tag{3.113}$$

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

$$p_N = s(t a_N^{-1}). \tag{3.114}$$

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 $t a_N^{-1}$ 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 3.70 : 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

$$p_1 = du \quad q_1^{(1)} = dv. \tag{3.115}$$

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

$$p_1 = q_1^{(1)} u v^{-1}. \tag{3.116}$$

Nous récrivons $p_1 \ldots p_k = q_1 \ldots q_m$ avec ces valeurs :

$$du p_2 \ldots p_k = dv q_2^{(1)} \ldots q_m^{(1)}. \tag{3.117}$$

Nous simplifions par d et nous avons

$$(up_2) p_3 \ldots p_k = (v q_2^{(1)}) q_3^{(1)} \ldots q_m^{(1)}. \tag{3.118}$$

Par récurrence nous construisons les σ_i et les $q_j^{(i)}$. □

Proposition 3.76.
Un corps est un anneau principal et un anneau factoriel.

Démonstration. Un anneau est principal quant :

— Commutatif

— intègre

— tous les idéaux sont principaux.

Un corps est toujours commutatif. Un corps est un anneau intègre par le lemme 1.193. 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 3.75. □

Exemple 3.77 ($\mathbb{Z}[i\sqrt{5}]$ 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 [25]

$$\begin{aligned} N\colon \mathbb{Z}[i\sqrt{5}] &\to \mathbb{N} \\ z &\mapsto z\bar{z}. \end{aligned} \tag{3.119}$$

Le fait que ce soit à valeurs dans $\mathbb{N}$ est un simple calcul :

$$N(x + iy\sqrt{5}) = (x + iy\sqrt{5})(x - iy\sqrt{5}) = x^2 + 5y^2. \tag{3.120}$$

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,

$$N(\alpha)N(\beta) = 1, \tag{3.121}$$

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 3.59) parce que

$$2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}). \tag{3.122}$$

Cela donne deux décompositions du nombre 6 en produit d'éléments non associés [26] (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 3.75. △

3.6 Anneau $\mathbb{Z}/6\mathbb{Z}$

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

$$1 \times [4]_6 = [4_6] \tag{3.123}$$

et ensuite

$$2 \times [4]_6 = [8]_6 = [2]_6, \tag{3.124}$$

puis

$$3 \times [4]_6 = [2 + 4]_6 = [6]_6 = [0]_6, \tag{3.125}$$

25. C'est le carré de la norme usuelle, mais c'est l'usage dans le milieu.
26. Définition 3.49.

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

(3.126)

Pour ne pas alourdir, nous n'avons pas écrit $[x]_6$ partout au lieu de x.

3.78 (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

$$U(\mathbb{Z}/6\mathbb{Z}) = \big\{[1]_6, [5]_6\big\}. \tag{3.127}$$

3.79 (Diviseurs de zéro)**.**
Les diviseurs de zéro sont ceux qui ont un $[0]_6$ dans leur table de multiplication, c'est-à-dire

$$\big\{[2]_6, [3]_6, [4]_6\big\}. \tag{3.128}$$

3.80 (Irréductibles)**.**
Les irréductibles sont ceux qui ne sont ni inversibles ni produit de deux éléments non inversibles. Les non inversibles sont :

$$\big\{[0]_6, [2]_6, [3]_6, [4]_6\big\}. \tag{3.129}$$

Ils sont candidats à être irréductibles. Les produits de ces éléments (on oublie les crochets) sont :

$$2 \times 2 = 4 \tag{3.130a}$$
$$2 \times 3 = 0 \tag{3.130b}$$
$$2 \times 4 = 2 \tag{3.130c}$$
$$3 \times 3 = 3 \tag{3.130d}$$
$$3 \times 4 = 0 \tag{3.130e}$$
$$4 \times 4 = 4. \tag{3.130f}$$

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.

3.81 (Éléments premiers)**.**
Les éléments non nuls et non inversibles sont 2, 3 et 4.

(i) **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.

(ii) **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

$$\{[2]_6,[3]_6,[4]_6\}. \tag{3.131}$$

Vous noterez que $\mathbb{Z}/6\mathbb{Z}$ a des éléments premiers non irréductibles. Cela est un contre-exemple à la proposition 3.71 dans le cas d'un anneau non-intègre.

Lemme 3.82 ([1])**.**
L'anneau $\mathbb{Z}/6\mathbb{Z}$ est noetherien, mais ni intègre ni principal[27].

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. □

Exemple 3.83.
Prouvons que $\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien. Pour cela nous démontrons que

$$\begin{aligned} N\colon \mathbb{Z}[i\sqrt{2}] &\to \mathbb{N} \\ a+bi\sqrt{2} &\mapsto a^2+2b^2 \end{aligned} \tag{3.132}$$

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

$$\frac{z}{t}=\alpha+\beta i\sqrt{2}. \tag{3.133}$$

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

$$q=(\alpha+\epsilon_1)+(\beta+\epsilon_2)i\sqrt{2} \tag{3.134}$$

et nous calculons $r=z-qt$:

$$2b'\epsilon_2-a'\epsilon_1+i\sqrt{2}\big(\epsilon_1 b'-a'\epsilon_2\big). \tag{3.135}$$

Nous trouvons

$$N(r)=a'^2\epsilon_1^2+4b'^2\epsilon_2^2+2a'^2\epsilon_1^2+2b'^2\epsilon_2^2\leqslant\frac{3}{4}a'^2+\frac{3}{2}b'^2. \tag{3.136}$$

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

$$N(zt)=(a^2+2b^2)(a'^2+2b'^2), \tag{3.137}$$

et tant que $t\neq0$ nous avons bien $N(zt)>N(z)$. △

Notons en particulier que $\mathbb{Z}[i\sqrt{2}]$ est factoriel et principal.

Exemple 3.84 (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 3.49) si et seulement si $a=\pm b$.

De plus si p est irréductible[28], alors $-p$ est irréductible. Les éléments irréductibles de $\mathbb{Z}[i\sqrt{2}]$

27. Toutes les définitions dans le thème 6.
28. Définition 1.183

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 3.87, mais nous l'isolons pour plus de clarté [29].

Lemme 3.85.
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 3.84 nous pouvons écrire

$$y = \pm p_1^{\sigma_1} \dots p_n^{\sigma_n} \tag{3.138a}$$
$$a = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n} \tag{3.138b}$$
$$b = \pm p_1^{\beta_1} \dots p_n^{\beta_n} \tag{3.138c}$$

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. □

3.6.1 Équations diophantiennes

Exemple 3.86.
L'équation diophantienne

$$x^2 = 3y^2 + 8 \tag{3.139}$$

n'a pas de solution. En effet si nous prenons l'équation modulo 3 nous obtenons

$$[x^2]_3 = [3y^2 + 8]_3 = [8]_3 = [2]_3. \tag{3.140}$$

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 $2^2 = 4 = 1 \neq 2$. △

Exemple 3.87.
Résolvons l'équation diophantienne

$$x^2 + 2 = y^3. \tag{3.141}$$

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 (3.132).

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

$$x = (i\sqrt{2})^\beta q \tag{3.142}$$

29. Merci à Marvoir pour m'avoir souligné le manque.

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 3.85). 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

$$\begin{cases} x = a^3 - 6ab^2 & \text{(3.143a)} \\ 1 = 3a^2b - 2b^3 & \text{(3.143b)} \end{cases}$$

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

$$(x, z) = (-5, 1 + i\sqrt{2}) \quad \text{(3.144a)}$$
$$(x, z) = (5, -1 + i\sqrt{2}) \quad \text{(3.144b)}$$
$$\text{(3.144c)}$$

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 $(-5, 3)$. △

3.6.2 Triplets pythagoriciens et équation de Fermat pour $n = 4$

Définition 3.88.
*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.

Définition 3.89.
*On dit qu'un triplet pythagoricien est **primitif** si les trois nombres sont premiers dans leur ensemble*[30].

Remarquons que c'est équivalent à montrer que les trois nombres sont premiers deux à deux : en effet, si deux parmi x, y et z sont divisibles par un nombre, alors tous les trois sont divisibles par ce nombre[31], donc les nombres x, y et z sont premiers deux à deux.

Lemme 3.90.
Dans un triplet pythagoricien primitif (x, y, z), on a toujours z impair et :

30. Définition 1.254.
31. Parce que k et k^2 ont les mêmes facteurs premiers.

— *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. □

Proposition 3.91 (Triplets pythagoriciens[111, 112])**.**
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

$$\begin{cases} x = d(u^2 - v^2) & (3.145a)\\ y = 2duv & (3.145b)\\ z = d(u^2 + v^2) & (3.145c) \end{cases}$$

ou

$$\begin{cases} x = 2duv & (3.146a)\\ y = d(u^2 - v^2) & (3.146b)\\ z = d(u^2 + v^2) & (3.146c) \end{cases}$$

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 (3.145) :

$$x^2 + y^2 = d^2(u^2 - v^2)^2 + 4d^2u^2v^2 = d^2(u^2 + v^2)^2, \tag{3.147}$$

qui correspond bien au z^2 proposé.

Une vérification du même style fonctionne pour (3.146).

Nous allons maintenant prouver la réciproque : toute solution est d'une des deux formes proposées. Déterminer les triplets primitifs suffira parce que si (x, y, z) n'est pas une solution primitive, alors en posant $k = \text{pgcd}(x, y, z)$, le triplet $\left(\frac{x}{k}, \frac{y}{k}, \frac{z}{k}\right)$ est primitif. Connaissant les triplets primitifs, nous obtenons tous les autres par simple multiplication.

Soit donc (x, y, z) un triplet pythagoricien primitif. Sans perte de généralité [32], grâce au lemme 3.90, nous pouvons supposer x pair tandis que y et z seront impairs. Comme $x^2 = (z + y)(z - y)$, nous avons

$$\left(\frac{x}{2}\right)^2 = \frac{1}{4}(z + y)(z - y). \tag{3.148}$$

Puisque z et y sont premiers entre eux, les nombres $z + y$ et $z - y$ sont également premiers entre eux [33]. Vu que $(z+y)(z-y)$ est divisible par 4, soit $z+y$ soit $(z-y)$ est divisible par 4. Pour fixer les idées nous supposons que c'est $z + y$, et nous écrivons

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z + y}{4}\right)(z - y). \tag{3.149}$$

Les facteurs premiers (qui arrivent au moins au carré) de $(x/2)$ sont chacun soit dans $(z + y)/4$ soit dans $(z - y)$. Tout deux sont donc des carrés parfaits. Nous posons

$$\frac{z + y}{4} = u^2, \quad z - y = v^2. \tag{3.150}$$

32. En échangeant les rôles de x et y ici, nous obtenons à la fin la seconde forme des solutions.
33. Si $z - y = kn$ et $z + y = km$, faisant la somme et la différence on voit que y et z sont divisibles par k.

Bien entendu u et v sont non nuls parce que nous avons exclu la possibilité de triplets dont un élément serait nul. Avec tout cela nous avons $(x/2)^2 = u^2v^2$ et donc $x = 2uv$ puis par somme et différence :

$$\begin{cases} x = 2uv & (3.151a) \\ y = v^2 - u^2 & (3.151b) \\ z = u^2 + v^2, & (3.151c) \end{cases}$$

ce qu'il fallait. □

Remarque 3.92.
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.

Proposition 3.93 ([111])**.**
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 [34]). 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 3.91, il existe $u, v \in \mathbb{N}^*$ premiers entre eux tels que, sans perte de généralité [35], on ait

$$\begin{cases} \bar{x} = 2uv & (3.152a) \\ \bar{y} = u^2 - v^2 & (3.152b) \\ z = u^2 + v^2. & (3.152c) \end{cases}$$

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 3.90 implique alors que v soit pair.

De l'équation 3.152b, 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 3.91, en se souvenant que v est pair : il existe donc deux nombres r et s premiers entre eux tels que

$$\begin{cases} v = 2rs & (3.153a) \\ y = r^2 - s^2 & (3.153b) \\ u = r^2 + s^2. & (3.153c) \end{cases}$$

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 :

$$\begin{cases} r = \alpha^2 & (3.154a) \\ s = \beta^2 & (3.154b) \\ r^2 + s^2 = \gamma^2. & (3.154c) \end{cases}$$

34. Voir quelque chose comme le lemme 1.137.
35. En inversant les rôles de x et y au besoin.

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 :

$$\begin{aligned} z &= u^2+v^2 && \text{par 3.152c}\\ &= r^2+s^2+4r^2s^2 && \text{par 3.153}\\ &= \gamma^2+4r^2s^2\\ &> \gamma^2, \end{aligned}$$

et a fortiori $\gamma<z$. □

3.7 Polynômes à coefficients dans un anneau commutatif

Lemme 3.94.
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

$$Q(\bar{X})=\overline{Q(X)}=\bar{Q}. \tag{3.155}$$

Démonstration. Si $Q=\sum_k a_kX^k$, alors par la linéarité de la prise de classes,

$$\bar{Q}=\sum_k a_k\overline{X^k}. \tag{3.156}$$

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 1.179). 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

$$\bar{Q}=\sum_k a_k\bar{X}^k=Q(\bar{X}). \tag{3.157}$$

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 1.359. □

3.7.1 Monômes

3.95.
Les éléments de la forme λX^k avec $\lambda\in A$ et $k\in\mathbb{N}$ sont des **monômes**.

Nous allons aussi considérer

$$A_n[X]=\{P\in A[X]\text{ tel que }\deg(P)\leqslant n\}. \tag{3.158}$$

Cet ensemble est un sous-module libre.

3.7.2 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 1.355 :

$$P(\alpha)=\sum_k a_k\alpha^k. \tag{3.159}$$

Cette somme est toujours finie.

3.96.
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 6.110 et l'exemple 19.34.

Définition 3.97.
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.

Proposition 3.98.
Soient un anneau A et un anneau B qui contient A (comme sous-anneau). Pour tout $\alpha \in B$ nous avons

$$A[\alpha] = \{P(\alpha) \text{ tel que } P \in A[X]\} \tag{3.160}$$

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

$$\{P(\alpha) \text{ tel que } P \in A[X]\} \subset A[\alpha]. \tag{3.161}$$

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. □

3.7.3 Polynômes sur un anneau intègre

Théorème 3.99.
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

$$\deg(PQ) = \deg(P) + \deg(Q) \tag{3.162}$$

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 $A[X]$. □

3.100.
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 3.101.
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. □

3.7.4 Division euclidienne

Le théorème suivant établit la **division euclidienne** dans $A[X]$ du polynôme P par un polynôme D.

Théorème 3.102.
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

$$P = QD + R \tag{3.163}$$

avec $\deg(R) < \deg(D)$.

Les polynômes Q et R sont déterminés de façon univoque par cette condition.

Définition 3.103.
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 $P = QD$.* [36]

3.104.
Le théorème 3.102 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.

Lemme 3.105 (Thème 18)**.**
Si $\mathbb{K}$ est un corps[37]*, 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 3.102. L'anneau $\mathbb{K}[X]$ est donc euclidien et par conséquent principal (proposition 1.247). □

Dans le théorème 6.43 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.

Définition 3.106 ([113])**.**
Soit un anneau A. Deux polynômes P et Q dans $A[X]$ sont dits ***étrangers*** *entre eux si* 1 *est un pgcd*[38] *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 3.107 ([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). △

3.7.5 Polynôme primitif

Définition 3.108.
Un ***contenu*** *du polynôme $P = \sum_i a_i X^i \in \mathbb{K}[X]$ est un pgcd de ses coefficients : $c(P) = \operatorname{pgcd}\big(\{a_i\}\big)$.*

3.109.
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 1.195 dit que

36. Ceci se rapproche tout naturellement des notions générales de divisibilité dans un anneau intègre, vues en sous-section 3.4.1.
37. Définition 1.202.
38. Définition 1.180.

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.

Définition 3.110 (Polynôme primitif[114]).
Il existe deux notions de polynômes primitifs. Vu qu'il existe des anneaux unitaires qui sont des corps finis[39]*, il faut faire attention au contexte.*

(1) *Si A est un anneau unitaire, P est un* ***polynôme primitif*** *$c(P)$ est inversible*[40].

(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.*

3.111.
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 1.252 pour avoir des nombres premiers entre eux.

(2) Le contenu de ses coefficients est 1. Parce que le contenu est précisément le pgcd, définition 3.108.

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 3.112.
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 3.113 ([115]).
Soit un anneau factoriel[41] *A. Soient des polynômes primitifs P_1 et P_2 dans $A[X]$. Soient $a_1, a_2 \in A^*$ tels que*

$$a_1P_1 = a_2P_2. \tag{3.164}$$

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 3.55 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 3.99). 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. □

Lemme 3.114 (de Gauss[115]).
Soit un anneau factoriel A. Soient $P, Q \in A[X]$.

(1) *Les polynômes P et Q sont primitifs si et seulement si le polynôme PQ est primitif.*

(2) *Il existe un inversible $u \in A$ tel que $c(PQ) = uc(P)c(Q)$.*

39. 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.
40. 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 définit qu'à inversible près. Voir aussi 3.109.
41. Définition 3.59. Je rappelle qu'un anneau factoriel est toujours commutatif.

Démonstration. En plusieurs parties.

(i) **(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 3.62 dit que l'anneau $B = A/pA$ est intègre [42].

Considérons la surjection canonique $\pi\colon A \to B$ que nous prolongeons en un morphisme d'anneaux

$$\begin{aligned}\phi\colon A[X] &\to B[X]\\ \sum_i a_iX^i &\mapsto \sum_i \pi(a_i)X^i.\end{aligned} \tag{3.165}$$

Notons que p ne divise pas tous les coefficients de P. En effet, sinon $c(P)$ serait un multiple de p (proposition 3.63) et ne pourrait pas être inversible. Donc $\phi(P) \neq 0$ dans $B[X]$. De même nous savons que $\phi(Q) \neq 0$.

L'anneau B est intègre parce que A est intègre (proposition 3.99). 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.

(ii) **(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 1.198). Par la partie précédente nous savons que P_1Q_1 est primitif. Nous avons donc l'égalité

$$PQ = c(P)c(Q)P_1Q_1 \tag{3.166}$$

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 [43]

$$c\Big(c(P)c(Q)P_1Q_1\Big) = c(P)c(Q)c(P_1Q_1) \tag{3.167}$$

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.

(iii) **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

$$c(P)c(Q)P_1Q_1 = PQ = c(PQ)R_1. \tag{3.168}$$

En prenant le contenu des deux côtés nous avons

$$c\Big(c(P)c(Q)P_1Q_1\Big) = c\Big(c(PQ)R_1\Big), \tag{3.169}$$

et en tenant compte du lemme 1.196, cela devient

$$c(P)c(Q)c(P_1Q_1) = c(PQ)c(R_1) \tag{3.170}$$

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

$$c(P)c(Q) = uc(PQ). \tag{3.171}$$

□

42. Ici, ma source [115] précise que p est premier. C'est vrai par la proposition 3.61, mais ça me semble inutile. Écrivez-moi pour me dire si le fait que p soit premier est important.

43. Utilisation du lemme 1.196.

3.115.
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 1.199, 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

$$c(P)c(Q) = uc(PQ), \tag{3.172}$$

en fait nous savons qu'il existe des représentants de $c(P)$, $c(Q)$ et $c(PQ)$ tels que

$$c(P)c(Q) = c(PQ). \tag{3.173}$$

3.7.6 Racines des polynômes

Définition 3.116 (Ordre d'un polynôme)**.**
Soit P un polynôme irréductible[44] *de degré n sur $\mathbb{F}_p[X]$. L'**ordre** de P est*

$$\min\{k \text{ tel que } P \mid X^k - 1\}. \tag{3.174}$$

Définition 3.117.
*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.*

Proposition 3.118.
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 6.100. 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[45] de P par μ : il existe des polynômes Q et R tels que

$$P = Q\mu + R \tag{3.175}$$

avec $\deg(R) < \deg(\mu)$. Donc R est une constante, élément de A : appelons-le a. En évaluant (3.175) en α, il vient

$$0 = P(\alpha) = Q(\alpha)\mu(\alpha) + a, \tag{3.176}$$

et nous en déduisons que $a = 0$, ce qui montre que $P = Q\mu$ et que μ divise P. □

Définition 3.119 (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**.*

3.120.
Pour une définition générale d'une racine simple de l'équation $f(x) = 0$, voir la définition 34.50. La proposition 3.118 nous indique que toute racine est de multiplicité au moins égale à 1.

Lemme 3.121.
Soient un anneau A ainsi que $x, r \in A$. Nous avons

$$x^n - r^n = (x - r)\sum_{k=0}^{n-1} x^k r^{n-k-1}. \tag{3.177}$$

44. Définition 1.183.
45. Théorème 3.102.

Démonstration. Nous effectuons la distribution, et nous calculons un peu :

$$(x-r)\sum_{k=0}^{n-1}x^kr^{n-k} = \sum_{k=0}^{n-1}x^{k+1}r^{n-k-1} - \sum_{k=0}^{n-1}x^kr^{n-k} \tag{3.178a}$$
$$= \sum_{k=1}^{n}x^kr^{n-k} - \sum_{k=0}^{n-1}x^kr^{n-k} \tag{3.178b}$$
$$= -r^n + \sum_{k=1}^{n-1}(x^kr^{n-k} - x^kr^{n-k}) + x^n \tag{3.178c}$$
$$= x^n - r^n. \tag{3.178d}$$

□

Proposition 3.122 ([116]).
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 3.121, 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).

Soit un polynôme P tel que $P(\alpha) = 0$. Nous pouvons écrire

$$P(x) = P(x) - P(\alpha) \tag{3.179a}$$
$$= \sum_{k=0}^{n}a_kx^k - \sum_{k=0}^{n}a_k\alpha^k \tag{3.179b}$$
$$= \sum_{k=1}^{n}a_k(x^k - \alpha^k) \tag{3.179c}$$
$$= \sum_{k=1}^{n}a_k(x-\alpha)S_k(x) \tag{3.179d}$$
$$= (x-\alpha)\sum_{k=1}^{n}a_lS_k(x) \tag{3.179e}$$
$$= (x-\alpha)Q(x) \tag{3.179f}$$

où Q est le polynômde de degré $n-1$ donné par $Q = \sum_{k=1}^{n}a_kS_k$. □

Proposition 3.123.
L'élément $\alpha \in A$ est une racine de multiplicité[46] 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

$$P = (X-\alpha)^hQ. \tag{3.180}$$

Si $Q(\alpha)$ était nul, la proposition 3.122 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. □

Lemme 3.124.
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 $\theta_\alpha(P) \neq \theta_\alpha(Q)$;

(2) $\theta_\alpha(PQ) \geqslant \theta_{\alpha(P)} + \theta_\alpha(Q)$, et l'égalité a lieu si A est intègre.

46. Multiplicité d'une racine, définition 3.119.

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.

Théorème 3.125.
Soit A un anneau intègre et $P \in A[X]\backslash\{0\}$, 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

$$P = Q \prod_{i=1}^{p} (X - \alpha_i)^{k_i} \tag{3.181}$$

et $Q(\alpha_i) \neq 0$ pour tout i.

(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 3.118 : 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

$$P = \underbrace{(X - \alpha_1)^{k_1} \dots (X - \alpha_{p-1})^{k_{p-1}}}_{S} R. \tag{3.182}$$

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 3.124 afin de dire que le degré de α_p pour $P = SR$ est k_p. Par conséquent

$$R = (X - \alpha_p)^{k_p} T \tag{3.183}$$

avec $T(\alpha_p) \neq 0$ et enfin

$$P = \prod_{i=1}^{p} (X - \alpha_i) T. \tag{3.184}$$

De plus $T(\alpha_i) \neq 0$, sinon $R(\alpha_i)$ serait nul. □

Corolaire 3.126.
Un polynôme de degré n sur un anneau intègre possède au maximum n racines distinctes.

Démonstration. Le théorème 3.125(2) dit que la somme des multiplicités des racines de P est au maximum n. Mais la proposition 3.118 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 3.127 ([117, 118])**.**
Soit un anneau intègre et $n > 0$. Les racines n^e de l'unité forment un groupe cyclique dont l'ordre divise n.

Lemme 3.128.
Soit le polynôme $P = X^2 - 1$ sur l'anneau intègre[47] *A. Si $1 \neq -1$*[48]*, alors les racines de P sont ± 1.*

47. Définition 1.192.

48. 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 ?

Démonstration. Le fait que ± 1 sont racines est le lemme 1.175(1)(4). Puisque par hypothèse $1 \neq -1$, le corolaire 3.126 termine la preuve. □

Corolaire 3.129 (Conséquence du lemme de Gauss[119])**.**
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*[49] *sur* $\mathrm{Frac}(A)[X]$.

Exemple 3.130.
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

$$P = \left(X - \frac{1+\sqrt{5}}{2}\right)\left(X - \frac{1-\sqrt{5}}{2}\right). \tag{3.185}$$

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 $\mathrm{Frac}\big(\mathbb{Z}[\sqrt{5}]\big)$. △

3.7.7 Quelques identités

Lemme 3.131 ([1, 120])**.**
Quelques identités de polynômes.

(1) Si n est impair, alors $1 + X$ divise $1 + X^n$.

(2) Pour tout n nous avons $X^n - 1 = (X - 1)(1 + X + \cdots + X^{n-1})$.

(3) $X^n - a^n = (X - a)\sum_{i=0}^{n-1} a^i X^{n-1-i}$.

Démonstration. Plusieurs points.

(i) **Pour (1)** Nous allons utiliser le lemme 3.1 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 (3.1), nous remarquons que $(-X)^n = (-1)^n X^n = -X^n$. Nous avons donc :

$$1 + X^n = (a - b)\sum_{k=0}^{n-1} a^{n-1-kb^k} = (1 + X)(\cdots). \tag{3.186}$$

Cela prouve que $1 + X$ divise $1 + X^n$.

(ii) **Pour (2)** Posons $P = X + \ldots + X^{n-1}$. Nous avons $XP = P - X + X^n$ et donc

$$(X - 1)(1 + P) = X + XP - 1 - P = X + (P - X + X^n) - 1 - P = X^n - 1. \tag{3.187}$$

(iii) **Pour (3)** Déjà fait dans (3.1).

□

3.7.8 Générateurs pour le groupe multiplicatif

Proposition 3.132 ([121])**.**
Si p est un nombre premier, tout sous-groupe de $\big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big)$ est cyclique[50].

Démonstration. Soit un sous-groupe H d'ordre $|H| = n$ de $(\mathbb{Z}/n\mathbb{Z})^*$. Nous prouvons par récurrence sur n que H est cyclique.

(i) $n = 1$ Si H est un sous-groupe d'ordre 1, alors $H = \{[1]_p\}$ et c'est cyclique, pas de problèmes.

49. Définition 3.110.
50. Définition 1.319.

(ii) **Récurrence** Nous supposons que tous les sous-groupes de $\big((\mathbb{Z}/n\mathbb{Z})^*$ 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.

(i) **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 2.14), 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 3.125. Contradiction. Donc H est cylcique.

(ii) **Cas général** Nous supposons que $|H|$ n'est pas la puissance d'un nombre premier.

(i) **Un morphisme** Le corolaire 3.18 nous indique que $n = ab$ pour deux nombres a, b tels que $\operatorname{pgcd}(a, b) = 1$. Nous considérons l'application

$$\begin{aligned} f\colon H &\to H \\ x &\mapsto x^a. \end{aligned} \tag{3.188}$$

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

$$\operatorname{Image}(f) \subset \{y \in H \text{ tel que } y^b = 1\}. \tag{3.189}$$

(ii) **Ordre du noyau et de l'image** Par le coup des racines distinctes de polynôme $X^b - 1$, nous avons $|\operatorname{Image}(f)| \leqslant b$. De même nous avons

$$\ker(f) = \{x \in H \text{ tel que } x^a = 1\}, \tag{3.190}$$

et donc $|\ker(f)| \leqslant a$.

Le premier théorème d'isomorphisme 2.6 nous indique que

$$\frac{H}{\ker(f)} \simeq \operatorname{Image}(f), \tag{3.191}$$

et comme tout est abélien, tous les sous groupes sont normaux [51], et nous avons, par le théorème de Lagrange 2.13 que

$$ab = |H| = \underbrace{|\ker(f)|}_{\leqslant a} \underbrace{|\operatorname{Image}(f)|}_{\leqslant b} \leqslant ab. \tag{3.192}$$

Le premier membre est égal au dernier. Donc toutes les inégalités sont des égalités. Nous avons donc $|\ker(f)| = a$ et $|\operatorname{Image}(f)| = b$.

(iii) **Hypothèse de récurrence** C'est le moment d'utiliser l'hypothèse de récurrence : les groupes $\ker(f)$ et $\operatorname{Image}(f)$ sont cycliques. Soient des générateurs h et h'. Quel est l'ordre de hh' ? Le lemme 3.27 nous indique que hh' est d'ordre $ab = n$. Donc hh' est générateur de H qui est donc cyclique.

□

51. « distingué » et « normal » sont synonymes.

Chapitre 4

Espaces vectoriels (début)

4.1 Parties libres, génératrices, bases et dimension

Nous avons déjà défini (dans 1.325) un espace vectoriel comme étant un module sur un corps commutatif. En explicitant un peu, cela donne ceci[122].

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 $k, k' \in \mathbb{K}$,

(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 $(E, +)$.

Définition 4.1 (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*

$$a_1u_1 + \cdots + a_nu_n = 0 \tag{4.1}$$

implique $a_i = 0$ pour tout i (ici les a_i sont dans le corps de base).

Remarque 4.2.
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 $\text{Span}(A)$ 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 4.3 (Partie génératrice)**.**
*Une partie B d'un espace vectoriel E est **génératrice** si* $\text{Span}(B) = E$.

Remarque 4.4.
Ces définitions demandent des commentaires en dimension infinie [1].

1. Nous n'avons pas encore défini le concept de dimension, mais nous nous adressons au lecteur trop pressé.

(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.

(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.

Définition 4.5 (Base)**.**
Une ***base*** *de l'espace vectoriel E est une partie à la fois génératrice et libre.*

4.6.
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.

Proposition 4.7 ([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 $I\backslash J$.

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

$$v = \sum_{j\in J} v_j e_j. \tag{4.2}$$

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

$$v = \sum_{j\in J} v_j e_j = \sum_{k\in K} w_k e_k. \tag{4.3}$$

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.

Nous posons $L = J \cup K$. Remarquez que les unions suivantes sont des unions disjointes :

$$L = (J\backslash K) \cup (J \cap K) \cup (K\backslash J) \tag{4.4a}$$
$$J = (J\backslash K) \cup (J \cap K) \tag{4.4b}$$
$$K = (K \cap J) \cup (K\backslash J). \tag{4.4c}$$

Écrivons $0 = v - v$ en utilisant les expressions de v de (4.3) et en décomposant les sommes :

$$0 = \sum_{j\in J} v_j e_j - \sum_{k\in K} w_k e_k \tag{4.5a}$$
$$= \sum_{j\in J\backslash K} v_j e_j + \sum_{j\in J\cap K} v_j e_j - \sum_{k\in K\cap J} w_k e_k - \sum_{k\in K\backslash J} w_k e_k \tag{4.5b}$$
$$= \sum_{j\in J\backslash K} v_j e_j + \sum_{j\in J\cap K} (v_j - w_j) e_j - \sum_{k\in K\backslash J} w_k e_k. \tag{4.5c}$$

Là-dessus, nous posons

$$\alpha_l = \begin{cases} v_l & \text{si } l \in J\backslash K \\ v_l - w_l & \text{si } l \in J \cap K \\ -w_l & \text{si } l \in K\backslash J. \end{cases} \tag{4.6}$$

Nous avons alors

$$\sum_{l\in L} \alpha_l e_l = 0. \tag{4.7}$$

Vu que $\{e_i\}_{i\in I}$ est libre, la partie $\{e_l\}_{l\in L}$ est également libre. Donc l'équation (4.7) implique que $\alpha_l = 0$ pour tout $l \in L$.

Nous devons prouver que

$$\{j \in J \text{ tel que } v_j \neq 0\} = \{k \in K \text{ tel que } w_k \neq 0\} \tag{4.8}$$

et que pour l dans cet ensemble, $v_l = w_l$.

Soit $j \in J$; il y a deux possibilités : soit $j \in J\backslash K$, 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 $k \in J \cap K$. □

Lemme 4.8 ([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 $f : E \to E$.

(i) **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.

(i) **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

$$0 = \sum_{j\in J} \lambda_j f(v_j) = f\big(\sum_{j\in J} \lambda_j v_j\big). \tag{4.9}$$

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.

(ii) **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

$$y = \sum_{j\in J} \lambda_j v_j. \tag{4.10}$$

Nous avons alors

$$x = f(y) = \sum_{j\in J} \lambda_j f(v_j), \tag{4.11}$$

qui montre que $\{f(v_i)\}_{i\in I}$ est bien génératrice de E

(ii) **Si f change les bases en bases** Soit un endomorphisme changeant toute base en une base. Nous devons prouver qu'il est bijectif.

(i) **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,

$$\sum_{j\in J} (\lambda_j - \mu_j) f(v_j) = 0. \tag{4.12}$$

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.

(ii) **Surjective** Soit $x \in E$. Puisque $\{f(v_i)\}_{i\in I}$ est une base, il existe des scalaires λ_j tels que

$$x = \sum_{j\in J} \lambda_j f(v_j) = f\Big(\sum_{j\in J} \lambda_j v_j\Big). \tag{4.13}$$

Donc f est surjective.

□

Lemme 4.9 ([1]).
Bases dans $\mathbb{R}^n$.

(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 4.10.
*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.

Lemme 4.11.
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

$$v_i = \sum_{k=1}^{n} \lambda_{i,k} e_k \tag{4.14}$$

3. Nous utilisons le fait que l'union de deux parties finies d'un ensemble est finie (lemme 1.123(2)).

Puisque

$$v_{n+1} = \sum_{k=1}^{n} \lambda_{n+1,k} e_k \neq 0, \tag{4.15}$$

quitte à changer la numérotation des e_i, nous pouvons supposer que $\lambda_{n+1,n} \neq 0$. Nous considérons les vecteurs

$$w_i = \lambda_{n+1,n} v_i - \lambda_{i,n} v_{n+1}. \tag{4.16}$$

En calculant un peu,

$$w_i = \lambda_{n+1,n} \sum_{k=1}^{n} \lambda_{i,k} e_k - \lambda_{i,n} \sum_{k=1}^{n} \lambda_{n+1,k} e_k \tag{4.17a}$$

$$= \sum_{k=1}^{n-1} \big(\lambda_{n+1,n}\lambda_{i,k} - \lambda_{i,n}\lambda_{n+1,k}\big) e_k \tag{4.17b}$$

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

$$0 = \sum_{i=1}^{n} \alpha_i w_i = \sum_{i=1}^{n} \alpha_i \lambda_{n+1,n} v_i - \sum_{i=1}^{n} \alpha_i \lambda_{i,n} v_{n+1}. \tag{4.18}$$

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 (4.18) est une combinaison linéaire nulle non triviale des vecteurs de $\{v_1, \dots, v_{n+1}\}$. Cette partie est donc liée. □

Lemme 4.12.
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 $\forall x \in G \backslash B$, 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 $x \in G \backslash B$; 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

$$\sum_{i=1}^{l} \lambda_i b_i + \lambda_x x = 0. \tag{4.19}$$

Si $\lambda_x = 0$ alors un de λ_i doit être non nul et l'équation (4.19) 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

$$x = -\frac{1}{\lambda_x} \sum_{i=1}^{l} \lambda_i b_i. \tag{4.20}$$

Donc tous les éléments de $G \backslash B$ 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. □

Théorème 4.13 (Théorème de la base incomplète)**.**
Soit E un espace vectoriel de type fini sur le corps $\mathbb{K}$.

4. Encore une fois, à part quelques cas triviaux, il n'est pas clair à ce point que ce maximum existe.

(1) Si L est une partie libre et si G est une partie génératrice contenant L, alors il existe une base B telle que $L \subset B \subset G$.

(2) Toute partie libre peut être étendue en une base.

(3) Toutes les bases sont finies et ont même cardinal.

(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 4.11. 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 4.12.

(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 4.11 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.

□

Remarque 4.14.
Le théorème de la base incomplète 4.13(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.

Définition 4.15.
*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 4.16.
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

$$\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \tag{4.21}$$

Les éléments de la base canonique de $\mathbb{R}^m$ peuvent donc être écrits $e_i = \sum_{k=1}^{m} \delta_{i,k} e_k$. △

5. Définition 1.121.
6. Le théorème de la base incomplète 4.13(3) montre que cette définition ne souffre d'aucune ambiguïté.

Le théorème suivant est essentiellement une reformulation du théorème 4.13.

Théorème 4.17.
Soit E un espace vectoriel de dimension finie et $\{e_i\}_{i\in I}$ une partie génératrice de E.

(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.

(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.

Proposition 4.18.
Si E est un espace vectoriel de dimension finie n, alors

(1) toute partie contenant $n+1$ éléments est liée.

(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 4.11.

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 4.11.

Pour la dernière assertion, soit une partie génératrice $\{v_i\}_{i\in I}$ où I contient n éléments. Par le théorème 4.17(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 4.13(3). □

Définition 4.19.
*Soit F un sous-espace vectoriel de l'espace vectoriel E. La **codimension** de F dans E est*

$$\operatorname{codim}_E(F) = \dim(E/F). \tag{4.22}$$

Lemme 4.20.
L'ensemble $\mathbb{Q}^n$ est un $\mathbb{Q}$-espace vectoriel de dimension n.

4.1.1 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 [7].

Lemme 4.21 ([123])**.**
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

(1) $V \cap W_1 = \{0\}$;

(2) $V + W_2 = E$.

Alors il existe un supplémentaire 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.

7. 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.

(i) **Un gros ensemble** Soit

$$\mathcal{A} = \left\{ S \subset E \text{ tel que } \begin{cases} S \text{ est un sous-espace vectoriel de } E \\ W_1 \subset S \subset W_2 \\ S \cap V = \{0\} \end{cases} \right\} \tag{4.23}$$

(ii) **Non vide** Puisque $W_1 \in \mathcal{A}$, cet ensemble n'est pas vide.

(iii) **Ordre** L'ensemble $\mathcal{A}$ est partiellement ordonné pour l'inclusion.

(iv) **$\mathcal{A}$ est inductif** Nous prouvons maintenant que $\mathcal{A}$ est inductif[8]. 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.

(v) **Utilisation de Zorn** Le lemme de Zorn 1.22 nous donne alors un élément maximal W de $\mathcal{A}$. Cet élément vérifie
(1) $W \cap V = \{0\}$,
(2) $W_1 \subset W \subset W_2$,
(3) pour tout $W' \in \mathcal{A}$, nous avons $W' \subset W$ par maximalité de W.

(vi) **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

$$x = v + w_2. \tag{4.24}$$

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,

$$y = w' + \lambda w_2 \tag{4.25}$$

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 (4.25) permet alors d'écrire $w_2 = (y - w')/\lambda$ et finalement

$$x = v + \frac{1}{\lambda}(y - w') = \underbrace{v + \frac{1}{\lambda}y}_{\in V} - \underbrace{\frac{1}{\lambda}w'}_{\in W}. \tag{4.26}$$

La somme d'espaces vectoriels $E = V + W$ est donc établie.

□

Corolaire 4.22.
Tout sous-espace vectoriel d'un espace vectoriel possède un supplémentaire.

Démonstration. Soit un espace vectoriel E ainsi qu'un sous-espace vectoriel V. Si $V = E$ nous sommes O.K. Sinon nous considérons $v \in E \backslash V$ 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 4.21 nous donne alors un supplémentaire de V. □

8. Définition 1.21.

Proposition 4.23 (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. □

Théorème 4.24 (Base incomplète, dimension quelconque)**.**
Soit une partie $\{e_i\}_{i\in I}$ génératrice de l'espace vectoriel E (ici, I est un ensemble quelconque[9]). 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 1.22. 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. □

4.25 ([12])**.**
Une preuve alternative du théorème de la base incomplète serait de prouver que l'ensemble des parties libres est inductif. De ce fait, la proposition 1.23 permet de dire que toute partie libre peut être complétée en une base.

4.1.2 Espace librement engendré

Définition 4.26 ([124])**.**
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[10].

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.

Lemme 4.27.
L'ensemble des applications δ_s données par

$$\begin{aligned} \delta_s : S &\to \mathbb{K} \\ t &\mapsto \begin{cases} 1 & \text{si } t = s \\ 0 & \text{sinon} \end{cases} \end{aligned} \tag{4.27}$$

avec $s \in S$ forment une base[11] *de $F_{\mathbb{K}}(S)$.*

9. Un cas d'utilisation intéressant est de poser $I = E$ et $e_i = i$. Pensez-y.
10. Parce que nous l'aimons bien, nous ne résistons pas à faire un renvoi vers la définition 1.112.
11. Définition 4.5.

Démonstration. Pour prouver que les δ_s sont générateurs, nous considérons $g\colon S \to \mathbb{K}$ non nul sur la partie finie $\{s_i\}_{i\in I}$ de S. Alors nous avons

$$g = \sum_{i\in I} g(s_i)\delta_{s_i}. \tag{4.28}$$

Pour prouver que les δ_s forment une partie libre, nous supposons avoir $\lambda_i \in \mathbb{K}$ tels que

$$g = \sum_{i\in I} \lambda_i \delta_{s_i} = 0 \tag{4.29}$$

Soit $j \in I$. Nous avons

$$0 = f(s_j) = \sum_{i\in I} \lambda_i \underbrace{\delta_{s_i}(s_j)}_{=\delta_{i,j}} = \lambda_j. \tag{4.30}$$

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 $\mathbb{K}$.

4.2 Applications linéaires

Le lien entre matrice et applications linéaires est la définition 4.67 et toutes les propriétés qui s'en suivent.

4.2.1 Définition

Définition 4.28.
*Soient des espaces vectoriels E et F sur le corps $\mathbb{K}$. Soit un sous-corps $\mathbb{L}$ de $\mathbb{K}$. Une application $T\colon E \to F$ 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 4.28 sont des égalités dans F.

4.29.
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 27.140.

Lemme-Définition 4.30.
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) $(T_1 + T_2)(x) = T_1(x) + T_2(x)$,

(2) $(\lambda T)(x) = \lambda T(x)$.

Exemple 4.31.
Pour tout b dans $\mathbb{R}$ la fonction $T_b(x) = bx$ est une application linéaire de $\mathbb{R}$ dans $\mathbb{R}$. En effet,

— $T_b(x+y) = b(x+y) = bx + by = T_b(x) + T_b(y)$,

— $T_b(ax) = b(ax) = abx = aT_b(x)$.

De la même façon on peut montrer que la fonction T_λ définie par $T_\lambda(x) = \lambda x$ est une application linéaire de $\mathbb{R}^m$ dans $\mathbb{R}^m$ pour tout λ dans $\mathbb{R}$ et m dans $\mathbb{N}$. △

Exemple 4.32.
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

$$U_\lambda(ax) = \lambda(ax) + v \neq a(\lambda x + v) = aU_\lambda(x).$$

△

Exemple 4.33.
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,

— $T_A(x + y) = A(x + y) = Ax + Ay = T_A(x) + T_A(y)$,

— $T_A(ax) = A(ax) = a(Ax) = aT_A(x)$.

△

Lemme 4.34.
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

$$f\big(f^{-1}(x) + f^{-1}(y)\big) = f\big(f^{-1}(x)\big) + f\big(f^{-1}(y)\big) = x + y = f\big(f^{-1}(x + y)\big). \tag{4.31}$$

En prenant f^{-1} des deux côtés, nous trouvons

$$f^{-1}(x) + f^{-1}(y) = f^{-1}(x + y). \tag{4.32}$$

De même :

$$f\big(\lambda f^{-1}(x)\big) = \lambda f\big(f^{-1}(x)\big) = \lambda x = f\big(f^{-1}(\lambda x)\big), \tag{4.33}$$

ce qui nous donne $\lambda f^{-1}(x) = f^{-1}(\lambda x)$. □

Définition 4.35 (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 4.30.*

— *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*[12] $\mathrm{GL}(E, F)$. *C'est un groupe par le lemme 4.34.*

Remarque 4.36.
Les ensembles définis en 4.35 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 11.230.

12. Le fait d'utiliser une notation similaire à celle des matrices inversibles n'est pas anodine : le lecteur en est sans doute conscient.

Définition 4.37.
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*[13]*, c'est-à-dire la partie*

$$\ker(f) = \{x \in X \text{ tel que } f(x) = 0\}. \tag{4.34}$$

Proposition 4.38.
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

$$f(x+y) = f(x) + f(y) = 0 + 0 = 0, \tag{4.35}$$

donc $x + y \in \ker(f)$, et

$$f(\lambda x) = \lambda f(x) = 0, \tag{4.36}$$

donc $\lambda x \in \ker(f)$. □

Lemme 4.39 ([1])**.**
Soit une application linéaire $f\colon V \to W$. Si $b \in W$ et si $m \in f^{-1}(b)$, alors

$$f^{-1}(b) - m = \ker(f). \tag{4.37}$$

Démonstration. Si $x \in f^{-1}(b) - m$, il existe $\alpha \in f^{-1}(b)$ tel que $x = \alpha - m$. Alors

$$f(x) = f(\alpha) - f(m) = b - b = 0. \tag{4.38}$$

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

$$f(z+m) = f(z) + f(m) = 0 + b = b = . \tag{4.39}$$

□

Proposition 4.40.
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.

(i) **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

$$T(v) = \sum_i v_i f_i \tag{4.40}$$

est une bonne définition et satisfait aux exigences.

(ii) **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 $T = U$.

□

Lemme 4.41 ([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

$$\begin{aligned} \varphi_{i\alpha}\colon V &\to W \\ v &\mapsto v_i f_\alpha \end{aligned} \tag{4.41}$$

où v_i est défini par la décomposition (unique) $v = \sum_i v_i e_i$.

Alors :

13. Définition 2.5.

(1) La partie $\{\varphi_{i\alpha}\}$ est une base de $\mathcal{L}(V,W)$.

(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.

(i) **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

$$b(v) = \sum_\alpha b_\alpha(v) f_\alpha. \tag{4.42}$$

Nous posons $b_{\alpha i} = b_\alpha(e_i)$. Ainsi,

$$b(v) = \sum_\alpha v_i b_{\alpha i} f_\alpha = \sum_{\alpha i} b_{\alpha i}\varphi_{i\alpha}(v). \tag{4.43}$$

Donc b peut être écrit comme combinaison linéaire des $\varphi_{i\alpha}$.

(ii) **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 $v \in V$:

$$0 = \sum_{i\alpha} a_{i\alpha}\varphi_{i\alpha}(v) = \sum_{i\alpha} a_{i\alpha} v_i f_\alpha, \tag{4.44}$$

mais comme les f_α forment une base, chaque terme de la somme sur α est nul :

$$\sum_i a_{i\alpha} v_i = 0. \tag{4.45}$$

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 4.15. □

4.2.2 Linéarité et bases

Proposition 4.42 ([125])**.**
Soient deux espaces vectoriels E et F. Une application linéaire[14] *$f\colon E \to F$ 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. □

Proposition 4.43 ([125])**.**
Soit $f \in \mathcal{L}(E,F)$ où E et F sont deux espaces vectoriels.

(1) Si f est injective et si $\{v_i\}_{i\in I}$ est libre, alors $\{f(v_i)\}_{i\in I}$ est libre.

(2) Si f est surjective et si $\{v_i\}_{i\in I}$ est génératrice, alors $\{f(v_i)\}_{i\in I}$ est génératrice.

(3) Si f est une bijection, alors l'image d'une base par f est une base.

Démonstration. En trois parties.

(i) **(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[15] tels que $\sum_{j\in J}\lambda_j f(v_j) = 0$. La linéarité de f donne[16]

$$f\Big(\sum_{j\in J}\lambda_j v_j\Big) = 0. \tag{4.46}$$

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 $j \in J$.

14. Définition 4.28.
15. Des éléments du corps de base $\mathbb{K}$.
16. Voir les propriétés de la définition 4.28.

(ii) **(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

$$x = \sum_{j\in J} \lambda_j v_j. \tag{4.47}$$

En appliquant f aux deux côtés, et en tenant compte de la linéarité de f,

$$y = f(x) = \sum_{j\in J} \lambda_j f(v_j), \tag{4.48}$$

ce qui prouve que y est une combinaison linéaire des $f(v_j)$.

(iii) **(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.

□

Corolaire 4.44 ([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 $f : E \to F$. Par la proposition 4.43(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. □

4.2.3 Rang

La proposition 4.45 et le théorème 4.46 sont valables également en dimension infinie ; ce sera une des rares incursions en dimension infinie de ce chapitre.

Proposition-Définition 4.45.
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 $f : E \to F$. 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. □

Théorème 4.46 (Théorème du rang)**.**
Soient E et F deux espaces vectoriels (de dimensions finies ou non) et soit $f : E \to F$ 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 $\mathrm{Image}(f)$ alors

$$(u_s)_{s\in s} \cup (v_t)_{t\in T} \tag{4.49}$$

est une base de E.

En dimension finie, nous avons en plus la formule suivante :

$$\mathrm{rk}(f) + \dim(\ker f) = \dim E, \tag{4.50}$$

c'est-à-dire que le rang[17] *de f est égal à la codimension*[18] *du noyau.*

17. Définition 4.45.
18. Définition 4.19.

Démonstration. Nous devons montrer que

$$(u_s)_{s\in S} \cup (v_t)_{t\in T} \tag{4.51}$$

est libre et générateur.

Soit $x \in E$. Nous définissons les nombres x_t par la décomposition de $f(x)$ dans la base $\big(f(v_t)\big)$:

$$f(x) = \sum_{t\in T} x_t f(v_t). \tag{4.52}$$

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) :

$$x - \sum_t x_t v_t = \sum_{s\in S} x_s u_s. \tag{4.53}$$

Par conséquent

$$x = \sum_s x_s u_s + \sum_t x_t v_t. \tag{4.54}$$

En ce qui concerne la liberté nous écrivons

$$\sum_t x_t v_t + \sum_s x_s u_s = 0. \tag{4.55}$$

En appliquant f nous trouvons que

$$\sum_t x_t f(v_t) = 0 \tag{4.56}$$

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 25.18.

Proposition 4.47 ([126])**.**
Soit E, un espace vectoriel de dimension finie sur le corps $\mathbb{K}$. Soient V et W des sous-espaces vectoriels de E. Alors

$$\dim(V + W) = \dim(V) + \dim(W) - \dim(V \cap W). \tag{4.57}$$

Démonstration. Nous considérons l'application

$$\begin{aligned} \varphi\colon V \times W &\to E \\ (x, y) &\mapsto x + y. \end{aligned} \tag{4.58}$$

C'est une application linéaire dont l'image est $V + W$. Nous avons donc, pour commencer

$$\dim(V + W) = \dim\big(\text{Image}(\varphi)\big). \tag{4.59}$$

Nous appliquons à présent le théorème du rang 4.46 à l'application φ :

$$\begin{aligned} \dim(V + W) &= \dim\big(\text{Image}(\varphi)\big) && \text{(4.60a)} \\ &= \dim(V \times W) - \dim\big(\ker(\varphi)\big) && \text{(4.60b)} \\ &= \dim(V) + \dim(W) - \dim\big(\ker(\varphi)\big). && \text{(4.60c)} \end{aligned}$$

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

$$\ker(\varphi) = \{(x, -x) \text{ tel que } x \in V \cap W\}. \tag{4.61}$$

Nous montrons à partir de cela que $\dim\big(\ker(\varphi)\big) = \dim(V \cap W)$ en montrant que l'application

$$\begin{aligned} \psi\colon V \cap W &\to \ker(\varphi) \\ x &\mapsto (x, -x) \end{aligned} \tag{4.62}$$

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 $\dim\big(\ker(\varphi)\big) = \dim(V \cap W)$. □

Corolaire 4.48.
Soient deux espaces vectoriels E et F de même dimension finie[19]*. 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 $\mathrm{rk}(f) = \dim(E)$, ce qui donne, par le théorème du rang 4.46, $\dim\big(\ker(f)\big) = 0$, 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 $\mathrm{rk}(f) = \dim(E)$ ou encore que f est surjective. □

Exemple 4.49.
Le corolaire 4.48 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. △

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 4.50 dit est que si $AB = \mathbb{1}$, alors $BA = \mathbb{1}$.

Corolaire 4.50.
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 4.48. 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 $g = h$.[20] □

C'est ce corolaire qui nous permet d'écrire f^{-1} sans plus de précisions dès que f est une bijection.

Exemple 4.51 (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

$$f(e_k) = e_{k+1}. \tag{4.63}$$

19. Les deux mots sont importants : les dimensions doivent être égales et finies.

20. C'est le même argument que celui employé pour la preuve du lemme 1.158 (2), à ceci près que nous devions montrer l'existence de l'inverse à droite.

Il est injectif, mais pas surjectif. Si on pose

$$g(e_k) = \begin{cases} e_{k-1} & \text{si } k \geqslant 1 \\ 0 & \text{si } k = 0 \end{cases} \tag{4.64}$$

alors nous avons $gf = \mathrm{Id}$, mais pas $fg = \mathrm{Id}$ parce que ce $(fg)(e_0) = 0$. △

Lemme 4.52.
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,

$$f\big(f^{-1}(x) + f^{-1}(y)\big) = f\big(f^{-1}(x)\big) + f\big(f^{-1}(y)\big) = x + y. \tag{4.65}$$

De la même façon,

$$f\big(\lambda f^{-1}(x)\big) = \lambda x, \tag{4.66}$$

donc $f^{-1}(\lambda x) = \lambda f^{-1}(x)$. □

Proposition 4.53.
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

$$x = \sum_j \lambda_j f(v_j) = f\big(\sum_j \lambda_j v_j\big), \tag{4.67}$$

ce qui prouve que f est surjective. Le corolaire 4.48 nous dit alors que f est une bijection. L'application inverse est également linéaire par le lemme 4.52.

Une application linéaire bijective (comme f^{-1}) transforme une base en une base par la proposition 4.43. Donc

$$f^{-1}\big(\{f(v_i)\}\big) \tag{4.68}$$

est une base. □

Proposition 4.54.
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

(i) **f est injective** Si $f(x) = f(y)$, alors en appliquant g nous avons

$$g\big(f(x)\big) = g\big(f(y)\big), \tag{4.69}$$

ce qui donne $x = y$.

(ii) **f est surjective** C'est maintenant le corolaire 4.48.

(iii) **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.

(iv) **g est injective** C'est maintenant le corolaire 4.48.

□

Lemme 4.55 ([127]).
Soit une application linéaire $f\colon E \to F$.

(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

$$\begin{aligned} g\colon F&\to E\\ \sum_k a_kf(x_k)&\mapsto\sum_k a_kx_k. \end{aligned}\tag{4.70}$$

Cela donne $f\circ g=\mathrm{Id}\,|_F$ parce que si $v\in F$ alors $v=\sum_k v_kf(x_k)$ avec $v_k\in\mathbb{K}$, et nous avons

$$(f\circ g)(v)=\sum_k v_k(f\circ g)\big(f(x_k)\big)=f\left(\sum_k v_kx_k\right)=\sum_k v_kf(x_k)=v.\tag{4.71}$$

Réciproquement, si il existe $g\colon F\to E$ tel que $f\circ g=\mathrm{Id}$ alors f doit être surjective, parce que

$$F=\mathrm{Image}(f\circ g)=f\big(\mathrm{Image}(g)\big)\subset\mathrm{Image}(f).\tag{4.72}$$

□

4.3 Matrices

Les matrices et les applications linéaires sont deux choses différentes. Une application linéaire [21] 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 4.67 et ce qui s'en suit.

4.3.1 Définitions

Les notions topologiques sur les espaces de matrices sont pour plus tard, à commencer par la définition 7.199.

Définition 4.56.
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

$$\{1,\dots,n\}\times\{1,\dots,m\}\to\mathbb{A},\tag{4.73}$$

*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 4.57.
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 $\mathbb{M}(n\times n,\mathbb{A})$,*

21. Définition 4.28.

— 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****.*

4.58.
On note les isomorphismes naturels $\mathbb{M}(1 \times m, \mathbb{A}) \simeq \mathbb{A}^m$ et $\mathbb{M}(n \times 1, \mathbb{A}) \simeq \mathbb{A}^n$.

Lemme-Définition 4.59.
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*[22].

Lemme-Définition 4.60.
Avec la multiplication

$$\begin{aligned} \mathbb{M}(n \times p, \mathbb{A}) \times \mathbb{M}(p \times m, \mathbb{A}) &\to \mathbb{M}(n \times m, \mathbb{A}) \\ (A, B) &\mapsto (AB)_{i,j} = \sum_{k=1}^{p} A_{i,k} B_{k,j}, \end{aligned} \tag{4.74}$$

l'espace $\mathbb{M}(n, \mathbb{K})$ *est une* $\mathbb{K}$*-algèbre*[23].

Définition 4.61.
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 4.62.
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 9.10.3 que la définition de transposée d'une application linéaire n'est pas tout à fait évidente ; elle sera la définition 9.183.

Ici nous avons bien défini la transposée d'une matrice, pas d'une application linéaire.

Remarque 4.63.
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

$$\mathbb{1}_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases} \tag{4.75}$$

Il est vite vu que si A est une matrice carrée d'ordre n, alors $A\mathbb{1} = \mathbb{1}A = A$.

Lemme 4.64 ([1])**.**
Si A*,* B *et* C *sont des matrices, nous avons*

22. Définition 1.323
23. Définition 1.340.

(1) $(AB)^t = B^t A^t$,
(2) $\mathrm{Tr}(ABC) = \mathrm{Tr}(CAB)$.

Démonstration. La première est un simple calcul :

$$(AB)^t_{i,j} = (AB)_{j,i} = \sum_k A_{j,k}B_{k,i} = \sum_k A^t_{k,j}B^t_{i,k} = (B^tA^t)_{i,j}. \tag{4.76}$$

Pour la seconde :

$$\mathrm{Tr}(ABC) = \sum_{ikl} A_{i,k}B_{k,l}C_{l,i} = \sum_{ikl} C_{l,i}A_{i,k}B_{k,l} = \sum_l (CAB)_{l,l} = \mathrm{Tr}(CAB). \tag{4.77}$$

□

4.65.
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 9.199.

Lemme 4.66.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$. Si pour tout $x, y \in \mathbb{K}^n$ nous avons

$$\sum_{ij} A_{i,j}x_i y_j = \sum_{ij} B_{i,j}x_i y_j \tag{4.78}$$

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

$$\sum_{ij} A_{i,j}\delta_{i,k}y_j = \sum_j A_{k,j}y_j. \tag{4.79}$$

Après avoir effectué toutes les sommes, nous nous retrouvons avec $A_{k,l} = B_{k,l}$, ce qui signifie $A = B$. □

4.3.2 Identifier matrices et applications linéaires

Voir dans l'index thématique, -2.1.1.

Soient deux espaces vectoriels de dimension finie E, F sur le corps $\mathbb{K}$. Nous considérons les bases[24] $\{e_i\}$ pour E et $\{f_\alpha\}$ pour F.

Définition 4.67.
Nous considérons l'application

$$\begin{aligned} \psi\colon \mathbb{M}(n \times m, \mathbb{K}) &\to \mathcal{L}(E, F) \\ A &\mapsto f_A \end{aligned} \tag{4.80}$$

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha,i}x_i f_\alpha \tag{4.81}$$

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

4.68.
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 structure que vous pouvez raisonnablement imaginer.

24. C'est le théorème 4.13 qui nous permet de considérer des bases. Et ce théorème ne fonctionne que parce que nous avons supposé une dimension finie.

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 [25].

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 12.117.

4.69.
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

$$(Ax)_i = \sum_j A_{i,j} x_j. \tag{4.82}$$

Autrement dit, $Ax = f_A(x)$.

Cette convention et de nombreuses autres à propos de matrice sera rappelée dans -2.1.

Proposition-Définition 4.70.
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

$$\begin{aligned} \psi\colon \mathbb{M}(n \times m, \mathbb{K}) &\to \mathcal{L}(E, F) \\ A &\mapsto f_A \end{aligned} \tag{4.83}$$

où f_A est définie par

$$f_A(x) = \sum_{i\alpha} A_{\alpha,i} x_i f_\alpha \tag{4.84}$$

si x_i sont les coordonnées de $x \in E$ dans la base $\{e_i\}$.

Alors

(1) Nous avons

$$f_A(e_i)_\alpha = A_{\alpha,i}. \tag{4.85}$$

(2) Nous avons

$$f_A(e_i) = \sum_\alpha A_{\alpha,i} f_\alpha. \tag{4.86}$$

(3) Nous avons

$$\big(f_A(x)\big)_\alpha = \sum_i A_{\alpha,i} x_i. \tag{4.87}$$

(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

$$f_A(e_j) = \sum_{i\alpha} A_{\alpha,i} (e_j)_i f_\alpha = \sum_\alpha A_{\alpha,j} f_\alpha, \tag{4.88}$$

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 4.84.

25. 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.

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

$$f_A(x) = \sum_{i\alpha} A_{\alpha,i}x_i f_\alpha = \sum_{i\alpha} f(e_i)_\alpha x_i f_\alpha = \sum_\alpha f(\sum_i x_i e_i)_\alpha f_\alpha = \sum_\alpha f(x)_\alpha f_\alpha = f(x). \tag{4.89}$$

□

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 $\mathbb{K}^n$.

Proposition 4.71 ([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[26]

$$\psi\colon \mathbb{M}(m\times n,\mathbb{K}) \to \mathcal{L}(E,F) \tag{4.90}$$

est un isomorphisme d'espaces vectoriels.

Démonstration. Le fait que ψ soit une bijection est la proposition 4.70. Nous devons montrer que c'est une application linéaire.

Pour $\lambda \in \mathbb{K}$ nous avons le calcul

$$\psi(\lambda A)(e_k) = f_{\lambda A}(e_k) = \sum_{\alpha i}(\lambda A)_{\alpha,i}\underbrace{(e_k)_i}_{=\delta_{k,i}} f_\alpha = \lambda\sum_\alpha A_{\alpha,k}f_\alpha = \lambda f_A(e_k). \tag{4.91}$$

Donc $\psi(\lambda A) = \lambda\psi(A)$.

Si $A, B \in \mathbb{M}(n,\mathbb{K})$ nous avons de la même façon, $f_{A+B} = f_A + f_B$. □

Proposition 4.72.
Soient des espaces vectoriels E, F et G de dimensions n, m et p munis de bases[27] *$\{e_i\}$, $\{f_i\}$ et $\{g_i\}$. Nous considérons les applications*

$$\psi\colon \mathbb{M}(m\times n,\mathbb{K}) \to \mathcal{L}(E,F) \tag{4.92a}$$
$$\psi\colon \mathbb{M}(p\times m,\mathbb{K}) \to \mathcal{L}(F,G) \tag{4.92b}$$
$$\psi\colon \mathbb{M}(p\times n,\mathbb{K}) \to \mathcal{L}(E,G). \tag{4.92c}$$

Nous avons

$$\psi(A)\circ\psi(B) = \psi(AB) \tag{4.93}$$

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

26. Notez la position du n et du m. Sachez noter les bornes des sommes écrites dans la démonstration.
27. Avec trois ensembles, nous renonçons à utiliser des alphabets différents pour numéroter les éléments des bases.

$f_B\colon E \to F$ et la composée $f_A \circ f_B\colon E \to G$. Et puis c'est le calcul :

$$(f_A \circ f_B)(e_k) = f_A\big(\sum_{ij} B_{i,j}(e_k)_j f_i\big) \tag{4.94a}$$
$$= \sum_i B_{i,k} f_A(f_i) \tag{4.94b}$$
$$= \sum_i B_{i,k} \sum_{rs} A_{r,s}(f_i)_s g_r \tag{4.94c}$$
$$= \sum_{ir} B_{i,k} A_{r,i} g_r \tag{4.94d}$$
$$= \sum_r (AB)_{r,k} g_r \tag{4.94e}$$
$$= f_{AB}(e_k). \tag{4.94f}$$

Donc $f_A \circ f_B = f_{AB}$ comme il se doit. □

Nous pouvons particulariser au cas où $E = F = G$.

Proposition 4.73.
Si E est un espace vectoriel muni d'une base $\{e_i\}$, alors l'application

$$\psi\colon \mathbb{M}(n, \mathbb{K}) \to \text{End}(E) \tag{4.95}$$

est un isomorphisme d'algèbre[28] *et d'anneaux*[29].

Démonstration. Le fait que ψ soit un isomorphisme d'algèbre est juste la combinaison entre les propositions 4.71 et 4.72.

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 $\psi(\delta) = f_\delta = \text{Id}$. Juste un calcul :

$$f_\delta(x) = \sum_{ij} \delta_{i,j} x_j e_i = \sum_i x_i e_i = x. \tag{4.96}$$

Donc oui, f_δ est l'identité. □

Le fait que ψ est continue sera la proposition 12.117.

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 $\text{End}(\mathbb{K}^n)$ qui est un isomorphisme d'anneaux et d'algèbres.

Nous verrons que ce ψ respecte encore les inverses[30] et les déterminants[31].

4.74.
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

$$\psi\colon \mathbb{M}(m \times n, \mathbb{K}) \to \mathcal{L}(E, F) \tag{4.97}$$

qui a toutes les propriétés imaginables[32].

28. Définition 1.340.
29. Définition 1.40
30. Proposition 4.93.
31. Proposition 9.11.
32. Et elle en aura encore plus lorsque nous aurons vu les déterminants.

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 [33].

4.75.
Tant que nous sommes à parler de matrice et d'applications linéaires, les plus acharnés anti-abus de language [34] 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 4.5). 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.

4.3.3 Déterminant

Définition 4.76.
*Si $A \in \mathbb{M}(n, \mathbb{K})$ nous définissons le **déterminant** de A par la formule*

$$\det(A) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i=1}^{n} A_{i,\sigma(i)} \tag{4.98}$$

où la somme est effectuée sur tous les éléments du groupe symétrique [35] 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.

4.3.4 Déterminant en petite dimension

En dimension deux, le déterminant de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est le nombre

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb. \tag{4.99}$$

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

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}. \tag{4.100}$$

33. 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.

34. Dont l'auteur de ces lignes fait partie.

35. Pour le groupe symétrique, c'est la définition 1.267, le fait que ce soit un groupe fini est le lemme 1.270, et pour la somme sur un groupe fini c'est la définition 1.302.

4.3.5 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.

Lemme 4.77 ([1]).
Si A et B sont des matrices, alors

$$(AB)^t = B^t A^t. \tag{4.101}$$

Démonstration. Il suffit de calculer les éléments de matrice :

$$(AB)^t_{i,j} = (AB)_{j,i} = \sum_k A_{j,k} B_{k,i} = \sum_k B^t_{i,k} A^t_{k,j} = (B^t A^t)_{i,j}. \tag{4.102}$$

□

Lemme 4.78 ([1, 128]).
Si A est une matrice, alors $\det(A) = \det(A^t)$.

Démonstration. Nous commençons par écrire la définition du déterminant :

$$\det(A^t) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} (A^t)_{i,\sigma(i)} = \sum_{\sigma} \epsilon(\sigma) \prod_i A_{\sigma(i),i}. \tag{4.103}$$

Pour chaque σ séparément, en utilisant la proposition 1.310 pour ré-indexer le produit :

$$\prod_i A_{\sigma(i),i} = \prod_i A_{i,\sigma^{-1}(i)}. \tag{4.104}$$

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 1.302 et faire la somme sur σ^{-1} :

$$\det(A^t) = \sum_{\sigma} \epsilon(\sigma) \prod_i A_{i,\sigma^{-1}(i)} = \sum_{\sigma} \epsilon(\sigma^{-1}) \prod_i A_{i,\sigma(i)} = \det(A) \tag{4.105}$$

où nous avons utilisé le fait que $\epsilon(\sigma^{-1}) = \epsilon(\sigma)$ (corolaire 1.294). □

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.

Lemme 4.79 ([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 :

$$C_{i,j} = \begin{cases} (A^t)_{i,j} & \text{si } j \neq k, j \neq l \\ (A^t)_{i,k} & \text{si } j = l \\ (A^t)_{i,l} & \text{si } j = k \end{cases} = \begin{cases} A_{j,i} & \text{si } j \neq k, j \neq l \\ A_{k,i} & \text{si } j = l \\ A_{l,i} & \text{si } j = k. \end{cases} \tag{4.106}$$

Ensuite nous prouvons que $C^t = B$ en écrivant les éléments de C^t :

$$(C^t)_{i,j} = C_{j,i} = \begin{cases} A_{i,j} & \text{si } i \neq k, i \neq l \\ A_{k,j} & \text{si } i = l \\ A_{l,j} & \text{si } i = k. \end{cases} \tag{4.107}$$

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

$$(E_{i,j})_{k,l} = \delta_{i,k}\delta_{j,l}. \tag{4.108}$$

Proposition 4.80 (Permuter des lignes ou des colonnes $L_k \leftrightarrow L_l$[129, 1])**.**
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 en permutant deux lignes ou deux colonnes, alors

$$\det(A) = -\det(B). \tag{4.109}$$

(2) Si B est la matrice obtenue à partir de A par la permutation de lignes $L_k \leftrightarrow L_l$. Alors

$$B = SA \tag{4.110}$$

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.

(3) La matrice S vérifie $\det(S) = -1$

(4) Nous avons

$$\det(SA) = \det(S)\det(A). \tag{4.111}$$

Démonstration. Point par point

(i) **(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 1.267). Nous avons

$$B_{i,j} = A_{i,\alpha(j)}, \tag{4.112}$$

ou encore : $A_{i,j} = B_{i,\alpha(j)}$. Par définition,

$$\det(A) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n} A_{i,\sigma(i)} \tag{4.113}$$

C'est le moment d'utiliser la proposition 1.306 à propos de somme sur des groupes avec $G = S_n$, $h = \alpha$ et

$$f(\sigma) = \epsilon(\sigma)\prod_i A_{i,\sigma(i)}. \tag{4.114}$$

Nous savons que $\epsilon(\alpha) = -1$ et que ϵ est un morphisme par la proposition 1.293(1), donc

$$f(\alpha\sigma) = \epsilon(\alpha\sigma)\prod_i A_{i,(\alpha\sigma)(i)} = -\epsilon(\sigma)\prod_i B_{i,\sigma(i)}. \tag{4.115}$$

Avec ça, nous concluons :

$$\det(A) = \sum_{\sigma\in S_n} f(\sigma) = \sum_{\sigma} f(\alpha\sigma) = -\sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n} B_{i,\sigma(i)} = -\det(B). \tag{4.116}$$

(ii) **(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 4.79 nous dit que $C^t = B'$. En utilisant le lemme 4.78 sur le déterminant de la transposée,

$$\det(B') = \det(C^t) = \det(C) = -\det(A^t) = -\det(A). \tag{4.117}$$

Voilà qui prouve le résultat pour les permutation de lignes.

(iii) **(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 :

$$(SA)_{i,j} = \sum_m S_{i,m}A_{m,j} = A_{i,j} + \sum_m (\delta_{k,i}\delta_{l,m} + \delta_{l,i}\delta_{l,m} - \delta_{k,i}\delta_{k,m} - \delta_{l,i}\delta_{l,m})A_{m,j} \tag{4.118a}$$

$$= A_{i,j} + \delta_{k,i}A_{l,j} + \delta_{l,i}A_{k,j} - \delta_{k,i}A_{k,j} - \delta_{l,i}A_{l,j}. \tag{4.118b}$$

Si $i \neq j$ et $i \neq l$, alors $(SA)_{i,j} = A_{i,j}$. Si $i = k$, alors

$$(SA)_{k,j} = A_{k,j} + A_{l,j} - A_{k,j} = A_{l,j}, \tag{4.119}$$

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 $SA = B$.

(iv) **(3)** En utilisant la définition du déterminant,

$$\det(S) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} S_{i,\sigma(i)} \tag{4.120a}$$

$$= \sum_{\sigma} \epsilon(\sigma) \prod_i \big(\delta_{i,\sigma(i)} + \delta_{k,i}\delta_{l,\sigma(i)} + \delta_{l,i}\delta_{k,\sigma(i)} - \delta_{k,i}\delta_{k,\sigma(i)} - \delta_{l,i}\delta_{l,\sigma(i)}\big). \tag{4.120b}$$

Nous utilisons l'associativité et la commutativité du produit pour séparer les facteurs $i = k$ et $i = l$ des autres :

$$\det(S) = \sum_{\sigma} \epsilon(\sigma) \prod_{\substack{i\neq k\\ i\neq l}} \delta_{i,\sigma(i)}(\delta_{k,\sigma(k)} + \delta_{l,\sigma(k)} - \delta_{k,\sigma(k)})(\delta_{l,\sigma(l)} + \delta_{k,\sigma(l)} - \delta_{l,\sigma(l)}). \tag{4.121}$$

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 $\sigma = \text{Id}$ et la permutation $\sigma = (k, l)$. Pour $\sigma = \text{Id}$, nous avons

$$\prod_{\substack{i\neq k\\ i\neq l}} \delta_{i,i}(\delta_{k,k} + \delta_{l,k} - \delta_{k,k})(\delta_{l,l} + \delta_{k,l} - \delta_{l,l}) = 0. \tag{4.122}$$

Dernier espoir : $\sigma = (k, l)$. Pour ce terme nous avons $\epsilon(\sigma) = -1$ et

$$\prod_{\substack{i\neq k\\ i\neq l}} \delta_{i,i}(\delta_{k,l} + \delta_{l,l} - \delta_{k,l})(\delta_{l,k} + \delta_{k,k} - \delta_{l,k}) = 1. \tag{4.123}$$

Au final dans $\det(S)$, il n'y a que le terme $\sigma = (k, l)$ qui est non nul, et il vaut -1. Donc

$$\det(S) = -1. \tag{4.124}$$

(v) **(4)** Il s'agit de mettre bout à bout les points déjà prouvés :

$$\det(SA) = -\det(A) = \det(S)\det(A). \tag{4.125}$$

□

Corolaire 4.81 ([129]).
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

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}. \tag{4.126}$$

Proposition 4.82 ([129]).
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

$$\det(B) = \det(A) + \det(C). \tag{4.127}$$

Démonstration. En utilisant l'associativité de la multiplication,

$$\begin{aligned}
\det(B) &= \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} B_{i,\sigma(i)} && \text{(4.128a)}\\
&= \sum_{\sigma} \epsilon(\sigma) \Big(\prod_{i \neq j} B_{i,\sigma(i)} \Big) B_{j,\sigma(j)} && \text{(4.128b)}\\
&= \sum_{\sigma} \epsilon(\sigma) \Big(\prod_{i \neq j} A_{i,\sigma(i)} \Big) (A_{j,\sigma(j)} + v_{\sigma(j)}) && \text{(4.128c)}\\
&= \sum_{\sigma} \epsilon(\sigma) \prod_{i} A_{i,\sigma(i)} + \sum_{\sigma} \epsilon(\sigma) \prod_{i \neq j} C_{i,\sigma(i)} v_{\sigma(j)} && \text{(4.128d)}\\
&= \det(A) + \sum_{\sigma} \epsilon(\sigma) \prod_{i \neq j} C_{i,\sigma(i)} C_{j,\sigma(j)} && \text{(4.128e)}\\
&= \det(A) + \det(C). && \text{(4.128f)}
\end{aligned}$$

Justifications :

— 4.128d parce que pour $i \neq j$ nous avons $A_{i,\sigma(i)} = C_{i,\sigma(i)}$

— 4.128e parce que $v_{\sigma(j)} = C_{j,\sigma(j)}$.

□

Proposition 4.83 (Combinaison de lignes ou colonnes $L_k \to L_k + \lambda L_l$[129]).
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

$$\det(A) = \det(B). \tag{4.129}$$

(2) Si B est la matrice A dans laquelle nous avons opéré la substitution $L_k \to L_k + \lambda L_l$, alors

$$B = UA \tag{4.130}$$

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

$$\det(UA) = \det(U)\det(A). \tag{4.131}$$

Démonstration. Point par point.

(i) **(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 4.82. Donc

$$\det(B) = \det(A) + \det(C). \tag{4.132}$$

Mais dans la matrice C, nous avons $L_k = \lambda L_l$, ce qui implique $\det(C) = 0$ par le corolaire 4.81. Donc $\det(A) = \det(B)$ comme il se devait.

(ii) **(2)** Encore un calcul :

$$(UA)_{i,j} = \sum_m \big(\delta_{i,m} + \lambda(E_{k,l})_{i,m}\big)A_{m,j} = A_{i,j} + \lambda\sum_m \delta_{k,i}\delta_{l,m}A_{m,j} = A_{i,j} + \lambda\delta_{l,i}A_{k,j}. \tag{4.133}$$

Cela donne, pour $i = k$ la ligne

$$(UA)_{k,j} = A_{k,j} + \lambda A_{l,j}, \tag{4.134}$$

ce qui correspond bien à $L_k \to L_k + \lambda L_l$.

(iii) **(3)** Nous calculons le déterminant de $U = \delta + \lambda E_{k,l}$ avec $k \neq l$. Nous avons dans un premier temps :

$$\det(U) = \sum_{\sigma\in S_n} \epsilon(\sigma)\prod_{i=1}^{n}(\delta_{i,\sigma(i)} + \lambda\delta_{k,i}\delta_{l,\sigma(i)}). \tag{4.135}$$

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 $i = k$:

$$(\delta_{k,\sigma(k)} + \lambda\delta_{k,k}\delta_{k,\sigma(k)})(\delta_{l,\sigma(l)} + \lambda\delta_{k,l}\delta_{k,\sigma(l)}). \tag{4.136}$$

Le dernier facteur est nul.

(iv) **(4)** En mettant bout à bout les résultats prouvés,

$$\det(UA) = \det(A) = \det(U)\det(A). \tag{4.137}$$

□

Proposition 4.84 (Multiplication par un scalaire d'une ligne ou colonne $L_k \to \lambda L_k$[129])**.**
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 $\lambda \in \mathbb{K}$.

(1) $\det(B) = \lambda\det(A)$

(2) En considérant la matrice $T = \delta + (\lambda - 1)E_{k,k}$, nous avons

$$B = TA, \tag{4.138}$$

c'est-à-dire que la matrice T est une matrice de multiplication de ligne par un scalaire.

(3) Nous avons $\det(T) = \lambda$.

(4) Et aussi : $\det(TA) = \det(T)\det(A)$

Démonstration. Point par point.

(i) **(1)** La matrice B est donnée par les éléments

$$B_{i,j} = \begin{cases} A_{i,j} & \text{si } i \neq k \\ \lambda A_{i,j} & \text{si } i = k \end{cases} \tag{4.139}$$

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 :

$$\det(B) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} B_{i,\sigma(i)} = \sum_{\sigma} \prod_{i} \big(1 + (\lambda - 1)\delta_{\sigma(i),k} A_{i,\sigma(i)}\big). \tag{4.140}$$

L'associativité du produit dans $\mathbb{K}$ nous permet de séparer le produit de la façon suivante :

$$\prod_{i=1}^{n} \big(1 + (\lambda - 1)\delta_{\sigma(i),k}\big)A_{i,\sigma(i)} = \prod_{i} \big(1 + (\lambda - 1)\delta_{\sigma(i),k}\big) \prod_{i} A_{i,\sigma(i)} = \lambda \prod_{i} A_{i,\sigma(i)}. \tag{4.141}$$

En remettant dans (4.140), nous trouvons $\det(B) = \det(A)$.

(ii) **(2)** C'est un cas particulier de la proposition 4.83(2) en prenant $k = l$ et en adaptant le λ.

(iii) **(3)** Nous calculons le déterminant de la matrice $T = \delta + (\lambda - 1)E_{k,k}$. La formule du déterminant donne

$$\det(T) = \sum_{\sigma} \epsilon(\sigma) \prod_{i=1}^{n} \big(\delta_{i,\sigma(i)} + (\lambda - 1)\delta_{k,i}\delta_{k,\sigma(i)}\big). \tag{4.142}$$

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

$$\det(T) = \prod_{i=1}^{n} \big(1 + (\lambda - 1)\delta_{k,i}\big) = \left(\prod_{i\neq k} 1\right)(1 + (\lambda - 1)) = \lambda \tag{4.143}$$

où nous avons utilisé encore l'associativité pour isoler le facteur $i = k$.

(iv) **(4)** Il faut mettre bout à bout les résultats déjà établis :

$$\det(TA) = \lambda \det(A) = \det(T)\det(A). \tag{4.144}$$

□

4.3.6 Réduction de Gauss

4.85.
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 4.80.

— Combinaisons de lignes $L_k \to L_k + \lambda L_l$: $U(n;k,l,\lambda) = \delta + \lambda E_{k,l}$, proposition 4.83.

— Multiplication d'une ligne par un scalaire $L_k \to \lambda L_k$: $T(n;k,\lambda) = \delta + (\lambda - 1)E_{k,k}$, proposition 4.84.

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.

Ces matrices seront dans la suite, notées G.

Lemme 4.86.
Si G est une matrice de manipulation de lignes, alors

$$\det(GA) = \det(G)\det(A) \tag{4.145}$$

pour toute matrice A.

Si H est une matrice de manipulation de colonnes, alors

$$\det(AH) = \det(A)\det(H) \tag{4.146}$$

pour toute matrice A.

Proposition 4.87 (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

$$G_1 \dots G_N A = \delta. \tag{4.147}$$

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

$$T(1; 1, \frac{1}{A_{1,1}})A = \delta \tag{4.148}$$

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 4.81). Il existe donc un k tel que $A_{k,1} \neq 0$.

Par la proposition 4.80, la matrice

$$B^{(1)} = S(n + 1; k, 1)A \tag{4.149}$$

est une matrice telle que $B^{(1)}_{1,1} = A_{k,1} \neq 0$. Ensuite, par la proposition 4.84 la matrice

$$B^{(2)} = T(n + 1; 1, \frac{1}{A_{k,1}})B^{(1)} \tag{4.150}$$

vérifie $B^{(2)}_{1,1} = 1$.

Puisque la multiplication par la matrice $U(n + 1; k; l; \lambda)$ réalise, par la proposition 4.83, la substitution $L_k \to L_k + \lambda L_l$, la matrice

$$B^{(3)} = \prod_{k=2}^{n+1} U(n + 1; k, 1, -B^{(1)}_{k,1})B^{(1)} \tag{4.151}$$

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 4.77 et 4.78 nous obtenons une matrice $U'(n + 1; k, l, \lambda)$ ayant la propriété que la matrice

$$B^{(4)} = \prod_{k=2}^{n+1} U'(n + 1; k, 1, -B^{(3)}_{1,k})B^{(3)} \tag{4.152}$$

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

$$B^{(4)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix} \tag{4.153}$$

où A' est une matrice de taille n.

Voyons quelques propriétés de A'. Nous savons que

$$B^{(4)} = \prod_i G_i A \tag{4.154}$$

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

$$\det(B^{(4)}) = \prod_i \det(G_i)\det(A), \tag{4.155}$$

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

$$G'_1 \dots G'_M A' = \delta \tag{4.156}$$

où les G'_i sont de taille n, ainsi que le δ. En remarquant que

$$S(n+1;k,l) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & S(n;k-1,l-1) & \\ 0 & & & \end{pmatrix}, \tag{4.157}$$

et pareillement pour les matrices T et U, nous voyons qu'en prenant

$$G_i = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & G'_i & \\ 0 & & & \end{pmatrix}, \tag{4.158}$$

nous avons

$$\prod_{i=1}^{M} G_i B^{(3)} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \prod_{i=1}^{M} G'_i A' & \\ 0 & & & \end{pmatrix} = \delta_{n+1} \tag{4.159}$$

où nous avons mis un indice sur le dernier δ pour être plus explicite. □

4.3.7 Matrices inversibles

Proposition-Définition 4.88.
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

$$AB_1 = B_1 A = \delta \tag{4.160}$$

et

$$AB_2 = B_2 A = \delta, \tag{4.161}$$

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 1.158. 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 $B_1 = B_2$. □

Lemme 4.89 ([129]).
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 4.70. Puisque $AB = \delta$, par la proposition 4.72, nous avons $f_A \circ f_B = f_{AB} = \mathrm{Id}$. La proposition 4.54 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 4.43. La proposition 4.53 dit alors que $\{f_B(e_i)\}$ est une base. Nous décomposons $f_B(e_k) - f_C(e_k)$ dans cette base :

$$f_B(e_k) - f_C(e_k) = \sum_j \alpha_j f_B(e_j) \tag{4.162}$$

où les α_j dépendent à priori de k. Puisque $f_A \circ (f_B - f_C) = 0$, nous avons

$$0 = f_A\big(f_B(e_k) - f_C(e_k)\big) = \sum_j (f_A \circ f_B)(e_j) = \sum_j \alpha_j e_j. \tag{4.163}$$

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 4.70(4). □

Proposition 4.90 ([129]).
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

$$AC = ABA - A + AB = AB = \delta. \tag{4.164}$$

Donc C est également un inverse à droite de A. Le lemme 4.89 donne alors $C = B$. □

Corolaire 4.91.
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 4.90 et de la définition 4.88. □

Lemme 4.92.
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

$$AB(AB)^{-1} = \delta. \tag{4.165}$$

Donc la matrice $B(AB)^{-1}$ est un inverse de A. Contradiction. □

Proposition 4.93.
Une matrice est inversible si et seulement si son application linéaire associée est inversible. Dans ce cas, nous avons

$$f_A^{-1} = f_{A^{-1}}. \tag{4.166}$$

Démonstration. Dans le sens direct, si A est inversible nous avons $AA^{-1} = \delta$. Donc

$$f_A \circ f_{A^{-1}} = f_{AA^{-1}} = f_\delta = \mathrm{Id} \tag{4.167}$$

où nous avons utilisé la proposition 4.72 pour la composition et la proposition 4.73 pour l'identité. L'égalité (4.167) 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

$$f_\delta = \mathrm{Id} = f_A \circ f_B = f_{AB}. \tag{4.168}$$

Le fait que l'application $\psi\colon A \to f_A$ soit une bijection[36] implique que $AB = \delta$, c'est-à-dire que A est inversible et que $B = A^{-1}$. □

Lemme 4.94 ([1]).
Soient une matrice inversible $A \in \mathbb{M}(n, \mathbb{R})$ et $r < n$. Il existe une permutation $\sigma \in S_n$ telle que la matrice $a \in \mathbb{M}(r, \mathbb{R})$ donnée par

$$a_{i,j} = A_{i,\sigma(j)} \tag{4.169}$$

soit inversible.

36. Proposition 4.70(4).

4.3.8 Inversibilité et déterminant

Proposition 4.95.
Une matrice au déterminant non nul est inversible.

Démonstration. Si A est une matrice telle que $\det(A) \neq 0$, alors la proposition 4.87 nous donne des matrices $G_1, \dots, G_N$ telles que

$$G_1 \dots G_N A = \delta. \tag{4.170}$$

Donc la matrice $G_1 \dots G_N$ est un inverse de A par le corolaire 4.91. □

Proposition 4.96.
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

$$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)}. \tag{4.171}$$

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

$$(AB)_{k,k} = \sum_l A_{k,l} B_{l,k}. \tag{4.172}$$

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. □

4.3.9 Quelques ensembles de matrices particuliers

Certains ensembles de matrices ont une importance particulière, que nous développerons plus tard.

Définition 4.97 (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,* $\mathrm{GL}(n, \mathbb{A}) = U(\mathbb{M}(n, \mathbb{A}))$.

Définition 4.98 (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.*

4.3.10 Déterminant et combinaisons de lignes et colonnes

Proposition 4.99.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ telles que $\det(A) \neq 0$ *et* $\det(B) \neq 0$. *Alors*

$$\det(AB) = \det(A)\det(B). \tag{4.173}$$

Démonstration. La proposition 4.87 nous donne des matrices de permutations de lignes et de colonnes $G_1, \dots, G_N$ et $G'_1, \dots, G'_N$ telles que[37]

$$G_1 \dots G_N A = \delta \tag{4.174a}$$

$$G'_1 \dots G'_N B = \delta. \tag{4.174b}$$

37. 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.

Nous avons

$$(G'_1 \dots G'_N) \underbrace{(G_1 \dots G_N)A}_{=\delta} B = \delta. \tag{4.175}$$

En prenant le déterminant des deux côtés et en tenant compte de (4.145),

$$1 = \det(\delta) = \det\left(G'_1 \dots G'_N G_1 \dots G_N AB\right) = \det(G'_1 \dots G'_N)\det(G_1 \dots G_N)\det(AB). \tag{4.176}$$

Mais en même temps, les équations 4.174 donnent

$$\det(G_1 \dots G_N) = \det(A)^{-1} \tag{4.177a}$$
$$\det(G'_1 \dots G'_N) = \det(B)^{-1}. \tag{4.177b}$$

Cela pour dire que

$$1 = \det(A)^{-1}\det(B)^{-1}\det(AB), \tag{4.178}$$

et donc ce qu'il nous fallait. □

Proposition 4.100.
Soient des matrices $A, B \in \mathbb{M}(n, \mathbb{K})$ telles que $\det(A) = 0$ et $\det(B) \neq 0$. Alors

$$\det(AB) = \det(BA) = \det(A)\det(B) = 0. \tag{4.179}$$

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

$$0 = \det(A) = \det(G_1 \dots G_N BA) = \det(G_1 \dots G_N)\det(BA). \tag{4.180}$$

Donc $\det(BA) = 0$. □

4.3.11 Transvections

Nous nommons $E_{i,j}$ la matrice remplie de zéros sauf à la case i, j qui vaut 1. Autrement dit

$$(E_{i,j})_{k,l} = \delta_{i,k}\delta_{j,l}. \tag{4.181}$$

Définition 4.101.
*Une **matrice de transvection** est une matrice de la forme*

$$T_{i,j}(\lambda) = \mathrm{Id} + \lambda E_{i,j} \tag{4.182}$$

avec $i \neq j$.

*Une **matrice de dilatation** est une matrice de la forme*

$$D_i(\lambda) = \mathrm{Id} + (\lambda - 1)E_{i,i}. \tag{4.183}$$

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*

$$(P_\sigma)_{i,j} = \delta_{i,\sigma(j)}. \tag{4.184}$$

Lemme 4.102.
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

$$L_i \to L_i + \lambda L_j. \tag{4.185}$$

La matrice $AT_{i,j}(\lambda)$ est la substitution

$$C_j \to C_j + \lambda C_i. \tag{4.186}$$

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 $E_{i,j}A$:

$$(E_{i,j}A)_{k,l} = \sum_m (E_{i,j})_{k,m}A_{m,l} \tag{4.187a}$$
$$= \sum_m \delta_{i,k}\delta_{j,m}A_{m,l} \tag{4.187b}$$
$$= \delta_{i,k}A_{j,l}. \tag{4.187c}$$

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

$$A + \lambda E_{i,j}A \tag{4.188}$$

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

$$(AE_{i,j}) = A_{k,i}\delta_{j,l}. \tag{4.189}$$

Pour les matrices de permutation, nous avons

$$(AP_\sigma)_{k,l} = A_{k,\sigma(l)} \tag{4.190}$$

et

$$(P_\sigma A)_{k,l} = \sum_m \delta_{k,\sigma(m)}A_{m,l} = \sum_m \delta_{\sigma^{-1}(k),m}A_{m,l} = A_{\sigma^{-1}(k),l}. \tag{4.191}$$

□

4.3.12 Mineur, rang

Pour la définition du rang d'une matrice, nous en donnons une qui est clairement inspirée de l'application linéaire associée.

Définition 4.103 ([129]).
*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 4.104 ([130]).
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 (4.80).

Lemme 4.105.
Soit $\mathbb{K}$ un corps commutatif[38]*. 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*

$$f_A(x_i) \neq 0 \tag{4.192}$$

pour $i \leqslant r$ et

$$f_A(x_i) = 0 \tag{4.193}$$

pour $i > r$.

38. Comme toujours.

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

$$v_i = f_A(e_i). \tag{4.194}$$

Les vecteurs v_i engendrent V, donc nous pouvons en extraire une base par le théorème 4.17(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 [39], mais les vecteurs ainsi complétant la base ne sont pas garantis de s'annuler par f_A. Voir l'exemple 4.106.

L'idée est d'utiliser le noyau de f_A qui est un sous-espace vectoriel par la proposition 4.38. Soit une base [40] $\{z_k\}$ 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 4.46 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. □

Exemple 4.106.
Soit la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}. \tag{4.195}$$

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

$$f_A(e_1) = \begin{pmatrix} 1 \\ 2 \end{pmatrix}. \tag{4.196}$$

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

$$f_A(v) = f_A(e_2) = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq 0. \tag{4.197}$$

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 $\{e_1, e_1 - e_2\}$. △

Proposition 4.107.
Le rang d'une application linéaire [41] *est égal au rang de sa matrice* [42] *dans n'importe quelle base.*

4.3.13 Matrices équivalentes et semblables

Définition 4.108.
Deux relations d'équivalence entre les matrices.

(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 $A = PBP^{-1}$.*

39. Théorème 4.13(2).
40. Cette base contient $n - r$ éléments, mais ce n'est pas très important pour la suite.
41. Définition 4.45.
42. Définition 4.103.

Lemme 4.109.
Une matrice de rang[43] r *dans* $\mathbb{M}(n,\mathbb{K})$ *est équivalente à la matrice par blocs*

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{4.198}$$

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 4.105.

Nous considérons la matrice inversible P telle que $Pe_i = f_i$; ses colonnes sont donc précisément les f_i, si bien que

$$APe_i = Af_i = \begin{cases} 0 & \text{si } i > r \\ \neq 0 & \text{sinon.} \end{cases} \tag{4.199}$$

La matrice AP se présente donc sous la forme

$$AP = \begin{pmatrix} M & 0 \\ * & 0 \end{pmatrix} \tag{4.200}$$

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

$$QAPe_i = \begin{cases} e_i & \text{si } i < r \\ 0 & \text{sinon.} \end{cases}. \tag{4.201}$$

Cela signifie que QAP est la matrice J_r. □

Corolaire 4.110 (Équivalence et rang)**.**
Deux matrices sont équivalentes[44] *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 4.109, 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[45] : $A = PBQ^{-1}$ avec P et Q inversibles. Alors

$$\begin{aligned} \mathrm{Image}(PBQ^{-1}) &= \{PBQ^{-1}v \text{ tel que } v \in \mathbb{K}^n\} && \text{(4.202a)} \\ &= PB\underbrace{\{Q^{-1}v \text{ tel que } v \in \mathbb{K}^n\}}_{=\mathbb{K}^n} && \text{(4.202b)} \\ &= P\big(B(\mathbb{K}^n)\big). && \text{(4.202c)} \end{aligned}$$

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

$$\dim\Big(\mathrm{Image}(PBQ^{-1})\Big) = \dim\big(B(\mathbb{K}^n)\big) = \mathrm{rk}(B). \tag{4.203}$$

Le membre de gauche de cela n'est autre que $\mathrm{rk}(A) = \dim\big(\mathrm{Image}(PBQ^{-1})\big)$. □

43. Définition 4.103.
44. Définition 4.108(1).
45. Définition 4.108.

4.3.14 Algorithme des facteurs invariants

Proposition 4.111 (Algorithme des facteurs invariants[102]).
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

$$U=P\begin{pmatrix}d_1&&&\\&\ddots&&0\\&&d_s&\\&0&&0\end{pmatrix}Q \tag{4.204}$$

avec $d_i\mid d_{i+1}$ pour tout i.

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

$$\begin{aligned}C_1&\leftrightarrow C_{j_0}\\L_1&\leftrightarrow L_{i_0}\end{aligned} \tag{4.205}$$

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

$$u_{i,1}=qu_{1,1}+r_i, \tag{4.206}$$

et nous faisons

$$L_i\to L_i-qL_1, \tag{4.207}$$

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 [46]. 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

$$C_1=\begin{pmatrix}u_{1,1}\\0\\\vdots\\0\end{pmatrix}, \tag{4.208}$$

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 [47]

$$U=\begin{pmatrix}u_{1,1}&0&\dots&0\\0&&&\\\vdots&&A&\\0&&&\end{pmatrix} \tag{4.209}$$

46. Si il est zéro, nous passons à la ligne suivante

47. Nous nommons toujours par la même lettre U la matrice originale et la matrice modifiée, comme il est d'usage en informatique.

Si l'élément $u_{1,1}$ ne divise pas un des éléments de A, disons $a_{i,j}$, alors nous opérons

$$C_1 \to C_1 - C_j. \tag{4.210}$$

Cela nous détruit un peu la première colonne, mais ne change pas $u_{1,1}$. Nous avons maintenant

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ * & & & \\ u_{i,j} & & A & \\ * & & & \\ 0 & & & \end{pmatrix} \tag{4.211}$$

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

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}, \tag{4.212}$$

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 (4.212) 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

$$U = \begin{pmatrix} u_{1,1} & & & 0 \\ & u_{2,2} & & \\ & 0 & & B \end{pmatrix}. \tag{4.213}$$

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 4.102). □

4.4 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

$$f_\alpha = \sum_i Q_{i,\alpha} e_i. \tag{4.214}$$

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.

4.4.1 Changement de base : vecteurs de base

Lemme 4.112.
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

$$e_i = \sum_\alpha Q^{-1}_{\alpha,i} f_\alpha. \tag{4.215}$$

Démonstration. Nous multiplions l'égalité $f_\alpha = \sum_i Q_{i,\alpha} e_i$ par le nombre[48] $Q^{-1}_{\alpha,j} \in \mathbb{K}$ et nous sommons sur α :

$$\sum_\alpha Q^{-1}_{\alpha,j} f_\alpha = \sum_{i\alpha} (A_{i,\alpha} Q^{-1}_{\alpha,j}) e_i = e_j. \tag{4.216}$$

□

4.4.2 Changement de base : coordonnées

Proposition 4.113.
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

(1) $y_\alpha = \sum_i Q^{-1}_{\alpha,i} x_i$

(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 :

$$x = \sum_i x_i e_i = \sum_\alpha y_\alpha f_\alpha. \tag{4.217}$$

En remplaçant e_i par sa valeur (4.215) nous avons l'égalité

$$\sum_{i\alpha} x_i Q^{-1}_{\alpha,i} f_\alpha = \sum_\alpha y_\alpha f_\alpha. \tag{4.218}$$

Puisque les f_α sont linéairement indépendants, l'égalité des sommes donne l'égalité de chacun des termes :

$$y_\alpha = \sum_i x_i Q^{-1}_{\alpha,i}. \tag{4.219}$$

En identifiant $x \in E$ au vecteur dans $\mathbb{K}^n$ de ses coordonnées dans la base $\{e_i\}$ nous pouvons écrire

$$y_\alpha = (Q^{-1} x)_\alpha, \tag{4.220}$$

Le point (1) est prouvé.

En ce qui concerne le point (2), nous repartons encore de (4.217), mais nous y substituons la définition des f_α :

$$\sum_i x_i e_i = \sum_{\alpha i} y_\alpha Q_{i,\alpha} e_i. \tag{4.221}$$

Vous voulez des détails ? Allez, une étape de plus que le strict nécessaire : nous écrivons

$$\sum_i \big(x_i - \sum_\alpha y_\alpha Q_{i,\alpha}\big) e_i = 0. \tag{4.222}$$

Par linéaire indépendance des e_i, nous avons annulation de tous les coefficients, c'est-à-dire

$$x_i = \sum_\alpha Q_{i,\alpha} y_\alpha, \tag{4.223}$$

comme annoncé. □

48. 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.

4.114.
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.

4.115.
Les formules de changement de coordonnées de la proposition 4.113 s'écrivent souvent de la façon suivante :

(1) $y_\alpha = (Q^{-1}x)_\alpha$
(2) $y = Q^{-1}x$.
(3) $x_i = (Qy)_i$
(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 4.70.

4.4.3 Changement de base : matrice d'une application linéaire

Proposition 4.116.
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

$$f_\alpha = \sum_i Q_{i,\alpha} e_i, \tag{4.224}$$

alors les matrices A et B sont liées par

$$B = Q^{-1}AQ. \tag{4.225}$$

Démonstration. L'hypothèse sur le fait que A et B sont les matrices de t signifie que pour tout $x \in E$,

$$t(x) = \sum_{ij} A_{j,i}x_i e_j = \sum_{\alpha\beta} B_{\alpha,\beta} y_\beta f_\alpha. \tag{4.226}$$

En remplaçant e_j par son expression (4.215) en termes des f_α et x_i par son expression $x_i = (Qy)_i$ (proposition 4.113), nous avons

$$\begin{aligned}(By)_\alpha &= \sum_{ij\alpha} A_{j,i}(Qy)_i Q^{-1}_{\alpha,j} f_\alpha && \text{(4.227a)}\\ &= \sum_{i\alpha} (Q^{-1}A)_{\alpha,i}(Qy)_i f_\alpha && \text{(4.227b)}\\ &= \sum_\alpha (Q^{-1}AQy)_\alpha f_\alpha. && \text{(4.227c)}\end{aligned}$$

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

$$B = Q^{-1}AQ. \tag{4.228}$$

□

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.

4.5 Espaces de polynômes

Attention : les polynômes en-soi, font l'objet de la définition 1.352.
Pour chaque $k > 0$ donné, nous définissons

$$\mathcal{P}^k_{\mathbb{R}} = \{p : \mathbb{R} \to \mathbb{R} \,|\, p : x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k,\ a_i \in \mathbb{R},\ \forall i = 0, \ldots, k\}. \tag{4.229}$$

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 $\mathcal{P}^k_{\mathbb{R}}$ est donc un espace vectoriel muni des opérations héritées de $\mathcal{P}_{\mathbb{R}}$.

La base canonique de l'espace $\mathcal{P}^k_{\mathbb{R}}$ est donnée par les monômes $\mathcal{B} = \{x \mapsto x^j \,|\, j = 0, \ldots, k\}$. Le fait que cela soit une base est vraiment facile à démontrer, et est un exercice très utile si vous ne l'avez pas encore vu dans un cours précédent.

Nous allons maintenant étudier trois applications linéaires de $\mathcal{P}^k_{\mathbb{R}}$ 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

$$\phi(x^j) = e_{j+1}, \qquad \forall j \in \{0, \ldots, k\}.$$

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 4.117.
Soit $k = 5$ on a

$$\phi(-8 - 7x - 4x^2 + 4x^3 + 2x^5) = \begin{pmatrix} -8 \\ -7 \\ -4 \\ 4 \\ 0 \\ 2 \end{pmatrix}. \tag{4.230}$$

△

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

$$d(x^0) = d(1) = 0, \qquad d(x^j) = j x^{j-1}, \quad \forall j \in \{1, \ldots, k\}.$$

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 4.118.
Soit $k = 3$ on a

$$d(-8 - 12x + 4x^3) = -12(1) + 4(3x^2) = -12 + 12x^2. \tag{4.231}$$

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

$$I(x^j) = \frac{x^{j+1}}{j+1}. \tag{4.232}$$

Bien entendu, la raison d'être et la motivation de cette définition apparaîtront lorsque nous développerons une théorie générale de l'intégration.

Exemple 4.119.
Soit $k = 4$ on a

$$I(6 + 2x + x^2 + x^4) = 6x + x^2 + \frac{x^3}{3} + \frac{x^5}{5}. \tag{4.233}$$

△

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 11.3.2, nous verrons que toutes les normes ne sont pas équivalentes sur l'espace des polynômes.

4.6 Projection et orthogonalité

Proposition 4.120.
Si nous écrivons $\texttt{proj}_Y$ *l'opération de projection sur la droite qui sous-tend* Y*, alors nous avons*

$$\| \texttt{proj}_Y X\| = \frac{X \cdot Y}{\|Y\|}. \tag{4.234}$$

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

$$X = \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}, \quad Y = \begin{pmatrix} l \\ 0 \\ 0 \end{pmatrix} \tag{4.235}$$

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 $\| \texttt{proj}_Y X\| = x$. Par conséquent,

$$\| \texttt{proj}_Y X\| = \frac{X \cdot Y}{l} = \frac{X \cdot Y}{\|Y\|}. \tag{4.236}$$

□

Corolaire 4.121.
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 4.120. □

4.7 Dualité

Proposition 4.122.
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.

Définition 4.123.
Soit E un espace vectoriel sur $\mathbb{K}$.

*Une **forme linéaire** sur E est une application linéaire de E sur son corps de base $\mathbb{K}$.*

*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 11.74.

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 11.62, la remarque 11.65 et la définition 25.1.

Lemme-Définition 4.124.
Si E est un espace vectoriel et si $\{b_i\}$ est une base de E, alors nous définissons

$$\begin{aligned} b_i^* \colon E &\to \mathbb{K} \\ b_j &\mapsto \delta_{ij}, \end{aligned} \tag{4.237}$$

*et sa prolongation par linéarité. Ces éléments du dual E^* forment une base appelée **base duale**.*

En particulier nous avons

$$\dim(E) = \dim(E^*). \tag{4.238}$$

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 $\{e_i\}$.

Lemme 4.125 (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

$$\beta_i = \sum_j A_{ij}^{-1} \alpha_j. \tag{4.239}$$

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 :

$$\delta_{ik} = \beta_i(Ae_k) = \sum_j B_{ij}\alpha_j(Ae_k) = \sum_{lj} B_{ij}A_{lk} \underbrace{\alpha_j(e_l)}_{=\delta_{jl}} = \sum_l B_{il}A_{lk} = (BA)_{ik}. \tag{4.240}$$

Nous avons donc $\delta_{ik} = (BA)_{ik}$, c'est-à-dire $BA = \mathbb{1}$ ou encore $B = A^{-1}$. □

Lemme 4.126 ([131])**.**
Soit un espace vectoriel E de dimension finie.

(1) Si α est une forme linéaire non nulle sur E, alors il existe $x \in E$ tel que $\alpha(x) = 1$.

(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.

(i) **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.

(ii) **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

$$\begin{aligned} \alpha\colon E &\to \mathbb{K} \\ y &\mapsto y_k/x_k \end{aligned} \tag{4.241}$$

fait l'affaire.

□

Lemme 4.127.
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

$$\begin{aligned} \Phi\colon E &\to \mathbb{K}^n \\ x &\mapsto \big(\alpha_1(x), \dots, \alpha_n(x)\big) \end{aligned} \tag{4.242}$$

est un isomorphisme d'espaces vectoriels.

Démonstration. En deux parties.

(i) **Φ est injective** Soit $z \in \ker(\Phi)$. Nous avons $\alpha_i(z) = 0$ pour tout i. Si $z \neq 0$, alors le lemme 4.126 dit qu'il existe $\beta \in E^*$ tel que $\beta(z) \neq 0$.
Décomposons un tel β dans la base de $\{\alpha_i\}$:

$$\beta = \sum_{i=1}^{n} \beta_i \alpha_i. \tag{4.243}$$

Alors nous avons

$$0 \neq \beta(z) = \sum_{i=1}^{n} \beta_i \underbrace{\alpha_i(z)}_{=0} = 0. \tag{4.244}$$

Contradiction. Donc $\ker(\Phi) = \{0\}$ et Φ est injective.

(ii) **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 4.48.

□

Proposition-Définition 4.128 ([131])**.**
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 $\mathcal{F}$.

(i) **Existence** Le lemme 4.127 nous indique que l'application

$$\begin{aligned} \Phi\colon E &\to \mathbb{K}^n \\ x &\mapsto \big(\alpha_1(x), \dots, \alpha_n(x)\big) \end{aligned} \tag{4.245}$$

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 :

$$\alpha_i(e_j) = \alpha_i\big(\Phi^{-1}(\epsilon_j)\big) \tag{4.246a}$$
$$= \Phi\big(\Phi^{-1}(\epsilon_j)\big)_i \tag{4.246b}$$
$$= (\epsilon_i)_j \tag{4.246c}$$
$$= \delta_{i,j} \tag{4.246d}$$

Justifications :

— Pour 4.246b, nous remarquons que $\alpha_i(x) = \Phi(x)_i$.

— Pour 4.246d, nous utilisons le fait que les ϵ_j forment la base canonique de $\mathbb{K}^n$.

(ii) **Unicité** Soit une base préduale (e_i) de (α_i). Nous avons, par définition, que $\alpha_i(e_j) = \delta_{i,j}$. Donc

$$\big(\alpha_1(e_j), \dots, \alpha_n(e_j)\big) = \epsilon_j. \tag{4.247}$$

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.

□

4.7.1 Orthogonal

Définition 4.129.
*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*

$$F^\perp = \{\alpha \in E^* \text{ tel que } \forall x \in F, \alpha(x) = 0\}. \tag{4.248}$$

Cette définition d'orthogonal via le dual n'est pas du pur snobisme. En effet, la définition « usuelle » qui ne parle pas de dual,

$$F^\perp = \{y \in E \text{ tel que } \forall x \in F, y \cdot x = 0\}, \tag{4.249}$$

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 4.129, au contraire, est intrinsèque : elle ne dépend que de la structure d'espace vectoriel.

Si $B \subset E^*$, on note B^o son orthogonal :

$$B^o = \{x \in E \text{ tel que } \omega(x) = 0, \forall \omega \in B\}. \tag{4.250}$$

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.

Proposition 4.130.
Soient un espace vectoriel E et F, un sous-espace vectoriel de E. Nous avons

$$\dim F + \dim F^\perp = \dim E. \tag{4.251}$$

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 4.13. 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 9.179 donnera une version plus terre à terre de la proposition 4.130 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.

4.8 Représentation de groupe

Définition 4.131 (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 $\rho: G \to \mathrm{GL}(E)$ vérifiant*

$$\rho(g) \circ \rho(h) = \rho(gh). \tag{4.252}$$

pour tout $g, h \in G$.

Définition 4.132.
Une représentation[49] *$\rho: G \to \mathrm{GL}(E)$ est **fidèle** si elle est injective*
*La dimension de E est le **degré** de la représentation (E, ρ).*

Le fait que la représentation $\rho: G \to \mathrm{GL}(E)$ soit fidèle ne dit pas que chacun des $\rho(g)$ est injectif.

Proposition 4.133.
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

$$\begin{aligned} \rho: G &\to \mathrm{GL}(\mathbb{K}^n) \\ A &\mapsto f_A \end{aligned} \tag{4.253}$$

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 4.67, dont nous connaissons beaucoup de propriétés. La proposition 4.73 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. □

4.9 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 $V \times W$.

Proposition-Définition 4.134 ([132, 133])**.**
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.*

Définition 4.135 (Sous-espaces en somme directe[134])**.**
*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) $u_i \in F_i$ *pout 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 7.161 qui donne des conditions de compatibilité entre les topologies.

49. Définition 4.131.

Lemme 4.136.
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

$$\begin{aligned} \psi\colon F_1 \times F_2 &\to E \\ (x, y) &\mapsto x + y \end{aligned} \tag{4.254}$$

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 $u = u_1 + u_2 = \psi(u_1, u_2)$. □

Lemme 4.137 ([1, 134])**.**
Soient un espace vectoriel E ainsi que des sous-espaces vectoriels F_i. Nous avons équivalence entre les assertions suivantes.

(1) Les F_i sont en somme directe[50]*.*

(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.

(3) Chaque espace F_k est en somme directe avec la somme des précédents, c'est-à-dire que pour tout k,

$$\left(\sum_{i=1}^{k-1} F_i\right) \cap F_k = \{0\}. \tag{4.255}$$

(4) Pour tout k,

$$F_k \cap \left(\sum_{i\neq k} F_i\right) = \{0\}. \tag{4.256}$$

Proposition 4.138 ([135])**.**
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 $E = F_1 \oplus F_2$.

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

$$\sum_i a_i e_i + \sum_\alpha b_\alpha f_\alpha = 0. \tag{4.257}$$

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

$$\sum_i a_i e_i = 0 \tag{4.258}$$

et

$$\sum_\alpha b_\alpha f_\alpha = 0. \tag{4.259}$$

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 4.18(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 4.18(2). □

50. Définition 4.135.

4.9.1 Structure réelle

Proposition-Définition 4.139 ([136, 133, 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.*

Démonstration. La proposition 4.23 nous permet de considérer une base $\{e_i\}_{i\in I}$ de E. Alors, nous définissons

$$\sigma\big(\sum_{i\in I}\lambda_i e_i\big) = \sum_{i\in I}\bar{\lambda}_i e_i. \tag{4.260}$$

Notez que la somme est toujours finie. □

Proposition 4.140.
Soit un espace vectoriel E sur $\mathbb{C}$ et une structure réelle[51] *σ sur E. Nous posons*

$$E_{\mathbb{R}} = \{v \in E \text{ tel que } \sigma(v) = v\}. \tag{4.261}$$

Alors

(1) La partie $E_{\mathbb{R}}$ est un espace vectoriel réel.

(2) Nous avons la décomposition en somme directe[52]

$$E = E_{\mathbb{R}} \oplus iE_{\mathbb{R}}. \tag{4.262}$$

Démonstration. En plusieurs parties.

(i) **Espace vectoriel réel** Si $v, w \in E_{\mathbb{R}}$, alors

$$\sigma(v + w) = \sigma(v) + \sigma(w) = v + w, \tag{4.263}$$

et si $\lambda \in \mathbb{R}$,

$$\sigma(\lambda x) = \lambda\sigma(x) = \lambda x. \tag{4.264}$$

Donc $E_{\mathbb{R}}$ est un espace vectoriel réel.

(ii) **Première somme directe** Nous définissons

$$E^+ = \{v \in E \text{ tel que } \sigma(v) = v\}, \tag{4.265a}$$
$$E^- = \{v \in E \text{ tel que } \sigma(v) = -v\} \tag{4.265b}$$

Nous prouvons que

$$\begin{aligned}\psi\colon E^+ \times E^- &\to E\\ (a, b) &\mapsto a + b\end{aligned} \tag{4.266}$$

est un isomorphisme d'espaces vectoriels.

Puisque ψ est linéaire, il suffit de prouver qu'elle est bijective.

(i) **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

$$v = v_+ + v_-, \quad v_+ \in E^+, \quad v_- \in E^-, \tag{4.267}$$

et donc $v = \psi(v_+, v_-)$.

(ii) **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 $a - \alpha = \beta - b = 0$.

51. Définition 4.139.
52. Définition 4.134.

Nous avons donc la somme directe $E = E^+ \oplus E^-$.

(iii) **Conclusion** Par définition, $E^+ = E_{\mathbb{R}}$. Il nous reste à voir que $E^- = iE^+$. Nous prouvons les inclusions dans les deux sens.

(i) $E^- \subset iE^+$ Soit $v \in E^-$. Nous avons $iv \in E^+$; en effet

$$\sigma(iv) = \bar{i}\sigma(v) = -i\sigma(v) = iv. \tag{4.268}$$

Donc $iv \in E^+$ pour $v \in E^-$.

(ii) $iE^+ \subset E^-$ Soit $v \in E^+$, et voyons que $iv \in E^-$. En effet,

$$\sigma(iv) = -i\sigma(v) = -iv. \tag{4.269}$$

□

4.141.
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 4.142.
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,

$$F_{\mathbb{R}} = \{v \in F \text{ tel que } \sigma(v) = v\}. \tag{4.270}$$

(i) $F_{\mathbb{R}} \subset F$ C'est dans la définition de $F_{\mathbb{R}}$ (sous-ensemble de F).

(ii) $F_{\mathbb{R}} \subset E_{\mathbb{R}}$ 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 5

Classification de certains groupes

5.1 Théorèmes de Sylow

Lemme 5.1.
Soient H et K des sous-groupes finis de G. Alors

$$\text{Card}(HK) = \frac{|H| \cdot |K|}{|H \cap K|}. \tag{5.1}$$

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 $hkh^{-1} \in K$, $\forall (h,k) \in H \times K$.

Théorème 5.2 (Théorème de Cauchy[137])**.**
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.

Lemme 5.3 (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

$$\begin{aligned} \varphi\colon G &\to S_n \\ \varphi(x)g &\mapsto xg \end{aligned} \tag{5.2}$$

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 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Lemme 5.4.
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 $\varphi(\sigma)e_i = e_{\sigma(i)}$. □

Remarque 5.5.
En mettant bout à bout les lemmes 5.3 et 5.4, nous trouvons que si p est un diviseur premier de $|G|$, alors G peut être vu comme un sous-groupe de $\text{GL}(n, \mathbb{F}_p)$.

Définition 5.6.
*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 5.7.
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 $|G : S| = |G|/|S|$.

Proposition 5.8.
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

$$\begin{aligned}\mathrm{Card}\left(\mathrm{GL}(n,\mathbb{F}_p)\right) &= (p^n-1)(p^n-p)\dots(p^n-p^{n-1}) && \text{(5.3a)}\\ &= p\cdot p^2\cdots p^{n-1}(p^n-1)(p^{n-1}-1)\dots(p-1) && \text{(5.3b)}\\ &= p^{\frac{n(n-1)}{2}}m && \text{(5.3c)}\end{aligned}$$

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

$$|T| = p^{\frac{n(n-1)}{2}}, \tag{5.4}$$

et T est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. □

Proposition 5.9.
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 (5.2), 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 2.13 de Lagrange). Le nombre r est alors une puissance de p. □

Lemme 5.10.
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

$$gSg^{-1} \cap H \tag{5.5}$$

soit un p-Sylow de H.

1. Définition 4.45.

Démonstration. Nous considérons l'ensemble G/S sur lequel H agit. Si $a \in G$, le stabilisateur de $[a]$ dans G/S est

$$\begin{aligned} \text{Fix}\big([a]\big) &= \{h \in H \text{ tel que } [ha] = [a]\} && (5.6a)\\ &= \{h \in H \text{ tel que } a^{-1}ha \in S\} && (5.6b)\\ &= aSa^{-1} \cap H. && (5.6c)\end{aligned}$$

Nous cherchons $a \in G$ tel que l'entier

$$\frac{\text{Card}(H)}{\text{Card}\big(aSa^{-1} \cap H\big)} \tag{5.7}$$

soit premier avec p. En effet, dans ce cas le groupe $\text{Fix}([a])$ est un p-Sylow de H parce que $|H : aSa^{-1} \cap H|$ ne divise pas p. La formule des orbites (équation (2.68)) nous dit que

$$\frac{|H|}{|aSa^{-1} \cap H|} = \text{Card}\big(\mathcal{O}_{[a]}\big). \tag{5.8}$$

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

$$p \mid \text{Card}(G/S) = \frac{|G|}{|S|} \tag{5.9}$$

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 (5.7) soit vérifiée. □

Théorème 5.11 (Théorème de Sylow)**.**
Soit G un groupe fini et p, un diviseur premier de $|G|$. Alors

(1) G possède au moins un p-Sylow[2]*.*

(2) Tout p-sous-groupe de G est contenu dans un p-Sylow.

(3) Les p-Sylow de G sont conjugués.

(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 5.5 que G est un sous-groupe de $\text{GL}_n(\mathbb{F}_p)$ et que ce dernier a un p-Sylow par la proposition 5.8. Par conséquent G possède un p-Sylow par le lemme 5.10.

(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 5.10 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,

$$H = aSa^{-1} \cap H \tag{5.10}$$

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

$$E_S = \{T \in E \text{ tel que } s \cdot T = T, \forall s \in S\}. \tag{5.11}$$

2. Définition 5.6.

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

$$|E| \equiv |E_S| \mod p. \tag{5.12}$$

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

$$sTs^{-1} = T \tag{5.13}$$

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

$$g = s_1 t_1 \cdots s_r t_r \tag{5.14}$$

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

$$gtg^{-1} = s_1 t_1 \dots s_r t_r t t_r^{-1} s_r^{-1} \dots t_1^{-1} s_1^{-1} \in T. \tag{5.15}$$

Donc T est un sous-groupe normal de N. Mais S et T sont conjugués dans N (parce que 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,

$$S = aTa^{-1} = T. \tag{5.16}$$

Ceci achève la démonstration des théorèmes de Sylow.

□

Proposition 5.12.
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

$$(gsg^{-1})^q = gs^q g^{-1} = e. \tag{5.17}$$

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. □

Lemme 5.13 ([138])**.**
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. □

Proposition 5.14 ([138])**.**
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 $H\backslash\{e\}$ 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 $H\backslash\{e\}$ où H parcourt les sous-groupes d'ordre p dans G. Chacun de ces ensembles possède $p-1$ éléments et le lemme 5.13 nous assure qu'ils sont disjoints. Par conséquent nous avons $n(p-1)$ éléments d'ordre p dans G. □

Corolaire 5.15.
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 5.14 nous dit alors que le nombre d'éléments d'ordre p dans G est $p-1$. Donc tout élément est générateur. □

5.2 Groupe monogène

Groupe monogène : définition 1.318 ; groupe cyclique : définition 1.319.

Le théorème suivant donne quelques informations à propos des groupes monogènes. Il impliquera dans le corolaire 5.41 qu'un groupe monogène d'ordre n possède $\varphi(n)$ générateurs où φ est la fonction indicatrice d'Euler définie en 5.29.

Théorème 5.16.
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

$$\begin{aligned} f\colon \mathbb{Z} &\to G \\ p &\mapsto a^p. \end{aligned} \tag{5.18}$$

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 2.6) nous indique que

$$\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} = \text{Image } f = G. \tag{5.19}$$

□

Le lemme suivant donne une démonstration alternative, avec une construction plus explicite de l'isomorphisme.

Lemme 5.17 ([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

$$\phi\colon G \to (\mathbb{Z}/n\mathbb{Z}, +) \tag{5.20}$$

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

$$\phi\colon G \to (\mathbb{Z}, +) \tag{5.21}$$

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.

3. Définition 1.318.

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.

(i) **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 :

$$\phi(g^m) = [m]_n. \tag{5.22}$$

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 $\mathbb{Z}/n\mathbb{Z}$.

(i) **Morphisme** Pour l'identité, si $x = e$ alors $m = 0$ et $\phi(e) = [0]_n$. Et si $x = g^k$, $y = g^l$ alors $\phi(xy) = \phi(g^{k+l}) = [k + l]_n = [k]_n + [l]_n = \phi(x) + \phi(y)$.

(ii) **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 $g^k = g^l$.

(iii) **Surjectif** La classe $[k]_n$ est l'image de g^k.

(ii) **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.

□

5.3 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.

Théorème 5.18 ([139]).
Pour chaque $x \in (\mathbb{Z}/n\mathbb{Z})^*$ nous considérons l'application

$$\begin{aligned} \sigma_x\colon \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ y &\mapsto xy. \end{aligned} \tag{5.23}$$

L'application

$$\sigma\colon \big((\mathbb{Z}/n\mathbb{Z})^*,\ \cdot\ \big) \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}, +\right) \tag{5.24}$$

ainsi définie est un isomorphisme de groupes.

L'énoncé de ce théorème s'écrit souvent rapidement par

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*, \tag{5.25}$$

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

$$f([r]) = f(r[1]) = rf([1]) = [r]f([1]). \tag{5.26}$$

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]

$$\begin{aligned}\sigma\colon \operatorname{Aut}((\mathbb{Z}/n\mathbb{Z},+)) &\to \big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big)\\ f &\mapsto f([1])\end{aligned} \tag{5.27}$$

est un isomorphisme.

Nous commençons par la surjectivité. Soit $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. Les élément $[a]$ 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 5.17. 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

$$f\big(g([1])\big) = f\big(g([1])[1]\big) = g([1])f([1]) = \sigma(f)\sigma(g). \tag{5.28a}$$

□

Ce dernier résultat s'étend aux groupes cycliques.

Proposition 5.19.
Si G est un groupe cyclique[5] *d'ordre n, alors*

$$\operatorname{Aut}(G) = \big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big). \tag{5.29}$$

Démonstration. Vu que G est cyclique, le lemme 5.17 nous dit que G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}),+$. Maintenant le théorème 5.18 nous indique que

Les égalités suivantes sont en réalité des isomorphismes de groupes :

$$\operatorname{Aut}(G) = \operatorname{Aut}\Big(\mathbb{Z}/n\mathbb{Z},+\Big) \tag{5.30a}$$

$$= \Big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\Big) \tag{5.30b}$$

Jusitifications.

— Pour (5.30a). Le lemme 5.17 nous dit que G est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$, et le lemme 1.38 dit que des groupes isomorphes ont des groupes d'isomorphismes isomorphes.

— Pour (5.30b). C'est le théorème 5.18.

□

Corolaire 5.20.
Si p divise $q-1$ alors $\operatorname{Aut}(\mathbb{F}_q)$ *possède un unique sous-groupe d'ordre p.*

Démonstration. Si a est un générateur de $\mathbb{F}_q^*$ alors le groupe

$$\operatorname{gr}\Big(a^{\frac{q-1}{p}}\Big) \tag{5.31}$$

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 3.29 nous enseigne que le groupe donné en (5.31) 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. □

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 1.319.

5.4 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 5.21 (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,

$$m = p^\alpha m' \tag{5.32a}$$
$$q = p^\beta q' \tag{5.32b}$$

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. □

Proposition 5.22.
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 $\varphi(x) = x$.

(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 $y \in G\backslash H$, 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 :

$$\begin{aligned} \tilde{\varphi}\colon \mathbb{Z}/b\mathbb{Z} \times H &\to \mathrm{gr}(x) \\ (\bar{k}, h) &\mapsto x^{kl}\varphi(h) \end{aligned} \tag{5.33}$$

où l est encore à déterminer, et

$$\begin{aligned} p\colon \mathbb{Z}/b\mathbb{Z} \times H &\to \mathrm{gr}(y, H) \\ (\bar{k}, h) &\mapsto y^k h. \end{aligned} \tag{5.34}$$

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

$$\begin{array}{ccccc} \ker(p) & \hookrightarrow & \mathbb{Z}/b\mathbb{Z} \times H & \xrightarrow{p} & \mathrm{gr}(y, H) \\ & & \downarrow{\scriptstyle \tilde{\varphi}} & \swarrow{\scriptstyle \hat{\varphi}} & \\ & & \mathrm{gr}(x) & & \end{array} \tag{5.35}$$

que l'on voudra être commutatif. Puisque p est surjective, les théorèmes d'isomorphismes nous disent que

$$\mathrm{gr}(y, H) \simeq \frac{\mathbb{Z}/b\mathbb{Z} \times H}{\ker p}. \tag{5.36}$$

Si $[\bar{k},h]$ est la classe de $(\bar{k},h)$ modulo $\ker(p)$ alors nous voudrions définir $\hat{\varphi}$ par

$$\hat{\varphi}\big([\bar{k},h]\big)=\tilde{\varphi}(\bar{k},h). \tag{5.37}$$

Pour que cela soit bien défini, il faut que si $(\bar{r},z)\in\ker p$, alors,

$$\hat{\varphi}\big([\bar{k}\bar{r},hz]\big)=\hat{\varphi}\big([\bar{k},h]\big), \tag{5.38}$$

c'est-à-dire que $\tilde{\varphi}(\bar{r},z)=e$. Du coup la définition (5.37) n'est bonne que si et seulement si

$$\ker(p)\subset\ker(\tilde{\varphi}). \tag{5.39}$$

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

$$\ker(p)=\{(-m\beta,y^{m\beta})\text{ tel que }m\in\mathbb{Z}\}. \tag{5.40}$$

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

$$\tilde{\varphi}(\beta,y^{-\beta})=x^{\beta l}\varphi(y^{-\beta})=x^{\beta l+\alpha}. \tag{5.41}$$

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,

$$e=\varphi(y^b)=\varphi(y^{-\beta b/\beta})=\varphi(y^{-\beta})^{b/\beta}=x^{b\beta/\alpha}. \tag{5.42}$$

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

$$\begin{aligned}\psi\colon G&\to\operatorname{gr}(x)\oplus\ker(\varphi)\\ g&\mapsto\big(\varphi(g),g\varphi(g)^{-1}\big)\end{aligned} \tag{5.43}$$

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,

$$\varphi\big(g\varphi(g)^{-1}\big)=\varphi(g)\varphi(g)^{-1}=e. \tag{5.44}$$

L'application ψ est un morphisme parce que, en utilisant le fait que G est abélien,

$$\begin{aligned}\psi(g_1g_2)&=\big(\varphi(g_1g_2),g_1g_2\varphi(g_1g_2)^{-1}\big) &\text{(5.45a)}\\ &=\big(\varphi(g_1)\varphi(g_2),g_1\varphi(g_1)^{-1}g_2\varphi(g_2)^{-1}\big) &\text{(5.45b)}\\ &=\psi(g_1)\psi(g_2). &\text{(5.45c)}\end{aligned}$$

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 2.6) appliqué à φ nous avons

$$|G|=|\operatorname{gr}(x)|\cdot|\ker(\varphi)|. \tag{5.46}$$

□

Théorème 5.23.
Si G est un groupe abélien fini non trivial, il exise un unique $r > 0$ et une unique liste de naturesl $(d_1, \dots, d_r)$ 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

$$H_1 = \mathrm{gr}(x_1) = \mathbb{F}_{n_1}. \tag{5.47}$$

D'après la proposition 5.22(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 $(s_1, \dots, s_q)$:

$$G = \mathbb{F}_{d_1} \oplus \dots \oplus \mathbb{F}_{d_r} = \mathbb{F}_{s_1} \oplus \dots \oplus \mathbb{F}_{s_q}. \tag{5.48}$$

L'exposant de G est d_r et s_q. Donc $d_r = s_q$. Les complémentaires étant égaux nous avons

$$\mathbb{F}_{d_1} \oplus \dots \oplus \mathbb{F}_{d_{r-1}} = \mathbb{F}_{s_1} \oplus \dots \oplus \mathbb{F}_{s_{q-1}}. \tag{5.49}$$

En continuant nous trouvons $r = q$ et $d_i = s_i$. □

5.5 Groupes d'ordre pq

Lemme 5.24.
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 5.11(1) le groupe G possède des q-Sylow et par 5.11(4),

$$n_q \in [1]_q. \tag{5.50}$$

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 5.11(3) parce que le conjugué de H est encore un q-Sylow alors que H est l'unique q-Sylow.

Vu que

$$1 < p = |H| < pq = |G|, \tag{5.51}$$

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 2.47.

Théorème 5.25 ([140]).
Soient deux nombres premiers distincts[7] *p et q avec $q > p$.*

6. Pas de sous-groupes normaux non triviaux, 1.170.
7. Le cas $p = q$ sera traité par la proposition 5.28.

(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 $\mathbb{Z}/pq\mathbb{Z}$.*

(2) *Si $p \mid q-1$, alors il n'existe que deux groupes d'ordre pq :*
   — *Le groupe abélien et cyclique $\mathbb{Z}/pq\mathbb{Z}$.*
   — *Le produit semi-direct non abélien*

$$G = \mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z} \tag{5.52}$$

   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.

(i) **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 5.11). 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 2.13) $|H \cap K|$ 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

$$\begin{aligned} \psi\colon H \times K &\to HK \\ (h,k) &\mapsto hk \end{aligned} \tag{5.53}$$

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

$$h^{-1}h' = (k'k^{-1})^{-1} \in H \cap K = \{e\}. \tag{5.54}$$

Par conséquent $|pq| = |H \times K| = |HK|$, et $HK = G$. Le corolaire 2.49 nous indique que

$$G = H \times_\varphi K \tag{5.55}$$

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.

(ii) **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 (5.55) est en réalité un produit direct (φ est triviale) et nous avons

$$G = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/pq\mathbb{Z}. \tag{5.56}$$

(iii) **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 2.6, nous avons

$$|\varphi(\mathbb{Z}/p\mathbb{Z})| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\ker\varphi|}, \tag{5.57}$$

8. Cette affirmation me semble très bizarre. Comment deux nombres premiers distincts pourraient ne pas être premiers entre eux ? ? ?

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 5.20 nous indique que $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ possède un unique sous-groupe d'ordre p que nous notons Γ ; c'est-à-dire que $\Gamma = \text{Image}(\varphi)$. Vu que $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme, Γ est généré par $\varphi(\bar{1})$ qui est alors un élément d'ordre p, comme annoncé.

(iv) **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

$$\begin{aligned} f\colon \mathbb{Z}/q\mathbb{Z} \times_\varphi \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/q\mathbb{Z} \times_{\varphi'} \mathbb{Z}/p\mathbb{Z} \\ (h,k) &\mapsto (h, \alpha(k)) \end{aligned} \tag{5.58}$$

où $\alpha = \varphi'^{-1} \circ \varphi$ est un isomorphisme de groupes. Le calcul est immédiat :

$$\begin{aligned} f(h_1,k_1)f(h_2mk_2) &= \big(h_1,\alpha(k_1)\big)(h_2,\alpha(k_2)) && \text{(5.59a)}\\ &= \big(h_1\varphi'(\alpha(k_1))h_2m\alpha(k_1k_2)\big) && \text{(5.59b)}\\ &= f\big(h_1\varphi(k_1)h_2, k_1k_2\big) && \text{(5.59c)}\\ &= f\big((h_1,k_1),(h_2,k_2)\big). && \text{(5.59d)} \end{aligned}$$

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 $7 = 1 \mod 3$.

Proposition 5.26 ([52]).
Soit G un groupe fini d'ordre pq où p et q sont deux nombres premiers distincts vérifiant

$$\begin{cases} p \neq 1 \mod q & \text{(5.60a)}\\ q \neq 1 \mod p. & \text{(5.60b)} \end{cases}$$

Alors G est cyclique, abélien et

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \tag{5.61}$$

Démonstration. Soient n_p et n_q les nombres de p-Sylow et q-Sylow. Par le théorème de Sylow 5.11, 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

$$\begin{aligned} (xyx^{-1})y^{-1} &\in T && \text{(5.62a)}\\ x(yx^{-1}y^{-1}) &\in S, && \text{(5.62b)} \end{aligned}$$

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

$$|ST| = |S||T| = pq = |G|. \tag{5.63}$$

Par conséquent $G = ST$. En nous rappelant que $S \cap T = \{e\}$ et que S et T sont normaux, le lemme 1.263 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

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \tag{5.64}$$

□

Théorème 5.27 (Théorème de Burnside[88])**.**
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 :

$$\mathcal{Z}_G = \{z \in G \text{ tel que } \sigma_x(z) = z, \forall x \in G\} = \text{Fix}_G(G). \tag{5.65}$$

Nous utilisons l'équation aux classes (2.38) 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. □

Proposition 5.28.
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 5.2 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 5.27, 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 $x \in G \backslash \mathcal{Z}$. Alors le stabilisateur de x pour l'action adjointe contient au moins $\mathcal{Z}$ et x, c'est-à-dire que $|\text{Fix}_G(x)| \geqslant p+1$. Étant donné que $\text{Fix}_G(x)$ 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. □

5.5.1 Fonction indicatrice d'Euler

Définition 5.29.
*La **fonction indicatrice d'Euler** est l'application*

$$\begin{aligned} \varphi\colon \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto \text{Card}\Big(\{m \in \mathbb{N}^* \text{ tel que } 1 \leqslant m \leqslant n, \text{pgcd}(m,n) = 1\}\Big). \end{aligned} \tag{5.66}$$

Note : voir le thème 11 pour des formules concernant l'indicatrice d'Euler.

Lemme 5.30 ([141])**.**
L'élément $[m]_n$ est inversible dans le groupe $\big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big)$ si et seulement si $\text{pgcd}(m,n) = 1$.

Démonstration. Dans les deux sens.

(i) $\Rightarrow$ 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 1.229 conclu que $\text{pgcd}(m,n) = 1$.

(ii) $\Leftarrow$ Si $\text{pgcd}(m,n)=1$, alors le théorème de Bézout 1.229 nous dit qu'il existe $u,v\in\mathbb{Z}$ tels que $um+vn=1$. Cela donne directemen t $um=1-vn\in[1]_n$ et donc $[u]_n$ est un inverse de $[m]_n$ dans le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}$.

□

Lemme 5.31.
Nous avons

$$\varphi(n)=\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right) \tag{5.67}$$

où $A^\times$ est le groupe des inversibles (pour la multiplication) dans l'anneau A.

Démonstration. En utilisant le lemme 5.30,

$$\begin{aligned}\left(\mathbb{Z}/n\mathbb{Z}\right)^\times&=\{[m]_n\text{ tel que }\text{pgcd}(m,n)=1\}&(5.68a)\\&=\{[m]_n\text{ tel que }1\leqslant m\leqslant n,\text{pgcd}(m,n)=1\}&(5.68b)\end{aligned}$$

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 $\{1\leqslant m\leqslant n\text{ tel que }\text{pgcd}(m,n)=1\}$. Donc

$$\varphi(n)=\text{Card}\left(\{[m]_n\text{ tel que }1\leqslant m\leqslant n,\text{pgcd}(m,n)=1\}\right)=\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right). \tag{5.69}$$

□

Lemme 5.32 ([142])**.**
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.

(i) $\Rightarrow$ Nous supposons que $d[r]_n=[0]_n$. Étant donné que $n=dq$ nous avons les implications suivantes :

$$d[r]_n=[0]_n\Rightarrow d\mid dr\Rightarrow dq\mid dr\Rightarrow q\mid r. \tag{5.70}$$

Nous avons donc $r=kq$ pour un certain $k\in\mathbb{Z}$. Par la division euclidienne 1.215, il existe $s,t\in\mathbb{N}$ tels que $k=sd+t$ avec $t<d$. Avec ça, nous avons le calcul

$$[r]_n=k[q]_n=sd[q]_n+t[q]_n=\underbrace{s[dq]_n}_{=[0]_n}+t[q]_n\in G. \tag{5.71}$$

(ii) $\Leftarrow$ Si $[r]_n\in G$, il existe $0\leqslant k\leqslant d-1$ tel que $[r]_n=k[q]_n$. De ce fait,

$$d[r]_n=dk[q]_n=k[dq]_n=[0]_n. \tag{5.72}$$

Et voila.

□

La proposition suivante est un pas important dans l'algorithme de Shor permettant aux ordinateurs quantiques de factoriser rapidement des grands nombres[143].

Théorème 5.33 (Euler-Fermat[144])**.**
Deux énoncés très similaires.

(1) Soient a,n premiers entre eux dans $\mathbb{N}$. Alors Nous avons la formule

$$a^{\varphi(n)}\in[1]_n. \tag{5.73}$$

(2) Soient $A,B\in\mathbb{N}$ premiers entre eux. Alors il existe $p,m\in\mathbb{N}$ tels que

$$A^p=mB+1. \tag{5.74}$$

Démonstration. Vu que $\operatorname{pgcd}(a,n)=1$, le théorème de Bézout 1.229 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

$$\begin{aligned} f\colon (\mathbb{Z}/n\mathbb{Z})^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ x &\mapsto [a]_n x \end{aligned} \tag{5.75}$$

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

$$\begin{aligned} P &= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x && \text{(5.76a)}\\ &= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} f(x) && \text{(5.76b)}\\ &= \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} [a]_n x && \text{(5.76c)}\\ &= \Big(\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times}[a]_n\Big)\Big(\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times}x\Big) && \text{(5.76d)}\\ &= [a]_n^{\operatorname{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)}P && \text{(5.76e)} \end{aligned}$$

En simplifiant par P dans $\mathbb{Z}/n\mathbb{Z}$ nous trouvons

$$[a]_n^{\operatorname{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)}=[1]_n. \tag{5.77}$$

Et comme le lemme 5.31 donne $\operatorname{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)=\varphi(n)$, nous avons trouvé $[a]_n^{\varphi(n)}=[1]_n$. Autrement dit,

$$a^{\varphi(n)}\in[1]_n. \tag{5.78}$$

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 $m\in\mathbb{N}$. □

Lemme 5.34 ([142]).
Soient $d\mid n$ dans $\mathbb{N}^*$. Nous considérons le groupe additif $G_d=\{k[q]_n$ 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 5.32, 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. □

Lemme 5.35 ([145]).
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). □

Lemme 5.36 ([145]).
Si G est un groupe cyclique d'ordre n, alors G possède $\varphi(n)$ générateurs.

9. Proposition 1.302. 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 1.261.

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 5.35 montre que $(\mathbb{Z}/n\mathbb{Z}, +)$ possède $\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)$ générateurs.

Mais le lemme 5.31 assure que $\text{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right) = \varphi(n)$. □

Proposition 5.37.
Nous avons la formule

$$n = \sum_{d|n} \varphi(d). \tag{5.79}$$

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 5.34 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 5.36) : $\text{Card}(H_d) = \varphi(d)$.

Vu que tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ ont un ordre qui divise n (corolaire 2.14), nous avons l'union disjointe

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n} H_d, \tag{5.80}$$

et donc au niveau des cardinals,

$$n = \text{Card}(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \text{Card}(H_d) = \sum_{d|n} \varphi(d). \tag{5.81}$$

□

Lemme 5.38.
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 $q \leqslant p^{n-1}$ [11]. Il y a évidemment p^{n-1} tels nombres.

Par conséquent le cardinal de P_{p^n} est $\varphi(p^n) = p^n - p^{n-1}$. □

¡¡ Avertissement/question au lecteur !! 5.39
P_n n'a pas été défini.

Définition proposée (et vue par après) : $P_n = \{m \in \mathbb{N}$ tel que $\text{pgcd}(m, n) = 1\}$. À mettre donc en lien avec Δ_d.

5.5.2 Générateurs

Proposition 5.40.
Soit $n \in \mathbb{N}\backslash\{0\}$ 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 $\text{gr}\left([1]_n\right) = \mathbb{Z}/n\mathbb{Z}$. 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

$$ux + vn = 1. \tag{5.82}$$

Cela signifie entre autres que [12] $x\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$, et aussi que $\text{pgcd}(x, n) = 1$ par le théorème de Bézout 1.229, et donc que $x \in P_n$. □

Corolaire 5.41.
Un groupe monogène d'ordre n possède $\varphi(n)$ générateurs, où φ est la fonction indicatrice d'Euler définie en 5.29.

Démonstration. Le théorème 5.16 nous dit qu'un groupe monogène d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. La proposition 5.40 nous indique que $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(n)$ générateurs. □

11. Corolaire 3.23.
12. Corolaire 1.231

5.5.3 Fonction indicatrice d'Euler (propriétés)

Corolaire 5.42.
Deux propriétés.

(1) L'indicatrice d'Euler est multiplicative : si p est premier avec q, alors

$$\varphi(pq) = \varphi(p)\varphi(q). \tag{5.83}$$

(2) Si p est un nombre premier,

$$\varphi(p) = (p-1). \tag{5.84}$$

Démonstration. Nous savons que si p et q sont premiers entre eux, alors le théorème 5.25 nous donne l'isomorphisme de groupe

$$(\mathbb{Z}/pq\mathbb{Z}, +) \simeq (\mathbb{Z}/p\mathbb{Z}, +) \times (\mathbb{Z}/q\mathbb{Z}, +). \tag{5.85}$$

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 5.40, 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. □

5.6 Groupe symétrique, groupe alterné

La définition des permutations et du groupe symétrique sont 1.267. Voir aussi le thème 8.

5.6.1 Le groupe alterné

Définition 5.43.
Le groupe A_n des permutations paires[13] *dans S_n est le* ***groupe alterné****.*

Proposition 5.44.
À propos du groupe alterné dans le groupe symétrique.

(1) Le groupe alterné A_n est un sous-groupe caractéristique[14] *de S_n*

(2) Le sous-groupe A_n est d'indice 2 dans S_n.

(3) Le sous-groupe A_n est l'unique sous-groupe d'indice[15] *2 de S_n.*

Démonstration. Soit $\alpha \in \mathrm{Aut}(S_n)$. Étant donné que $\epsilon \circ \alpha$ est un homomorphisme 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 2.6, il existe un isomorphisme

$$f : S_n/\ker(\epsilon) \to \mathrm{Image}(\epsilon). \tag{5.86}$$

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 3.28, 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 $\varphi : S_n \to S_n/H$:

$$S_n \xrightarrow{\varphi} S_n/H \xrightarrow{\theta} \{-1, 1\}. \tag{5.87}$$

La composition $\theta \circ \varphi$ est alors un homomorphisme surjectif de S_n sur $\{-1, 1\}$ et nous avons $\theta \circ \varphi = \epsilon$ par la proposition 1.293. L'enchainement (5.87) nous montre que $H = \ker(\theta \circ \varphi) = \ker(\epsilon) = A_n$. □

13. Définition 1.289.
14. Définition 1.168.
15. Définition 2.12.

Proposition 5.45 ([146]).
Le groupe symétrique S_n peut être écrit comme un produit semi-direct[16] *du groupe alterné :*

$$S_n = A_n \times_\varphi \mathbb{Z}/2\mathbb{Z} \tag{5.88}$$

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

$$1 \xrightarrow{i} A_n \xrightarrow{i} S_n \xrightarrow{\epsilon} \{\pm 1\} \longrightarrow 1 \tag{5.89}$$

où les i représentent des inclusions et ϵ est la signature définie en 1.290. 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 2.48 nous dit que

$$S_n \simeq A_n \times_\varphi \{\mathrm{Id}, \sigma\} \tag{5.90}$$

où φ est l'action adjointe de $\{\mathrm{Id}, \sigma\}$ sur A_n. □

Proposition 5.46.
Si $\beta \in S_n$ est une transposition, nous avons les égalités suivantes d'ensembles :

$$S_n = A_n \cup A_n\beta = A_n \cup \beta A_n. \tag{5.91}$$

Démonstration. Les parties A_n et βA_n ont le même nombre d'éléments. En effet, l'application

$$\begin{aligned} \varphi\colon A_n &\to A_n\beta \\ \sigma &\mapsto \sigma\beta \end{aligned} \tag{5.92}$$

est une bijection.

De plus ces deux ensembles sont disjoints à cause de la proposition 1.293. 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, donc $\epsilon(\sigma\beta) = \epsilon(\sigma)\epsilon(\beta) = -1$.

Enfin, la proposition 5.44(2) dit que A_n est d'indice deux dans S_n. Donc la partie

$$A_n \cup A_n\beta \tag{5.93}$$

contient $|S_n|/2 + |S_n|/2 = |S_n|$ éléments. C'est donc S_n. □

Lemme 5.47.
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. □

Proposition 5.48 ([147]).
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

$$c_i = (1, 2, i) = (1, 2)(2, i), \tag{5.94}$$

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. □

16. Définition 2.47.

Proposition 5.49.
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 $\{1, \dots, n\}\backslash\{j_1, j_2, j_3\}$ et poser $\tau = (st)$. Puisque la signature est un homomorphisme et que τ et α sont impairs, l'élément $\tau\alpha$ est pair (lemme et proposition 1.292 et 1.288) et est donc dans A_n. Les supports de τ et φ étant disjoints, ces derniers commutent et nous avons

$$(\tau\alpha)\sigma(\tau\alpha)^{-1} = \tau(\alpha\sigma\alpha^{-1})\tau^{-1} = \tau\varphi\tau^{-1} = \varphi. \tag{5.95}$$

Donc σ et φ sont conjugués par $\tau\alpha$ qui est dans A_n. □

Théorème 5.50 ([52]).
Le groupe alterné A_n est simple[17] *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 5.48) et que tous les 3-cycles sont conjugués dans A_n (proposition 5.49), 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 $k \in \{1, \dots, n\}\backslash\{i, j, \sigma^{-1}(i)\}$ et $m = \sigma(k)$. Nous considérons la permutation $\alpha = (ijk)$. Étant donné que N est normal, l'élément

$$\theta = (\alpha^{-1}\sigma\alpha)\sigma^{-1} \tag{5.96}$$

est dans N. De plus en utilisant le lemme 1.283 et le fait que $\alpha^{-1} = (ikj)$ nous avons

$$\theta = (ikj)(j\sigma(j)m). \tag{5.97}$$

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 :

— $i \neq j = \sigma(i)$, 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

$$\theta = (ik)(j\sigma(j)). \tag{5.98}$$

C'est à priori un 2×2-cycle. Mais si de plus $\sigma(j) = i$, alors

$$\theta = (ijk) \tag{5.99}$$

qui est un 3-cycle ; et si $\sigma(j) = k$, alors

$$\theta = (ikj) \tag{5.100}$$

17. Pas de sous-groupes normaux non triviaux, définition 1.170.

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

$$\theta = (i, j, \sigma(j), m, k) \tag{5.101}$$

est un 5-cycle. Si $\sigma(j) = i$, alors

$$\theta = (ikj)(jim) = (imk) \tag{5.102}$$

qui est un 3-cycle. Si $\sigma(j) = k$, alors

$$\theta = (ikj)(jkm) = (ikm) \tag{5.103}$$

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 $e \in \{1, \dots, n\} \backslash \{a, b, c, d\}$ et nous avons

$$\underbrace{(abe)^{-1}\theta(abe)}_{\in N}\theta^{-1} = (aeb)(ab)(cd)(abe)(an)(cd) = (abe) \in N. \tag{5.104}$$

Si θ est le 5-cycle $(abcde)$, alors l'élément suivant est dans N :

$$(abc)^{-1}\theta(abc)\theta^{-1} = (acb)(abcde)(abc)(aedcb) = (acd). \tag{5.105}$$

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.

Lemme 5.51.
Le groupe alterné[18] 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 5.11(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. □

Le théorème suivant montre que tout groupe peut être vu, en agissant sur lui-même, comme une partie du groupe symétrique.

Théorème 5.52.
Un groupe G est isomorphe à un sous-groupe de son groupe symétrique $S(G)$.

18. Définition 5.43.

Démonstration. Nous considérons φ, la translation à gauche :

$$\begin{aligned}\varphi\colon G &\to S(G)\\ g &\mapsto t_g\end{aligned} \tag{5.106}$$

où $f_g(h) = gh$. Étant donné que

$$\varphi(gh) = ghx = g(t_h x) = t_g \circ t_h(x), \tag{5.107}$$

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. □

Lemme 5.53.
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

$$a' = s(a) = (\tau s \tau^{-1})(a) = (\tau s)(b) = \tau(b') \tag{5.108a}$$

$$b' = s(b) = (\tau s \tau^{-1})(b) = (\tau s)(a) = \tau(a'). \tag{5.108b}$$

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,

$$\{b\} = \{b, c\} \cap \{a, b\} = \{s(b)\}. \tag{5.109}$$

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 $\{\mathrm{Id}\}$.

□

Proposition 5.54 ([148, 138])**.**
Tout groupe simple[19] *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 5.11(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 :

$$g \cdot S = gSg^{-1}. \tag{5.110}$$

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

$$(gkg^{-1}) \cdot S = gkg^{-1}Ggk^{-1}g^{-1} \tag{5.111a}$$

$$= gkTk^{-1}g^{-1} \tag{5.111b}$$

$$= gTg^{-1} \tag{5.111c}$$

$$= S \tag{5.111d}$$

19. Définition 1.170.

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

$$G = D(G) \subset D(S_6) = A_6 \tag{5.112}$$

parce que le groupe dérivé du groupe symétrique est le groupe alterné (lemme 5.47).

L'ensemble $\theta^{-1}(A_6)$ est distingué dans G. En effet si $\sigma \in A_6$ et si $g \in G$ nous avons

$$\theta\big(g\theta^{-1}(\sigma)g^{-1}\big) = \theta(g)\sigma\theta(g)^{-1} \in A_6. \tag{5.113}$$

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

$$[\sigma] = \{h\sigma \text{ tel que } h \in H\}. \tag{5.114}$$

Évidemment A_6 agit sur X de façon naturelle. Au niveau de la cardinalité,

$$\text{Card}(X) = \frac{|A_6|}{|G|} = \frac{360}{60} = 6. \tag{5.115}$$

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. □

5.6.2 Sous-groupes normaux

5.55 ([149]).
Soit le groupe V_4 engendré par les doubles transpositions de S_4. Nous savons de l'exemple 1.287(5) 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 5.56.
Les sous-groupes $\text{Fix}_{S_n}(a)$ *(avec* $a \in \{1, \dots, n\}$*) sont conjugués entre eux.*

Démonstration. Soit $\sigma \in \text{Fix}(a)$ 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

$$(s\sigma s^{-1})(b) = (s\sigma)(a) = s(a) = b. \tag{5.116}$$

Donc $s\,\text{Fix}(a)s^{-1} \subset \text{Fix}(b)$.

Dans l'autre sens, si $\sigma \in \text{Fix}(b)$ alors $s^{-1}\sigma s \in \text{Fix}(a)$. Mais $\sigma = s(s^{-1}\sigma s)s^{-1}$, donc $\sigma \in s\,\text{Fix}(a)s^{-1}$. □

Proposition 5.57 (Sous-groupes normaux de S_n [149]).
Les sous-groupes normaux de S_n *ne sont pas légions.*

(1) Pour $n = 4$*, les sous-groupes normaux de* S_4 *sont* $\{\text{Id}\}$*,* 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 5.53, 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 1.288), 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 1.287). 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 $sts^{-1}t^{-1} = \mathrm{Id}$ impliquerait $st = ts$.

Soient donc deux transpositions $t_1, t_2 \in H$ telles que $t_1t_2 \neq \mathrm{Id}$. Les supports de t_1 et t_2 ont soit 1 soit aucun élément communs.

(i) **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 1.287) et que A_n est engendré par ceux-ci (proposition 5.48), $A_n \subset H$. 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.

(ii) **Second cas** Le groupe H contient un élément de la forme $(ab)(cd)$ avec a, b, c, d distincts dans $\{1, \dots, n\}$.

  (i) **Si $n = 3$** Impossible parce que avec $n = 3$ nous n'avons pas quatre éléments distincts.

  (ii) **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

$$4 \leqslant |H| \leqslant 24. \tag{5.117}$$

  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 5.44(3)). Quid de $|H| = 8$?
  D'après le corolaire 2.14 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 $x = \mathrm{Id}$. Ordre 8, pas possible parce que S_4 n'a pas d'éléments d'ordre 8.

    (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.

    (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).

  (iii) **Si $n \geqslant 5$** Soit un élément e[20] distinct de a, b, c et d. Par notre liste préférée des classes de conjugaison (exemple 1.287(5)), 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 :

$$(ce)(ab)(ab)(cd) = (ce)(cd) = (ecd). \tag{5.118}$$

  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.

(iv) **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 $n = 4$.

□

20. e n'est pas l'élément neutre ici

5.6.3 Indice

Théorème 5.58.
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.

(i) **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

$$H = \{\mathrm{Id}, (12)\} \tag{5.119}$$

ou l'identité avec (23), ou avec (13). Dans tous les cas c'est isomorphe à S_2.

(ii) **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 5.25 nous dit que H est soit cyclique[21] (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

$$H = \mathbb{Z}_3 \times_\varphi \mathbb{Z}_2 \tag{5.120}$$

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 (5.120). 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 5.18 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 5.45, 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 5.45 que $S_n = A_n \times_\varphi \mathbb{Z}_2$; en comparant avec (5.120) 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 $(\mathbb{Z}_3, +)$.

(iii) **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 $g \cdot [s] = [gs]$.

(i) **Morphisme $\varphi\colon S_n \to S_E$** Le φ défini par l'action est un morphisme parce que

$$\varphi(g_1g_2)[s] = [g_1g_2s] = \varphi(g_1)[g_2s] = \varphi(g_1)\varphi(g_2)[s]. \tag{5.121}$$

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 $gs_1 = gs_2h$, ce qui prouve que $s_1 = s_2h$ 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.

(ii) **$\ker(\varphi)$ 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 $\varphi(\sigma z \sigma^{-1}) = \varphi(\sigma)\varphi(z)\varphi(\sigma^{-1}) = \mathrm{Id}_E$.

(iii) **$\ker(\varphi) = \bigcap_{g \in S_n} gHg^{-1}$** 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

$$\varphi(z)[s] = [zs] = [shs^{-1}s] = [sh] = [s], \tag{5.122}$$

21. Définition 1.319.

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.

(iv) **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

$$|\ker(\varphi)| \leqslant |H| = (n-1)! < |A_n|. \tag{5.123}$$

Mais les seuls sous-groupes normaux de S_n sont A_n, S_n et $\{\mathrm{Id}\}$ (proposition 5.57). 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

$$\varphi\colon S_n \to S_E. \tag{5.124}$$

Soit une fonction de numérotation $\psi\colon E \to \{1, \ldots, n\}$. Avec cela nous définissons un isomorphisme de groupes

$$\begin{aligned} \tilde{\psi}\colon S_E &\to S_n \\ \sigma &\mapsto \psi\sigma\psi^{-1}. \end{aligned} \tag{5.125}$$

(v) **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 $\psi[\mathrm{Id}]$:

$$(\tilde{\psi} \circ \varphi)(h)\psi[\mathrm{Id}] = \psi \circ \varphi(h)[\mathrm{Id}] = \psi[h] = \psi[\mathrm{Id}]. \tag{5.126}$$

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

$$\big(\tilde{\psi}(s) \circ \psi\big)[\mathrm{Id}] = \psi[\mathrm{Id}], \tag{5.127}$$

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 $\sigma = \tilde{\psi}\big(\varphi(h)\big)$.

(vi) **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,

$$\tilde{\psi} \circ \varphi\colon H \to \mathrm{Fix}\big(\psi[\mathrm{Id}]\big) \tag{5.128}$$

est un isomorphisme de groupe. Mais le stabilisateur d'un point dans S_n est S_{n-1}.

□

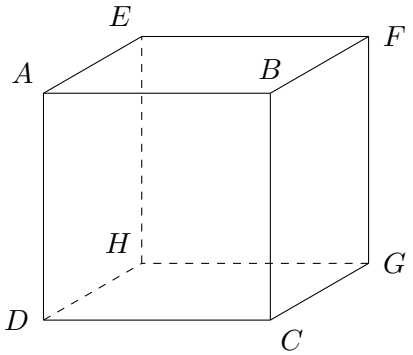
5.7 Isométries du cube

Les isométries du cube proviennent de [102].

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

$$\mathcal{D} = \{D_1, \ldots, D_4\} \tag{5.129}$$

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

$$\rho\colon G \to S_4. \tag{5.130}$$

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,

$$\overrightarrow{ON} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \quad \overrightarrow{OF} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}. \tag{5.131}$$

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 :

$$\ker(\rho) = \{\mathrm{Id}, s_0\}. \tag{5.132}$$

Le premier théorème d'isomorphisme 2.6 nous permet d'écrire le quotient de groupes :

$$\frac{G}{\{\mathrm{Id}, s_0\}} \simeq S_4. \tag{5.133}$$

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

$$\begin{aligned} \varphi\colon \frac{G}{\{\mathrm{Id}, s_0\}} &\to G^+ \\ [g] &\mapsto \begin{cases} g & \text{si } \det(g) > 0 \\ g \circ s_0 & \text{sinon} \end{cases} \end{aligned} \tag{5.134}$$

est un isomorphisme de groupes. Et enfin nous pouvons écrire

$$G^+ \simeq S_4. \tag{5.135}$$

Nous allons maintenant utiliser le corolaire 2.49 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

$$G \simeq S_4 \times_\sigma \mathbb{Z}/2\mathbb{Z}. \tag{5.136}$$

Mais étant donné que la conjugaison par s_0 est triviale, le produit semi-direct est un produit direct :

$$G \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}. \tag{5.137}$$

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 1.287.

(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 :

$$B \to D \to E \to B. \tag{5.138}$$

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 [22], c'est-à-dire les rotations d'angle π autour des mêmes axes. Cela fait 3 éléments d'ordre 2.

22. En fait c'est (13)(24), le carré de la précédente, mais c'est la même classe de conjugaison.

Chapitre 6

Corps

6.1 Généralités

6.1.
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 19.29 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 [102] 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.

6.1.1 Corps ordonnés

Nous avons vu la définition de corps totalement ordonné en 1.367.

Définition 6.2 ([71]).
Un corps est ***formellement réel*** *si* -1 *n'est pas une somme de carrés.*

Proposition 6.3.
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 1.367(1b). Si $a \leqslant 0$ alors $-a \geqslant 0$ et

$$a^2 = (-a)^2 \geqslant 0. \tag{6.1}$$

Comme $-1 < 0$, il ne peut donc pas être écrit comme un carré. A fortiori comme somme de carrés. □

6.1.2 Automorphismes de $\mathbb{R}$ et $\mathbb{C}$

Proposition 6.4 ([150, 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,

$$\sigma(a) = \sigma(1a) = \sigma(1)\sigma(a). \tag{6.2}$$

Donc $\sigma(1) = 1$.

(i) **Identité sur les rationnels** De plus

$$\sigma(n) = \sigma(1 + \ldots + 1) = \sigma(1) + \ldots + \sigma(1) = n, \tag{6.3}$$

et

$$\sigma\left(\frac{1}{n}\right) + \ldots + \sigma\left(\frac{1}{n}\right) = \sigma\left(\frac{1}{n} + \ldots + \frac{1}{n}\right) = \sigma(1) = 1. \tag{6.4}$$

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.

(ii) **Positive sur les positifs** Si $x > 0$ alors $\sigma(x) = \sigma(\sqrt{x})^2 > 0$.

(iii) **Croissance** Si $x > y$ alors $x - y > 0$ et $\sigma(x - y) > 0$. Cela donne $\sigma(x) > \sigma(y)$.

(iv) **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 $\mathbb{Q}$,

$$q_i + \epsilon > \sigma(x). \tag{6.5}$$

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,

$$q_i < \sigma(x) < q_i + \epsilon \tag{6.6}$$

pour tout $\epsilon > 0$ dans $\mathbb{Q}$ et $i > N$. Ce ϵ étant fixé nous pouvons prendre la limite des inégalités (6.6) :

$$x \leqslant \sigma(x) \leqslant x + \epsilon. \tag{6.7}$$

Cela étant valable pour tout $\epsilon > 0$ dans $\mathbb{Q}$, nous avons bien $x = \sigma(x)$.

□

Remarque 6.5.
Certains[150] 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

$$\phi\big(\phi^{-1}(x) + \phi^{-1}(y)\big) = x + y \tag{6.8}$$

parce que ϕ est un morphisme. D'autre part,

$$\phi\big(\phi^{-1}(x) + \phi^{-1}(y)\big) = \phi(a + b). \tag{6.9}$$

Donc

$$\phi^{-1}(x + y) = \phi^{-1}\big(\phi(a) + \phi(b)\big) = \phi^{-1}\big(\phi(a + b)\big) = a + b = \phi^{-1}(x) + \phi^{-1}(y). \tag{6.10}$$

Proposition 6.6.
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 6.4.

En ce qui concerne les imaginaires purs,

$$-1 = \sigma(-1) = \sigma(ii) = \sigma(i)^2. \tag{6.11}$$

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 $x \in \mathbb{R}$

6.1.3 Corps premier

Définition 6.7.
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.*

Lemme 6.8.
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 6.9.
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. □

Définition 6.10.
Soit p un nombre premier. Nous notons $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Nous verrons plus loin (section 19.4) comment nous pouvons définir $\mathbb{F}_{p^n}$ lorsque p est premier, ainsi que l'unicité d'un tel corps.

Nous avons par exemple

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\} \tag{6.12}$$

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 6.11.
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 3.58 que $\mathbb{F}_p$ est un corps lorsque p est premier. □

Lemme 6.12.
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

$$\begin{aligned} s\colon \mathbb{Z} &\to \mathbb{K} \\ k &\mapsto k_{\mathbb{K}} \end{aligned} \tag{6.13}$$

est un morphisme d'anneaux.

Si la caractéristique de $\mathbb{K}$ est 0, alors s est injective.

Proposition 6.13 (Sous-corps premier[151])**.**
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 $\mathbb{K}$.

2. Quand p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, proposition 3.58.
3. Je rappelle que tous les corps du Frido sont commutatifs, sauf mention explicite du contraire.

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

$$\mathbb{Z}1_{\mathbb{K}} \subset \mathbb{P} \subset \mathbb{K}. \tag{6.14}$$

Maintenant, le lemme 1.345 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.

(i) **Si $p > 0$** Nous avons $\mathbb{Z}1_{\mathbb{K}} \simeq \mathbb{Z}/p\mathbb{Z}$ par le lemme 1.345. 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 $\mathbb{K}$.

(ii) **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

$$\begin{aligned} \psi\colon \mathbb{Q} &\to \mathbb{P} \\ ab^{-1} &\mapsto a_{\mathbb{K}} b_{\mathbb{K}}^{-1} \end{aligned} \tag{6.15}$$

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

$$a_{\mathbb{K}} y_{\mathbb{K}} = x_{\mathbb{K}} b_{\mathbb{K}}. \tag{6.16}$$

Étant donné le lemme 6.12, 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 1.379.

□

Proposition 6.14.
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 6.13 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,

$$\sigma(k_{\mathbb{K}} l_{\mathbb{K}}^{-1}) = \sigma(k_{\mathbb{K}})\sigma(l_{\mathbb{K}})^{-1} = k_{\mathbb{K}} l_{\mathbb{K}}^{-1}. \tag{6.17}$$

Et voila. □

6.1.4 Petit théorème de Fermat

Théorème 6.15 (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 $x^{-1} = x^{p-2}$.

(4) Si x est premier avec p, alors $x^{p-1} \in [1]_p$.

4. Définition 6.7.
5. Dans le cas de caractéristique non nulle, $\mathbb{P} = \mathbb{Z}$ et vous pouvez vous arrêter ici.

Démonstration. Étant donné que $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif et que p est premier, la proposition 3.44 nous indique que $\sigma(x) = x^p$ est un automorphisme. La proposition 6.14 nous indique alors que

$$a^p = a. \tag{6.18}$$

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 6.16.
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

$$-142 = -113 = -84 = -55 = -26 = 3 = 32 = 61 = 90 = 119. \tag{6.19}$$

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,

$$x^{-a} = (x^a)^{27} = x^{27a}. \tag{6.20}$$

Le nombre $27a$ peut être grand par rapport à 29. Mais en réutilisant le fait que $1 = x^{28}$, on obtient

$$x^{-a} = x^{[27a]_{28}}. \tag{6.21}$$

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. △

6.1.5 Nombres de Sophie Germain

Définition 6.17.
*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[152], l'existence d'une infinité de nombres premiers de Sophie Germain est encore une question ouverte[6].

Lemme 6.18 ([153, 154])**.**
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 6.15 nous dit que $m^{q-1} \in [1]_q$. Mais $m^{q-1} = m^{2p} = (m^p)^2$. Donc

$$(m^p)^2 \in [1]_q. \tag{6.22}$$

Puisque q est premier, l'anneau $\mathbb{Z}/q\mathbb{Z}$ est intègre par le corolaire 1.236. Comme $1 \neq -1$, la proposition 3.128 s'applique et nous avons $m^p \in [\pm 1]_q$. □

Théorème 6.19 ([153, 154, 155])**.**
Soit un nombre premier de Sophie Germain (définition 6.17). Il n'existe pas de solution (x, y, z) dans $\mathbb{Z}^3$ au système

$$\begin{cases} x^p + y^p + z^p = 0 \\ [xyz]_p \neq 0. \end{cases} \tag{6.23}$$

Démonstration. Nous supposons que $(x, y, z) \in \mathbb{Z}^3$ est une solution telle que $\text{pgcd}(x, y, z) = 1$.

6. Si vous lisez ce paragraphe dans un futur où la question est tranchée, n'hésitez pas à m'écrire pour mettre à jour.

(i) **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 3.17 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).

(ii) **Le fameux u** Nous introduisons à présent une nouvelle variable intermédiaire qui va beaucoup nous aider. En utilisant le lemme 3.43,

$$-x^p = y^p + z^p = (y + z) \sum_{k=0}^{p-1} y^k (-z)^{p-1-k} = (y + z)u \tag{6.24}$$

où nous avons posé $u = \sum_{k=0}^{p-1} y^k(-z)^{p-1-k}$.

(iii) **$\text{pgcd}(u, y + z) = 1$** Soit α un nombre premier qui divise u et $y + z$.

D'abord α divise x^p et donc x (lemme 3.17). Autrement dit : $[x]_\alpha = 0$.

Ensuite, $0 = [x + z]_\alpha$, de telle sorte que

$$[y]_\alpha = -[z]_\alpha \tag{6.25}$$

Enfin, en prenant la classe de u modulo α, et en substituant (6.25) :

$$\begin{aligned} 0 = [u]_\alpha &= \Big[\sum_{k=0}^{p-1} y^k (-z)^{p-1-k} \Big]_\alpha && \text{(6.26a)} \\ &= \sum_{k=0}^{p-1} [y^k]_\alpha [y^{p-1-k}]_\alpha && \text{(6.26b)} \\ &= \sum_{k=0}^{p-1} [y]_\alpha^{p-1} && \text{(6.26c)} \\ &= p[y]_\alpha^{p-1}. && \text{(6.26d)} \end{aligned}$$

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 $\text{pgcd}(u, y + z) = 1$.

(iv) **Utilisation d'un lemme** Pour rappel, p est impair. Nous avons $(-x)^p = (y + z)u$. Le lemme 3.21 nous dit qu'il existe $a, \alpha \in \mathbb{Z}$ tels que

$$\begin{cases} y + z = a^p \\ u = \alpha^p. \end{cases} \tag{6.27}$$

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

$$\begin{aligned} y + z &= a^p && \text{(6.28a)} \\ x + z &= b^p && \text{(6.28b)} \\ x + y &= c^p. && \text{(6.28c)} \end{aligned}$$

7. Corolaire 1.236.
8. Proposition 1.192.

(v) 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 6.18 dit que $x^p \in [\pm 1]_q$, $y^p \in [\pm 1]_q$ et $z^p \in [\pm 1]_q$. Donc les valeurs possibles pour $[x^p + y^p + z^p]_q$ sont $[\pm 3]_q$ et $[\pm 1]_q$.

Mais nous avons supposé que $x^p + y^p + z^p = 0$ et que $q \geqslant 5$ de telle sorte que $[\pm 3]_q \neq 0$. 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.

(vi) q **divise** x Jusqu'à présent x, y et z avaient des rôles symétriques. Maintenant nous supposons que q divise x.

(vii) $[y^p]_q = [\pm 1]_q$ Nous savons que $c^p = x + y$. En passant aux classes modulo q, nous avons

$$[c^p]_q = [x]_q + [y]_q = [y]_q \tag{6.29}$$

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 3.17.
$\Rightarrow$ $c^p \in [\pm 1]_q$ par le lemme 6.18.
$\Rightarrow$ $y \in [\pm 1]_q$ toujours parce que $[y]_q = [c^p]_q$.

(viii) $[z^p]_q = [\pm 1]_q$ Parce que les rôles de y et z sont symétriques. Donc ce que nous avons fait pour obtenir $[y^p]_q = [\pm 1]_q$ tient pour avoir $[z^p]_q = [\pm 1]_q$.

(ix) q **divise** $y + z$ Nous avons dit que q divisait x. Il divise donc aussi $2x$. Nous avons :

$$2x = (x + y) + (x + z) - (y + z) = c^p + b^p - a^p. \tag{6.30}$$

En passant au modulo q, à gauche nous avons $[2x]_q = 0$. Donc

$$\begin{aligned}
[a^p]_q &= [c^p]_q + [b^p]_q && \text{(6.31a)}\\
&= [y]_q + [z]_q && \text{(6.31b)}\\
&= [\pm 1]_q + [\pm 1]_q && \text{(6.31c)}\\
&\in \{[2]_q, [-2]_q, [0]_q\}. && \text{(6.31d)}
\end{aligned}$$

En tout état de cause, $[a^p]_q$ n'est pas $[\pm 1]_q$. La contraposée du lemme 6.18 nous dit alors que q divise $a^p = y + z$.

(x) $[y]_q = [-z]_q$ Il s'agit seulement du fait que q divise $y + z$.

(xi) $[u]_q = [p]_q$ Par définition, $u = \sum_{k=0}^{p-1} y^k (-z)^{p-1-k}$. On passe au modulo q, en substituant $[-z]_q$ par $[y]_q$:

$$[u]_q = \sum_{k=0}^{p-1} [y]_q^k [y]_q^{p-1-k} = \sum_{k=0}^{p-1} [y]_q^{p-1} = p[y]_q^{p-1} = [p]_q \tag{6.32}$$

La dernière égalité est le fait que $[y]_q = [\pm 1]_q$ et que $p - 1$ est pair.

(xii) **La contradiction** Vous vous souvenez de (6.27) 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. □

6.2 Théorème des deux carrés

Proposition 6.20.
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. □

6.2.1 Un peu de structure dans $\mathbb{Z}[i]$

Lemme 6.21.
L'application

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{N} \\ a + bi &\mapsto a^2 + b^2 \end{aligned} \tag{6.33}$$

est un stathme euclidien pour $\mathbb{Z}[i]$.

Démonstration. Soient $t, z \in \mathbb{Z}[i]\backslash\{0\}$ dont le quotient s'écrit

$$\frac{z}{t} = x + iy \tag{6.34}$$

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

$$|\frac{z}{t} - q| \leqslant \frac{|1+i|}{2} = \frac{\sqrt{2}}{2} < 1. \tag{6.35}$$

On pose $r = z - qt$ qui est bien un élément de $\mathbb{Z}[i]$. De plus

$$|r| = |z - qt| = |t||\frac{z}{t} - q| < |t|, \tag{6.36}$$

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 1.247).

Lemme 6.22.
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

$$1 = N(zz') = N(z)N(z'), \tag{6.37}$$

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

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}. \tag{6.38}$$

□

Définition 6.23 ([156]).
*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 $x, y \in E$,*

9. Dans l'exemple 1.246, nous prenions toujours l'inférieur parce que le stathme tenait compte de la positivité.

(1) $x*(y*z)=(x*y)*z$ *(associativité)*

(2) $e*x=x*e=x$ *(e est un neutre).*

Nous notons $\Sigma=\{a^2+b^2 \text{ tel que } a,b\in\mathbb{N}\}$.

Lemme 6.24.
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 6.21). 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

$$N(zz')=N(z)N(z')=nm. \tag{6.39}$$

Donc nm est l'image de zz' par N, ce qui prouve que $nm\in\Sigma$. □

Théorème 6.25 (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

$$\mathbb{Z}[i]=\{a+bi \text{ tel que } a,b\in\mathbb{Z}\}. \tag{6.40}$$

puis l'application

$$\begin{aligned} N\colon \mathbb{Z}[i]&\to\mathbb{N}\\ a+bi&\mapsto a^2+b^2. \end{aligned} \tag{6.41}$$

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 6.22).

Le lemme 6.21 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 1.247).

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 $a\neq0$ et $b\neq0$. 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 $\{\pm1,\pm i\}$. En appliquant N nous avons

$$p^2=N(p)=N(z)N(z'). \tag{6.42}$$

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 1.237 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

10. Définition 6.23.

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

$$\mathbb{Z}[i]/(p) = (\mathbb{Z}[X]/(p))/(X^2+1) = \mathbb{F}_p[X]/(X^2+1). \tag{6.43}$$

Nous avons donc équivalence des propositions suivantes :

$$p \in \Sigma \tag{6.44a}$$
$$\mathbb{F}_p[X]/(X^2+1) \text{ n'est pas intègre} \tag{6.44b}$$
$$X^2+1 \text{ n'est pas irréductible dans } \mathbb{F}_p \tag{6.44c}$$
$$X^2+1 \text{ admet une racine dans } \mathbb{F}_p \tag{6.44d}$$
$$-1 \in (\mathbb{F}_p^*)^2 \tag{6.44e}$$
$$\exists y \in \mathbb{F}_p^* \text{ tel que } y^2 = -1. \tag{6.44f}$$

Le point (6.44c) vient de la proposition 6.20. 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,

$$(-1)^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1 \tag{6.45}$$

parce que dans $\mathbb{F}_p$ nous avons $y^{(p-1)} = 1$ par le petit théorème de Fermat (théorème 6.15). Ainsi p doit vérifier

$$1 = (-1)^{(p-1)/2}, \tag{6.46}$$

c'est-à-dire $\frac{p-1}{2} = 0 \mod 2$ ou encore $p = 1 \mod 4$. □

Remarque 6.26.
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 6.27 (Théorème des deux carrés[102])**.**
Soit $n \geqslant 2$ un nombre dont nous notons

$$n = \prod_{p\in\mathcal{P}} p^{v_p(n)} \tag{6.47}$$

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. (i) **Condition suffisante.** Le produit (6.47) 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

$$\prod_{p\in\mathcal{P}\cap[1]_4} p^{v_p(n)} \in \Sigma. \tag{6.48}$$

— Le seul nombre premier dans $[2]_4$ est 2. C'est un élément de Σ.

— Le produit

$$\prod_{p\in\mathcal{P}\cap[3]_4} p^{v_p(n)} \tag{6.49}$$

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 6.24.

(ii) **Condition nécessaire.** Soit p, un nombre premier. Nous voulons montrer que

$$\{v_p(n) \text{ tel que } n \in \Sigma\} \subset [2]_2. \tag{6.50}$$

Pour montrer cela nous allons procéder par récurrence sur les ensembles

$$E_k = \{v_p(n) \text{ tel que } n \in \Sigma\} \cap \{0, \dots, k\}. \tag{6.51}$$

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

$$n = a^2 + b^2 = (a + bi)(a - bi) \tag{6.52}$$

Comme $\mathbb{Z}[i]$ est principal, le lemme de Gauss 3.69 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

$$p^2 \mid a^2 + b^2 = n. \tag{6.53}$$

Posons $a = pa'$ et $b = pb'$ avec $a', b' \in \mathbb{N}$. Nous avons

$$\frac{n}{p^2} = \frac{p^2a'^2 + p^2b'^2}{p^2} = a'^2 + b'^2 \in \Sigma. \tag{6.54}$$

Mais par construction,

$$v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 < k. \tag{6.55}$$

Donc $v_p(\frac{n}{p^2})$ est pair et par conséquent, $v_p(n)$ doit également être pair.

□

6.2.2 Résultats chinois

Nous allons maintenant parler du système d'équations

$$\begin{cases} x = a_1 \mod p & \text{(6.56a)} \\ x = a_2 \mod q & \text{(6.56b)} \end{cases}$$

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 [157].

Notons que le système (6.56), en suivant les notations usuelles du Frido s'écrit plutôt

$$x \in [a_1]_p \cap [a_2]_q. \tag{6.57}$$

Lemme 6.28 (Lemme chinois [158])**.**
Soient n_1, n_2 deux entiers premiers entre eux[11]*. Soient $a_1, a_2 \in \mathbb{Z}$.*

(1) Il existe $u_1, u_2 \in \mathbb{Z}$ tels que

$$u_1n_1 + u_2n_2 = 1. \tag{6.58}$$

(2) Nous posons

$$a = a_1u_2n_2 + a_2n_1u_1. \tag{6.59}$$

Nous avons

$$[a_1]_{n_1} \cap [a_2]_{n_2} = [a]_{n_1n_2}. \tag{6.60}$$

11. Définition 1.252.

Démonstration. En plusieurs points.

(i) **Pour (1)** Il suffit d'utiliser le théorème de Bézout 1.229

(ii) **Pour (2) première inclusion** Soit $x \in [a]_{n_1n_2}$, et vérifions que $x \in [a_1]_{n_1}$. Il existe $k \in \mathbb{Z}$ tel que

$$x = a_1u_2n_2 + a_2n_1u_1 + kn_1n_2. \tag{6.61}$$

En remplaçant u_2n_2 par $1 - u_1n_1$, nous avons

$$x = a_1(1 - u_1n_1) + a_2n_1u_1 + kn_1n_2 \in [a_1]_{n_1} \tag{6.62}$$

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].

(iii) **Pour (2) seconde inclusion** Soit $x \in [a_1]_{n_1} \cap [a_2]_{n_2}$. Il existe $k \in \mathbb{Z}$ tel que $x = a_1 + kn_2$. Donc

$$\begin{aligned} x - a &= a_1 + kn_1 - (a_1u_2n_2 + a_2n_1u_1) && \text{(6.63a)}\\ &= a_1 - a_1u_2n_2 + k'n_1 && \text{(6.63b)}\\ &= a_1 \underbrace{(1 - u_2n_2)}_{=u_1n_1} + k'n_1 && \text{(6.63c)}\\ &= a_1u_1n_1 + k'n_1, && \text{(6.63d)} \end{aligned}$$

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

$$x - a = kn_1 = ln_2. \tag{6.64}$$

En particulier n_1 divise ln_2 alors que n_1 et n_2 sont premiers entre eux. Le lemme de Gauss 3.69 dit alors que n_1 divise l. Il existe donc $s \in \mathbb{Z}$ tel que $l = sn_1$. En remettant ce l dans (6.64), nous trouvons

$$x - a = ln_1 = sn_1n_2, \tag{6.65}$$

et donc $x - a$ est divisible en n_1n_2, c'est-à-dire

$$x \in [a]_{n_1n_2}, \tag{6.66}$$

ce qu'il fallait prouver.

□

Théorème 6.29 (Théorème chinois[159]).
Soient p, q deux naturels premiers entre eux. Si $p, q \geqslant 2$ alors l'application

$$\begin{aligned} \phi\colon \mathbb{Z}/pq\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\\ [x]_{pq} &\mapsto \big([x]_p, [x]_q\big) \end{aligned} \tag{6.67}$$

est un isomorphisme d'anneaux.

Démonstration. Nous devons prouver que l'application ϕ respecte la somme, le produit et qu'elle est bijective. En ce qui concerne la somme,

$$\begin{aligned} \phi([q]_{pq} + [y]_{pq}) &= \phi\big((x + y) \mod pq\big) && \text{(6.68a)}\\ &= \big([x + y]_p, [x + y]_q\big) && \text{(6.68b)}\\ &= \big([x]_p + [y]_p, [x]_q + [y]_q\big) && \text{(6.68c)}\\ &= \big([x]_p, [x]_q\big) + \big([y]_p, [y]_q\big) && \text{(6.68d)}\\ &= \phi(x) + \phi(y). && \text{(6.68e)} \end{aligned}$$

12. Je dis ça au hasard ; je n'ai pas vérifié. Faites-moi signe si c'est bon.

En ce qui concerne le produit, c'est le même jeu : nous obtenons

$$\phi\big([xy]_{pq}\big) = \phi([x]_{pq})\phi([y]_{pq}) \tag{6.69}$$

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

$$\phi([x]_{pq}) = \big([y_1]_p, [y_2]_q\big) \tag{6.70}$$

revient à demander de résoudre le système

$$\begin{cases} [x]_p = [y_1]_p & \text{(6.71a)} \\ [x]_q = [y_2]_q & \text{(6.71b)} \end{cases}$$

pour l'inconnue $x \in \mathbb{Z}$. Le lemme chinois 6.28 nous assure qu'une solution existe.

En ce qui concerne l'injectivité, nous supposons que x et y soient deux entiers tels que

$$\phi([x]_{pq}) = \phi([y]_{pq}). \tag{6.72}$$

Nous en déduisons le système

$$\begin{cases} [x]_p = [y]_p & \text{(6.73a)} \\ [x]_q = [y]_q & \text{(6.73b)} \end{cases}$$

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

$$kp + lq = 0. \tag{6.74}$$

Étant donné que p et q sont premiers entre eux, le lemme de Gauss 3.12 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. □

Théorème 6.30 (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.

(i) **Définition de J_k** Pour $k \in \{1, \dots, n\}$ nous notons J_k le produit $J_k = \prod_{l \neq k} I_l$.

(ii) **Si $k \neq i$ alors $J_k \subset I_i$** Un élément de J_k est de la forme

$$\prod_{l \neq k} a_j = a_i \prod_{\substack{l \neq k \\ l \neq i}} a_l \tag{6.75}$$

avec $a_l \in I_l$. Vu que a_i est dans I_i qui est un idéal, tout le produit (6.75) est dans I_i.

(iii) $I_i + J_i = A$ En effet, soit $k \neq i$. Nous avons $J_i \subset I_k$ et donc

$$I_i + J_i \subset I_i + I_k = A. \tag{6.76}$$

(iv) **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

$$\alpha_i + \beta_i = 1. \tag{6.77}$$

(v) **Et enfin** Nous posons $x = \sum_{i=1}^{n} \beta_i x_i$. Pour chaque k nous avons

$$x - x_k = \sum_{i=1}^{n} \beta_i x_i - x_k \tag{6.78a}$$
$$= \sum_{i \neq k} \beta_i x_i + (\beta_k - 1)x_k \tag{6.78b}$$
$$= \sum_{i \neq k} \beta_i x_i - \alpha_k x_k. \tag{6.78c}$$

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 6.31.
Ce théorème chinois est bien une généralisation du lemme chinois 6.28. 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 1.231.

6.3 Polynômes à coefficients dans un corps

Nous supposons que $\mathbb{K}$ est un corps commutatif, et nous étudions l'anneau $\mathbb{K}[X]$, défini en 1.352.

Lemme 6.32 ([115]).
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

$$P = \frac{1}{s} \sum_{j=1}^{n} a'_j X^j \tag{6.79}$$

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,

$$P = \frac{d}{s} \sum_j b_j X^j. \tag{6.80}$$

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. □

Lemme 6.33 ([40]).
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

$$P = (qQ)(rR) \tag{6.81}$$

avec qQ, rR dans $A[X]$.

13. Définition 1.362.
14. Définition 3.110(1).

Démonstration. En utilisant le lemme 6.32, nous considérons $qQ = Q_1$ et $rR = R_1$ avec Q_1 et R_1 primitifs dans $A[X]$. Avec ces éléments nous avons

$$R_1Q_1 = rqPQ = qrP. \tag{6.82}$$

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.

(i) $qr \in A$ 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 (6.82) 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

$$\frac{sa_i}{t} = b_i, \tag{6.83}$$

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 3.69 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

$$\frac{s}{t} = \frac{st^{-1}}{tt^{-1}} = st^{-1} \in A. \tag{6.84}$$

Nous avons prouvé que $qr \in A$.

(ii) qr **est inversible** Comme qr est dans A nous pouvons l'utiliser dans le lemme 1.196. Nous savons que $c(P)$ est inversible, disons $c(P) = u$. Nous avons donc, en utilisant le lemme 3.114,

$$qru = qr\,c(P) = u\,c(qrP) = u\,c(Q_1R_1) = uv\,c(Q_1)c(R_1) \in A^\times \tag{6.85}$$

pour un certain inversible $v \in A^\times$. Donc qru est inversible et comme u est inversible, qr est inversible.

(iii) **Conclusion** Nous avions $P = QR$, et nous avions posé $qQ = Q_1$, $rR = R_1$. Maintenant, en posant $u = (qr)^{-1}$ nous avons

$$(uqQ)(rR) = uqrQR = P. \tag{6.86}$$

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.

□

Théorème 6.34 ([40]).
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),

(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 $\geqslant 1$.

(i) **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.

(i) 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.

15. Définition 1.183.
16. Cette notation $\mathcal{P}$ de (1.478) devrait être utilisée plus souvent ; dans le meilleur des mondes, on n'utiliserait jamais $A[X]$.

(ii) *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 $\mathcal{P}(A)$.

(ii) **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.

(iii) **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 6.33, il existe $q, r \in \mathbb{K}$ tels que

$$P = (qQ)(rR) \tag{6.87}$$

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 $\mathcal{P}(\mathbb{K})^\times$.

(iv) **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

$$P = qR. \tag{6.88}$$

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 (6.88) en appliquant le lemme 1.196 : $c(P) = q\,c(R)$. Nous savons que $c(P)$ est inversible dans A ; nous multiplions par $c(P)^{-1}$:

$$1 = qc(R)c(P)^{-1}. \tag{6.89}$$

Nous voyons que $c(R)c(P)^{-1}$ est un inverse de q dans A. Donc P est irréductible dans $\mathcal{P}(A)$.

□

Théorème 6.35 ([40])**.**
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.

(i) **Si** $\deg(P) = 0$ L'unique coefficient de P est un élément de A, et se décompose en irréductibles parce que A est factoriel.

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.

(ii) **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

$$P = c_1 P_1 \tag{6.90}$$

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.

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

$$P = p_1 \dots p_k P_1 \tag{6.91}$$

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 6.33 permet d'écrire alors

$$P_1 = QR = Q_1 R_1 \tag{6.92}$$

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

$$P_1 = Q_1 R_1 = S_1 \dots S_l. \tag{6.93}$$

Au final, nous avons la décomposition [18]

$$P = p_1 \dots p_k S_1 \dots S_l. \tag{6.94}$$

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.

(i) **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 3.114 et 1.196, l'égalité

$$c(p_1 \dots p_k S_1 \dots S_m) = c(q_1 \dots q_l T_1 \dots T_n) \tag{6.95}$$

devient

$$p_1 \dots p_k c(S_1 \dots S_m) = q_1 \dots q_l c(T_1 \dots T_n). \tag{6.96}$$

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 1.186) et donc

$$p_1 \dots p_k = (uq_1) q_2 \dots q_l \tag{6.97}$$

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 $q_{\sigma(i)}$.

18. Ici [115] utilise le théorème 6.34. Certes, il présente sa récurrence de façon un peu différente, mais j'espère n'avoir pas loupé une étape. Soyez prudente et écrivez-moi si vous voyez une erreur.

(ii) **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 6.34.

L'anneau $\mathcal{P}(\mathbb{K})$ est euclidien par 3.105 et donc principal par 1.247. Or dans un anneau principal, les irréductibles sont premiers par 1.227. 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 6.34). 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

$$\frac{sb_j}{t} = a_j, \tag{6.98}$$

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

$$q = \frac{s}{t} = \frac{st^{-1}}{tt^{-1}} = st^{-1} \in A. \tag{6.99}$$

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

$$S_1 \dots S_m = T_1 \dots T_n \tag{6.100}$$

peut être alors récrite

$$S_1 \dots S_m = qT_1 \dots T_{i-1} S_1 T_{i+1} \dots T_n \tag{6.101}$$

Comme A est factoriel, il est intègre, et donc $\mathcal{P}(A)$ est intègre (théorème 3.99). Nous pouvons donc simplifier par S_1 et il reste

$$S_2 \dots S_m = uT_1 \dots T_{i-1} T_{i+1} \dots T_n. \tag{6.102}$$

Par récurrence, nous avons que chacun des S_i est associé à un des T_j.

□

Proposition 6.36 ([115, 160]).
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 3.76), donc le théorème 6.35 conclu que l'anneau des polynômes sur un corps est factoriel. □

6.3.1 Irréductibilité

Pour rappel, un élément irréductible dans un anneau est la définition 1.183 : non inversible et pas les produit de deux non inversibles.

Lemme 6.37.
Soit un corps $\mathbb{K}$. Les éléments inversibles dans $\mathbb{K}[X]$ sont les polynômes constants non nuls.

19. Définition 3.59.

Exemple 6.38.
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

$$P = (X^2 + 1)(X^2 + 2), \tag{6.103}$$

mais n'a pas de racines dans $\mathbb{Z}$. Si on veut réduire plus, il faut sortir de $\mathbb{Z}$.

△

Définition 6.39 (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 6.40 (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 3.110) 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 (3.69) 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 3.129 nous dit alors que P est irréductible sur $\mathbb{Z}[X]$. □

Exemple 6.41.
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 $\mathbb{Q}[X]$. △

6.3.2 Idéaux

Soit $P \in \mathbb{K}[X]$ un polynôme. Nous notons (P) l'idéal engendré par P :

$$(P) = \{PR \text{ tel que } R \in \mathbb{K}[X]\}. \tag{6.104}$$

Lemme 6.42.
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. □

Théorème 6.43.
Soit $\mathbb{K}$ un corps commutatif.

(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 $(P) = I$.

(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 3.105 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 3.102 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 6.43 que nous verrons plus bas est que tout polynôme annulateur d'un endomorphisme est divisé par le polynôme minimal (proposition 9.96).

Corolaire 6.44.
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 6.43, par conséquent la proposition 1.239(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

$$\sum_{k=0}^{n-1} a_k X^k = SP, \tag{6.105}$$

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

$$\bar{X}^{n+l} = \bar{X}^n \bar{X}^l = (\bar{P} - \bar{Q})\bar{X}^l = \bar{Q}\bar{X}^l. \tag{6.106}$$

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. □

6.45.
Ce corolaire prendra une nouvelle jeunesse lorsque nous parlerons de polynômes d'endomorphismes, en particulier la proposition 9.106 va donner des précisions.

Lemme 6.46 ([161]).
Soit un isomorphisme de corps $\tau : \mathbb{K} \to \mathbb{K}'$. Alors

(1) L'application étendue

$$\begin{aligned} \tau : \mathbb{K}[X] &\to \mathbb{K}'[X] \\ \sum_i a_i X^i &\mapsto \sum_i \tau(a_i) X^i \end{aligned} \tag{6.107}$$

20. Ici $\mathbb{K}$ est un corps et donc l'hypothèse d'inversibilité est automatiquement vérifiée.

est un isomorphisme d'anneaux ;

(2) pour tout $P \in \mathbb{K}[X]$, le passage au quotient

$$\begin{aligned} \phi_\tau \colon \mathbb{K}[X]/(P) &\to \mathbb{K}'[X]/\big(\tau(P)\big) \\ \bar{Q} &\mapsto \overline{\tau(Q)} \end{aligned} \tag{6.108}$$

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 (1.481). 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 :

$$\tau(PQ) = \tau\Big(\sum_k \big(\sum_{l=0}^{k} P_l Q_{k-l}\big) X^k\Big) \tag{6.109a}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P_l Q_{k-l}) \tag{6.109b}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P_l)\tau(Q_{k-l}) \tag{6.109c}$$
$$= \sum_k X^k \sum_{l=0}^{k} \tau(P)_l \tau(Q)_{k-l} \tag{6.109d}$$
$$= \sum_i \big(\tau(P)_i X^i\big) \sum_j \big(\tau(Q)_j X^j\big) \tag{6.109e}$$
$$= \tau(P)\tau(Q). \tag{6.109f}$$

Passons à l'isomorphisme d'anneaux donné par ϕ_τ.

(i) **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,

$$\phi_\tau(Q_2) = \overline{\tau(Q_2)} = \overline{\tau(Q_1) + \tau(RP)} \tag{6.110a}$$
$$= \overline{\tau(Q_1) + \tau(R)\tau(P)} \tag{6.110b}$$
$$= \overline{\tau(Q_1)}. \tag{6.110c}$$

L'application ϕ_τ est donc bien définie.

(ii) **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

$$\tau(Q_1) = \tau(Q_2) + R\ \tau(P) \tag{6.111}$$

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 :

$$Q_1 = Q_2 + \tau^{-1}(R)P, \tag{6.112}$$

ce qui signifie que $\bar{Q}_1 = \bar{Q}_2$.

(iii) **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 $\overline{\tau^{-1}(Q)} \in \mathbb{K}[X]/(P)$.

(iv) **Morphisme** Nous vous laissons vérifier que l'application ϕ_τ est un morphisme d'anneaux.

□

6.3.3 Identité de Bézout

Théorème 6.47 (Bézout)**.**
Les polynômes $P_1, \dots, P_n$ dans $\mathbb{K}[X]$ sont étrangers entre eux si et seulement si il existe des polynômes $Q_1, \dots, Q_n \in \mathbb{K}[X]$ tels que

$$P_1Q_1 + \cdots + P_nQ_n = 1. \tag{6.113}$$

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 :

$$xP + yQ = 0; \tag{6.114}$$

cette dernière pourra être écrite en termes de la matrice de Sylvester, voir sous-section 9.1.7.

Lemme 6.48.
Soient $(P_i)_{i=1,\dots,n} \in \mathbb{K}[X]$ des polynômes étrangers deux à deux. Alors les polynômes

$$Q_i = \prod_{j \neq i} P_j \tag{6.115}$$

sont étrangers entre eux[21].

Lemme 6.49 ([162])**.**
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 $\phi \in \mathbb{A}[X]$.

6.3.4 Lemme et théorème de Gauss

Théorème 6.50 (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

$$R = PUR + QVR = PUR + VPS = P(UR + VS), \tag{6.116}$$

ce qui signifie que P divise R. □

Le lemme suivant est une généralisation du lemme de Gauss dans $\mathbb{Z}$ (lemme 3.69).

Lemme 6.51 (Lemme de Gauss[111])**.**
Soient les polynômes unitaires $P, Q \in \mathbb{Q}[X]$. Si $PQ \in \mathbb{Z}[X]$, alors P et Q sont tous deux dans $\mathbb{Z}[X]$.

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

$$\pi_p \colon \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]. \tag{6.117}$$

21. Et non seulement deux à deux.
22. théorème 6.47.

Par définition $abPQ = P_1Q_1 \in \mathbb{Z}[X]$; en prenant la projection,

$$\pi_p(P_1)\pi_p(Q_1) = \pi_p(P_1Q_1) = \pi_P(ab)\pi_p(PQ) = 0 \tag{6.118}$$

parce que $\pi_p(ab) = 0$. Étant donné que $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre (théorème 3.99), 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. □

6.3.5 Polynômes sur un corps et pgcd

Nous savons qu'un corps est un anneau intègre (lemme 1.193). De plus l'ensemble des polynômes sur un anneau intègre est lui-même un anneau intègre (théorème 3.99). Donc la notion de pgcd à utiliser dans le cas de $\mathbb{K}[X]$ est celle de la définition 1.180.

Lemme 6.52 (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 $k \in \mathbb{K}$.

(2) Il existe un unique polynôme unitaire dans $\text{pgcd}(S)$.

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,

$$\delta_1 = AB\delta_1. \tag{6.119}$$

Mais $\mathbb{K}[X]$ possède la propriété de simplification par la proposition 1.192(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 $\text{pgcd}(S)$. Existence : si $P = \sum_{k=0}^{n} a_k X^k \in \text{pgcd}(S)$, alors le polynôme P/a_n est unitaire et également dans $\text{pgcd}(S)$. Unicité : supposons que P est unitaire dans $\text{pgcd}(S)$ et que Q est dans $\text{pgcd}(S)$. Il existe $k \in \mathbb{K}$ tel que $Q = kP$. Vu que P est unitaire, Q ne l'est pas. □

6.53.
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 6.52. En particulier, si P et Q sont des polynômes, nous notons $\text{pgcd}(P, Q)$ l'unique polynôme unitaire parmi les PGCD de P et Q.

Lemme 6.54 ([163])**.**
Soit un corps commutatif $\mathbb{K}$, deux polynômes quelconques $A, B \in \mathbb{K}[X]$ et un polynôme unitaire G.

Nous avons $G = \text{pgcd}(A, B)$ 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.

(i) $\Rightarrow$ 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 $B = GB_1$.

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

23. Définition 1.180.

$GD|G$; 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 6.47, il existe donc U et V tels que $A_1U + B_1V = 1$. En multipliant par G, nous obtenons l'égalité voulue : $AU + BV = G$.

(ii) $\Leftarrow$ 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 ».

Lemme 6.55 ([164])**.**
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

(1) S *divise* $\operatorname{pgcd}(P, Q)$

(2) $\deg(S) \leqslant \deg\big(\operatorname{pgcd}(P, Q)\big)$.

Démonstration. Il faut bien relire la définition 1.180 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 $\operatorname{pgcd}(P, Q)$. □

Lemme 6.56 ([163])**.**
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 6.50 : $B|Q_1$.

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. □

Lemme 6.57 ([163])**.**
Quelques propriétés du PGCD[24] *dans les polynômes. Soient des polynômes $P, Q, R \in \mathbb{K}[X]$.*

(1) Nous avons l'égalité[25]

$$\operatorname{pgcd}(P, PQ + R) = \operatorname{pgcd}(P, R). \tag{6.120}$$

(2) Si Q et R sont premiers entre eux,

$$\operatorname{pgcd}(P, QR) = \operatorname{pgcd}(P, Q)\operatorname{pgcd}(P, R) \tag{6.121}$$

(3) Si P et Q sont premiers entre eux,

$$\operatorname{pgcd}(P, QR) = \operatorname{pgcd}(P, R) \tag{6.122}$$

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 1.180.
25. Notez l'analogie avec le lemme 3.6.

(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

$$R = AB_2 - PQ = AB_2 - AB_1Q = A(B_2 - B_1Q), \tag{6.123}$$

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

$$PQ + R = AB_1Q + AB_2 = A(B_1Q + B_2), \tag{6.124}$$

et A divise $PQ + R$.
Conclusion : les paires $\{P, PQ+R\}$ et $\{P, R\}$ ont même ensemble de diviseurs, et donc même pgcd.

(2) 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 6.54.

(i) $\exists U, V$ **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 6.54). On a de même : $G_2 = PU_2 + RV_2$. En prenant le produit :

$$G_1G_2 = (PU_1 + QV_1)(PU_2 + RV_2) = P(PU_1U_2 + RU_1V_2 + QV_1V_2) + QR(V_1V_2). \tag{6.125}$$

Donc c'est bon pour ce point.

(ii) 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 1.252).

(iii) $G_1G_2 \mid QR$ En effet : $G_1|Q$ et $G_2|R$ donc $G_1G_2|QR$.

(iv) $G_1G_2 \mid P$ 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 6.56 conclut que P est divisible par G_1G_2.

(3) Supposons d'abord que $A \in \mathbb{K}[X]$ divise P et QR. Le théorème de Bézout 6.47 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 :

$$1 = PU + QV = AB_1U + QV. \tag{6.126}$$

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 6.50.
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.

□

6.4 Extension de corps

Lemme 6.58.
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*

$$\text{Card}(\mathbb{L}) = \text{Card}(\mathbb{K})^s. \tag{6.127}$$

26. Définition 1.202.

Démonstration. Le corps $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie. Si s est la dimension alors nous avons la formule (6.127) parce que chaque élément de $\mathbb{L}$ est un s-uple d'éléments de $\mathbb{K}$. □

Définition 6.59 ([165])**.**
Soit $\mathbb{K}$ un corps commutatif. Une ***extension*** *de $\mathbb{K}$ est un couple $(\mathbb{L}, j)$ où $\mathbb{L}$ est un corps et $j : \mathbb{K} \to \mathbb{L}$ 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 $\mathbb{K}$.

Lemme-Définition 6.60.
Si $(\mathbb{L}, i)$ est une extension de $\mathbb{K}$, alors $\mathbb{L}$ devient un espace vectoriel sur $\mathbb{K}$ si nous posons

$$\lambda \cdot x = i(\lambda)x \tag{6.128}$$

pour tout $\lambda \in \mathbb{K}$ et $x \in \mathbb{L}$. La multiplication du membre de droite est celle du corps $\mathbb{L}$.

Définition 6.61.
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.*

Exemple 6.62.
L'ensemble $\mathbb{C}$ est une extension de $\mathbb{R}$ et son degré est $[\mathbb{C} : \mathbb{R}] = 2$. △

Proposition 6.63 (Composition des degrés[166])**.**
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 :

$$[\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_2 : \mathbb{L}_1][\mathbb{L}_1 : \mathbb{K}]. \tag{6.129}$$

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 (6.129) 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

$$a = \sum_\alpha a_\alpha w_\alpha. \tag{6.130}$$

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 :

$$a = \sum_{\alpha i} a_{\alpha i} v_i w_\alpha, \tag{6.131}$$

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

$$\sum_{\alpha i} a_{\alpha i} v_i w_\alpha = 0. \tag{6.132}$$

En récrivant sous la forme

$$\sum_\alpha \Big(\sum_i a_{\alpha i} v_i \Big) w_\alpha = 0, \tag{6.133}$$

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 : $a_{\alpha i} = 0$. □

6.4.1 Extension et polynôme minimal

Lemme-Définition 6.64 (Polynôme minimal)**.**
Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $a \in \mathbb{L}$. Nous considérons la partie

$$I_a = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\} \tag{6.134}$$

que nous supposons non réduite à $\{0\}$[27]

(1) La partie I_a est un idéal dans $\mathbb{K}[X]$,

(2) la partie I_a est un idéal principal dans $\mathbb{K}[X]$,

(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.

(i) **Pour (1)** Soit $P \in I_a$: $P(a) = 0$. Si $Q \in \mathbb{K}[X]$ alors la proposition 1.356 nous indique que

$$(PQ)(a) = P(a)Q(a) = 0. \tag{6.135}$$

Donc $PQ \in I_a$. Comme de plus I_a est clairement vectoriel, I_a est un idéal.
Notez que nous avons utilisé la règle du produit nul justifiée par le fait que $\mathbb{K}$ soit un corps[28] et donc soumis au point (3) de la proposition 1.192.

(ii) **Pour (2)** Nous savons par le théorème 6.43 que $\mathbb{K}[X]$ est un anneau principal. En particulier, tous ses idéaux sont principaux, c'est dans la définition 1.221 d'un anneau principal.

(iii) **Pour (3)** Le théorème 6.43(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.

6.65.
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 9.91.

Exemple 6.66.
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 $\mathbb{Q}[X]$. △

Proposition 6.67 ([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

(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.

27. 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.
28. Si vous connaissez un contre-exemple à cette proposition dans le cas où $\mathbb{K}$ serait remplacé par un anneau, écrivez-moi.
29. Définition 1.183.
30. Définition 3.106.

(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

$$0 = P(a)Q(a). \tag{6.136}$$

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 :

$$\mu_a = S\mu_a Q \tag{6.137}$$

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.

(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

$$0 = \mu_a(a) = P(a)k, \tag{6.138}$$

donc $P(a) = 0$. Mais alors

$$Q(a) = P(a)R_2(a) = 0, \tag{6.139}$$

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.

□

Définition 6.68.
*Deux éléments α et β dans $\mathbb{L}$ sont dit **conjugués** s'ils ont même polynôme minimal. Par exemple i et $-i$ sont conjugués dans $\mathbb{C}$ vu comme extension de $\mathbb{Q}$.*

6.4.2 Extensions algébriques et éléments transcendants

6.4.2.1 Éléments algébriques et transcendants

6.69.
Mise en garde pour les gens qui aiment avoir des notations précises. Dans les lemmes 6.71 et 6.73 ainsi que dans la définition 6.75 il faut garder en tête qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est une application $\iota : \mathbb{K} \to \mathbb{L}$. 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.

Définition 6.70.
L'ensemble $A[X]$ devient un $\mathbb{K}$-espace vectoriel avec la définition

$$(\lambda P)_k = \lambda P_k. \tag{6.140}$$

Voici une définition d'un élément algébrique sur un corps. Une caractérisation plus « pratique » sera donnée dans le lemme 6.73.

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 1.193 et qu'un anneau intègre est justement un anneau sur lequel nous avons la règle du produit nul, voir la définition 1.192.

Lemme-Définition 6.71 (Élément algébrique et transcendant[167]).
Soit une extension $\mathbb{L}$ de $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned}\varphi\colon \mathbb{K}[X] &\to \mathbb{L}\\ P &\mapsto P(\alpha).\end{aligned} \tag{6.141}$$

Alors

(1) L'application φ est un morphisme d'anneaux[33].

(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 1.356 déjà prouvé.

Pour le morphisme de $\mathbb{K}$-espace vectoriel, il faut seulement ajouter le calcul

$$\varphi(\lambda P) = (\lambda P)(\alpha) = \lambda P(\alpha) = \lambda\varphi(P). \tag{6.142}$$

Notons la justification suivante qui n'est pas tout à fait triviale :

$$(\lambda P)(\alpha) = \sum_k (\lambda P)_k \alpha^k = \sum_k \lambda P_k \alpha^k = \lambda P(\alpha) \tag{6.143}$$

qui utilise la définition 6.70. □

Exemple 6.72.
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 6.71.

Lemme 6.73.
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 6.71. 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. □

Définition 6.74.
*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 12.90 que $\mathbb{C}$ est un corps algébriquement clos.

Définition 6.75 (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*[34] *sur $\mathbb{K}$, c'est-à-dire sont racines de polynômes à coefficients dans $\alpha(\mathbb{K})$, voir le lemme 6.73.*

33. Définition 1.40.
34. Définition 6.71.

(2) *L'extension* $\mathbb{L}$ *est* ***algébriquement close*** *si le corps* $\mathbb{L}$ *est algébriquement clos (définition 6.74).*

(3) *L'extension* $\mathbb{L}$ *est une* ***clôture algébrique*** *du corps* $\mathbb{K}$ *si elle est une extension algébrique qui est algébriquement close.*

6.76.
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.

Exemple 6.77.
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 6.130. △

Lemme 6.78.
Un corps est algébriquement clos si et seulement si tous ses polynômes sont scindés[35].

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 3.122 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,

$$P = (X-a_n)Q = \prod_{k=1}^{n}(X-a_k) \tag{6.144}$$

et P est scindé. □

Lemme 6.79.
Soient un corps $\mathbb{K}$ *et un polynôme* $P \in \mathbb{K}[X]$. *Nous supposons que* P *est scindé :*

$$P = \prod_{k=1}^{n}(X-a_k). \tag{6.145}$$

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

$$\prod_{k=1}^{n}(\alpha-a_k) = 0 \tag{6.146}$$

Un corps est toujours un anneau intègre (lemme 1.193), c'est-à-dire que la règle du produit nul est utilisable. Dans notre cas, le produit nul (6.146) nous indique que $\alpha - a_k = 0$ pour (au moins) un des k. Donc effectivement α est l'un des a_k. □

Lemme 6.80.
Soient un corps algébriquement clos $\mathbb{K}$ *ainsi qu'une extension algébrique* $\alpha\colon \mathbb{K} \to \mathbb{L}$. *Alors* $\alpha(\mathbb{K}) = \mathbb{L}$.

35. Définition 6.39

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 6.78) :

$$Q = \prod_{k=1}^{n}(X - b_k) \tag{6.147}$$

avec $b_k \in \mathbb{K}$. Nous avons alors aussi la factorisation

$$P = \prod_{k=1}^{n}(X - \alpha(b_k)) \tag{6.148}$$

dans $\mathbb{L}[X]$. Nous avons vu que l était une racine de P. Donc l est un des $\alpha(b_k)$ (lemme 6.79). Cela prouve que $l \in \alpha(\mathbb{K})$. □

6.4.3 Extension algébrique et polynôme minimal

Proposition 6.81 ([91])**.**
Soit une extension algébrique[36] $\mathbb{L}$ *du corps* $\mathbb{K}$*.*

(1) Pour tout $a \in \mathbb{L}$*, il existe un polynôme* $P \in \mathbb{K}[X]$ *tel que* $P(a) = 0$*.*

(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 6.75 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 6.64 et le fait qu'il soit irréductible est la proposition 6.67(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 $\mu_1 = \mu$. □

Lemme 6.82.
Soient un corps $\mathbb{K}$*, une extension* $\mathbb{L}$ *de* $\mathbb{K}$ *et* $\alpha \in \mathbb{L}$*, un élément algébrique*[37] *sur* $\mathbb{K}$*. Si* μ *est le polynôme minimal de* α *sur* $\mathbb{K}$ *alors*

$$\begin{aligned}\varphi\colon \mathbb{K}[\alpha] &\to \mathbb{K}[X]/(\mu)\\ Q(\alpha) &\mapsto \bar{Q}\end{aligned} \tag{6.149}$$

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 6.64.

Ensuite, le fait que $\mathbb{K}[X]/(\mu)$ soit un corps est le corolaire 6.44. 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.

36. Définition 6.75.
37. Définition 6.71.

(i) **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 3.98. 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

$$Q_1(\alpha) = Q_2(\alpha) + R(\alpha), \tag{6.150}$$

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 $\bar{Q}_1 = \bar{Q}_2$.

(ii) **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.

(iii) **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 $\varphi\big(Q_1(\alpha) + Q_2(\alpha)\big) = \varphi\big((Q_1 + Q_2)(\alpha)\big) = \overline{Q_1 + Q_2} = \bar{Q}_1 + \bar{Q}_2$.

□

6.4.4 Extensions et polynômes

Nous savons déjà depuis la définition 1.352 ce qu'est $A[X]$ pour tout anneau A et donc, à fortiori, pour un corps.

Définition 6.83.
Soit un corps commutatif[38]*. Nous notons $\mathbb{K}(X)$ le corps des fractions*[39] *de $\mathbb{K}[X]$.*

Lemme-Définition 6.84.
Si $R \in \mathbb{K}(X)$, avec $R = P/Q$ et si $\mathbb{L}$ est une extension[40] *de $\mathbb{K}$ contenant l'élément α, alors nous définissons*

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \tag{6.151}$$

Cela est une bonne définition au sens où elle ne dépend pas du choix du représentant (P, Q) pris dans la classe P/Q.

Démonstration. Supposons $R = P_1/Q_1 = P_2/Q_2$. Par définition des classes (définition 1.362) nous avons

$$P_1Q_2 = Q_1P_2. \tag{6.152}$$

Puisque l'évaluation est un morphisme $\mathbb{K}[X] \to \mathbb{K}$[41] nous pouvons évaluer l'équation (6.152) en α :

$$P_1(\alpha)Q_2(\alpha) = Q_1(\alpha)P_2(\alpha). \tag{6.153}$$

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

$$P_1(\alpha)Q_1(\alpha)^{-1} = P_2(\alpha)Q_2(\alpha)^{-1}, \tag{6.154}$$

38. Sauf mention du contraire, tous les corps du Frido sont commutatifs.
39. Définition 1.362.
40. Définition 6.59.
41. Lemme 1.356. Certes ce lemme ne parle que d'anneaux, mais à y bien penser, dans le passage de (6.152) à (6.153), nous ne considérons que les structures d'anneaux sur $\mathbb{K}[X]$ et $\mathbb{K}$.

c'est-à-dire

$$(P_1/Q_1)(\alpha) = (P_2/Q_2)(\alpha). \tag{6.155}$$

□

Proposition-Définition 6.85 ([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[42] 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 $j_{\mathbb{L}}$. □

Lemme 6.86.
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

$$\alpha = x + y\sqrt{n}. \tag{6.156}$$

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

$$\sqrt{n} = \frac{x-a}{b-y}. \tag{6.157}$$

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 6.87.
Nous avons

$$\mathbb{Q}(\sqrt{2})_{\mathbb{R}} = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}} \tag{6.158}$$

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 $\sqrt{2}\sqrt{2} = 2$. △

Lemme 6.88.
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[43]

$$\psi\colon \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \to \mathbb{Q}(\sqrt{3})_{\mathbb{R}}. \tag{6.159}$$

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

$$\psi(\alpha)^2 - 2 = \psi(\alpha^2) - \psi(2) = \psi(\alpha^2 - 2) = \psi(0) = 0. \tag{6.160}$$

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 $\mathbb{Q}(\sqrt{3})_{\mathbb{R}}$. □

42. Définition 6.59.
43. Définition 1.40. Oui, c'est un bête morphisme d'anneaux. Il n'y a pas plus de structure dans un corps que dans un anneau.

Exemple 6.89.
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 [44] $\mathbb{K}(\alpha)_{\mathbb{L}_2} = \mathbb{K}(\alpha)_{\mathbb{L}}$.

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

$$\{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}, \tag{6.161}$$

de $\mathbb{R}$.

Mais cette fois nous définissons la multiplication suivante :

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 3bd + (ad + bc)\sqrt{2}. \tag{6.162}$$

C'est un corps parce que tout élément non nul est inversible. En effet, l'équation

$$(a + b\sqrt{2})(x + y\sqrt{2}) = 1 \tag{6.163}$$

donne

$$\begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{6.164}$$

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

$$a^2 - 3b^2 = 0. \tag{6.165}$$

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 (6.163) 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

$$\begin{aligned} \psi\colon \mathbb{K} &\to \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \\ a + b\sqrt{2} &\mapsto a + b\sqrt{3} \end{aligned} \tag{6.166}$$

est un isomorphisme de corps. Pour le produit, nous avons

$$\begin{aligned} \psi\big((a + b\sqrt{2})(c + d\sqrt{2})\big) &= \psi\big(ac + 3bd + (ad + bc)\sqrt{2}\big) && \text{(6.167a)} \\ &= ac + 3bd + (ad + bc)\sqrt{3} && \text{(6.167b)} \\ &= (a + b\sqrt{3})(c + d\sqrt{3}) && \text{(6.167c)} \\ &= \psi(a + b\sqrt{2})\psi(c + d\sqrt{2}). && \text{(6.167d)} \end{aligned}$$

Remarques :

— L'application ψ est bien définie grâce au lemme 6.86 couplé au théorème 3.36 appliqué à $n = 2$ et $n = 3$.

— Dans le membre de gauche de (6.167a), $b\sqrt{2}$ est un produit dans $\mathbb{R}$ (d'où l'importance du lemme 6.86 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 (6.167b) et (6.167c), tous les produits sont dans $\mathbb{R}$.

En comparant avec le lemme 6.88, nous avons alors

$$\mathbb{Q}(\sqrt{2})_{\mathbb{K}} = \mathbb{Q}(\sqrt{3})_{\mathbb{R}} \neq \mathbb{Q}(\sqrt{2})_{\mathbb{R}} \tag{6.168}$$

△

44. Vérifiez-le tout de même.

6.90.
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 [45]), 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 $\mathbb{Q}(\sqrt{2})$.

Exemple 6.91.
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. △

Définition 6.92.
Soit une extension [46] *de corps $j : \mathbb{K} \to \mathbb{L}$. Soit $A \subset \mathbb{L}$.*

(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 [47], 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 6.93.
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 6.94.
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 6.95.
Nous avons déjà vu à l'occasion de la définition 1.352 que $A[X]$ est l'anneau de tous les polynômes de degré fini en X. Cela rentre dans le cadre de la définition 6.92 parce qu'un anneau contenant X doit contenir tous les X^n.

45. En lisant quelques pages de Wikipédia, vous pourrez briller en société, mais ne tentez pas le coup à l'agrégation.
46. Définition 6.59.
47. 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 $\mathbb{L}$.

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 [48]. Par contre, $\mathbb{K}(X)$ est un corps parce qu'il contient également les fractions rationnelles. △

Exemple 6.96.
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 $\mathbb{K}$.

Proposition 6.97 ([1]).
Soit une extension $\mathbb{L}$ du corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$. Alors nous avons les isomorphismes de corps suivants :

(1) $\mathbb{K}(\alpha)_{\mathbb{L}} = \text{Frac}\big(\mathbb{K}[\alpha]_{\mathbb{L}}\big)$,

(2) $\mathbb{K}(\alpha)_{\mathbb{L}} = \{R(\alpha)_{\mathbb{L}}$ *tel que* $R \in \mathbb{K}(X)\}$.

Démonstration. Le corps $\mathbb{K}(\alpha)$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}[\alpha]$ comme sous-anneau. La proposition 1.363 nous dit alors que l'application suivante est un morphisme injectif de corps :

$$\begin{aligned}\epsilon\colon \text{Frac}\big(\mathbb{K}[\alpha]\big) &\to \mathbb{K}(\alpha)\\ P/Q &\mapsto PQ^{-1}.\end{aligned} \tag{6.169}$$

Pour rappel, la notation P/Q est bien une notation pour la classe d'équivalence du couple (P, Q) pour la relation définie en 1.362.

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 $\mathbb{K}(\alpha)$ [49]. Cela prouve que

$$\mathbb{K}(\alpha) \subset \epsilon\Big(\text{Frac}\big(\mathbb{K}[\alpha]\big)\Big). \tag{6.170}$$

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 1.365 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

$$R(\alpha) = P(\alpha)Q(\alpha)^{-1}. \tag{6.171}$$

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

$$\{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\} \subset \mathbb{K}(\alpha). \tag{6.172}$$

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 6.89 ? Lorsque nous écrivons

$$\mathbb{K}(\alpha) = \{R(\alpha) \text{ tel que } R \in \mathbb{K}(X)\}, \tag{6.173}$$

48. Lorsqu'on multiplie, les degrés montent toujours.
49. Pour rappel, la définition 6.92(1) donne $\mathbb{K}(\alpha)$ comme une intersection.

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 6.89, et en réalité $\mathbb{K}(\alpha)$ peut ne pas être ce que l'on croit.

Le corolaire suivant montre que les choses s'arrangent.

Corolaire 6.98.
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

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \mathbb{K}(\alpha)_{\mathbb{L}_2}. \tag{6.174}$$

Démonstration. La proposition 6.97 nous dit que

$$\mathbb{K}(\alpha)_{\mathbb{L}_1} = \{R(\alpha)_{\mathbb{L}_1} \text{ tel que } R \in \mathbb{K}(X)\} \tag{6.175a}$$
$$\mathbb{K}(\alpha)_{\mathbb{L}_2} = \{R(\alpha)_{\mathbb{L}_2} \text{ tel que } R \in \mathbb{K}(X)\}. \tag{6.175b}$$

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 $\mathbb{C}$.

Proposition 6.99.
Soit un corps $\mathbb{K}$, une extension $\mathbb{L}$ et un élément $\alpha \in \mathbb{L}$. Nous considérons l'application

$$\begin{aligned}\varphi\colon \mathbb{K}[X] &\to \mathbb{L}\\ P &\mapsto P(\alpha).\end{aligned} \tag{6.176}$$

(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[50] 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 3.98). Donc φ est surjective sur $\mathbb{K}[\alpha]$, et est donc bijective. Elle est un isomorphisme[51] parce que le lemme 6.71 dit déjà que c'est un morphisme.

(2) Nous supposons encore que α est transcendant et nous considérons l'application

$$\begin{aligned}\psi\colon \mathbb{K}(X) &\to \mathbb{K}(\alpha)\\ P &\mapsto R(\alpha).\end{aligned} \tag{6.177}$$

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 6.97(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 $\mathbb{L}$).

50. Définition 6.64.

51. 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 ».

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 6.64.

□

Proposition 6.100.
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[52] *tout polynôme annulateur.*

Autrement dit, l'idéal engendré par le polynôme minimal est l'idéal des polynômes annulateurs.

Démonstration. Nous considérons l'idéal

$$I = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}. \tag{6.178}$$

Le fait que cela soit un idéal est simplement dû à la définition du produit : $(PQ)(a) = P(a)Q(a)$. Par le théorème 6.43, 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. □

6.4.4.1 Extension algébrique, degré

Proposition 6.101.
Toute extension finie est algébrique.

Démonstration. Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ de degré[53] 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 4.11 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. □

Proposition 6.102 (Propriétés d'extensions algébriques[1])**.**
Soit $\mathbb{K}$ un corps commutatif[54] *et a un élément algébrique*[55] *sur $\mathbb{K}$, de polynôme minimal μ_a de degré n. Alors*

(1) En considérant l'application d'évaluation

$$\begin{aligned} \varphi_a \colon \mathbb{K}[X] &\to \mathbb{L} \\ Q &\mapsto Q(a), \end{aligned} \tag{6.179}$$

nous avons $\mathbb{K}[a] = \text{Image}(\varphi_a)$.

(2) Une base de $\mathbb{K}[a]$ comme espace vectoriel sur $\mathbb{K}$ est donnée par $\{1, a, a^2, \dots, a^{n-1}\}$.

(3) Le degré de l'extension $\mathbb{K}[a]$ est égal au degré du polynôme minimal :

$$\big[\mathbb{K}[a] : \mathbb{K}\big] = n. \tag{6.180}$$

(4) L'anneau $\mathbb{K}[a]$ est l'ensemble des polynômes en a de degré jusqu'à $n-1$ à coefficient dans $\mathbb{K}$.

(5) $\mathbb{K}(a) = \mathbb{K}[a]$.

52. Définition 3.103.
53. Définition 6.61.
54. Juste en passant nous rappelons que tous les corps considérés ici sont commutatifs
55. Définition 6.71.

(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 6.64, 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 :

$$Q(X) = Q_1(X) + X^n Q_2(X) \tag{6.181}$$

où $\deg(Q_1) \leqslant n-1$ et $\deg(Q_2) = p - n$. Nous évaluons cette égalité en a :

$$Q(a) = Q_1(a) + S(a)Q_2(a). \tag{6.182}$$

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 6.67). Donc le théorème de Bézout 6.47 affirme l'existence d'éléments $U, V \in \mathbb{K}[X]$ tels que

$$U\mu_a + VQ = 1 \tag{6.183}$$

dans $\mathbb{K}[X]$. Nous évaluons cette égalité en a en tenant compte de $\mu_a(a) = 0$ dans $\mathbb{K}[a]$:

$$U(a)\mu_a(a) + V(a)Q(a) = 1 \tag{6.184}$$

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

$$\begin{aligned} \psi\colon \mathbb{K}[X]/(\mu_a) &\to \mathbb{K}[a] \\ \bar{R} &\mapsto R(a) \end{aligned} \tag{6.185}$$

et nous montrons qu'elle convient. Pour cela, nous nous souvenons que la proposition 6.100 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 1.205 de l'idéal (μ_a). Cela étant mis au point, nous passons à la preuve.

(i) **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 $Q(a) = 0$.

(ii) **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 $x = \psi(\bar{Q})$.

(iii) **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 6.103.
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 6.102. Du point de vue de Bézout, $\mu_{\sqrt{2}}(X) = X^2 - 2$, et nous cherchons des polynômes U et V tels que

$$U(X^2 - 2) + VX = 1. \tag{6.186}$$

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 $\sqrt{2}$:

$$V(\sqrt{(2)}) = \frac{1}{2}\sqrt{2}. \tag{6.187}$$

△

Proposition 6.104 ([167]).
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 :

(1) *α est algébrique sur $\mathbb{K}$,*

(2) *$\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$,*

(3) *$\mathbb{K}[\alpha]$ est un $\mathbb{K}$-espace vectoriel de dimension finie.*

Si ces affirmation 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.

(i) **(1) implique (2)** Soit α algébrique sur $\mathbb{K}$. Nous considérons le polynôme minimal de α sur $\mathbb{K}$ (définition 6.64). Nous savons par le lemme 6.82 (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 1.237 dit que (μ) est un idéal maximum ; la proposition 1.239 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 $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

(ii) **(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 6.99(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.

(iii) **(1) implique (3)** L'élément α est maintenant algébrique et nous considérons son polynôme minimal μ. Nous savons par le lemme 6.82 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.

(iv) **(3) implique (1)** Nous démontrons la contraposée. En supposant que α est transcendant nous avons $\mathbb{K}[\alpha] = \mathbb{K}[X]$ par la proposition 6.99. Or $\mathbb{K}[X]$ n'est pas de dimension finie sur $\mathbb{K}$, donc $\mathbb{K}[\alpha]$ non plus.

□

Lemme 6.105 ([168]).
Soit $\mathbb{L}$ un corps commutatif et $(\mathbb{K}_i)_{i\in I}$ une famille de sous-corps de $\mathbb{L}$. Alors $\bigcup_{i\in I}\mathbb{K}_i$ est un sous-corps de $\mathbb{L}$.

Lemme 6.106.
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 6.44. Nous identifions $\mathbb{K}$ avec $\phi(\mathbb{K})$ où

$$\phi\colon \mathbb{K}[X] \to \mathbb{L} \tag{6.188}$$

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 $Q = \sum_i Q_i a^i$. □

Proposition 6.107 ([91]).
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

$$I_a = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}; \tag{6.189a}$$
$$I_b = \{Q \in \mathbb{K}[X] \text{ tel que } Q(b) = 0\}. \tag{6.189b}$$

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

$$P = \mu_a Q. \tag{6.190}$$

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 6.67, 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 (6.190) 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 6.108.
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. △

6.4.5 Racines de polynômes

Corolaire 6.109 (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 6.100 : 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. □

Avant de lire l'énoncé suivant, allez relire la définition 3.96 pour savoir ce qu'est un polynôme nul.

Théorème 6.110 (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 $\alpha_1, \ldots, \alpha_{n+1}$, 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

$$\begin{cases} a\alpha + b = 0 & (6.191a) \\ a\beta + b = 0. & (6.191b) \end{cases}$$

La différence entre les deux donne $a(\alpha - \beta) = 0$. Puisque $\alpha \neq \beta$, la règle du produit nul (lemme 1.193) 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 6.109 nous donne un polynôme Q de degré n tel que

$$P = (X - \alpha_1)Q. \tag{6.192}$$

Étant donne que pour tout $i \neq 1$ nous avons $\alpha_i \neq \alpha_1$,

$$0 = P(\alpha_i) = \underbrace{(\alpha_i - \alpha_1)}_{\neq 0} Q(\alpha_i), \tag{6.193}$$

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 (6.192) sont alors également nuls. □

Exemple 6.111.
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 6.184 une condition pour qu'un polynôme à plusieurs variables s'annule du fait qu'il ait « trop » de racines. △

Remarque 6.112.
L'intérêt du théorème 6.110 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 13.25.

6.4.6 Corps de rupture

Définition 6.113.
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 $\mathbb{L} = \mathbb{K}(a)$.*

6.114.
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 6.4.11.

Exemple 6.115.
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 $\mathbb{L}$:

$$P = (X - \sqrt{2})(X + \sqrt{2}). \tag{6.194}$$

Le corps $\mathbb{Q}(\sqrt{2})$ est donc un corps de rupture pour P. △

Exemple 6.116.
Dans l'exemple 6.115, nous avions un corps de rupture dans lequel le polynôme P était scindé. Il n'en est pas toujours ainsi. Prenons

$$P = X^3 - 2 \tag{6.195}$$

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 6.117.
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.

Lemme 6.118.
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 3.105. Donc $\mathbb{K}[X]/(P)$ sera un corps si et seulement si (P) est un idéal maximum (proposition 1.213), et cela sera le cas si et seulement si (P) est engendré par un polynôme irréductible (proposition 1.237).

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. □

Proposition 6.119 (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 6.59). Le fait que ce soit un corps est le lemme 6.118. 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 1.301).

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 1.19.2.2, 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).

(i) $P(\bar{X}) = 0$ C'est le moment de nous souvenir comment la notation des X fonctionne, et en particulier la pirouette autour de (1.490). 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

$$P(\bar{X}) = \overline{P(X)} = \bar{P} = 0. \tag{6.196}$$

(ii) **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 3.94 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 6.120.
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 :

$$(X + \bar{X})(X - \bar{X}) = X^2 - \bar{X}^2 = X^2 + 1, \tag{6.197}$$

c'est-à-dire que P est bien factorisé, et que nous avons retrouvé la multiplication $x^2 + 1 = (x + i)(x - i)$. △

6.121.
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

$$P = X^4 - X^2 - 2 \tag{6.198}$$

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 $\mathbb{Q}(i)$.

6.122.
La proposition suivante donne une unicité du corps de rupture dans le cas d'un polynôme irréductible. Et nous comprenons pourquoi : un polynôme irréductible n'a fondamentalement qu'une seule racine « indépendante ». Par exemple $X^2 - 2$ a pour racines $\pm\sqrt{2}$. Autre exemple, le polynôme $X^2 + 6X + 13$ a pour racines, dans $\mathbb{C}$, les nombres complexes conjugués $z = -3 + 2i$ et $\bar{z} = -3 - 2i$.

Proposition 6.123 ([161]).
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

$$\psi\colon \mathbb{K}[X]/(P) \to \mathbb{L} \tag{6.199}$$

tel que $\psi(\bar{X}) = \alpha$.

Dans un tel cas,

(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 6.64 s'applique donc et nous avons μ, le polynôme minimal de α dans $\mathbb{K}[X]$. Il divise P qui est irréductible, donc

$$P = \lambda\mu \tag{6.200}$$

pour un certain $\lambda \in \mathbb{K}$.

Nous posons

$$\begin{aligned} \psi\colon \mathbb{K}[X]/(P) &\to \mathbb{L} \\ \bar{Q} &\mapsto Q(\alpha). \end{aligned} \tag{6.201}$$

(i) **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 $\psi(\bar{Q}_1) = Q_1(\alpha) = Q_2(\alpha) + R(\alpha)P(\alpha) = Q_2(\alpha)$.

(ii) **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 $\bar{Q}_1 = \bar{Q}_2$.

(iii) **Morphisme** Laissé comme exercice ; la paresse de l'auteur de ces lignes attend vos contributions.

(iv) **La condition** Le morphisme ψ respecte de plus la condition

$$\psi(\bar{X}) = X(\alpha) = \alpha. \tag{6.202}$$

En ce qui concerne l'unicité, fixer $\psi(\bar{X})$ est suffisant pour fixer un morphisme. En effet si $\psi(\bar{X}) = \alpha$, alors

$$\psi(\bar{Q}) = \psi\Big(\sum_k a_k \bar{X}^k\Big) = \sum_k a_k \psi(\bar{X})^k = \sum_k a_k \alpha^k. \tag{6.203}$$

Pour le second point de l'énoncé, il faut remarquer que α est algébrique et non transcendant. Donc en utilisant les propositions 3.98 et 6.102(5) nous trouvons

$$\text{Image}(\psi) = \{Q(\alpha) \text{ tel que } Q \in \mathbb{K}[X]\} = \mathbb{K}[\alpha] = \mathbb{K}(\alpha). \tag{6.204}$$

Et finalement pour le dernier point, un morphisme de corps est toujours injectif. Si il est également surjectif, il sera bijectif. □

6.4.7 Pile d'extensions

Lemme 6.124 ([1]).
Soient un corps $\mathbb{K}$, des extensions $\mathbb{L}_1, \ldots, \mathbb{L}_n$ et des éléments $\alpha_i \in \mathbb{L}_i$ tels que

$$\mathbb{L}_1 = \mathbb{K}(\alpha_1)_{\mathbb{L}_1} \tag{6.205}$$

et

$$\mathbb{L}_k = \mathbb{L}_{k-1}(\alpha_k)_{\mathbb{L}_k}. \tag{6.206}$$

Alors

$$\mathbb{L}_n = \mathbb{K}(\alpha_1, \ldots, \alpha_n)_{\mathbb{L}_n}. \tag{6.207}$$

Démonstration. Nous démontrons par récurrence sur n. Le cas $n = 1$ est simplement l'hypothèse (6.205).

Supposons donc que le lemme soit correct pour n, et étudions le cas $n + 1$. Nous avons, par définition et par hypothèse de récurrence :

$$\mathbb{L}_{n+1} = \mathbb{L}_n(\alpha_{n+1})_{\mathbb{L}_{n+1}} = \Big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\Big)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \tag{6.208}$$

Notre tâche sera donc de montrer que

$$\Big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\Big)(\alpha_{n+1}) = \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \tag{6.209}$$

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

$$\mathbb{K}(\alpha_1, \dots, \alpha_{n+1}) \subset \big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})_{\mathbb{L}_{n+1}}. \tag{6.210}$$

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 6.97(2), de la forme $r(\alpha_{n+1})$ avec $r \in \mathbb{K}(\alpha_1, \dots, \alpha_n)(X)$, c'est-à-dire

$$P(\alpha_{n+1})Q(\alpha_{n+1})^{-1} \tag{6.211}$$

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

$$P(\alpha_{n+1}) = \sum_i a_i \alpha_{n+1}^i. \tag{6.212}$$

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

$$r(\alpha_{n+1}) = P(\alpha_{n+1})Q(\alpha_{n+1})^{-1}. \tag{6.213}$$

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 :

$$\big(\mathbb{K}(\alpha_1, \dots, \alpha_n)_{\mathbb{L}_n}\big)(\alpha_{n+1})_{\mathbb{L}_{n+1}} \subset \mathbb{K}(\alpha_1, \dots, \alpha_{n+1}). \tag{6.214}$$

Les inclusions (6.210) et (6.214) prouvent l'égalité d'ensembles (6.209) que nous voulions montrer. □

6.4.8 Clôture algébrique

Le concept de clôture algébrique a été défini dans 6.75. Voici un lemme qui dit qu'une clôture algébrique est en quelque sorte une extension algébrique maximale.

Lemme 6.125 ([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[56].

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 6.119 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. □

56. Définition 6.75(2).

6.126.
Nous avons défini le concept d'extension algébrique en 6.75. Nous allons en construire un petit exemple très piéton.

Souvenez vous que la proposition 1.455 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 1.393.

Proposition 6.127 ([169]).
Soit $\mathbb{L} = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}$.

(1) C'est un sous-corps de $\mathbb{R}$.

(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 1.39) 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 $a, b, a', b' \in \mathbb{Q}$,

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2} \in \mathbb{L}. \tag{6.215}$$

— Les neutres 0 et 1 sont dans $\mathbb{L}$.

— Si $\alpha \in \mathbb{L}$, alors $-\alpha \in \mathbb{L}$:

$$-(a + b\sqrt{2}) = -a - b\sqrt{2}. \tag{6.216}$$

— La partie $\mathbb{L}$ est stable pour le produit parce que

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + ba')\sqrt{2}. \tag{6.217}$$

— 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 1.401. Donc pour tout $a, b \in \mathbb{R}$, le nombre

$$\frac{1}{a + b\sqrt{2}} \tag{6.218}$$

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 1.393. Nous pouvons donc faire le coup de multiplier le numérateur et le dénominateur par le binôme conjugué :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}. \tag{6.219}$$

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 6.128.
Soit $\mathbb{L} = \{a + b\sqrt{2}\}_{a,b\in\mathbb{Q}}$.

(1) C'est un espace vectoriel de dimension 2 *sur* $\mathbb{Q}$.

(2) Si $\alpha \in \mathbb{L}$, *alors il existe un polynôme* $P \in \mathbb{L}[X]$ *de degré* 2 *ou moins tel que* $P(\alpha) = 0$.

(3) Le corps $\mathbb{L}$ *est une extension algébrique de* $\mathbb{Q}$.

Démonstration. En plusieurs parties.

(i) **(1)** Pour la dimension, notez que $\{1, \sqrt{2}\}$ est une partie libre et génératrice de $\mathbb{L}$.

(ii) **(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 4.7. 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 $P = cX^2 + bX + a$.

(iii) **(3)** Nous venons de voir que tous les éléments de $\mathbb{L}$ sont des racines de polynômes de $\mathbb{Q}[X]$.

□

Lemme 6.129.
Si $\mathbb{K}$ est un corps infini, alors $\mathbb{K}[X]$ est équipotent[57] *à $\mathbb{K}$.*

Démonstration. Notons provisoirement $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré n. Nous avons une surjection

$$\begin{aligned} \varphi\colon \mathbb{K}^{n+1} &\to \mathbb{K}_n[X] \\ (k_0, \dots, k_n) &\mapsto \sum_{i=0}^{n} k_i X^i. \end{aligned} \tag{6.220}$$

Par récurrence sur le théorème[58] 1.156, nous avons $\mathbb{K}^{n+1} \approx \mathbb{K}$. La surjection (6.220) dit alors que

$$\mathbb{K}_n[X] \preceq \mathbb{K}^{n+1} \approx \mathbb{K}. \tag{6.221}$$

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 1.140 dit alors que $\mathbb{K}_n[X] \approx \mathbb{K}$.

Le lemme 1.157 nous permet alors de conclure que

$$\mathbb{K}[X] = \bigcup_{n=0}^{\infty} \mathbb{K}_n[X] \approx \mathbb{K}. \tag{6.222}$$

□

Proposition 6.130 ([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.

(i) **Si $\mathbb{K}$ est fini** Un polynôme non nul possède toujours au maximum un nombre fini de racines (éventuellement zéro) par la proposition 6.110. Par ailleurs, chaque degré de polynôme ayant seulement un nombre fini de possibilités, l'ensemble $\mathbb{K}[X]$ est au plus dénombrable (proposition 1.133).
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

$$\begin{aligned} \varphi\colon \mathbb{K}[X] \times \mathbb{N} &\to \mathbb{L} \\ (P, n) &\mapsto \varphi_P(n). \end{aligned} \tag{6.223}$$

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 1.130). Il existe donc une surjection d'un ensemble dénombrable vers $\mathbb{L}$. Le lemme 1.132 conclut que $\mathbb{L}$ est fini ou dénombrable.

57. Définition 1.110.
58. 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.

(ii) **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

$$\begin{aligned}\varphi\colon \mathbb{K}[X]\times\mathbb{N}&\to\mathbb{L}\\(P,n)&\mapsto\varphi_P(n).\end{aligned}\tag{6.224}$$

Cette application est encore surjective : $\mathbb{L}\preceq\mathbb{K}[X]\times\mathbb{N}$. Le lemme 6.129 nous assure que $\mathbb{K}[X]\approx\mathbb{K}$ parce que $\mathbb{K}$ est infini. Ensuite la proposition 1.150 nous dit que $\mathbb{K}[X]\times\mathbb{N}\approx\mathbb{K}[X]$. Donc

$$\mathbb{K}\approx\mathbb{K}[X]\approx\mathbb{K}[X]\times\mathbb{N}\geq\mathbb{F}.\tag{6.225}$$

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 1.140 implique que $\mathbb{K}\approx\mathbb{F}$.

□

Lemme 6.131 ([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 $P=\sum_k P_kX^k$. Si $a\in\mathbb{K}$ est une racine de P, alors $\sum_k P_ka^k=0$. 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 $\rho(P)$. □

Lemme 6.132 ([170]).
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 $\sigma|_{\alpha(\mathbb{K})}=\beta$.

Note : 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.

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 6.102 disent que $\mathbb{L}\simeq\mathbb{K}[a]\simeq\mathbb{K}[X]/(\mu_a)$. Pour référence ultérieure, nous considérons un isomorphisme

$$\varphi\colon\mathbb{L}\to\mathbb{K}[X]/(\mu_a).\tag{6.226}$$

Les coefficients de μ_a sont dans $\mathbb{K}$, donc nous pouvons voir $\mu_a\in\mathbb{F}[X]$. Plus précisément, si $\mu_a=\sum_k a_kX^k$, nous définissons

$$\mu'_a=\sum_k\beta(a_k)X^k\in\mathbb{F}[X].\tag{6.227}$$

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

$$\begin{aligned}\sigma'\colon\mathbb{K}[X]/(\mu_a)&\to\mathbb{F}\\\overline{\sum_k s_kX^k}&\mapsto\sum_k\beta(s_k)b^k.\end{aligned}\tag{6.228}$$

(i) **σ' est bien définie** Si $P=\sum_k s_kX^k$ et $\mu_a=\sum_k a_kX^k$ $(a_k,s_k\in\mathbb{K})$, alors

$$\sigma'(\overline{P+\mu_a})=\sigma'\big(\overline{\sum_k(a_k+s_k)X^k}\big)=\sum_k\beta(a_k)b^k+\sum_k s_kb^k=\mu'_a(b)+\sigma'(\overline{P})=\sigma'(\overline{P}).\tag{6.229}$$

(ii) **σ' est un morphisme de corps** À justifier.

(iii) $\varphi\big(\alpha(k)\big) = \bar{k}$ Quand nous parlons de $\bar{k}$, nous parlons de la classe du polynôme de degré zéro donné par $k \in \mathbb{K}$.

(iv) **La réponse** Nous posons

$$\sigma = \sigma' \circ \varphi. \tag{6.230}$$

Pour tout $k \in \mathbb{K}$,

$$(\sigma'\varphi\alpha)(k) = \sigma'(\bar{k}) = \beta(k), \tag{6.231}$$

c'est ce qu'il fallait.

□

Lemme 6.133 ([170]).
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 1.22 sur l'ensemble

$$\mathcal{A} = \left\{ (\mathbb{M}, \varphi) \text{ tel que } \begin{cases} \mathbb{M} \text{ est un sous-corps de } \mathbb{L} \\ \alpha(\mathbb{K}) \subset \mathbb{M} \\ \varphi\colon \mathbb{M} \to \mathbb{F} \text{ est une extension de corps} \\ \varphi \circ \alpha = \beta \end{cases} \right\}. \tag{6.232}$$

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 6.132. Il existe donc un morphisme de corps $\sigma\colon \mathbb{M}(l) \to \mathbb{F}$ tel que $\sigma|_{\mathbb{M}} = \varphi$.

Nous avons

$$\sigma \circ \alpha = \sigma|_{\sigma(\mathbb{K})} \circ \alpha = \sigma|_{\mathbb{M}} \circ \alpha = \varphi \circ \alpha = \beta. \tag{6.233}$$

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. □

Théorème 6.134 (Steinitz[171, 172]).
À propos de clôture algébrique.

(1) Tout corps possède une clôture algébrique[59].

(2) Si $\alpha_1\colon \mathbb{K} \to \mathbb{F}_1$ et $\alpha_2\colon \mathbb{K} \to \mathbb{F}_2$ sont deux clôtures algébriques du même corps $\mathbb{K}$, alors il existe un isomorphisme de corps $\varphi\colon \mathbb{F}_1 \to \mathbb{F}_2$ tel que $\varphi \circ \alpha_1 = \alpha_2$.

Démonstration. Nous commençons par l'existence, en plusieurs points.

(i) **Un ensemble** Nous considérons un ensemble Ω qui contient $\mathbb{K}$, qui est strictement surpotent[60] 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 1.143).

59. Définition 6.75.
60. Définition 1.110.

(ii) **L'ensemble pour Zorn** Nous considérons l'ensemble des extensions algébriques de $\mathbb{K}$ contenues dans Ω, c'est-à-dire

$$\mathcal{A} = \left\{ (\mathbb{L}, +_{\mathbb{L}}, \times_{\mathbb{L}}) \text{ tel que } \begin{cases} \mathbb{K} \subset \mathbb{L} \subset \Omega \\ (\mathbb{L}, +_{\mathbb{L}}, \times_{\mathbb{L}}) \text{ est une extension algébrique de } (\mathbb{K}, +, \times). \end{cases} \right\} \tag{6.234}$$

Nous ordonnons $\mathcal{A}$ par l'inclusion : nous disons que

$$(\mathbb{L}_1, +_1, \times_1) < (\mathbb{L}_2, +_2, \times_2) \tag{6.235}$$

lorsque $(\mathbb{L}_2, +_2, \times_2)$ est un sur-corps de $(\mathbb{L}_1, +_1, \times_1)$ (en particulier $\mathbb{L}_1 \subset \mathbb{L}_2$).

(iii) **$\mathcal{A}$ 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

$$\begin{cases} a +_{\mathbb{L}} b = a +_k b & \text{(6.236a)} \\ a \times_{\mathbb{L}} b = a \times_k b & \text{(6.236b)} \end{cases}$$

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.

(iv) **Lemme de Zorn** Nous utilisons le lemme de Zorn 1.22. 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.

(v) **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 6.125).

(vi) **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 6.130. 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 1.152 permet de dire

$$\mathbb{E}\backslash\mathbb{F} \preceq \mathbb{E} \prec \Omega \approx \Omega\backslash\mathbb{F}. \tag{6.237}$$

(vii) **Quelques injections** Il existe donc une injection $\varphi : \mathbb{E}\backslash\mathbb{F} \to \Omega\backslash\mathbb{F}$. Nous posons

$$\begin{aligned} f : \mathbb{E} &\to \Omega \\ x &\mapsto \begin{cases} x & \text{si } x \in \mathbb{F} \\ \varphi(x) & \text{si } x \notin \mathbb{F}. \end{cases} \end{aligned} \tag{6.238}$$

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 $\varphi(y) \in \Omega\backslash F$; 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 $f : \mathbb{E} \to \Omega$.

(viii) **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 $x \in \mathbb{E}\backslash\mathbb{F}$, alors $f(x) \in \Omega\backslash\mathbb{F}$. Donc en réalité nous avons aussi $\mathbb{E} \subset \mathbb{F}$.

(ix) **Conclusion** En conclusion $\mathbb{E} = \mathbb{F}$ et le lemme 6.125 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 6.133 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 6.79 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 $\sigma \circ \alpha_1 = \alpha_2$. □

6.135.
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.

Lemme 6.136.
Le corps $\mathbb{C}$ n'est pas une clôture algébrique[61] *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 1.378. 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 1.135. Enfin l'ensemble des polynômes à coefficients sur $\mathbb{Q}$ est l'union des polynômes de degré fixés, donc dénombrable par la proposition 1.133.

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 3.126. 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. □

6.4.9 Polynômes à plusieurs variables

Nous avons déjà vu $A[X, Y]$ lorsque A est un anneau en la définition 3.45.

Définition 6.137.
Soit un corps $\mathbb{K}$. Le corps $\mathbb{K}(X_1, \dots, X_n)$ est le corps des fractions de l'anneau $\mathbb{K}[X_1, \dots, X_n]$.

Définition 6.138.
Soient un corps $\mathbb{K}$ et une extension $\mathbb{L}$ de $\mathbb{K}$ contenant les éléments $\alpha_1, \dots, \alpha_n$ 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 6.97(2).

Lemme 6.139 ([1])**.**
Soient un corps $\mathbb{K}$, une extension $\mathbb{L}$ et des éléments $\alpha_1, \dots, \alpha_n$ dans $\mathbb{L}$. Alors

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \{r(\alpha_1, \dots, \alpha_n) \text{ tel que } r \in \mathbb{K}(X_1, \dots, X_n)\}. \tag{6.239}$$

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

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) \subset \big\{r(\alpha_1, \dots, \alpha_n) \text{ tel que } r \in \mathbb{K}(X_1, \dots, X_n)\big\}. \tag{6.240}$$

61. Clôture algébrique, définition 6.75.

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 $r\in\mathbb{K}[X_1,\dots,X_n]$. □

6.4.10 Corps de décomposition

Définition 6.140.
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.

Proposition 6.141 ([173])**.**
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.

(i) **Si racine dans $\mathbb{K}$** Alors le corolaire 6.109 nous permet de factoriser $X-\alpha$:

$$P=(X-\alpha)Q \tag{6.241}$$

avec $\deg(Q)=\deg(P)-1$. Dans ce cas, $\mathbb{K}$ est un corps de rupture de P.

(ii) **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 6.119 qui donne l'existence d'un corps de rupture). Dans $\mathbb{L}_1$ nous avons

$$P=(X-\alpha)Q \tag{6.242}$$

avec $Q\in\mathbb{L}_1[X]$ et $\deg(Q)=\deg(P)-1$.

(iii) **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

$$\mathbb{L}=\mathbb{K}(\alpha_1,\dots,\alpha_{n-1}). \tag{6.243}$$

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

$$\mathbb{D}=\mathbb{K}(\alpha_1,\dots,\alpha_{n-1},\alpha) \tag{6.244}$$

est un corps de décomposition de P. Vu que $\mathbb{D}$ contient $\mathbb{K}(\alpha)$ (comme cas particulier du lemme 6.139), 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

$$Q=(X-\alpha_1)\dots(X-\alpha_{n-1}). \tag{6.245}$$

Donc nous avons dans $\mathbb{D}$ l'égalité

$$P=(X-\alpha)(X-\alpha_1)\dots(X-\alpha_{n-1}). \tag{6.246}$$

□

Lemme 6.142 ([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 6.36.

Le polynôme P est scindé dans $\mathbb{L}$, c'est-à-dire que, en notant n le degré de P,

$$P = \prod_{i=1}^{n}(X - \lambda_i) \tag{6.247}$$

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

$$P = \prod_{k=1}^{n}(X - \mu_k) \tag{6.248}$$

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 (6.247) et (6.248) 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 3.59), 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 $\mathbb{L}$. □

Théorème 6.143 ([161]).
Soient :

(1) un isomorphisme de corps $\tau : \mathbb{K} \to \mathbb{K}'$;

(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 $\sigma : \mathbb{L} \to \mathbb{L}'$.

Démonstration. Soit m le nombre de racines de P dans $\mathbb{L}\backslash\mathbb{K}$. Nous faisons une récurrence sur m.

Si $m = 0$ alors $\mathbb{K}$ est un corps de rupture de P ; nous avons

$$P = (X - \lambda_1) \dots (X - \lambda_n) \tag{6.249}$$

avec $\lambda_i \in \mathbb{K}$. Dans ce cas nous avons aussi

$$\tau(P) = \big(X - \tau(\lambda_1)\big) \dots \big(X - \tau(\lambda_n)\big) \tag{6.250}$$

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 $\mathbb{L}\backslash\mathbb{K}$. Soit

$$P = P_1 \dots P_r \tag{6.251}$$

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 6.36 que $\mathbb{K}[X]$ est un anneau factoriel. Le lemme 6.142 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 6.82 :

$$\begin{aligned}\psi\colon \mathbb{K}[X]/(P_1) &\to \mathbb{K}[\alpha]\\ \bar{Q} &\mapsto Q(\alpha).\end{aligned} \tag{6.252}$$

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

$$\tau(P) = \tau(P_1)\dots\tau(P_r), \tag{6.253}$$

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

$$\psi'\colon \mathbb{K}'[X]/\big(\tau(P_1)\big) \to \mathbb{K}'[\beta]. \tag{6.254}$$

De plus, par le lemme 6.46, nous savons que τ passe aux classes :

$$\phi_\tau\colon \mathbb{K}[X]/(P_1) \to \mathbb{K}'[X]/\big(\tau(P_1)\big) \tag{6.255}$$

est un isomorphisme d'anneaux. Et enfin, dernier résultat externe à invoquer, la proposition 6.102 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 [62] :

$$\tau_1 = \psi' \circ \phi_\tau \circ \psi^{-1}\colon \mathbb{K}_1 \to \mathbb{K}[X]/(P_1) \to \mathbb{K}'[X]/\big(\tau(P_1)\big) \to \mathbb{K}'_1. \tag{6.256}$$

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

$$\begin{array}{ccccc}\mathbb{K} & \xrightarrow{i} & \mathbb{K}_1 & \xrightarrow{i} & \mathbb{L}\\ \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau_1} & & \\ \mathbb{K}' & \xrightarrow[i]{} & \mathbb{K}'_1 & \xrightarrow{i} & \mathbb{L}'\end{array} \tag{6.257}$$

Le corps $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}_1$, et le nombre de racines de P dans $\mathbb{L}\backslash\mathbb{K}_1$ est strictement plus petit que m parce qu'il y en a exactement m dans $\mathbb{L}\backslash\mathbb{K}$ 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 $\mathbb{L}\backslash\mathbb{K}_1$ 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 :

Proposition 6.144.
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 $f|_{\mathbb{K}} = \mathrm{Id}$.

62. 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.

Démonstration. C'est un cas particulier du théorème 6.143, où nous considérons $\mathbb{K} = \mathbb{K}'$ muni de l'isomorphisme identité. □

Cependant le passage par l'énoncé plus compliqué 6.143 est nécessaire pour les besoins de la récurrence.

6.145.
À propos de terminologie. Lorsque nous disons « *un* corps de décomposition » nous référons à la définition 6.140 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 6.141 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.

6.146.
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.

Exemple 6.147.
Soit le polynôme $P = X^4 - 5X^2 + 6$. Sa factorisation en irréductibles est :

$$P = (X^2 - 2)(X^2 - 3). \tag{6.258}$$

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

$$P_1 = X^2 - 2 \tag{6.259a}$$
$$P_2 = X^2 - 3, \tag{6.259b}$$

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

$$P_1 = (X + \sqrt{2})(X - \sqrt{2}). \tag{6.260}$$

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

$$P_2 = (X - \sqrt{3})(X + \sqrt{3}). \tag{6.261}$$

Nous savons (par le lemme 6.124) que

$$\mathbb{L}_2 = \mathbb{L}_1(\sqrt{3}) = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}). \tag{6.262}$$

Nous pouvons donc écrire en toute confiance, dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ la factorisation

$$P = (X + \sqrt{2})(X - \sqrt{2})(X + \sqrt{3})(X - \sqrt{3}). \tag{6.263}$$

Et nous notons que si nous avions commencé par P_2 au lieu de P_1, nous aurions eu le même résultat final. △

Corolaire 6.148 ([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 6.141.

Vu que le lemme 6.124 donne

$$\mathbb{K}(\alpha_1,\dots,\alpha_n) = \big(\mathbb{K}(\alpha_1,\dots,\alpha_{n-1})\big)(\alpha_n), \tag{6.264}$$

le corps $\mathbb{D}$ se construit comme une pile d'extensions finies. Les degrés se composant par le lemme 6.63, au final ce corps de décomposition est une extension finie.

Soit maintenant un corps de décomposition quelconque $\mathbb{L}$. La proposition 6.144 donne un isomorphisme de corps[63] $f\colon \mathbb{L} \to \mathbb{D}$ 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 $\mathbb{K}$[64] ? □

6.4.11 Non irréductible ou pas corps ?

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 $P \in \mathrm{Frac}(A)[X]$ 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 6.149.
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.

△

6.4.12 Clôture algébrique

Théorème 6.150.
Tout corps $\mathbb{K}$ possède une clôture algébrique[65] *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 6.151.
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. □

Exemple 6.152.
Soit p un nombre premier. Montrons que le polynôme

$$Q(X) = X^p - X + 1 \tag{6.265}$$

63. Un isomorphisme de corps est juste un isomorphisme d'anneaux.
64. Personnellement, je n'ai pas vérifié. Vérifiez vous-même et écrivez-moi pour dire si c'est bon ou non.
65. Définition 6.75.

est irréductible dans $\mathbb{F}_p$.

Nous supposons qu'il n'est pas irréductible, c'est-à-dire que

$$Q(X) = R(X)S(X) \tag{6.266}$$

avec R et S, des polynômes de degrés $\geqslant 1$ dans $\mathbb{F}_p[X]$

Soit $\bar{\mathbb{F}}_p$ une clôture algébrique[66] 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

$$\begin{aligned} Q(\alpha + a) &= (\alpha + a)^p - (\alpha + a) + 1 && (6.267a)\\ &= \alpha^p + a^p - \alpha - a + 1 && (6.267b)\\ &= \alpha^p - \alpha + 1 && (6.267c)\\ &= Q(\alpha) && (6.267d)\\ &= 0 && (6.267e) \end{aligned}$$

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

$$R(X) = \prod_{i=1}^{k} \big(X - (\alpha + a_i)\big) \tag{6.268}$$

où les a_i sont les éléments de $\mathbb{F}_p$. En développant un peu,

$$R(X) = X^k - \sum_{i=1}^{k}(\alpha + a_i)X^{k-1} + \text{termes de degré plus bas en } X. \tag{6.269}$$

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 :

$$Q(\alpha) = \alpha^p - \alpha + 1 = 1 \neq 0. \tag{6.270}$$

Le polynôme $X^p - X + 1$ est donc irréductible sur $\mathbb{F}_p$. △

6.4.13 Dérivée de polynômes

Définition 6.153 ([174]).
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***

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}. \tag{6.271}$$

Lemme 6.154 (Règle de Leibnitz[174]).
Soit un anneau A. Nous considérons l'application dérivée[67]

$$\begin{aligned} D\colon A[X] &\to A[X]\\ P &\mapsto P'. \end{aligned} \tag{6.272}$$

(1) L'application D est A-linéaire.

(2) Elle vérifie $(PQ)' = PQ' + P'Q$.

66. Définition 6.75. Pour l'existence c'est le théorème 6.150.
67. Définition 6.153.

Lemme 6.155 ([174]).
Soit un corps $\mathbb{K}$. Nous considérons l'application de dérivation[68] $D: \mathbb{K}[X] \to \mathbb{K}[X]$.

(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

$$\mathbb{K}[X^p] = \{Q(X^p) \text{ tel que } Q \in \mathbb{K}[X]\}. \tag{6.273}$$

6.4.14 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 6.170.

Lemme 6.156 ([174]).
Soit un corps $\mathbb{K}$. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Nous avons équivalence entre :

(1) a est une racine multiple[69] *de P.*

(2) $(X-a) \mid P$ et $(X-a) \mid P'$.

(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

$$P = (X-a)^n Q \tag{6.274}$$

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

$$P' = n(X-a)^{n-1}Q + (X-a)^n Q'. \tag{6.275}$$

Nous faisons maintenant la preuve.

(i) **(1) implique (2)** Nous supposons que a est une racine multiple, c'est-à-dire $n \geqslant 2$. Les relations (6.274) et (6.275) nous montrent que $(X-a)$ divise aussi bien P que P'.

(ii) **(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 $P(a) = P'(a) = 0$.

(iii) **(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 (6.275) pour la dérivée :

$$P' = n(X-a)^{n-1}Q(a) + (X-a)^n Q'. \tag{6.276}$$

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 6.157.
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 6.144 qui donne l'unicité du corps de décomposition à $\mathbb{K}$-isomorphisme près. Soit donc $\psi: \mathbb{L} \to \mathbb{L}'$ 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

$$P = a(X-\alpha_1)\dots(X-\alpha_n) \tag{6.277}$$

68. Voir lemme 6.154.
69. Racine multiple, définition 3.119.

avec $a \in \mathbb{K}$ et $\alpha_i \in \mathbb{L}$. Nous avons donc

$$P = \psi(P) = a(X - \psi(\alpha_1)) \dots (X - \psi(\alpha_n)). \tag{6.278}$$

Donc les racines de P dans $\mathbb{L}'$ sont les éléments $\psi(\alpha_i)$ qui sont distincts. □

Exemple 6.158.
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

$$P = X^p - T^p \tag{6.279}$$

dans $\mathbb{K}[X]$. Par le morphisme de Frobenius nous avons

$$P = (X - T)^p \tag{6.280}$$

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 6.159.
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 6.160.
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. △

Proposition 6.161 ([175])**.**
Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Les propriétés suivantes sont équivalentes.

(1) Il existe une extension de $\mathbb{K}$ dans laquelle P a une racine multiple.

(2) P a une racine multiple dans tout corps de décomposition .

(3) P et P' ont une racine commune dans une extension de $\mathbb{K}$.

(4) le degré de $\operatorname{pgcd}(P, P')$ est $\geqslant 1$.

Démonstration. En plusieurs parties.

(i) **(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

$$P\big(\psi(a)\big) = \psi\big(P(a)\big). \tag{6.281}$$

(ii) **(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 $P = (X - a)^2 Q$ avec $Q \in \mathbb{L}[X]$. En dérivant,

$$P' = 2(X - a)Q + (X - a)^2 Q', \tag{6.282}$$

et donc a est également une racine de P'.

(iii) **(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

$$AP + BP' = D. \tag{6.283}$$

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 $\deg(D) \geqslant 1$.

(iv) **(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

$$P = (X - a)Q, \tag{6.284}$$

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.

Lemme 6.162 ([164]).
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 $\deg(P) \geqslant 1$.

(i) $\Rightarrow$ Nous supposons que P divise Q. Alors P est un diviseur commun de P et Q. Le lemme 6.55 (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

$$0 < \deg(P) \leqslant \deg\big(\operatorname{pgcd}(P, Q)\big). \tag{6.285}$$

Donc le polynôme $\operatorname{pgcd}(P, Q)$ est un polynôme non constant et n'est en particulier pas 1.

(ii) $\Leftarrow$ 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

$$P = kD. \tag{6.286}$$

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 (6.286) nous avons

$$Q = TD = k^{-1}TP, \tag{6.287}$$

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 1.180 et l'unicité de l'unitaire est dans le lemme 6.52(2).

Proposition-Définition 6.163 ([174, 176]).
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[70] *$\mathbb{M}$ pour P. Alors les propriétés suivantes sont équivalentes*[71] *:*

70. Tout polynôme admet un corps de décomposition, proposition 6.141.
71. Pour lee polynôme dérivé P', définition 6.153.

(1) $\text{pgcd}(P, P') = 1$.

(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.*

(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*

$$P = \beta \prod_{i=1}^{n} (X - \alpha_i) \tag{6.288}$$

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.*

Proposition 6.164 ([174, 176]).
Soit un corps $\mathbb{K}$ et un polynôme irréductible non nul $P \in \mathbb{K}[X]$. Les conditions suivantes sont équivalentes :

(1) *P est séparable*[72]

(2) $P' \neq 0$

(3) *Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P a une racine simple.*

Démonstration. En plusieurs parties.

(i) **(3) implique (2)** Soient une extension $\mathbb{L}$ de $\mathbb{K}$ ainsi qu'une racine simple $a \in \mathbb{L}$. Nous utilisons la proposition 3.123 : 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 Leibnitz (lemme 6.154) : $P' = (X - a)'Q(X) + (X - a)Q'(X) = Q(X) + (X - a)Q'(X)$. En évaluant en a,

$$P'(a) = Q(a) \neq 0. \tag{6.289}$$

(ii) **(2) implique $\text{pgcd}(P, P') = 1$** Notons $D = \text{pgcd}(P, P')$. 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

$$\deg(D) \leqslant \deg(P') < \deg(P). \tag{6.290}$$

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[73], nous avons $D = 1$.

(iii) **(2) implique (1)** Nous avons déjà vu que dans le cas (2) nous avons $\text{pgcd}(P, P') = 1$. La proposition-définition 6.163(1) nous indique qu'alors P est séparable.

72. Polynôme séparable, définition 6.163.
73. Le pgcd de deux polynômes est l'unitaire parmi tous les pgcd, voir 6.53.

(iv) **(1) implique (3)** La proposition 6.141 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 6.163(5).

□

Corolaire 6.165.
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 6.161. □

Définition 6.166.
Soit $\mathbb{L}$ une extension algébrique de $\mathbb{K}$.

*(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 6.163).*

*(2) L'extension $\mathbb{L}$ est **séparable** si tous ses éléments sont séparables.*

Proposition 6.167.
Soit $\mathbb{K}$ un corps. Les conditions suivantes sont équivalentes :

(1) toutes les extensions algébriques de $\mathbb{K}$ sont séparables ;

(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.

(i) **(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 6.148. 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

$$P = \prod_{i=1}^{n}(X - a_i), \tag{6.291}$$

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 :

$$P = k\mu = \prod_{i=1}^{n}(X - a_i). \tag{6.292}$$

Or le polynôme μ est irréductible par la proposition 6.67(1), et l'extension $\mathbb{L}$ est séparable, donc μ n'a que des racines simples, Donc tous les a_i sont distincts.

(ii) **(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 6.165. □

Corolaire 6.168.
Toute les extensions algébriques de $\mathbb{Q}$ sont séparables.

Démonstration. Le corps $\mathbb{Q}$ est de caractéristique nulle (définition 1.343). Le corolaire 6.165 dit alors que tout polynôme sur $\mathbb{Q}$ est séparable. La proposition 6.167 conclut en disant que toutes les extensions algébriques de $\mathbb{Q}$ sont séparables. □

Théorème 6.169 ([98]).
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

$$x^\omega = 1 \tag{6.293}$$

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 3.32. □

Théorème 6.170 (Théorème de l'élément primitif[98]).
Toute extension de corps séparable finie admet un élément primitif[74].

Autrement dit, soient des éléments algébriques $\alpha_1, \dots, \alpha_n$ séparables[75] *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 6.169. 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

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n), \tag{6.294}$$

et donc si $\mathbb{K}(\alpha_1, \dots, \alpha_{n-1}) = \mathbb{K}(\theta)$, nous avons

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\theta, \alpha_n) \tag{6.295}$$

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

$$\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r \tag{6.296}$$

de P dans $\mathbb{E}$ et les racines

$$\beta_1 = \beta, \beta_2, \dots, \beta_s \tag{6.297}$$

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[76] une solution donnée le cas échéant par

$$x = (\alpha_i - \alpha_1)(\beta_1 - \beta_k)^{-1} \tag{6.298}$$

74. Définition 6.92.
75. Définition 6.166(1).
76. La solution (6.298) peut être dans $\mathbb{L}$ et non dans $\mathbb{K}$. L'équation peut donc très bien ne pas avoir de solutions $x \in \mathbb{K}$.

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 (6.298) :

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1. \tag{6.299}$$

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

$$S(\beta_1) = P(\theta - c\beta_1) = P(\alpha_1 + c\beta_1 - c\beta_1) = P(\alpha_1) = 0. \tag{6.300}$$

D'autre part, si $k \geqslant 2$, alors

$$S(\beta_k) = P(\alpha_1 + c\beta_1 - c\beta_k) = P\big(\alpha_1 + c(\beta_1 - \beta_k)\big) \neq 0 \tag{6.301}$$

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 (6.299)).

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,

$$R = X - \beta \in \mathbb{K}(\theta)[T], \tag{6.302}$$

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 6.171.
Le théorème de l'élément primitif 6.170 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 6.172.
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. △

6.5 Idéal maximum

6.5.1 Idéal maximum

Définition 6.173.
*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).*

Théorème 6.174 ([177])**.**
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 $\mathbb{K}$.

Théorème 6.175 ([177])**.**
Si $\mathbb{K}$ est un corps algébriquement clos, les idéaux maximaux[77] *de $\mathbb{K}[X_1, \dots, X_n]$ sont de la forme*

$$(X_1 - a_1, \dots, X_n - a_n) \tag{6.303}$$

où les a_i sont des éléments de $\mathbb{K}$.

77. Définition 1.212.

Démonstration. Nous commençons par montrer que

$$J = (X_1 - a_1, \dots, X_n - a_n) \tag{6.304}$$

est un idéal maximum. Pour cela nous considérons le morphisme surjectif d'anneaux

$$\begin{aligned} \phi\colon \mathbb{K}[X_1, \dots, X_n] &\to \mathbb{K} \\ P &\mapsto P(a_1, \dots, a_n). \end{aligned} \tag{6.305}$$

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 :

$$P = (X - a_1)Q_1 + \cdots + (X_n - a_n)Q_n + R \tag{6.306}$$

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 (6.306) à $(a_1, \dots, a_n)$ et en nous rappelant que $P \in \ker(\phi)$ nous obtenons

$$0 = P(a_1, \dots, a_n) = R, \tag{6.307}$$

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 $J = \ker(\phi)$.

Vu que J est le noyau de l'application $\mathbb{K}[X_1, \dots, X_n] \to \mathbb{K}$, nous avons

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{J} = \mathbb{K}. \tag{6.308}$$

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

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{I} \tag{6.309}$$

est une $\mathbb{K}$-algèbre de type fini (définition 6.173). De plus c'est un corps par la proposition 1.213. C'est donc une extension algébrique finie de $\mathbb{K}$ par le théorème 6.174. Mais $\mathbb{K}$ étant algébriquement clos, il est sa propre et unique extension algébrique ; nous en déduisons que

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{I} = \mathbb{K}. \tag{6.310}$$

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 6.176.
Soit $\mathbb{K}$ un corps algébriquement clos et I, un idéal de $\mathbb{K}[X_1, \dots, X_n]$. Si nous notons

$$V(I) = \{x \in \mathbb{K}^n \text{ tel que } P(x_1, \dots, x_n) = 0, \forall P \in I\} \tag{6.311}$$

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 1.214). Nous savons déjà par le théorème 6.175 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

$$P(a_1, \dots, a_n) = 0, \tag{6.312}$$

c'est-à-dire que $(a_1, \dots, a_n) \in V(I)$ et donc que $V(I) \neq \varnothing$. □

6.6 Polynômes symétriques et alternés

6.6.1 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 1.361.

Définition 6.177.
Un polynôme Q en n indéterminées est

(1) ***symétrique*** *si $\sigma \cdot Q = Q$ 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.

6.6.2 Polynôme symétrique élémentaire

Définition 6.178.
*Le k-ième **polynôme symétrique élémentaire** à n inconnues est le polynôme*

$$\sigma_k(T_1, \dots, T_n) = \sum_{s \in F_k} \prod_{i=1}^{k} T_{s(i)} \tag{6.313}$$

où F_k est l'ensemble des fonctions strictement croissantes $\{1, 2, \dots, k\} \to \{1, 2, \dots, n\}$.

Une autre façon de décrire ces polynômes élémentaires est

$$\sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} X_{i_1} \dots X_{i_k}. \tag{6.314}$$

Par exemple

$$\sigma_1(T_1, \dots, T_n) = T_1 + T_2 + \dots + T_n \tag{6.315a}$$
$$\sigma_2(T_1, \dots, T_n) = T_1T_2 + \dots + T_1T_n + T_2T_3 + \dots + T_2T_n + \dots + T_{n-1}T_n \tag{6.315b}$$
$$\sigma_n(T_1, \dots, T_n) = T_1 \dots T_n. \tag{6.315c}$$

En particulier, $\sigma_2(x, y, z) = xy + yz + xz$.

Théorème 6.179 ([178]).
Si Q est un polynôme symétrique en $T_1, \dots, T_n$, alors il existe un et un seul polynôme P en n indéterminées tel que

$$Q(T_1, \dots, T_n) = P\big(\sigma_1(T_1, \dots, T_n), \dots, \sigma_n(T_1, \dots, T_n)\big). \tag{6.316}$$

Exemple 6.180.
Nous voulons décomposer $P(x, y, z) = x^3 + y^3 + z^3$ en polynômes symétriques élémentaires, c'est-à-dire en

$$\begin{cases} \sigma_1 = x + y + z & (6.317a) \\ \sigma_2 = xy + xz + yz & (6.317b) \\ \sigma_3 = xyz. & (6.317c) \end{cases}$$

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

$$P = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \tag{6.318}$$

△

Lemme 6.181 ([111]).
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) $\deg \bar{P} = \delta \deg(P)$

(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 6.167 et du corolaire 6.168, $\mathbb{K}$ est une extension séparable de $\mathbb{Q}$, et donc vérifie le théorème de l'élément primitif (6.170). 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

$$\{1, \theta, \dots, \theta^{\delta-1}\}. \tag{6.319}$$

Mais par ailleurs la proposition 6.102(2) nous indique qu'une base de $\mathbb{Q}(\theta)$ sur $\mathbb{Q}$ est donnée par

$$\{1, \theta, \dots, \theta^{n-1}\} \tag{6.320}$$

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

$$\begin{aligned} \sigma_k \colon \mathbb{Q}(\theta) &\to \mathbb{Q}(\theta_k) \\ \sum_i q_i \theta^i &\mapsto \sum_i q_i \theta_k^i \end{aligned} \tag{6.321}$$

Nous avons $\sigma_1 : \mathbb{K} \to \mathbb{K}$ qui est l'identité.

Notons N le degré du polynôme $P \in \mathbb{K}[T_1, \ldots, T_m]$ dont il est question dans l'énoncé. Nous le décomposons alors en

$$P = \sum_{l=0}^{N} \sum_{i=1}^{m} c_{il} T_i^l \tag{6.322}$$

avec $c_{il} \in \mathbb{K}$. Nous voyons $c_{i,.}$ comme un élément de $\mathbb{K}^m$ et donc nous écrivons [78]

$$P = \sum_{l=0}^{N} \sum_{i=1}^{m} c_l(\theta)_i T_i^l \tag{6.323}$$

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

$$P^{\sigma_k} = \sum_{l,i} c_l(\theta_k)_i T_i^l \in \mathbb{Q}(\theta_k)[T_1, \ldots, T_m], \tag{6.324}$$

et $\bar{P} = PP^{\sigma_2} \ldots P^{\sigma_k}$. Le coefficient de T_i^l dans $\bar{P}$ est

$$\bar{c}_l(\theta_1, \ldots, \theta_\delta)_i = \sum_{l_1 + \cdots + l_\delta = l} c_{l_1}(\theta_1)_i \ldots c_{l_\delta}(\theta_\delta)_i. \tag{6.325}$$

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 6.179 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 $\bar{P} \in \mathbb{Q}[T_1, \ldots, T_m]$. Par ailleurs nous avons que

$$\deg(\bar{P}) = \delta \deg(P) \tag{6.326}$$

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. □

6.6.3 Relations coefficients racines

Théorème 6.182 (Relations coeffitients-racines)**.**
Soit le polynôme $P = a_n X^n + \cdots + a_1 X + a_0$ et r_i ses n racines. Alors nous avons pour chaque $1 \leqslant k \leqslant n$ la relation

$$\sigma_k(r_1, \ldots, r_n) = (-1)^k \frac{a_{n-k}}{a_n} \tag{6.327}$$

où σ_k est le k^epolynôme symétrique défini en 6.178.

Exemple 6.183.
Soit le polynôme

$$P(x) = x^3 + 2x^2 + 3x + 4 \tag{6.328}$$

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 [79] nous donnent $\sigma_1(a, b, c) = -2$ et $\sigma_2(a, b, c) = 3$, donc

$$a^2 + b^2 + c^2 = (-2)^2 - 2 \cdot 3 = -2. \tag{6.329}$$

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) :

78. Il me semble qu'il manque la somme sur i dans [111].
79. Théorème 6.182

```
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

Proposition 6.184 (Annulation de fonctions polynomiales[179])**.**
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[80]*.*

Démonstration. Nous prouvons le résultat par récurrence sur le nombre n d'indéterminées. Si $n=1$, cela est le théorème 6.110. Nous classons les monômes du polynôme P par ordre de puissance de X_n et nous le factorisons :

$$P=\sum_{i=1}^{m}P_iX_n^i \tag{6.330}$$

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

$$Q(T)=P(a_1,\dots,a_{n-1},T)=\sum_{i=1}^{m}P_i(a_1,\dots,a_{n-1})T^i. \tag{6.331}$$

Le polynôme Q s'annule sur A_n avec $\deg(Q)=\deg_{X_n}(P)<\text{Card}(A_n)$ et le théorème 6.110 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

$$\deg_{X_j}(P_i)\leqslant\deg_{X_j}P<\text{Card}(A_j), \tag{6.332}$$

donc l'hypothèse de récurrence donne $P_i=0$. Par suite, $P=0$ également. □

6.7 Minuscule morceau sur la théorie de Galois

Vous trouverez des détails et des preuves à propos de la théorie de Galois dans [180, 98].

Définition 6.185.
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 $\mathbb{K}$.

80. 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 6.186.
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*

$$\sum \alpha_{i_1 \dots i_n} b_1^{i_1} \dots b_n^{i_n} = 0 \tag{6.333}$$

avec $\alpha_{i_1 \dots i_n} \in \mathbb{K}$.

Nous disons que l'équation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{6.334}$$

est l'**équation générale** de degré n si les coefficients a_i sont algébriquement indépendants sur $\mathbb{K}$.

Théorème 6.187.
Le groupe de Galois d'un polynôme de degré n est isomorphe au groupe symétrique S_n.

Corolaire 6.188 ([181])**.**
L'équation générale de degré n est résoluble par radicaux si et seulement si $n \leqslant 5$.

Chapitre 7

Topologie générale

7.1 Éléments généraux de topologie

7.1.1 Définitions et propriétés de base

Définition 7.1 ([182])**.**
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 $\mathcal{T}$.*

(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 7.37.

7.1.2 Base de topologie

Proposition-Définition 7.2 (Base de topologie[183, 184])**.**
Soit un espace topologique $(X, \mathcal{T})$. Soit une partie $\mathcal{B}$ de $\mathcal{T}$. Les propriétés suivantes sont équivalentes :

(1) Tout élément de $\mathcal{T}$ est une réunion d'éléments de $\mathcal{B}$.

(2) Pour tout $x \in X$ et pour tout ouvert $\mathcal{O}$ contenant x, il existe $B \in \mathcal{B}$ tel que

$$x \in B \subset \mathcal{O}. \tag{7.1}$$

Une partie $\mathcal{B}$ de $\mathcal{T}$ qui vérifie ces propriétés est une ***base de topologie*** *pour X.*

Démonstration. En deux parties.

(i) **(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 $x \in B \subset \mathcal{O}$.

(ii) **(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.

7.1.3 Fermés

Définition 7.3.
*Si X est un espace topologique, un sous-ensemble F de X est dit **fermé** si son complémentaire, $X\backslash F$, est ouvert.*

Définition 7.4.
*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 $\mathcal{O} \subset V$.*

Définition 7.5 (Base de voisinage[185])**.**
*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 $U_k \subset V$.*

Lemme 7.6.
Union et intersection de fermés.

(1) Une intersection quelconque de fermés est fermée.

(2) Une union finie de fermés est fermée.

Démonstration. Soit $\{F_i\}_{i\in I}$ un ensemble de fermés ; nous avons

$$\left(\bigcap_{i\in I} F_i\right)^c = \bigcup_{i\in I} F_i^c. \tag{7.2}$$

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]. □

Lemme 7.7.
Si F est fermé et si $\mathcal{O}$ est ouvert, alors $F\backslash\mathcal{O}$ est fermé.

Démonstration. Nous savons par le lemme 1.27 que $(F\backslash\mathcal{O})^c = F^c \cup \mathcal{O}$. Vu que F^c et $\mathcal{O}$ sont ouverts, l'union est ouverte. Le complémentaire de $F\backslash\mathcal{O}$ étant ouvert, il est fermé. □

Dans un espace topologique, nous avons une caractérisation très importante des ouverts.

Théorème 7.8.
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,

$$A = \bigcup_{x\in A} \mathcal{O}_x \tag{7.3}$$

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 7.208 est une version particulière de celui-ci, pour l'espace topologique $\mathbb{R}$. Une autre application typique est la proposition 7.2 et le théorème 7.180.

2. Un bon exercice est d'écrire ces unions et intersections, pour se convaincre que ça fonctionne.

7.1.4 Quelques exemples

7.1.4.1 Une première vague

Exemple 7.9.
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**. △

Exemple 7.10.
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**. △

Exemple 7.11 (Toutes les topologies d'un ensemble à 3 éléments)**.**
On pose $X = \{1, 2, 3\}$. Alors on peut munir X de 29 topologies différentes[186] ; saurez-vous les retrouver toutes ? △

7.1.4.2 Topologie engendrée

Proposition-Définition 7.12 (Topologie engendrée, prébase[187])**.**
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 $\mathcal{T}_0$:

$$B(\mathcal{T}_0) = \Big\{ \bigcap_{j\in J} \mathcal{O}_j \Big\}_{J \text{ fini dans } I} \tag{7.4}$$

où nous convenons que $\bigcap_{j\in\varnothing} \mathcal{O}_j = X$ [3].

(3) Soit A un ensemble qui indexe $B(\mathcal{T}_0)$:

$$B(\mathcal{T}_0) = \{B_\alpha\}_{\alpha\in A}. \tag{7.5}$$

(4) Nous posons

$$\tau(\mathcal{T}_0) = \Big\{ \bigcup_{\alpha\in S} B_\alpha \Big\}_{S\subset A}. \tag{7.6}$$

Alors :

(1) $\tau(\mathcal{T}_0)$ est une topologie sur X.

(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 7.1 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

$$\bigcup_{l\in L} D_l = \bigcup_{\alpha\in S} B_\alpha \in \tau(\mathcal{T}_0). \tag{7.7}$$

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

$$\bigcup_{\alpha\in S_1} B_\alpha \cap \bigcup_{\beta\in S_2} B_\beta = \bigcup_{\alpha,\beta\in S_1\times S_2} (B_\alpha \cap B_\beta). \tag{7.8}$$

Mais B_α et B_β sont dans $B(\mathcal{T}_0)$. Donc $B_\alpha \cap B_\beta \in B(\mathcal{T}_0)$. Donc (7.8) 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 7.12, $B(\mathcal{T}_0) \subset \mu$.

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.

Définition 7.13 (Convergence de suite)**.**
*Une suite (x_n) d'éléments de X **converge** vers un élément y de X si pour tout ouvert $\mathcal{O}$ contenant y , il existe un $K \in \mathbb{N}$ tel que $k \geqslant K$ implique $x_k \in \mathcal{O}$.*

La proposition suivante montre que vérifier la convergence d'une suite sur une prébase suffit pour vérifier la convergence.

Proposition 7.14.
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]

$$x_n \xrightarrow{(X,\tau(\mathcal{T}_0))} x. \tag{7.9}$$

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 7.12 :

$$\mathcal{O} = \bigcup_{\alpha\in S} B_\alpha \tag{7.10}$$

avec $B_\alpha \in B(\mathcal{T}_0)$. Donc pour chaque α, il existe un ensemble fini J_α tel que

$$B_\alpha = \bigcap_{j\in J_\alpha} A_j \tag{7.11}$$

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, $x_k \in \mathcal{O}$. □

7.1.5 Topologie produit

Définition 7.15 (Produit d'espaces topologiques, thème 27)**.**
*Soient $\{(X_i, \tau_i)\}_{i=1,\dots,n}$ des espaces topologiques. Leur **produit** est l'ensemble*

$$X = \prod_{i=1}^{n} X_i \tag{7.12}$$

muni de la topologie

$$\mathcal{T} = \{\mathcal{O} \subset X \text{ tel que } \forall x \in U, \exists U_i \in \tau_i \text{ tel que } x \in U_1 \times \dots \times U_n \subset \mathcal{O}\}. \tag{7.13}$$

4. Définition 7.13.

Dans le cas d'espaces normés, nous verrons dans le lemme 7.203 que la topologie produit est la même que celle obtenue par la norme produit.

Proposition 7.16 (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

$$(a_k^{(1)}, \dots, a_k^{(n)}) \xrightarrow{X_1 \times \dots \times X_n} (a^{(1)}, \dots, a^{(n)}) \tag{7.14}$$

si et seulement si $a_k^{(i)} \to a^{(i)}$ pour chaque i.

Démonstration. En deux parties.

(i) **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.

(ii) **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 7.15 de la topologie produit et la définition 7.12 de ce qu'est une prébase.

La proposition 7.14 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 7.14 permet de conclure.

□

7.1.6 Adhérence, fermeture, intérieur, point d'accumulation et point isolé

Définition 7.17.
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 quex $\in \mathcal{O} \subset A$.*

*(2) L'**intérieur** de A, notée $\text{Int}(A)$, est l'union de tous les ouverts de X contenus dans A.*

Lemme 7.18.
Quelques propriétés en vrac.

(1) L'intérieur de A est l'ensemble de tous les points intérieurs de A.

(2) Pour tout $A \subset X$, l'ensemble $\text{Int}(A)$ est un ouvert.

(3) On a $\text{Int}(A) \subset A$

(4) Nous avons $\text{Int}(A) = A$ si et seulement si A est un ouvert.

Démonstration. En plusieurs morceaux.

(i) **(1)** Si $a \in \text{Int}(A)$, 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 $\mathcal{O} \subset \text{Int}(A)$, et en particulier $a \in \text{Int}(A)$.

(ii) **(2)** L'ensemble $\text{Int}(A)$ est une union d'ouverts.

(iii) **(3)** L'ensemble $\text{Int}(A)$ est une union d'ensembles contenus dans A.

(iv) **(4)** Supposons que $\text{Int}(A) = A$. Puisque $\text{Int}(A)$ 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 $A \subset \text{Int}(A)$. Mais comme $\text{Int}(A) \subset A$, nous avons l'égalité.

□

7.1.6.1 Adhérence et fermeture

Disons-le tout de suite : « 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.

Définition 7.19.
*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 $\bar{A}$.*

Lemme 7.20.
À propos d'adhérence.

(1) L'adhérence de A est l'intersection de tous les fermés de X contenant A.

(2) Nous avons l'égalité

$$\mathrm{Int}(A)^c = \mathrm{Adh}(A^c). \tag{7.15}$$

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.

(i) **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 : $x \in \mathrm{Adh}(A^c)$.

(ii) $\mathrm{Adh}(A^c) \subset \mathrm{Int}(A)^c$ 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 $\mathrm{Int}(A)$.

□

Remarque 7.21.
Comme corolaire du lemme 7.20, 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 7.20, si bien que A est fermé si et seulement si $(\bar{A})^c = A^c$, ou encore… ce qu'on affirmait au début.

Définition 7.22.
*Soit X un espace topologique. Un sous-ensemble A de X est **dense** dans X si $\bar{A} = X$.*

7.1.6.2 Frontière

Définition 7.23.
*Soit X un espace topologique, et $A \subset X$. La **frontière** de A, notée ∂A, est l'ensemble des points adhérents de A qui ne sont pas intérieurs à A. Ainsi,*

$$\partial A = \mathrm{Adh}(A) \backslash \mathrm{Int}(A). \tag{7.16}$$

7.1.6.3 Topologie induite

Proposition-Définition 7.24 (Topologie induite[188])**.**
Soit un espace topologique (X, τ_X), et soit $Y \subset X$. Nous définissons

$$\tau_Y = \{Y \cap \mathcal{O} \text{ tel que } \mathcal{O} \in \tau_X\}. \tag{7.17}$$

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 7.1.

(i) $\underline{Y \in \tau_Y}$ Parce que $Y = X \cap Y$ et que X est un ouvert de X.

(ii) $\underline{\varnothing \in \tau_Y}$ Parce que $\varnothing = Y \cap \varnothing$ et que $\varnothing$ est un ouvert de X.

(iii) **Union quelconque** Soient des ouverts A_i de X. Nous avons

$$\bigcup_{i\in I} Y \cap A_i = Y \cap \big(\bigcup_{i\in I} A_i\big). \tag{7.18}$$

Comme les A_i sont des ouverts de X, leur union est encore un ouvert de X. Donc (7.18) est encore dans τ_Y.

(iv) **Intersection finie** Nous avons

$$\bigcap_{i\in I} Y \cap A_i = Y \cap \left(\bigcap_{i\in I} A_i\right). \tag{7.19}$$

□

Lemme 7.25 ([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 $S\backslash F = S \cap \Omega$. Si maintenant nous considérons le complémentaire de F dans X nous avons

$$F^c = (S\backslash F) \cup (X\backslash S) = (S \cap \Omega) \cup S^c = (S \cap \Omega) \cup (S^c \cap \Omega) \cup S^c = \Omega \cup S^c. \tag{7.20}$$

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. □

Lemme 7.26.
Si $B \subset A$ alors la fermeture de B pour la topologie de A (induite de X) que nous noterons $\tilde{B}$ est

$$\tilde{B} = \bar{B} \cap A \tag{7.21}$$

où $\bar{B}$ est la fermeture de B pour la topologie de X.

Démonstration. Si $a \in \bar{B} \cap A$, un ouvert de A autour de a est un ensemble de la forme $\mathcal{O} \cap A$ où $\mathcal{O}$ est un ouvert de X. Comme $a \in \bar{B}$, l'ensemble $\mathcal{O}$ intersecte B et donc $(\mathcal{O} \cap A) \cap B \neq \emptyset$. Donc a est bien dans l'adhérence [5] de B au sens de la topologie de A.

Pour l'inclusion inverse, soit $a \in \tilde{B}$, montrons que $a \in \bar{B} \cap A$. Par définition $a \in A$, parce que $\tilde{B}$ est une fermeture dans l'espace topologique A. Il faut donc seulement montrer que $a \in \bar{B}$. Soit donc $\mathcal{O}$ un ouvert de X contenant a ; par hypothèse $\mathcal{O} \cap A$ intersecte B (parce que tout ouvert de A contenant a intersecte B). Donc $\mathcal{O}$ intersecte B. Cela signifie que tout ouvert (de X) contenant a intersecte B, ou encore que $a \in \bar{B}$. □

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.

Lemme 7.27.
La partie $\mathbb{Q}$ dans $\mathbb{R}$ est d'intérieur vide, et sa fermeture est $\mathbb{R}$.

Exemple 7.28.
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.

Exemple 7.29.
Quid de la boule ouverte $B(1, \epsilon)$ dans le fermé $[0, 1]$? Par définition c'est

$$B(1, \epsilon) = \{x \in [0, 1] \text{ tel que } |x - 1| < \epsilon\} =]1 - \epsilon, 1]. \tag{7.22}$$

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

$$B(\frac{1}{2}, 10) \subset [0, 1], \tag{7.23}$$

mais vous avez intérêt à être très clair sur la topologie sous-entendue. △

7.1.6.4 Points d'accumulation et isolés

Définition 7.30.
*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 $A \backslash \{s\}$.*

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 7.213.

Notons qu'un point d'accumulation de A dans X n'est pas spécialement dans A.

Définition 7.31.
*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 $A \cap \mathcal{O} = \{s\}$.*

La définition suivante est *la* définition de la continuité dans tous les cas.

Définition 7.32 (Application continue[189])**.**
Deux définitions :

5. Définition 7.19.

(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 $f(V) \subset W$.*

(2) *Une continue $f\colon X \to Y$ est* ***continue*** *sur X si pour tout ouvert $\mathcal{O}$ de Y, l'ensemble*

$$f^{-1}(\mathcal{O}) = \{x \in X \text{ tel que } f(x) \in \mathcal{O}\} \tag{7.24}$$

est ouvert dans X.

Proposition 7.33 ([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.

(i) $\Rightarrow$ 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 $f(V) \subset W$.

(ii) $\Leftarrow$ 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 $f^{-1}(\mathcal{O}) \subset V$.

□

Lemme 7.34.
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 7.35 ([1])**.**
Un truc bien avec la définition 7.32(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

$$\begin{aligned} f\colon \{a\} &\to \mathbb{R} \\ a &\mapsto 4. \end{aligned} \tag{7.25}$$

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. △

Lemme 7.36.
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. □

7.1.6.5 Isomorphismes

Définition 7.37 (Isomorphisme d'espaces topologiques)**.**
Un ***isomorphisme*** *d'espaces topologiques est une application bijective continue*[6] *entre deux espaces topologiques dont la réciproque est continue. On dit également* ***homéomorphisme****.*

6. Application continue, définition 7.32.

Un isomorphisme d'un espace avec lui-même est un ***automorphisme****.*

Lemme 7.38 ([1])**.**
Si $f: X \to Y$ est un homéomorphisme[7] *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. □

7.2 Topologie rendant continue

Proposition 7.39 (Topologie qui rend continue[190])**.**
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

$$\Lambda = \{(i, \omega_i) \text{ tel que } i \in I, \omega_i \in \tau_i\}. \tag{7.26}$$

Pour chaque Γ fini dans Λ, nous posons

$$\Phi_\Gamma = \bigcap_{(i,\omega_i)\in\Gamma} \varphi_i^{-1}(\omega_i). \tag{7.27}$$

Enfin nous posons

$$\tau_I = \bigcup_{\Gamma \text{ fini dans } \Lambda} \Phi_\Gamma. \tag{7.28}$$

Nous avons :

(1) τ_I est une topologie sur X.

(2) Toutes les applications φ_i sont continues[8] *pour cette topologie.*

(3) La topologie τ_I est la plus faible topologie sur X pour laquelle toutes les φ_i sont continues.

La topologie ainsi définie est souvent référée comme la plus petite topologie qui rend les applications φ_i continues.

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 7.43.

Lemme 7.40 ([190])**.**
Soient des espaces topologiques $\{(Y_i, \tau_i)\}_{i\in I}$, et X, un ensemble. Nous considérons des applications $\varphi_i: X \to Y_i$ ainsi que τ, la topologie minimale sur X telle que les applications φ_i soient continues[9]
Soit

$$L = \{(i, V) \text{ tel que } i \in I, V \in \tau_i\}. \tag{7.29}$$

Alors l'ensemble

$$\Big\{ \bigcup_{(j,V)\in J} \varphi_j^{-1}(V) \Big\}_{J \text{ fini dans } I} \tag{7.30}$$

est une base de la topologie τ.

Lemme 7.41 ([190])**.**
Soient des espaces topologiques $\{(Y_i, \tau_i)\}_{i\in I}$, et X, un ensemble. Nous considérons des applications $\varphi_i: X \to Y_i$ 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 $i \in I$.

7. Définition 7.37.
8. Application continue, définition 7.32.
9. Proposition 7.39.

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 7.40, il existe un J fini dans I ainsi que des ouverts $\{V_j\}_{j\in J}$ tels que

$$x \in W = \bigcap_{j\in J} \varphi_j^{-1}(V_j) \subset U \tag{7.31}$$

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 [10] $N = \max\{N_j\}_{j\in J}$, 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. □

Proposition 7.42 ([190]).
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 [11] 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

$$\Lambda = \{(i, \omega) \text{ tel que } i \in I, \omega \in \tau_i\}, \tag{7.32}$$

il existe un Γ fini dans Λ tel que

$$U = \bigcap_{(i,\omega)\in\Gamma} \varphi_i^{-1}(\omega). \tag{7.33}$$

Nous avons donc

$$\psi^{-1}(U) = \bigcap_{(i,\omega_i)\in\Gamma} (\psi \circ \varphi_i^{-1})(\omega_i). \tag{7.34}$$

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 d'ouverts. □

7.2.1 Topologie quotient

Définition 7.43 ([191]).
*Soit un espace topologique X ainsi qu'une relation d'équivalence $\sim$ sur X. La **topologie quotient** sur l'ensemble $X/\sim$ est la plus petite topologie qui rend continue [12] la projection canonique $p\colon X \to X/\sim$.*

Proposition 7.44.
Soit un espace topologique X muni d'une relation d'équivalence $\sim$. Une partie $\mathcal{O}$ est $X/\sim$ est ouverte [13] si et seulement si $p^{-1}(\mathcal{O})$ est ouverte dans X.

Proposition 7.45 ([191]).
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.

10. Notez l'utilisation du lemme 1.71 pour justifier que le maximum existe.
11. Proposition 7.39.
12. Définition 7.39.
13. La topologie est définie en 7.43.

Définition 7.46 (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***

$$\begin{aligned}\tilde{f}\colon X/\sim &\to E\\ [x]&\mapsto f(x).\end{aligned}\tag{7.35}$$

Lemme 7.47 ([192])**.**
Soient deux espaces topologiques X et Y. Soit une relation d'équivalence $\sim$ sur X. Nous considérons une application continue[14] *$f\colon X\to Y$ capable de descendre aux classes*[15]*. 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 7.44). Nous avons

$$p^{-1}\big(\tilde{f}^{-1}(\mathcal{O})\big)=(\tilde{f}\circ p)^{-1}(\mathcal{O}).\tag{7.36}$$

Mais $\tilde{f}\circ p=f$ parce que $(\tilde{f}\circ p)(x)=\tilde{f}([x])=f(x)$. Donc

$$p^{-1}\big(\tilde{f}^{-1}(\mathcal{O})\big)=(\tilde{f}\circ p)^{-1}(\mathcal{O})=f^{-1}(\mathcal{O})\tag{7.37}$$

qui est ouvert parce que f est continue. □

Lemme 7.48 ([192])**.**
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

(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

$$\tilde{f}\big([x]\big)=(g\circ p)(x)=g\big([x]\big),\tag{7.38}$$

donc $\tilde{f}=g$ et le lemme est démontré. □

7.3 Suites et convergence

7.49.
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.

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.

14. Définition 7.32.
15. Voir la définition 7.46.

7.3.1 Convergence dans un fermé

Proposition 7.50 ([1])**.**
Une suite contenue dans un fermé ne peut converger 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 7.8, 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. □

Corolaire 7.51.
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 7.50. □

Lemme 7.52.
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 $x_n \in A \cap \mathcal{O} \subset \mathcal{O}$. □

7.3.2 Pour des limites uniques : séparabilité

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 7.13 dit que toute suite convergeant vers y converge aussi vers x...

Exemple 7.53.
Oui, il y a moyen de converger vers plusieurs points distincts si l'espace n'est pas super cool. Nous pouvons par exemple [193] 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 [16].

Définition 7.54 (Espace topologique Hausdorff)**.**
Si deux points distincts admettent toujours deux voisinages disjoints [17], nous disons que l'espace est ***séparé*** *ou* ***de Hausdorff****.*

Attention, cette notion est à ne pas confondre avec :

Définition 7.55 (Espace topologique séparable)**.**
Un espace topologique est ***séparable*** *si il possède une partie dénombrable [18] dense [19].*

Proposition 7.56.
Dans un espace topologique séparé, si une suite converge, alors sa limite est unique.

16. Voir la proposition 7.104.
17. Définition 1.3.
18. Définition 1.124.
19. Définition 7.22.

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. □

7.57.
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.

Lemme 7.58 ([1])**.**
Soit $a \neq 0$ dans un espace vectoriel topologique[20] *Hausdorff*[21]*. 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 7.19 de la fermeture de V). □

Proposition 7.59 ([1])**.**
La convergence de suite pour la topologie de l'espace produit[22] *est équivalente à la convergence des suites « composante par composante ».*

Démonstration. En deux parties

(i) **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.

(ii) **Dans l'autre sens** Nous considérons l'espace produit[23] $X = \prod_{i=1}^{n} X_i$. Nous supposons pour chaque i, avoir une suite convergente $(x_i)_k \xrightarrow{X_i} x_i$.
Nous allons prouver que

$$\big((x_1)_k, \dots, (x_n)_k\big) \xrightarrow{X} (x_1, \dots, x_n). \tag{7.39}$$

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 $U_1 \times \dots U_n \subset \mathcal{O}$.
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

$$\big((x_1)_k, \dots, (x_n)_k\big) \in U_1 \times \dots \times U_n \subset \mathcal{O}. \tag{7.40}$$

□

Lemme 7.60 ([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. □

20. Définition 7.158.
21. Définition 7.54
22. Définition 7.15.
23. 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.

7.3.3 Fonctions équivalentes

Proposition-Définition 7.61 ([194]).
Soit un espace topologique X et $D \subset X$. Soient encore des fonctions $f, g : D \to \mathbb{C}$ et un point $a \in \mathrm{Adh}(D)$[24].

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 $\alpha : V \to \mathbb{R}$ telles que

(1) $\lim_{x\to a} \alpha(x) = 0$,

(2) pour tout $x \in (V \cap D)\backslash\{a\}$,

$$f(x) = \big(1 + \alpha(x)\big)g(x). \tag{7.41}$$

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 1.30 de relation d'équivalence.

(i) **Réflexive** Il suffit de poser $\alpha(x) = 0$.

(ii) **Symétrique** Si $f \sim g$, il existe une fonction α vérifiant ce qu'il faut telle que

$$f(x) = \big(1 + \alpha(x)\big)g(x). \tag{7.42}$$

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

$$g(x) = \frac{1}{1 + \alpha(x)} f(x). \tag{7.43}$$

Nous posons alors $\beta(x) = -\alpha(x)/\big(1 + \alpha(x)\big)$. Cela vérifie

$$g(x) = \big(1 + \beta(x)\big)f(x). \tag{7.44}$$

Et

$$\lim_{x\to a} \beta(x) = 0 \tag{7.45}$$

parce que $\lim_{x\to a} \big(1 + \alpha(x)\big) = 1$ et $\lim_{x\to a} -\alpha(x) = 0$.

(iii) **Transitive** Soit $f \sim g$ et $g \sim h$. Sur un voisinage V de a nous avons

$$f(x) = \big(1 + \alpha(x)\big)g(x), \tag{7.46}$$

sur un voisinage W de a nous avons

$$g(x) = \big(1 + \beta(x)\big)h(x). \tag{7.47}$$

Sur le voisinage $V \cap W$ nous avons

$$f(x) = \big(1 + \beta(x) + \alpha(x) + (\alpha\beta)(x)\big)h(x). \tag{7.48}$$

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.

24. Adhérence ou fermeture, c'est la même chose. Voir la définition 7.19 et le lemme 7.20.

Lemme 7.62.
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

$$\frac{f(x)}{g(x)} \in B(1, \epsilon) \tag{7.49}$$

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 (7.41) par $g(x)$ nous trouvons

$$\frac{f(x)}{g(x)} = 1 + \alpha(x). \tag{7.50}$$

Donc

$$|\frac{f(x)}{g(x)} - 1| = |\alpha(x)| \leqslant \epsilon, \tag{7.51}$$

ce qu'il fallait prouver. □

7.4 Connexité

L'idée de la connexité, c'est de s'assurer qu'un ensemble est « d'un seul tenant ».

Définition 7.63.
*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*

$$A = (A \cap O_1) \cup (A \cap O_2), \tag{7.52}$$

*et tels que $A \cap O_1 \neq \varnothing$, et $A \cap O_2 \neq \varnothing$. Si un sous-ensemble n'est pas non-connexe, alors on dit qu'il est **connexe**.*

Une autre façon d'exprimer la condition (7.52) 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.

Lemme 7.64 ([1])**.**
Si C est un connexe de l'espace topologique X, alors C muni de la topologie induite de X est connexe.

Proposition 7.65 ([195])**.**
Soit un espace topologique X. Soient $(C_i)_{i\in I}$ des connexes de X tels que $\bigcup_{i\in I} C_i \neq \varnothing$. Alors $\bigcup_{i\in I} C_i$ est connexe.

Démonstration. Nous notons $C = \bigcup_{i\in I} C_i$. Soient des ouverts disjoints A et B recouvrant C. Nous devons démontrer que soit $A \cap C$ soit $B \cap C$ est vide.

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 $A_i \cup B_i = C_i$. Le lemme 7.64 nous dit que C_i est connexe pour la topologie induite de X ; or dans cette topologie, les parties A_i et B_i sont ouvertes. Nous en déduisons que soit A_i soit B_i est vide. Mais lequel ?

Par hypothèse, $\bigcup_{i\in I} C_i$ 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

$$\varnothing = \bigcup_{i\in I} B_i = \bigcup_{i\in I} (C_i \cap B) = B \cap C. \tag{7.53}$$

Dans le second cas nous obtenons de même que $A \cap C = \varnothing$. □

Proposition-Définition 7.66 ([196]).
Soient un espace topologique X et un point $x \in X$.

(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 7.65.

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. □

Proposition 7.67 ([1]).
Soit X un espace topologique. Les conditions suivantes sont équivalentes.

(1) L'espace X est connexe.

(2) Si $X = O_1 \cup O_2$ avec O_1 et O_2 des ouverts disjoints, alors soit $O_1 = \varnothing$ soit $O_2 = \varnothing$.

(3) Si $X = F_1 \cup F_2$ avec F_1 et F_2 fermés disjoints dans X, alors $F_1 = \varnothing$ ou $F_2 = \varnothing$.

(4) Si $A \subset X$ avec A ouvert et fermé en même temps, alors $A = \varnothing$ ou $A = X$.

Démonstration. En quatre parties.

(i) **(1) implique (2)** Par rapport à la définition 7.63, 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

$$X = O_1 \cup O_2 = (O_1 \cap X) \cup (O_2 \cap X), \tag{7.54}$$

ce qui prouverait que X est non connexe. Contradiction. Un des O_i est vide.

(ii) **(2) implique (3)** Soit une union disjointe de fermés $X = F_1 \cup F_2$. Puisque l'union est disjointe, nous avons $F_1 = X \backslash F_2$ et $F_2 = X \backslash F_1$, 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 $F_2 = \varnothing$.

(iii) **(3) implique (4)** Soit A une partie ouverte et fermée de X. Nous supposons que A est ouvert et fermé, donc $X \backslash A$ est également ouvert et fermé : c'est la définition 7.3 d'un fermé. Nous avons évidemment l'union $X = A \cup (X \backslash A)$ qui est une union disjointe de fermés. Par hypothèse nous avons soit $A = \varnothing$ soit $X \backslash A = \varnothing$.

(iv) **(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 $O_1 = X \backslash O_2$, 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 7.191) une autre caractérisation de la connexité basée sur la continuité des fonctions $X \to \mathbb{Z}$.

Proposition 7.68 ([1]).
Soient un espace topologique X ainsi que $S \subset X$. Si $U \subset X$ est connexe[25] *et si $U \subset S \subset \bar{U}$, alors S est connexe.*

25. Définition 7.63.

Démonstration. Supposons que S ne soit pas connexe. Il existe des ouverts disjoints A et B tels que $S \subset A \cup B$ et $S \cap A \neq \emptyset$, $S \cap B \neq \emptyset$. 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 $U \cap A \neq \emptyset$. Soit $x \in S \cap A$. Vu que $x \in S \subset \bar{U}$, tout voisinage de x intersecte U (c'est la définition 7.19 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 $V \cap U \neq \emptyset$. Donc $A \cap U \neq \emptyset$.

Le même raisonnement tient pour B. □

Proposition 7.69.
Stabilité de la connexité par union.

(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 $A_i \cap A_{i+1} \neq \emptyset$, 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) $C_j \cap A \neq \emptyset$ parce que p est dans l'intersection,

(1c) $C_j \cap B \neq \emptyset$ 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 [26]. 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.

□

Proposition 7.70 ([197])**.**
Soit un espace topologique X. Nous avons équivalence entre les points suivants :

(1) X est localement convexe.

(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.

Lemme 7.71 ([198])**.**
Soit un espace topologique localement connexe X. Soient un fermé F de X, et D, une composante connexe de $X\backslash F$. Alors la frontière de D est dans F :

$$\partial D \subset F. \tag{7.55}$$

Démonstration. En plusieurs parties.

(i) **∂D est fermé** Par définition, $\partial D = \bar{D}\backslash D$. Utilisant 1.27(3) nous écrivons

$$X\backslash\partial D = (X\backslash\bar{D}) \cap D. \tag{7.56}$$

Vu que $\bar{D}$ est fermé, $X\backslash\bar{D}$ est ouvert. De plus D est ouvert par la proposition 7.70. Donc $X\backslash\partial D$ est ouvert.

26. Parce qu'on a la flemme de rédiger correctement une récurrence.

(ii) **Par l'absurde** Supposons qu'il existe $p \in \partial D \backslash F$. 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 7.69 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.

□

7.5 Compacité

La compacité est le thème 32.

7.5.1 Définition et notions connexes

Soit E, un sous-ensemble de $\mathbb{R}$. Nous pouvons considérer les ouverts suivants :

$$\mathcal{O}_x = B(x,1) \tag{7.57}$$

pour chaque $x \in E$. Évidemment,

$$E \subseteq \bigcup_{x \in E} \mathcal{O}_x. \tag{7.58}$$

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 7.72.
Soit E, un sous-ensemble de $\mathbb{R}$. Une collection d'ouverts $\mathcal{O}_i$ est un ***recouvrement*** *de E si $E \subseteq \bigcup_i \mathcal{O}_i$.*

Définition 7.73.
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 7.74.
Certaines sources (dont wikipédia) disent que pour être compact il faut aussi être séparé [27]. Pour ces sources, un espace qui ne vérifie que la propriété de Borel-Lebesgue est alors dit **quasi-compact**.

7.75.
La définition 7.73 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 $X \subset \bigcup_{i \in I} A_i$.

Lemme 7.76.
Si $a, b \in \mathbb{R}$, alors la partie $[a,b]$ est compacte[28] *dans $\mathbb{R}$.*

Lemme 7.77.
Si K est une partie compacte de l'espace topologique X, alors K est un espace topologique compact pour la topologie induite[29] *de X.*

27. Définition 7.54.
28. Définition 7.73.
29. Définition 7.24.

Démonstration. Nous notons τ la topologie de X et τ_K la topologie induite de X vers K, c'est-à-dire

$$\tau_K = \{\mathcal{O} \cap K \text{ tel que } \mathcal{O} \in \tau\}. \tag{7.59}$$

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

$$K = \bigcup_{i\in I}(K \cap \mathcal{O}_i) \subset \bigcup_{i\in I}\mathcal{O}_i. \tag{7.60}$$

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

$$K \subset \bigcup_{j\in J}\mathcal{O}_j. \tag{7.61}$$

Nous avons donc aussi

$$K \subset \bigcup_{j\in J} K \cap \mathcal{O}_j = \bigcup_{j\in J} A_j. \tag{7.62}$$

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. □

Proposition 7.78 ([199])**.**
Soit K compact dans $\mathbb{C}$. Si $\mathcal{O}$ est une composante connexe[30] *de $\mathbb{C}\backslash K$, alors $\partial\mathcal{O} \subset K$.*

Démonstration. Supposons que $\partial\mathcal{O}$ n'est pas inclus dans K, et considérons $w \in \partial\mathcal{O}\backslash K$. Nous posons $A = \mathcal{O} \cup \{w\}$. Vu que $w \in \partial\mathcal{O}$, nous avons $w \in \bar{\mathcal{O}}$. Donc

$$\mathcal{O} \subset A \subset \bar{\mathcal{O}}. \tag{7.63}$$

La proposition 7.68 fait que A est connexe parce que $\mathcal{O}$ est connexe. Donc A est un connexe de $\mathbb{C}\backslash K$ contenant strictement $\mathcal{O}$. Impossible parce que $\mathcal{O}$ est une composante connexe de $\mathbb{C}\backslash K$. Contradiction.

Nous en déduisons que $\partial\mathcal{O} \subset K$. □

7.5.2 Espace localement compact

Définition 7.79.
*Une partie d'un espace topologique est **relativement compact** si sa fermeture est compacte.*

Définition 7.80.
*Un espace topologique est **localement compact** si tout élément possède un voisinage compact.*

Lemme 7.81.
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.

Lemme 7.82.
Soient un espace localement compact X, un compact K et un ouvert $\mathcal{O}$ tel que $K \subset \mathcal{O}$. Il existe un ouvert relativement compact V tel que

$$K \subset V \subset \bar{V} \subset \mathcal{O}. \tag{7.64}$$

30. Définition 7.66.

7.5.3 Autres compacité

Définition 7.83 (Séquentiellement compact)**.**
Nous disons qu'un espace topologique est ***séquentiellement compact*** *si toute suite admet une sous-suite convergente.*

Définition 7.84.
Un espace topologique est ***dénombrable à l'infini*** *si il est réunion dénombrable de compacts.*

Définition 7.85.
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.*

Proposition 7.86.
Soient X un espace topologique et $K \subset X$. Les propriétés suivantes sont équivalentes :

(1) K est compact.

(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 $\bigcap_{i\in A} F_i \cap K = \varnothing$.

(3) Si $\{F_i\}_{i\in I}$ est une famille de fermés telle que pour tout choix de A fini dans I, $\bigcap_{i\in A} F_i \cap K \neq \varnothing$, alors l'intersection complète est non vide : $\bigcap_{i\in I} F_i \cap K \neq \varnothing$.

(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[31] 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 :

$$K \subset \bigcup_{i\in A} \mathcal{O}_i \tag{7.65}$$

pour un certain sous-ensemble fini A de I. Pour ce même choix A, nous avons alors aussi

$$\bigcap_{i\in A} F_i \cap K = \varnothing. \tag{7.66}$$

L'implication (2) ⇒ (1) est la même histoire de passage aux complémentaires. □

Le théorème 7.270 est en général celui qu'on nomme « théorème des fermés emboîtés », mais le corolaire suivant en mériterait également le nom.

Corolaire 7.87 ([1])**.**
Soient un espace topologique compact X et une suite $(F_i)_{i\in\mathbb{N}}$ de fermés emboîtés[32] *dans X telle que*

$$\bigcap_{i\in\mathbb{N}} F_i = \varnothing. \tag{7.67}$$

Alors il existe $j_0 \in \mathbb{N}$ tel que $F_i = \varnothing$ pour tout $i \geqslant j_0$.

Démonstration. La proposition 7.86 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

$$\varnothing = \bigcap_{j\in J} F_j = F_{j_0}. \tag{7.68}$$

Dès que $F_{j_0} = \varnothing$, tous les suivants sont également vides. □

31. 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.
32. C'est-à-dire que $F_{i+1} \subset F_i$.

7.5.4 Quelques propriétés

Lemme 7.88.
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 7.2 : 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 7.89 (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. △

Lemme 7.90 (Compacts et fermés[200])**.**
À propos de parties fermées dans un compact.

(1) Une partie fermée d'un compact est compacte.

(2) Tout compact d'un espace topologique séparé est fermé.

Démonstration. En deux parties.

(i) **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 $\{\mathcal{O}_i\}_{i\in I} \cup \{K\backslash F\}$ 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 $K\backslash F$, ça reste un sous-recouvrement fini de F tout en étant extrait de $\{\mathcal{O}_i\}_{i\in I}$.

(ii) **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[33] 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

$$K \subset \bigcup_{x\in S} V_x. \tag{7.69}$$

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 7.8), en d'autres termes, que K est fermé.

□

Corolaire 7.91.
Dans un espace séparé, une intersection d'un compact avec un fermé est compacte.

33. Oui, la notation du voisinage peut surprendre, mais elle est quand même pratique pour ce qu'on veut en faire.

Démonstration. Soient un compact K et un fermé F. Par 7.90(2), K est fermé. La partie $K \cap F$ est donc fermée en tant qu'intersection de fermés (lemme 7.6(1)).

La partie $K \cap F$ est un fermé dans le compact K. Le lemme 7.90(1) dit alors que $K \cap F$ est compact. □

Lemme 7.92 ([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

$$\bigcup_i K_i \subset \bigcup_{s\in\bigcup_i S_i} \mathcal{O}_s. \tag{7.70}$$

□

Proposition 7.93 ([201])**.**
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 7.90(2). Donc l'intersection

$$K = \bigcap_{i\in I} K_i \tag{7.71}$$

est un fermé de X par le lemme 7.6(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 7.90. □

Exemple 7.94 (Intersection de compacts non compacte[201])**.**
Un exemple d'intersection de compacts qui n'est pas compacte. Vu la proposition 7.93, 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 $K_2 = \mathbb{N} \cup \{x_2\}$.

(i) 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.

(ii) $K_1 \cap K_2 = \mathbb{N}$ C'est immédiat parce que x_1 et x_2 sont distincts.

(iii) $\mathbb{N}$ **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.

△

Proposition 7.95.
Si V est une partie de l'espace topologique X muni de la topologie induite[34] *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. □

34. Définition 7.24.

Proposition 7.96 ([1]).
Soient des espaces topologiques X et Y. Nous considérons des ouverts A de X et B de Y. Soit un compact M dans $A \times B$[35]*. 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 :

$$K = \{a \in A \text{ tel que } \exists b \in B \text{ tel que } (a,b) \in M\}, \tag{7.72}$$

et

$$L = \{b \in B \text{ tel que } \exists a \in A \text{ tel que } (a,b) \in M\}. \tag{7.73}$$

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

$$\{U_i \times V_j\}_{\substack{i\in I\\ j\in J}} \tag{7.74}$$

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

$$\{U_i \times V_j\}_{\substack{i\in I_0\\ j\in J_0}} \tag{7.75}$$

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. □

7.5.5 Compactifié d'Alexandrov

Proposition-Définition 7.97 ([202]).
Soit un espace topologique séparé localement compact[36] *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 $X\backslash A$ 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 7.1). 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.

(i) **L'espace lui-même** $\hat{X} \in \hat{\tau}$ parce que $\hat{X} = X \cup \{\omega\}$ et que $X\backslash X = \varnothing$ est compact.

(ii) **Le vide** $\varnothing \in \tau \subset \hat{\tau}$.

(iii) **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 $I_2 = I\backslash I_1$. Nous avons

$$\bigcup_{i\in I} A_i = \big(\bigcup_{i\in I_1} A_i\big) \cup \big(\bigcup_{i\in I_2} A_i\big) = B \cup \big(\bigcup_{i\in I_2} B_i \cup \{\omega\}\big) \tag{7.76}$$

où B et les B_i sont des ouverts de X tels que $X\backslash B_i$ est compact dans X. Nous récrivons ça sous la forme

$$\bigcup_{i\in I} A_i = B \cup \big(\bigcup_{i\in I_2} B_i\big) \cup \{\omega\}. \tag{7.77}$$

35. Topologie produit, définition 7.15
36. Définition 7.80.

La question est de savoir si

$$X\backslash\Big(B\cup\big(\bigcup_{i\in I_2}B_i\big)\Big) \tag{7.78}$$

est compact dans X. Un peu de réécriture :

$$X\backslash\Big(B\cup\big(\bigcup_{i\in I_2}B_i\big)\Big)=(X\backslash B)\cap X\backslash\big(\bigcup_{i\in I_2}B_i\big)=(X\backslash B)\cap\big(\bigcap_{i\in I_2}(X\backslash B_i)\big). \tag{7.79}$$

La partie $X\backslash B$ est fermée dans X parce que B est ouverte. La proposition 7.93 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 [37]. Donc nous sommes en présence de l'intersection de deux fermés. Donc $(X\backslash B)\cap\big(\bigcap_{i\in I_2}(X\backslash B_i)\big)$ est fermé. Mais c'est contenu dans le compact $\bigcap_{i\in I_2}(X\backslash B_i)$. Fermé dans un compact, donc compact (lemme 7.90).

(iv) **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 $X\backslash B_i$ compact. Alors

$$\bigcap_{i=1}^{n}(B_i\cup\{\omega\})=\Big(\bigcap_{i=1}^{n}B_i\Big)\cup\{\omega\} \tag{7.80}$$

Mais le lemme 1.25 (appliqué un nombre fini de fois) donne

$$X\backslash\Big(\bigcap_{i=1}^{n}B_i\Big)=\bigcup_{i=1}^{n}(X\backslash B_i) \tag{7.81}$$

qui est compact en tant qu'union finie de compacts [38].

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 :

$$A_i=\begin{cases}B_i & \text{si } i\leqslant q\\ C_i\cup\{\omega\} & \text{si } q<i\leqslant n\end{cases} \tag{7.82}$$

où B_i sont ouverts et C_i sont des parties de X telles que $X\backslash C_i$ est compacte.

Nous avons

$$\bigcap_{i=1}^{n}A_i=\Big(\bigcap_{i=1}^{q}B_i\Big)\cap\Big(\bigcap_{i=q+1}^{n}(C_i\cup\{\omega\})\Big) \tag{7.83a}$$

$$=B\cap\Big(\bigcap_{i=q+1}^{n}C_i\Big). \tag{7.83b}$$

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

$$X\backslash E=X\backslash\Big(\bigcap_{i=q+1}^{n}C_i\Big)=\bigcup_{i=q+1}^{n}(X\backslash C_i). \tag{7.84}$$

37. Lemme 7.90(2).
38. Lemme 7.92.

Vu que $X\backslash C_i$ est compact, il est fermé [39]. La partie $X\backslash E$ est donc fermée comme union finie de fermés [40]. Et donc E est ouvert. Et finalement

$$\bigcap_{i=1}^{n} A_i = B \cap E \tag{7.85}$$

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 $X\backslash B$ compact dans X.

Les ouverts $\{A_i\}_{i\in I}$ forment un recouvrement de $X\backslash B$ par des ouverts. Nous pouvons en extraire un sous-recouvrement fini :

$$X\backslash B \subset \bigcup_{i\in I_1} A_i. \tag{7.86}$$

Nous avons alors

$$\hat{X} \subset \bigcup_{i\in I_1\cup\{i_0\}} A_i. \tag{7.87}$$

Et voilà que $\hat{X}$ est recouvert par un nombre fini des A_i. Notez que (7.87) est une égalité, mais nous n'en avons pas besoin. □

7.98.
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 1.145). 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 12.27.

Pour $\mathbb{C}$, nous donnerons une caractérisation de la limite en ∞ dans le lemme 12.85.

7.5.6 Propriété d'intersection finie

Définition 7.99 (Propriété d'intersection finie[203])**.**
Soit un ensemble X. Une famille non vide $\mathcal{A}$ de parties de X a la ***propriété d'intersection finie*** *si toutes les intersections finies d'éléments de $\mathcal{A}$ est non vide.*

Théorème 7.100 ([203])**.**
Un espace est compact si et seulement si toute famille de parties fermées ayant la propriété d'intersection finie [41] *a une intersection non vide.*

7.6 Limite de fonction

Définition 7.101 (Limite d'une fonction, thème 29[204])**.**
Soient des espaces topologiques X et Y ainsi que $\Omega \subset X$ et $a \in \mathrm{Adh}(\Omega)$. Soit une application $f : \Omega \to Y$. 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*

$$f\Big((U \cap \Omega)\backslash\{a\}\Big) \subset V. \tag{7.88}$$

39. Par le lemme 7.90(2) et le fait que nous considérons un espace séparé.
40. Par le lemme 7.6(2).
41. Définition 7.99.

Si un tel élément est unique[42]*, alors nous disons que cet élément est la* ***limite*** *de f et nous notons*

$$\lim_{x\to a} f(x) = \ell. \tag{7.89}$$

7.102.
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.

Dans ce cas, nous aurions écrit (7.88) sous la forme

$$f\Big(U\backslash\{a\}\Big) \subset V \tag{7.90}$$

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[205]. Mais bon...si ça va sans dire, ça va encore mieux en le disant.

Remarque 7.103.
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

$$\lim_{x\to 1} \frac{x^2-1}{x-1} = 2, \tag{7.91}$$

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 (12.164). Dans la formule

$$f'(a) = \lim_{x\to a} \frac{f(x)-f(a)}{x-a}, \tag{7.92}$$

la fonction sur laquelle nous prenons la limite n'est *jamais* définie en $x = a$.

Proposition 7.104 (Unicité de la limite pour un espace séparé)**.**
Soient X un espace topologique, A une partie de X et Y un espace topologique séparé[43]*. 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 :

$$\begin{cases} f(W\cap A) \subset V & \text{(7.93a)}\\ f(W'\cap A) \subset V'. & \text{(7.93b)} \end{cases}$$

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

$$f(W\cap W'\cap A) \subset f(W\cap A) \subset V, \tag{7.94}$$

et

$$f(W\cap W'\cap A) \subset f(W'\cap A) \subset V', \tag{7.95}$$

42. Rappelons que ce n'est pas toujours le cas, mais que ça l'est si l'espace topologique est séparé – définition 7.54.
43. Définition 7.54.

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 $y = y'$. □

Proposition 7.105.
À propos de séparation.

(1) *Tout espace métrique 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 7.56 et 7.104. □

7.7 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.

7.7.1 Distance et topologie métrique

Définition 7.106.
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****.*

Le lemme suivant est similaire à la proposition 7.147.

Lemme 7.107.
Si (E, d) est un espace métrique et si $x, y, z \in E$, nous avons

$$|d(x, z) - d(y, z)| \leqslant d(x, y). \tag{7.96}$$

La définition-théorème suivante donne une topologie sur les espaces métriques en partant des boules.

Théorème-Définition 7.108 (Topologie métrique)**.**
Soit (E, d) un espace métrique. Nous définissons les ***boules ouvertes*** *par*

$$B(a, r) = \{x \in E \text{ tel que } d(a, x) < r\}. \tag{7.97}$$

pout tout $a \in E$ et $r > 0$. Alors en posant

$$\mathcal{T} = \big\{\mathcal{O} \subset E \text{ tel que } \forall a \in \mathcal{O}, \exists r > 0 \text{ tel que } B(a, r) \subset \mathcal{O}\big\} \tag{7.98}$$

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 $\varnothing \in \mathcal{T}$ parce que tout élément de l'ensemble vide ...heu ...enfin parce que, d'accord hein [44]. Ensuite si les $\{A_i\}_{i\in I}$ sont des éléments de $\mathcal{T}$ 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 $\{A_i\}_{i\in\{1,\dots,n\}}$ 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 $r = \min\{r_i\}_{i=1,\dots,n}$ nous avons $B(x,r) \subset \bigcap_{i=1}^n A_i$. □

Proposition 7.109.
La topologie sur un espace métrique [45] *est la topologie engendrée* [46] *par ses boules ouvertes.*

7.110.
Si vous avez un peu de temps, vous pouvez vérifier que si $\mathbb{K}$ est un corps totalement ordonné, alors avec toutes les définitions de 1.367, en posant $d(x,y) = |x-y|$ nous avons une distance sur $\mathbb{K}$.

De plus, les boules définies en 1.367 sont alors les mêmes que celles définies en (7.97), ce qui donne à tout corps totalement ordonné une structure d'espace topologique.

Proposition 7.111 ([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 $d(a_n,\ell) \leqslant r_1 + r_2$. □

7.7.2 Topologie métrique et induite

Lemme 7.112.
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 métrique $\big(M, \|.\|\big)$.

7.7.3 Intérieur, adhérence et frontière

7.113.
Choses déjà faites :

— Intérieur, définition 7.17.

— Adhérence, qui est la même chose que fermeture, définition 7.19, et précisé par le lemme 7.20.

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 :

$$x \in \operatorname{Adh} A \overset{\text{def}}{\iff} \forall \epsilon > 0, B(x,\epsilon) \cap A \neq \varnothing \tag{7.99}$$

Proposition 7.114.
Pour $A \subset \mathbb{R}^n$, nous avons

$$\operatorname{Int} A \subseteq A \subseteq \operatorname{Adh} A$$

Définition 7.115.
*La **frontière** ou le **bord** de A est défini par $\partial A = \operatorname{Adh} A \setminus \operatorname{Int} A$.*

Lemme 7.116.
Une partie A d'un espace topologique est ouverte si $A = \operatorname{Int} A$, et fermée si $A = \operatorname{Adh} A$.

Lemme 7.117 (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.

44. Pour qui ne serait pas d'accord, ajoutez $\varnothing$ dans la définition des ouverts et puis c'est tout.
45. Définition 7.108.
46. Définition 7.12

Démonstration. Supposons que tout voisinage de x contienne un point de S et un point de S^c. Alors $x \in Adh(S)$ (définition 7.19), 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 7.118.
Un ensemble et son complémentaire ont même frontière.

Démonstration. Conséquence du lemme 7.117. 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 7.119.
Soit $X = [0, 1]$ muni de la topologie de la distance $|x - y|$ (définition 7.108). 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

$$B(1, r) = \{x \in X \text{ tel que } |x - 1| < r\} =]1 - r, 1] \tag{7.100}$$

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 $\mathbb{R}$. △

Lemme 7.120 (Passage de douane[206, 207])**.**
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 γ la partie connexe qui intersecte A et A^c. Les ouverts $\text{Int}(A)$ et $X\backslash\bar{A}$ ne peuvent pas recouvrir γ parce que ce sont deux ouverts disjoints alors que γ est connexe (voir la définition 7.63 de la connexité). Donc γ 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 7.121.
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 7.122.
Si $A \subset \mathbb{R}^n$ et $A^c = \mathbb{R}^n\backslash A$, 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,

Exemple 7.123.
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 $\bar{A} \cap \bar{B} = \{1\}$. △

7.7.4 Boules ouvertes, fermées, sphères

Définition 7.124.
Soit un espace métrique (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*[47] *de la boule : $S(a,r) = \partial B(a,r)$.*

7.125.
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.

Lemme 7.126.
Quelques liens entre les boules et les sphères.

(1) La sphère est donnée par $S(a,r) = \{x \in V \text{ tel que } d(x,a) = r\}$.

(2) La fermeture de la boule est $\overline{B(a,r)} = \{x \in V \text{ tel que } d(x,a) < r\}$;

(3) Nous avons $\overline{B(a,r)} = B(a,r) \cup S(a,r)$.

7.7.5 Continuité séquentielle

Corolaire 7.127 (Caractérisation séquentielle de la continuité en un point[1])**.**
Une application entre deux espaces topologiques continue en un point y est séquentiellement 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[48] que $f(a)$ est une limite de f en a, c'est-à-dire[49] qu'il existe un voisinage W de a tel que $f(W\backslash\{a\}) \subset V$.

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 $f(x_k) \to f(a)$. □

7.7.5.1 Les boules, une base de topologie

Proposition 7.128.
Un espace métrique séparable[50] *accepte une base de topologie*[51] *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

$$\mathcal{B} = \{B(a_i, r_j)\}_{i,j\in\mathbb{N}} \tag{7.101}$$

est une base de la topologie[52] *de E.*

47. Frontière, définition 7.115.
48. C'est la définition 7.32 de la continuité en un point.
49. Définition 7.101 d'une limite.
50. Qui possède une partie dense dénombrable, définition 7.55.
51. Base de topologie, définition 7.2.
52. Définition 7.2.

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 1.424).

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

$$\|y-x\| \leqslant \|y-a\| + \|a-x\| < \frac{2}{3}r + \frac{1}{3}r = r. \tag{7.102}$$

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. □

Remarque 7.129.
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 11.46).

Voir aussi le corolaire 14.245 qui donnera tout ouvert comme union de pavés presque disjoints.

Définition 7.130.
*Soit (X,d) un espace métrique. Un sous-ensemble $A \subset X$ est **borné** si il existe une boule de X contenant A.*

Proposition 7.131.
Toute réunion finie d'ensembles bornés est un ensemble borné. Toute partie d'un ensemble borné est un ensemble borné.

7.7.6 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.

Lemme 7.132 (de Lebesgue[208])**.**
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. □

Lemme 7.133 ([208])**.**
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. □

Théorème 7.134 (Bolzano-Weierstrass[208], thème 32)**.**
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

$$X_n = \overline{\{x_k \text{ tel que } k > n\}}. \tag{7.103}$$

Ce sont des fermés ayant la propriété d'intersection finie non vide, et donc la proposition 7.86 nous dit qu'ils ont une intersection non vide. Un élément de cette intersection est automatiquement un point d'accumulation de la suite [53].

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 7.132, 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 7.133, 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. □

Exemple 7.135 (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 7.134 a l'importante conséquence suivante.

Théorème 7.136 (Weierstrass)**.**
Une fonction continue à valeurs réelles définie sur un compact est bornée et atteint ses bornes.

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 :

$$A = f(K) = \{f(x) \text{ tel que } x \in K\}. \tag{7.104}$$

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 1.442).

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 7.134. Afin d'alléger la notation, nous allons noter (x_n) la sous-suite convergente. Nous avons donc

$$x_n \to x \in K. \tag{7.105}$$

Par la proposition 7.127, nous savons que f prend en x la valeur

$$f(x) = \lim_{n\to\infty} f(x_n). \tag{7.106}$$

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.

53. Définition 7.30.

Afin de prouver que f atteint sa borne, c'est-à-dire que $M \in A$, nous considérons les inégalités

$$M - \frac{1}{n} < f(x_n) \leqslant M. \tag{7.107}$$

En passant à la limite $n \to \infty$, ces inégalités deviennent

$$M \leqslant f(x) \leqslant M, \tag{7.108}$$

et donc $f(x) = M$, ce qui prouve que f atteint sa borne M au point $x \in K$. □

Lemme 7.137 ([1])**.**
Soient des compacts A, B et une fonction continue $f\colon A \times B \to \mathbb{R}$. Alors

$$\sup_{(x,y)\in A\times B} |f(x,y)| = \sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big). \tag{7.109}$$

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[54] 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[55] :

$$\sup_{(x,y)\in A\times B} |f(x,y)| = |f(x_0,y_0)|. \tag{7.110}$$

Nous avons d'une part

$$\sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big) = \sup_{x\in A}|f\big(x,y_M(x)\big)| \leqslant |f(x_0,y_0)| \tag{7.111}$$

Et d'autre part, quelques calculs avec justifications en-dessous :

$$\begin{aligned}
\sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big) &\leqslant \sup_{x\in A}\sup_{y\in B}|f(x_0,y_0)| && \text{(7.112a)}\\
&= |f(x_0,y_0)| && \text{(7.112b)}\\
&\leqslant |f\big(x_0,y_M(x_0)\big)| && \text{(7.112c)}\\
&\leqslant \sup_{x\in A}|f\big(x,y_M(x)\big)| && \text{(7.112d)}\\
&\leqslant \sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big). && \text{(7.112e)}
\end{aligned}$$

Justifications.

— Pour (7.112a). Le point (x_0, y_0) est un maximum de $|f|$.

— Pour (7.112c). y_M est définie pour maximiser, en fonction de x, la quantité $|f(x, y_M(x))|$.

— Pour (7.112d). 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 (7.112) sont égaux, toutes les inégalités sont en réalité des égalités. En particulier, en reprenant (7.110),

$$\sup_{(x,y)\in A\times B} |f(x,y)| = |f(x_0,y_0)| = \sup_{x\in A}\big(\sup_{y\in B}|f(x,y)|\big). \tag{7.113}$$

□

54. Théorème 7.136.
55. Encore une fois, ce point n'est pas déterminé de façon unique par cette propriété.

7.7.7 Distance à un ensemble

Définition 7.138.
Si A est une partie de l'espace métrique (X,d), et si $b\in X$, nous définissons

$$d(b,A)=\inf_{y\in A} d(b,y). \tag{7.114}$$

Lemme 7.139 ([1]).
Si A est fermé dans (X,d), et si $b\in X$ vérifie $d(b,A)=0$, alors $b\in A$.

Démonstration. Puisque A est fermé, le complémentaire A^c est ouvert (c'est la définition 7.3). Supposons que $b\in A^c$. Alors il existe $r>0$ tel que $B(b,r)\subset A^c$. Si $a\in A$ nous avons alors $d(b,A)\geqslant d(b,a)\geqslant r>0$. Cela contredit l'hypothèse $d(b,A)=0$.

Nous en déduisons que b n'est pas dans A^c et qu'il est donc dans A. □

Exemple 7.140 (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. △

Lemme 7.141 ([1]).
Soient un espace métrique (X,d) ainsi qu'une partie $A\subset X$. Soit $r>0$. La partie

$$\mathcal{O}=\{x\in X \text{ tel que } d(x,A)<r\} \tag{7.115}$$

est ouverte.

Démonstration. Soit $y\in\mathcal{O}$; nous avons $d(y,A)<r$. Autrement dit,

$$\inf_{a\in A} d(y,a)<r \tag{7.116}$$

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

$$d(z,a)\leqslant d(z,y)+d(y,a)<r-\delta+\delta=r. \tag{7.117}$$

□

Lemme 7.142 ([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 7.50 nous dit alors que $a\in F$. □

Lemme 7.143 ([1]).
Si A est une partie de (X,d), alors la fonction

$$\begin{aligned} f\colon\Omega&\to[0,\infty[\\ x&\mapsto d(x,A)\end{aligned} \tag{7.118}$$

est continue.

7.7.8 Convexité

Définition 7.144 (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.

Proposition 7.145 ([209]).
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

$$\{tx + (1-t)y\}_{t\in[0,1]} \subset \bigcap_{i\in I} C_i, \tag{7.119}$$

et donc le résultat attendu. □

7.7.9 Norme

Définition 7.146 ([210], 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 $N : E \to [0, \infty[$ telle que*

(1) $N(x) \geqslant 0$
(2) $N(x) = 0$ *si et seulement si* $x = 0$;
(3) $N(\lambda x) = |\lambda| N(x)$
(4) $N(x + y) \leqslant N(x) + N(y)$

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 $N(-x) = N(x)$.

Proposition 7.147.
Toute norme N sur l'espace vectoriel E vérifie l'inégalité

$$\big|N(x) - N(y)\big| \leqslant N(x - y) \tag{7.120}$$

pour tout $x, y \in E$.

Démonstration. Nous avons, en utilisant le point (4) de la définition 7.146,

$$N(x) = N(x - y + y) \leqslant N(x - y) + N(y), \tag{7.121a}$$
$$N(y) = N(y - x + x) \leqslant N(y - x) + N(x). \tag{7.121b}$$

Supposons d'abord que $N(x) \geqslant N(y)$. Dans ce cas, en utilisant (7.121a),

$$\big|N(x) - N(y)\big| = N(x) - N(y) \leqslant N(x - y) + N(y) - N(y) = N(x - y). \tag{7.122}$$

Si par contre $N(x) \leqslant N(y)$, alors nous utilisons (7.121b) et nous trouvons

$$\big|N(x) - N(y)\big| = N(y) - N(x) \leqslant N(y - x) + N(x) - N(x) = N(y - x) = N(x - y). \tag{7.123}$$

Dans les deux cas, nous avons retrouvé l'inégalité annoncée. □

Cette proposition signifie aussi que

$$-N(x - y) \leqslant N(x) - N(y) \leqslant N(x - y). \tag{7.124}$$

Le lemme suivant dit que nous pouvons remplacer l'inégalité triangulaire par la convexité de la boule unité dans la définition de norme.

Lemme 7.148 ([211]).
Soit une application $N\colon E \to [0,\infty[$ 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

$$B = \{x \in E \text{ tel que } N(x) \leqslant 1\} \tag{7.125}$$

est convexe[56].

Démonstration. Dans les deux sens.

(i) $\Rightarrow$ 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

$$\begin{aligned} N\big(\lambda x + (1-\lambda)y\big) &\leqslant N(\lambda x) + N\big((1-\lambda)y\big) && \text{(7.126a)}\\ &= \lambda N(x) + (1-\lambda)N(y) && \text{(7.126b)}\\ &\leqslant \lambda + (1-\lambda) && \text{(7.126c)}\\ &= 1. && \text{(7.126d)} \end{aligned}$$

Nous avons utilisé diverses propriétés de la norme, ainsi que la majoration $N(x), N(y) \leqslant 1$.

(ii) $\Leftarrow$ 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

$$z = \frac{x+y}{N(x)+N(y)} \tag{7.127}$$

et la subtilité sera d'écrire z de telle sorte à être une somme de deux éléments de B. L'astuce est de poser

$$\lambda = \frac{N(x)}{N(x)+N(y)}. \tag{7.128}$$

Une simple vérification montre qu'alors

$$z = \lambda \frac{x}{N(x)} + (1-\lambda)\frac{y}{N(y)}. \tag{7.129}$$

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 (7.127) :

$$\frac{N(x+y)}{N(x)+N(y)} \leqslant 1. \tag{7.130}$$

Cela signifie exactement $N(x+y) \leqslant N(x) + N(y)$.

□

7.149.
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 7.147 s'énoncera donc

$$\big|\|x\| - \|y\|\big| \leqslant \|x-y\|. \tag{7.131}$$

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.

56. Définition 7.144.

Une autre inégalité utile de temps en temps.

Corolaire 7.150.
Si a et b sont dans un espace vectoriel normé, alors

$$\big|\|a-b\|-\|b\|\big| \leqslant \|a\|. \tag{7.132}$$

Démonstration. Il s'agit seulement de la proposition 7.147 avec $x = a-b$ et $y = b$. □

Lemme-Définition 7.151 (Distance induite par une norme)**.**
Soit un espace vectoriel normé $(E, \|.\|)$. Nous posons

$$d(x,y) = \|x-y\|. \tag{7.133}$$

Alors

(1) *d est invariante par translations : $d(a,b) = d(a+u, b+u)$*
(2) *d est une distance*[57] *sur E.*

*C'est la **distance induite** par la norme.*

Démonstration. Le fait que la formule (7.133) 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

$$d(x,y) = \|x-y\| = \|x-z+z-y\| \leqslant \|x-z\| + \|z-y\| = d(x,z) + d(z,y). \tag{7.134}$$

□

Définition 7.152.
La topologie associée à une norme est celle associée à la distance donnée en 7.151 par le théorème 7.108.

Corolaire 7.153.
Un espace vectoriel normé est un espace vectoriel topologique : en d'autres mots, l'addition et la multiplication par un élément du corps sont continues.

Proposition 7.154.
La norme est une application continue sur un espace vectoriel normé.
Plus précisément, si $(E, \|.\|)$ est un espace vectoriel normé, alors l'application

$$\begin{aligned} f\colon E &\to \mathbb{R} \\ x &\mapsto \|x\| \end{aligned} \tag{7.135}$$

est continue.

Proposition 7.155.
La norme sur un espace vectoriel normé est une fonction de classe C^∞.

Lemme 7.156 ([1])**.**
Soient un espace vectoriel normé E ainsi qu'une partie libre $\{a_i\}$ dans E. Si nous avons $\|\sum_i \lambda_i a_i\| < M$, alors nous avons

$$|\lambda_i|\|a_i\| < M \tag{7.136}$$

pour chaque i.

Lemme 7.157.
Soient un espace vectoriel normé $(V, \|.\|)$ ainsi qu'une isométrie $f\colon V \to V$. Si A est une partie de V telle que $f(A) \subset A$, alors

$$\bar{A} = f(\bar{A}). \tag{7.137}$$

Nous étudierons plus en détail les espaces vectoriels topologiques à partir de la définition 7.158.

57. Définition 7.106.

7.8 Espaces vectoriels topologiques

Définition 7.158.
Un espace vectoriel V sur le corps valué[58] $\mathbb{K}$ *muni d'une topologie est un* ***espace vectoriel topologique*** *si*

(1) la somme de deux vecteurs est une application continue $V \times V \to V$; et

(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[59] 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...

Proposition 7.159 ([212]).
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 :

$$T_x : V \to V \qquad \text{et} \qquad M_\lambda : V \to V \tag{7.138}$$
$$y \mapsto x + y \qquad\qquad y \mapsto \lambda y \tag{7.139}$$

sont des automorphismes[60] *de l'espace topologique V.*

Démonstration. Ce sont des bijections continues, dont les inverses sont respectivement T_{-x} et $M_{1/\lambda}$. □

Corolaire 7.160 (Invariance de la topologie[212]).
Toute base de voisinage de 0 se transporte en tout point de l'espace vectoriel topologique.

Plus précisément, si $\{A_i\}_{i\in I}$ est une base de voisinage de 0, alors $\{A_i + a\}_{i\in I}$ est une base de voisinage de a.

7.8.0.1 Somme directe topologique

Proposition-Définition 7.161 ([213, 214, 1]).
Soit V un espace vectoriel topologique et une décomposition en somme directe[61] *$V = V_1 \oplus V_2$. Alors les trois conditions suivantes sont équivalentes.*

(1) La bijection

$$\begin{aligned} \psi \colon V_1 \times V_2 &\to V \\ (x_1, x_2) &\mapsto x_1 + x_2 \end{aligned} \tag{7.140}$$

est un homéomorphisme[62].

(2) Les parties V_1 et V_2 sont fermées dans V et la projection $s \colon V_2 \to V/V_1$ est un homéomorphisme.

(3) Les parties V_1 et V_2 sont fermées dans V et la projection $\pi_2 \colon V \to V_2$ est continue.

Lorsqu'une décomposition en somme directe vérifie ces conditions, nous disons que la décomposition est ***topologique****.*

Démonstration. Avant de commencer, nous rappelons les topologies.

58. Définition 1.456.
59. Définition 1.202
60. Définition 7.37.
61. Définition 4.135.
62. 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 7.15.

— Sur V_1 et V_2 nous avons la topologie induite, définition 7.24.

— La topologie produit sur $V_1 \times V_2$ est la définition 7.15.

— La topologie quotient sur V/V_1 est la définition 7.43.

Voici quelques points qui ne dépendent pas des hypothèses (1), (2) ou (3).

(i) **La projection $p\colon V \to V/V_1$ est continue** La projection est toujours continue pour la topologie quotient ; c'est la définition même, voir 7.43.

(ii) **ψ est une bijection continue** Le fait que ψ soit continue fait partie de la définition 7.158 d'un espace vectoriel topologique. Pour que ce soit une bijection, c'est le lemme 4.136.

(iii) **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 $v - w \in V_1 \cap V_2 = \{0\}$.

(iv) **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 $[x] = s(x_2)$.

(v) **s est continue** Soit un ouvert $\mathcal{O}$ de V/V_1. La partie $p^{-1}(\mathcal{O})$ est ouverte dans V (proposition 7.44), et donc

$$s^{-1}(\mathcal{O}) = p^{-1}(\mathcal{O}) \cap V_2 \tag{7.141}$$

est ouvert dans V_2 parce que la topologie sur V_2 est celle induite[63] de la topologie de V.

Et maintenant on prouve les équivalences.

(i) **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 7.38. Mais comme $\psi\big(V_1 \times \{0\}\big) = V_1$, nous avons que V_1 est fermé dans V.

(ii) **(1) ⇒ (3)** Nous supposons que $\psi\colon V_1 \times V_2 \to V$ est un homéomorphisme. Nous considérons l'application

$$\begin{aligned} \sigma\colon V_1 \times V_2 &\to V_1 \times V_2 \\ (x, y) &\mapsto (0, y). \end{aligned} \tag{7.142}$$

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.

(iii) **(3) ⇒ (2)** L'application $\pi\colon V \to V_2$ est constante sur les classes (modulo V_1). Donc elle descend aux classes[64] en l'application

$$\begin{aligned} \tilde{\pi}\colon V/V_1 &\to V_2 \\ [x] &\mapsto \pi(x). \end{aligned} \tag{7.143}$$

Cette application est continue parce que π l'est et parce que le lemme 7.47 le dit. Le point à remarquer est que $s^{-1} = \tilde{\pi}$ parce que pour tout $x \in V_2$ nous avons

$$s\Big(\tilde{\pi}\big([x]\big)\Big) = s\big(\pi(x)\big) = s(x) = [x] \tag{7.144}$$

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.

(iv) **(2) ⇒ (1)** Nous pouvons écrire la projection $\pi_2\colon V \to V_2$ 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 savon 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.

□

63. Topologie induite, définition 7.24.
64. Voir la définition 7.46.

7.162 ([215]).
Si V est normé, il existe une façon plus directe (mais pas spécialement plus simple) de prouver l'implication (1) ⇒ (2), et en particulier la continuité de s^{-1}. Voyez 11.67.

Si V est de Banach, la continuité de s^{-1} peut venir du théorème d'isomorphisme de Banach 27.1 parce que s est une bijection continue entre espaces de Banach. Attention toutefois à vérifier que V/V_1 est de Banach [65].

7.8.0.2 Limite dans un espace vectoriel topologique

Lemme 7.163 (Changement de variables).
Soient un espace vectoriel topologique [66] 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

$$g(U') = f(U - a + b + a - b) = f(U) \subset V. \tag{7.145}$$

Donc $\lim_{x\to b} g(x) = \ell$. C'est cette égalité qui signifie $\lim_{x\to b} f(x+a-b)$. □

Proposition 7.164 (Limite de fonction composée[216]).
Soient des fonctions $f, g\colon \mathbb{R} \to \mathbb{R}$ *telles que*

$$\lim_{y\to l} f(y) = z \tag{7.146a}$$

$$\lim_{x\to a} g(x) = l. \tag{7.146b}$$

Nous supposons qu'il existe un intervalle ouvert I *contenant* l *tel que* $g(x) \neq l$ *sur* $I\backslash\{a\}$.
Alors

$$\lim_{x\to a}(f\circ g)(x) = \lim_{y\to l} f(y) = z. \tag{7.147}$$

Proposition 7.165 (Limite de fonction composée[216]).
Soient des fonctions $f, g\colon \mathbb{R} \to \mathbb{R}$ *telles que*

$$\lim_{y\to l} f(y) = z \tag{7.148a}$$

$$\lim_{x\to a} g(x) = l. \tag{7.148b}$$

Nous supposons que f *est continue en* l.
Alors

$$\lim_{x\to a}(f\circ g)(x) = \lim_{y\to l} f(y) = z. \tag{7.149}$$

Proposition 7.166.
Toute application linéaire entre espaces vectoriels topologiques de dimension finie est continue.

7.8.1 Corps topologique

Définition 7.167 (Anneau topologique[217]).
Un ***anneau topologique*** *est un anneau* [67] *muni d'une topologie dans laquelle l'addition et la multiplication sont continues* [68].

65. 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.
66. Définition 7.158.
67. Définition 1.39.
68. Définition 7.32(2).

Proposition-Définition 7.168.
Si $(\mathbb{K}, |.|)$ *est un corps valué*[69]*, alors l'application*

$$\begin{aligned} d\colon \mathbb{K}\times\mathbb{K} &\to \mathbb{R}^+ \\ (x,y) &\mapsto |x-y| \end{aligned} \tag{7.150}$$

est une distance[70].

Un corps valué muni de sa topologie métrique[71] *est un corps topologique*[72].

Lemme 7.169.
Les corps $\mathbb{R}$ *et* $\mathbb{C}$ *sont des corps valués. Leur topologie métrique (en tant que corps valués) est leur topologie usuelle.*

7.8.2 Voisinage symétrique et équilibré

Définition 7.170 (Partie symétrique[212])**.**
Une partie U *d'un espace vectoriel topologique est* ***symétrique*** *si* $x \in U$ *implique* $-x \in U$.

Définition 7.171 (Partie équilibrée[212])**.**
Une partie U *d'un espace vectoriel topologique* V *est* ***équilibrée*** *si pour tout* $|\alpha| < 1$ *dans* $\mathbb{K}$, $\alpha U \subset U$.

Lemme 7.172 ([212, 1])**.**
Soit un espace vectoriel topologique.

(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* $|\lambda| < \delta$.

(2) Tout voisinage de 0 *contient un ouvert équilibré.*

(3) Tout voisinage de 0 *contient un ouvert équilibré et symétrique.*

Démonstration. En plusieurs parties.

(i) **Pour (1)** Nous savons que $0 \cdot 0 = 0$ et que l'application

$$\begin{aligned} f\colon \mathbb{K}\times V &\to V \\ \lambda, x &\mapsto \lambda x \end{aligned} \tag{7.151}$$

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[73], il existe une boule $S' = B(0,\delta) \subset S$. Donc nous avons $f(S' \times W) \subset A$ et pour tout $|\lambda| < \delta$, $\lambda W \subset A$.

(ii) **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

$$U = \{\lambda w < \text{ tel que } |\lambda| < \delta, w \in W\}. \tag{7.152}$$

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 $\mu\lambda w \in U$.

(iii) **Pour (3)** Nous considérons U équilibré comme dans (2). Ensuite nous posons $U' = U \cap (\overline{-U})$. 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 :

69. Définition 1.456
70. Distance, définition 7.106.
71. Définition 7.108.
72. Définition 7.167.
73. Le corps $\mathbb{K}$ est un corps valué, et donc métrique par la définition 7.168.

— $x \in U$ et U est équilibré, donc $\lambda x \in U$.

— $x \in -U$ 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.

□

Lemme 7.173 ([218]).
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

$$U_1 + U_2 \subset \mathcal{O}. \tag{7.153}$$

Démonstration. Par définition d'un espace vectoriel topologique, l'application

$$\begin{aligned} f\colon V \times V &\to V \\ x, y &\mapsto x + y \end{aligned} \tag{7.154}$$

est continue. Donc la partie $f^{-1}(\mathcal{O})$ est un ouvert de $V \times V$ (c'est la définition 7.32(2) de la continuité). La définition 7.15 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

$$U_1 \times U_2 \subset f^{-1}(\mathcal{O}). \tag{7.155}$$

Donc $f(U_1 \times U_2) \subset \mathcal{O}$ et en particulier $U_1 + U_2 \subset \mathcal{O}$. □

Proposition 7.174 ([212, 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,

(2) U est équilibré

(3) U vérifie $U + U \subset \mathcal{O}$.

(4) U vérifie $U + U + U + U \subset \mathcal{O}$.

Démonstration. En plusieurs petits pas.

(i) **Le point de départ** Le lemme 7.173 donne des voisinages ouverts U_1 et U_2 de 0 dans V tels que $U_1 + U_2 \subset \mathcal{O}$.

(ii) **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.

(iii) **équilibré** C'est le moment d'utiliser le lemme 7.172. La partie U' contient un voisinage ouvert U'' de 0 qui est symétrique et équilibré. Ce U'' vérifie encore $U'' + U'' \subset \mathcal{O}$.

(iv) **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 $U + U \subset \mathcal{O}$.

□

Lemme 7.175 ([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 $\lambda U = \mathcal{O}$. □

7.8.3 Limite de suites

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

$$x_n \xrightarrow{V} x, \tag{7.156}$$

nous sous-entendons seulement que x est une limite.

De même, dans la proposition 7.177, 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 [74], nous ne pouvons pas exactement dire que le processus de limite est une opération linéaire sur l'ensemble des suites convergentes.

Lemme 7.176.
Soient un espace vectoriel topologique V ainsi qu'une suite (x_n) dans V. Nous avons

$$x_n \xrightarrow{V} x \tag{7.157}$$

si et seulement si

$$x_n - x \xrightarrow{V} 0. \tag{7.158}$$

Proposition 7.177 ([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

(1)

$$x_n + y_n \xrightarrow{V} x + y. \tag{7.159}$$

(2)

$$\lambda x_n \xrightarrow{V} \lambda x. \tag{7.160}$$

Démonstration. En deux parties.

(i) **(1)** Nous allons montrer que $x_n + y_n - (x + y) \xrightarrow{V} 0$; ce sera suffisant par le lemme 7.176.
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 7.173).
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 $x_n + y_n \xrightarrow{V} x + y$.

(ii) **(2)** En plusieurs étapes.

(i) $x_n - x \xrightarrow{V} 0$ C'est le lemme 7.176.

(ii) $\lambda x_n - \lambda x \xrightarrow{V} 0$ Soit un ouvert $\mathcal{O}$ autour de 0. Par le lemme 7.175, 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 $\lambda x_n - \lambda x \xrightarrow{V} 0$.

(iii) **Conclusion** Encore le lemme 7.176 nous permet de déduire que $\lambda x_n \xrightarrow{V} \lambda x$.

□

74. La proposition 7.56 dit qu'il y a unicité de la limite dans les espaces topologiques séparés.

7.9 Applications continues

7.9.1 Continuité

La définition de la continuité d'une fonction est donnée en 7.32.

7.178.
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 $\mathbb{R}$.

Proposition 7.179 ([219])**.**
Soient deux espaces topologiques X et Y. Une application $f\colon X \to Y$ est continue[75] *si et seulement si pour tout $x \in X$ et pour tout voisinage*[76] *V de $f(x)$, la partie $f^{-1}(V)$ est un voisinage de x dans X.*

Démonstration. En deux parties.

(i) $\Rightarrow$ 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.

(ii) $\Leftarrow$ 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 7.8.
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

$$x \in V \subset f^{-1}(\mathcal{O}). \tag{7.161}$$

Nous en déduisons que $f^{-1}(\mathcal{O})$ contient bien un ouvert autour de chacun de ses points.

□

La proposition 7.269 donnera des détails sur ce qu'il se passe lorsque l'espace est métrique.

Théorème 7.180.
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.

(i) $\Rightarrow$ 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.

(ii) $\Leftarrow$ 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 7.8 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 $f(W) \subset \mathcal{O}$.

75. Définition 7.32.
76. Définition 7.4

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 7.181.
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 7.53 et la proposition 7.104.

Lemme 7.182 ([1])**.**
Soient une fonction $f\colon X \to Y$, et un point d'accumulation $a \in X$[77]*. La fonction f est continue en a si et seulement si $f(a)$ est une limite de f en a.*

Démonstration. En deux parties.

(i) $\Rightarrow$ 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[78] a, il existe un voisinage U de a tel que $f(U) \subset V$. À fortiori, $f\big(U\backslash a\big) \subset W$ comme le demande la définition de la limite.

(ii) $\Leftarrow$ 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 $f\big(V\backslash a\big) \subset W$. Mais puisque $f(a) \in W$, nous avons $f(V) \subset W$.

□

7.9.1.1 Continuité séquentielle

Définition 7.183.
*Si X et Y sont deux espaces topologiques, une fonction $f\colon X \to \mathbb{R}$ 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.*

7.184.
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 7.231 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.

Proposition 7.185 (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

$$\lim_{x\to a} f(x) = \ell, \tag{7.162}$$

alors, pour toute suite (x_k) telle que $x_k \to a$, on a

$$\lim f(x_k) = \ell. \tag{7.163}$$

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 7.101 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. □

77. 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.

78. Continuité en un point, définition 7.32(1).

7.9.1.2 Application réciproque

Définition 7.186 (injection, surjection, bijection)**.**
Soient des ensembles A et B ainsi qu'une application $f\colon A \to B$.

*(1) La fonction f est **injective** si $f(x_1) = f(x_2)$, implique $x_1 = x_2$.*

*(2) La fonction f est **surjective** si tous les éléments de B sont atteints, c'est-à-dire si pour tout $y \in B$ il existe $x \in A$ tel que $f(x) = y$.*

*(3) La fonction f est une **bijection** entre A et B si elle est injective et surjective, c'est-à-dire si pour tout $y \in B$ il existe un unique $x \in A$ tel que $f(x) = y$.*

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 le domaine sur laquelle nous la considérons.

Définition 7.187.
*Soit $f\colon A \to B$ une bijection. L'**application réciproque** de f est la fonction*

$$\begin{aligned} f^{-1}\colon B &\to A \\ y &\mapsto \text{le } x \in A \text{ tel que } f(x) = y. \end{aligned} \tag{7.164}$$

Plus généralement si $f\colon X \to Y$ est une application quelconque et si $S \subset Y$ nous notons

$$f^{-1}(S) = \{x \in X \text{ tel que } f(x) \in S\}, \tag{7.165}$$

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 $f^{-1}(S) = \{x\}$.

Les plus acharnées parmi les lectrices se rendront compte de la différence ontologique fondamentale entre x et $\{x\}$.

7.9.2 Continuité et topologie induite

Proposition 7.188 ([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[79] de X.

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

$$f\big(W\backslash\{a\}\big) \subset V. \tag{7.166}$$

La partie $W \cap A$ est un voisinage de a pour la topologie de A, et vérifie

$$f\big(W \cap A\backslash\{a\}\big) \subset V. \tag{7.167}$$

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.

Exemple 7.189.
Que signifie d'être continue pour une fonction $f\colon \mathbb{Q} \to \mathbb{R}$? D'après le théorème 7.180, il s'agit d'être continue en chaque point de $\mathbb{Q}$. Il s'agit donc, par la définition 7.32 que pour tout $q \in \mathbb{Q}$, le nombre $f(q)$ soit une limite de f pour $x \to q$.

79. Définition 7.24.

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 7.24 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. △

Lemme 7.190 (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

$$\begin{aligned} g\colon X_2 &\to Y \\ x_2 &\mapsto f(x_1, x_2) \end{aligned} \tag{7.168}$$

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 :

$$g^{-1}(\mathcal{O}) = \{x_2 \in X_2 \text{ tel que } (x_1, x_2) \in f^{-1}(\mathcal{O})\}. \tag{7.169}$$

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 7.15 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

$$(x_1, x_2) \in A_1 \times A_2 \subset f^{-1}(\mathcal{O}). \tag{7.170}$$

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

$$g(y_2) = f(x_1, y_2) \in \mathcal{O}. \tag{7.171}$$

Cela termine la démonstration. □

7.9.3 Continuité et connexité

Proposition 7.191.
Un espace topologique X est connexe si et seulement si toute application continue[80] *$X \to \mathbb{Z}$ est constante.*

Démonstration. En deux parties.

(i) $\Rightarrow$ 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

$$\begin{aligned} A &= f^{-1}(u) \\ B &= X \backslash A. \end{aligned} \tag{7.172}$$

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.

Voila. Ce sont deux parties ouvertes non vides, disjointes qui recouvrent X. Donc X n'est pas connexe.

80. 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.

(ii) $\Leftarrow$ 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

$$\begin{aligned} f\colon X &\to \mathbb{Z} \\ x &\mapsto \begin{cases} 0 & \text{si } x \in A \\ 1 & \text{si } x \in B, \end{cases} \end{aligned} \tag{7.173}$$

nous avons une fonction continue non constante sur X à valeurs dans $\mathbb{Z}$.

□

7.192.
Pour mettre les idées au clair, dire qu'une partie A n'est pas connexe[81] signifie qu'il existe des ouverts $\mathcal{O}_1$ et $\mathcal{O}_2$ vérifiant

(1) $\mathcal{O}_i \cap A \neq \varnothing$
(2) $\mathcal{O}_1 \cap \mathcal{O}_2 = \varnothing$
(3) $A \subset \mathcal{O}_1 \cup \mathcal{O}_2$.

Lemme 7.193.
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 7.192.

(i) **A_i est ouvert** Les parties A_i sont ouvertes parce qu'elles sont images inverses d'ouverts par une fonction continue (définition 7.32(2)).

(ii) **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 $x \in f^{-1}(y) \cap A \subset A_i \cap A$.

(iii) **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 $f^{-1}(\mathcal{O}_2)$.

(iv) **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 10.87.

Exemple 7.194.
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 $E = f\big(\mathbb{R}\backslash\{0\}\big)$ et $z_0 = f(0)$. Puisque f est bijective nous avons

$$E = \mathbb{R}^2\backslash\{z_0\}, \tag{7.174}$$

qui est connexe.

Comme E est connexe et que f^{-1} est continue, le lemme 7.193 nous dit que $f^{-1}(E)$ est connexe. Mais par définition, $f^{-1}(E) = \mathbb{R}\backslash\{0\}$ qui n'est pas connexe. □

81. Connexe, définition 7.63.

7.9.4 Continuité et compacité

Théorème 7.195.
L'image d'un compact[82] *par une fonction continue est un compact.*

Dans le cadre des espaces vectoriels normés, ce théorème est démontré en la proposition 7.265.

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

$$f(K) \subseteq \bigcup_{\mathcal{O}\in\Omega} \mathcal{O}. \tag{7.175}$$

Par construction, nous avons aussi

$$K \subseteq \bigcup_{\mathcal{O}\in\Omega} f^{-1}(\mathcal{O}), \tag{7.176}$$

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

$$K \subseteq \bigcup_{i=1}^{n} f^{-1}(\mathcal{O}_i). \tag{7.177}$$

Dans ce cas, nous avons

$$f(K) \subseteq \bigcup_{i=1}^{n} \mathcal{O}_i, \tag{7.178}$$

ce qui prouve la compacité de $f(K)$. □

7.9.5 Continuité de la réciproque sur un compact

Lemme 7.196.
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.

Lemme 7.197 ([220])**.**
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 7.36 conclura. Si F est fermé dans K, alors F est compact (lemma 7.90(1)). Le théorème 7.195 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 7.90(2)). Bref, $f(F)$ est fermé. □

Lemme 7.198 ([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.

Alors en posant $S = f\big([a,b[\big)$, l'application réciproque

$$f^{-1}\colon S \to [a,b[\tag{7.179}$$

est continue.

82. Définition 7.73.

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 $f\colon [a,x] \to V_x$ vérifie le lemme 7.197. Donc l'application réciproque $f^{-1}\colon V_x \to [a,x]$ est continue.

Le théorème 7.180 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 point est dans un V_x. Le théorème 7.180 (dans l'autre sens) montre alors que ${}^{-1}\colon S \to [a,b[$ est continue. □

7.9.6 Topologie et matrices

Lemme-Définition 7.199 (Topologie sur les matrices)**.**
Si $\mathbb{K}$ est un corps valué[83]*, alors l'opération*

$$\begin{aligned}\|.\|_{\mathbb{M}}\colon \mathbb{M}(n\times m,\mathbb{K}) &\to \mathbb{R}^+\\ M &\mapsto \max_{kl}\|M_{kl}\|_{\mathbb{K}}.\end{aligned} \tag{7.180}$$

est une norme[84]*.*

Cette norme est appelée ***norme maximum*** *et nous considérons sur $\mathbb{M}(n\times m,\mathbb{K})$ la topologie associée à cette norme*[85]

Proposition 7.200.
La multiplication matricielle est une opération continue.

7.10 Produit fini d'espaces vectoriels normés

Dans cette section nous parlons de produits finis d'espaces. Cela ne signifie pas que chacun des espaces soient séparément de dimension finie.

7.10.1 Distance et norme produit

Proposition-Définition 7.201 (Distance produit)**.**
Si (E_1,d_1),..., (E_n,d_n) sont des espaces métriques alors la formule

$$d(x,y) = \max_{i=1,\dots,n} d_i(x_i,y_i) \tag{7.181}$$

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 7.201 :

Lemme-Définition 7.202 ([221])**.**
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. □

Lemme-Définition 7.203.
Soient deux espaces vectoriels normés V et W.

83. Définition 1.456.
84. Définition 7.146.
85. Définition 7.152.

(1) L'opération

$$\|(v,w)\|_{V\times W} = \max\{\|v\|_V, \|w\|_W\}. \tag{7.182}$$

est une norme[86] *sur* $V\times W$.

(2) La topologie de cette norme[87] *est la même que la topologie produit*[88] *sur* $V\times W$.

Démonstration. En plusieurs parties.

(i) **Norme** On doit vérifier les trois conditions de la définition 7.146.

— 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 :

$$\|a(v,w)\|_{V\times W} = \max\{\|av\|_V, \|aw\|_W\} = |a|\max\{\|v\|_V, \|w\|_W\} = |a|\|(v,w)\|_{V\times W}. \tag{7.183}$$

— Soient (v_1,w_1) et (v_2,w_2) dans $V\times W$.

$$\begin{aligned}\|(v_1,w_1)+(v_2,w_2)\|_{V\times W} &= \max\{\|v_1+v_2\|_V, \|w_1+w_2\|_W\}\\ &\leqslant \max\{\|v_1\|_V + \|v_2\|_V, \|w_1\|_W + \|w_2\|_W\}\\ &\leqslant \max\{\|v_1\|_V, \|w_1\|_W\} + \max\{\|v_2\|_V, \|w_2\|_W\}\\ &= \|(v_1,w_1)\|_{V\times W} + \|(v_2,w_2)\|_{V\times W}.\end{aligned} \tag{7.184}$$

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.

(ii) **Équivalence** (i) **Dans un sens** La définition 7.15 de la topologie produit dit qu'une prébase de $V\times W$ est donnée par

$$\big\{B(v,r)\times B(w,s) \text{ tel que } v\in V; w\in W; r,s>0\big\}. \tag{7.185}$$

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

$$d\big((v_1,w_1),(v_0,w_0)\big) = \delta < \max\{r,s\}. \tag{7.186}$$

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 :

$$\begin{aligned} d\big((v,w),(v_0,w_0)\big) &\leqslant d\big((v,w),(v_1,w_1)\big) + d\big((v_1,w_1),(v_0,w_0)\big) && \text{(7.187a)}\\ &< \epsilon+\delta. && \text{(7.187b)}\end{aligned}$$

Si ϵ est assez petit, le tout reste plus petit que $\max\{r,s\}$.

Donc S est bien un ouvert métrique par le théorème 7.8. 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.

(ii) **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

$$B\big((v_0,w_0),r\big)\subset\mathcal{O}. \tag{7.188}$$

86. Définition 7.146.
87. Topologie associée à une norme : c'est la topologie associée à la distance correspondante, définition 7.152.
88. Topologie produit, définition 7.15.

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

$$d\big((v_1,w_1),(v_0,w_0)\big)=\max\{\|v_1-v_0\|,\|w_1-w_0\|\}<r \tag{7.189}$$

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.

□

7.204.
En particulier, pour la topologie de la norme maximum, la convergence d'une suite implique la convergence « composante par composante » par la proposition 7.59.

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 $\texttt{proj}_V$ et $\texttt{proj}_W$ et sont définies par

$$\begin{aligned}\texttt{proj}_V\colon V\times W&\to V\\(v,w)&\mapsto v\end{aligned} \tag{7.190}$$

et

$$\begin{aligned}\texttt{proj}_W\colon V\times W&\to W\\(v,w)&\mapsto w.\end{aligned} \tag{7.191}$$

Les inégalités suivantes sont évidentes

$$\begin{aligned}\|\texttt{proj}_V(v,w)\|_V&\leqslant\|(v,w)\|_{V\times W}\\\|\texttt{proj}_W(v,w)\|_W&\leqslant\|(v,w)\|_{V\times W}.\end{aligned} \tag{7.192}$$

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 $\texttt{proj}_V$ (respectivement $\texttt{proj}_W$) 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 $\text{Int}(A\times B)=\text{Int}\,A\times\text{Int}\,B$.

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 le lemme 11.68.

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 7.205.
Si V et W sont deux espaces vectoriels, nous pouvons considérer le produit $E=V\times W$. Les projections $\texttt{proj}_V$ et $\texttt{proj}_W$, définies dans la section 7.10, sont des applications linéaires.

En effet, la projection $\texttt{proj}_V : V \times W \to V$ est donnée par $\texttt{proj}_V(v,w) = v$. Alors,

$$\begin{aligned}\texttt{proj}_V\big((v,w)+(v',w')\big) &= \texttt{proj}_V\big((v+v'),(w+w')\big)\\ &= v+v'\\ &= \texttt{proj}_V(v,w)+\texttt{proj}_V(v',w'),\end{aligned} \tag{7.193}$$

et

$$\texttt{proj}_V\big(\lambda(v,w)\big) = \texttt{proj}_V\big((\lambda v,\lambda w)\big) = \lambda v = \lambda\,\texttt{proj}_V(v,w). \tag{7.194}$$

Nous laissons au lecteur le soin d'adapter ces calculs pour montrer que $\texttt{proj}_W$ est également une projection[89]. △

Proposition 7.206.
Si $\mathcal{O}$ est un voisinage de (a,b) dans $V\times W$ alors $\mathcal{O}$ contient un ouvert de la forme $B(a,r)\times B(b,r)$.

Démonstration. Puisque $\mathcal{O}$ est un voisinage, il contient un ouvert et donc une boule

$$B\big((a,b),r\big) = \{(v,w)\in V\times W \text{ tel que } \max\{\|v-a\|,\|w-b\|\}<r\}. \tag{7.195}$$

Évidemment l'ensemble $B(a,r)\times B(b,r)$ est dedans. □

7.11 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 7.203.

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 10.90.

7.11.1 Ouverts et fermés

La proposition suivante est évidemment à mettre en rapport avec le théorème 7.8.

Proposition 7.207.
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 7.98 de la topologie métrique. □

Lemme 7.208.
Pour tout $x\in\mathbb{R}^n$ et tout $r>0$ la boule[90] *$B(x,r)$ 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,

$$d(x,p') \leqslant d(x,p)+d(p,p') \leqslant d(x,p)+r-d(p,x) = r. \tag{7.196}$$

□

89. Écrivez-moi si ça pose un problème.
90. Définition 7.108.

7.11.2 Point d'accumulation, point isolé

Les définitions de point d'accumulation et de point isolé sont 7.30 et 7.31. Nous voyons maintenant ce que ces définitions donnent dans le cas de l'espace topologique $\mathbb{R}$.

Lemme 7.209.
Soit $D \subset \mathbb{R}$. Un point $a \in D$ est isolé dans D si et seulement si il existe $\varepsilon > 0$ tel que

$$[a-\varepsilon, a+\varepsilon] \cap D = \{a\}. \tag{7.197}$$

Autrement dit, il existe un intervalle autour de a dans lequel a est le seul élément de D.

Lemme 7.210.
Un point $a \in \mathbb{R}$ est un point d'accumulation de D si pour tout $\varepsilon > 0$,

$$\Big([a-\varepsilon, a+\varepsilon]\backslash\{a\}\Big) \cap D \neq \varnothing. \tag{7.198}$$

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 7.211.
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 7.212.
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. △

Exemple 7.213.
Soit $D =]1,2[\cup \{12\}$. Le point 12 est adhérence, mais pas d'accumulation parce que le voisinage $]9,14[$ n'intersectionne pas $D\backslash\{12\}$. △

7.11.3 Limite de suite

Définition 7.214 (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*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ tel que } \forall n \geqslant N,\ \|x_n - \ell\| < \varepsilon. \tag{7.199}$$

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 7.215.
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 7.216 (Unicité de la limite)**.**
Il ne peut pas y avoir deux nombres différents qui satisfont à la condition (7.199). 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

$$\|x_n - \ell\| < \varepsilon \tag{7.200}$$

pour tout $n \geqslant N$, et $N' > 0$ tel que

$$\|x_n - \ell'\| < \epsilon \tag{7.201}$$

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

$$\|\ell - \ell'\| = \|\ell - x_n + x_n - \ell'\| \leqslant \|\ell - x_n\| + \|x_n - \ell'\| < 2\varepsilon. \tag{7.202}$$

Cela prouve que $\|\ell - \ell'\| = 0$. □

Le théorème de Bolzano-Weierstrass 7.134 dit que dans le cas métrique, la compacité séquentielle est équivalente à la compacité.

7.12 Topologie et distance

Lemme 7.217.
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

$$\big\{B(y_1, r_1) \times B(y_2, r_2)\big\}_{\substack{y_i \in A_i \\ r_i \in \mathbb{Q}^+}} \tag{7.203}$$

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 [91], 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

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}). \tag{7.204}$$

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

$$d_i(z_i, x_i) \leqslant d(z_i, y_i) + d(y_i, x_i) \leqslant \frac{r_i}{2} + \frac{r_i}{2} = r_i. \tag{7.205}$$

Au final,

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}) \subset \mathcal{O}. \tag{7.206}$$

□

Définition 7.218.
*Si (X, d_X) et (Y, d_Y) sont des espaces métriques, une **isométrie** est une application bijective $f : X \to Y$ telle que pour tout $x, y \in X$ nous ayons*

$$d_Y\big(f(x), f(y)\big) = d_X(x, y). \tag{7.207}$$

Remarque 7.219.
Une application vérifiant (7.207) est automatiquement injective. En pratique, il ne faut donc vérifier que la surjectivité.

Exemple 7.220 (Manque de surjectivité)**.**
Si $X = [0, \infty[$ et $f(x) = x + 1$ alors f vérifie (7.207) pour la distance $d(x, y) = |x - y|$, mais n'est pas surjective. △

Proposition-Définition 7.221 (Groupe des isométries)**.**
Si (X, d) est un espace métrique,

91. Définition 7.15.

(1) l'ensemble des isométries de X, noté $\mathrm{Isom}(X)$ *est un groupe pour la composition.*

(2) Ce groupe agit fidèlement[92] *sur X.*

Proposition 7.222.
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 7.223.
Si X est un ensemble, nous pouvons écrire la **distance discrète** :

$$d(x,y) = \begin{cases} 0 & \text{si } x = y \\ 1 & \text{si } x \neq y. \end{cases} \tag{7.208}$$

La topologie résultante est la topologie discrète, côtoyée dans l'exemple 7.10[93].

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. △

7.12.0.1 Distance point-ensemble

Définition 7.224.
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*

$$d(x,A) = \inf_{a\in A} d(x,a). \tag{7.209}$$

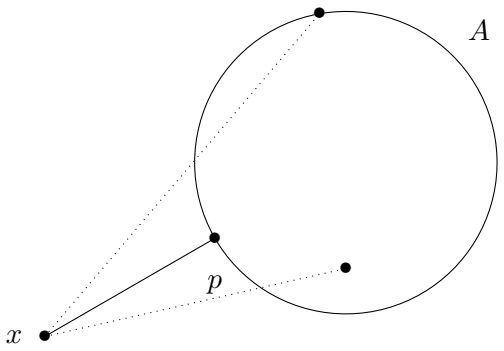


FIGURE 7.1 – La distance entre x et A est donnée par la distance entre x et p. Les distances entre x et les autres points de A sont plus grandes que $d(x,p)$.

7.12.1 Suites et espaces métriques

Proposition 7.225 (Caractérisation séquentielle de la limite[1])**.**
Soient deux espaces métriques X et Y ainsi qu'une fonction $f\colon X \to Y$. Soit $a \in X$ et $\ell \in Y$. On a

$$\lim_{x\to a} f(x) = \ell, \tag{7.210}$$

si et seulement si, pour toute suite (x_k) telle que $x_k \to a$, on a

$$\lim f(x_k) = \ell. \tag{7.211}$$

Par ailleurs, l'une des deux limites existe si et seulement si l'autre existe.

92. Si vous ne savez pas ce que c'est, alors vous avez zappé la définition 2.30.
93. Vérifiez-le tout de même !

Démonstration. Le sens direct est la proposition 7.185. 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.

Corolaire 7.226 (Caractérisation séquentielle de la continuité en un point[1])**.**
Si X et Y sont des espaces métriques, alors une fonction $f\colon X \to Y$ 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 7.227 (Fermeture séquentielle[222])**.**
*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.

Proposition 7.228 (Caractérisation séquentielle d'un fermé)**.**
Soient X un espace métrique 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.

Démonstration. Une suite contenue dans un fermé ne peut converger que vers un élément de ce fermé : c'était la proposition 7.50. 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 $X\backslash F$ ne soit pas ouvert. Alors il existe $x \in X\backslash F$ 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 7.51 ; mais, donnons-en une preuve tout de même.

Lemme 7.229.
Soit X un espace métrique, 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[94] $B(\ell,r) \cap A = \varnothing$. 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 $x_n \to \ell$. □

Corolaire 7.230.
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.

94. Une autre manière de dire la même chose : si $\ell \notin \bar{A}$, alors $d(\ell,A) > 0$.

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 de la lectrice.). □

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.

Proposition 7.231 (Caractérisation séquentielle de la continuité[1])**.**
Soient X et Y deux espaces topologiques séparés. Nous supposons que X est métrisable. Une application $f: X \to Y$ est continue sur X si et seulement si elle est séquentiellement continue sur X.

Démonstration. Le sens direct est déjà prouvé dans la proposition 7.185. Nous nous concentrons donc sur la réciproque.

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 $x_k \in X\backslash f^{-1}(\mathcal{O})$ pour tout k. Nous allons montrer que $x \in X\backslash f^{-1}(\mathcal{O})$ et la caractérisation séquentielle [95] de la fermeture conclura que $X\backslash f^{-1}(\mathcal{O})$ est fermé.

Pour tout k, nous avons $f(x_k) \in X\backslash\mathcal{O}$, 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 $Y\backslash\mathcal{O}$, la limite est également dans $Y\backslash\mathcal{O}$. Nous en déduisons que $f(x) \in Y\backslash\mathcal{O}$, de telle sorte que $x \in X\backslash f^{-1}(\mathcal{O})$. □

Proposition 7.232.
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 7.127, ou proposition 7.226). 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

$$f(a_n) \to f(x) \tag{7.212a}$$
$$g(a_n) \to g(x), \tag{7.212b}$$

mais pour tout n, $f(a_n) = g(a_n)$. Par unicité de la limite [96] dans Y, $f(x) = g(x)$. □

7.12.2 Espace métrisable

Définition 7.233 (Espace vectoriel topologique métrisable[223])**.**
*Un espace topologique est **métrisable** si il existe une distance compatible avec la topologie.*

Proposition 7.234 ([224])**.**
Soit un espace topologique métrisable X.

(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

$$V_n = \{x \in X \text{ tel que } d(x, A) < \frac{1}{n}\}. \tag{7.213}$$

Et juste pour faire simple nous notons $V_0 = X$.

95. Proposition 7.228, valable parce que la topologie de X provient d'une métrique.
96. Proposition 7.104.

(i) **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 7.8. 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

$$d(y,a) \leqslant d(y,x) + d(x,a) < \epsilon + \frac{1}{n}. \tag{7.214}$$

Nous pouvons donc choisir ϵ de telle sorte que $d(y,a) < 1/n$. Avec ce ϵ, nous avons, pour tout $y \in B(x,\epsilon)$:

$$d(y,A) \leqslant d(y,a) < \frac{1}{n} \tag{7.215}$$

et donc $y \in V_n$.

(ii) **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 7.139.

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

$$\mathcal{O}^c = \bigcap_{n\in\mathbb{N}} V_n, \tag{7.216}$$

ce qui donne immédiatement

$$\mathcal{O} = \bigcup_{n\in\mathbb{N}} V_n^c \tag{7.217}$$

où les V_n^c sont fermés. □

Corolaire 7.235.
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 7.234. □

7.13 Suites de Cauchy, métrique et espaces complets

7.13.1 Généralités

Définition 7.236 (Suite de τ-Cauchy, espace vectoriel topologique[225, 212])**.**
*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 $k,l \geqslant N$.*

Définition 7.237 (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*[97] *vers un élément de A.*

Définition 7.238 (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 1.367). Dans ce contexte, le ϵ était pris dans le corps lui-même.

97. Définition 7.13.

Définition 7.239 (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.*

7.240.
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 7.242 que le même espace topologique peut accepter plusieurs distances différentes (donnant la même topologie) donnant lieu à des suites de Cauchy différentes.

(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.

Définition 7.241 (espace de Banach, algèbre de Banach[226])**.**
Un ***espace de Banach*** *est un espace vectoriel normé complet*[98] *pour la topologie de la norme.*

Une ***algèbre de Banach*** *est une algèbre commutative et associative qui est un espace vectoriel normé complet.*

Exemple 7.242 (La complétude n'est pas une propriété topologique[227])**.**
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 $\mathbb{N}$:

$$d_1(x,y) = \left|\frac{1}{x} - \frac{1}{y}\right|. \tag{7.218}$$

Pour vérifier que cette formule définit bien une distance (définition 7.106), le seul point non immédiat est l'inégalité triangulaire :

$$d_1(x,y) = \left|\frac{1}{x} - \frac{1}{y}\right| \leqslant \left|\frac{1}{x} - \frac{1}{z}\right| + \left|\frac{1}{z} - \frac{1}{y}\right| = d_1(x,z) + d_1(z,y). \tag{7.219}$$

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

$$\left|\frac{1}{x} - \frac{1}{y}\right| < \epsilon \tag{7.220}$$

pour $y \in \mathbb{N}$. Nous trouvons que $\frac{1}{y} > \frac{1}{x} - \epsilon$ et $\frac{1}{y} < \frac{1}{x} + \epsilon$, soit

$$\begin{cases} y > \dfrac{1}{\frac{1}{x} + \epsilon} & \text{(7.221a)} \\ y < \dfrac{1}{\frac{1}{x} - \epsilon}. & \text{(7.221b)} \end{cases}$$

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.

98. Définition 7.239.

L'espace topologique associé à $(\mathbb{N}, d_1)$ est donc la topologie discrète[99].

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

$$(\mathbb{N}, d) \simeq (\mathbb{N}, d_1). \tag{7.222}$$

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 1.424) nous avons, pour $n, m > N$:

$$\left|\frac{1}{n} - \frac{1}{m}\right| < \frac{1}{n} < \frac{1}{N} < \epsilon. \tag{7.223}$$

Or cette suite ne converge pas. Soit en effet un candidat limite k. Calculons

$$d_1(x_n, k) = \left|\frac{1}{n} - \frac{1}{k}\right| \to \frac{1}{k} \neq 0. \tag{7.224}$$

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.

△

Proposition 7.243 ([228])**.**
Le dual[100] *d'un espace de Banach*[101] *est de Banach.*

7.13.2 Espace topologique métrique

Dans les espaces vectoriels topologiques métriques, il n'y a pas d'ambiguïté.

Proposition 7.244 (Caractérisations avec la distance d)**.**
Soit (E, d) un espace vectoriel topologique métrique.

(1) Une suite (x_n) dans E est convergente[102] *vers x si et seulement si pour tout $\epsilon \in \mathbb{R}$ 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[103] *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 :

(i) **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 $d(x, x_k) \leqslant \epsilon$.

99. Celle dont toutes les parties sont des ouverts.
100. Définition 4.123.
101. Définition 7.241.
102. Définition 7.13.
103. Définition 7.236.

(ii) **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 7.108 et en particulier la liste des ouverts est donnée par (7.98). Il existe donc une boule $B(x, \epsilon)$ incluse à $\mathcal{O}$. Pour tout $k > N_\epsilon$ nous avons alors $x_k \in B(x, \epsilon) \subset \mathcal{O}$.

En ce qui concerne les suites de Cauchy :

(i) **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 7.151(1)) nous avons

$$d(u, 0) = d(x_p - x_q, 0) = d(x_p, x_q). \tag{7.225}$$

Par conséquent $d(x_p, x_q) \leqslant \epsilon$.

(ii) **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

$$d(x_p, x_q) = d(x_p - x_q, 0), \tag{7.226}$$

et comme cela est plus petit que ϵ, nous avons $x_p - x_q \in B(0, \epsilon) \subset \mathcal{O}$.

□

Proposition 7.245 ([229]).
Toute suite convergente dans un espace métrique est de Cauchy.

Démonstration. Nous utilisons les caractérisations de la proposition 7.244 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 7.244(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

$$d(x_n, x_m) \leqslant d(x_m, \ell) + d(l, x_m) \leqslant 2\epsilon. \tag{7.227}$$

Cela prouve que (x_n) est une suite de Cauchy. □

7.13.3 Compacts, fermés

Proposition 7.246 (Séparation [212, 230]).
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

$$(K + U) \cap (F + U) = \varnothing. \tag{7.228}$$

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.

(i) **Quelque chose sans intersection avec F** Par la proposition 7.174, il existe un ouvert symétrique U_x autour de 0 tel que

$$U_x + U_x + U_x + U_x \subset F^c - x. \tag{7.229}$$

En enlevant un des éléments de la somme, nous gardons la même inclusion :

$$U_x + U_x + U_x \subset F^c - x. \tag{7.230}$$

Et en passant le x de l'autre côté :

$$x + U_x + U_x + U_x \subset F^c. \tag{7.231}$$

Cela pour dire que nous avons, pour chaque $x \in K$ un voisinage ouvert U_x de 0 tel que

$$(x + U_x + U_x + U_x) \cap F = \varnothing. \tag{7.232}$$

(ii) $\underline{(x + U_x + U_x) \cap (U_x + F) = \varnothing}$ 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)

$$f = z - v \in z + U_x \tag{7.233}$$

Mais z est aussi dans $x + U_x + U_x$. Donc

$$f \in z + U_x \subset x + U_x + U_x + U_x. \tag{7.234}$$

Cela prouve que $x + U_x + U_x + U_x \cap F \neq \varnothing$, en contradiction avec (7.232). Nous en concluons que

$$(x + U_x + U_x) \cap (U_x + F) = \varnothing. \tag{7.235}$$

(iii) **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 7.73 d'un compact) : nous avons $\{x_i\}_{i=1,\dots,n}$ tels que

$$K \subset \bigcup_{i=1}^{n} (x_i + U_{x_i}). \tag{7.236}$$

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 (7.235) pour chacun des x_i :

$$(x + U_{x_i} + U_{x_i}) \cap (F + U_{x_i}) = \varnothing. \tag{7.237}$$

Lorsqu'on enlève des éléments dans une intersection vide, l'intersection reste vide. Donc en remplaçant des U_{x_i} par des U dans (7.237), nous conservons une intersection vide :

$$(x + U_{x_i} + U) \cap (F + U) = \varnothing. \tag{7.238}$$

(iv) **Conclusion** Aucun ensemble de la forme $x + U_{x_i} + U$ n'intersecte $F + U$. L'union ne l'intersecte pas non plus :

$$\bigcup_{i=1}^{n} (x + U_{x_i}) + U \cap (F + U) = \varnothing. \tag{7.239}$$

Et donc

$$(K + U) \cap (F + U) = \varnothing, \tag{7.240}$$

comme nous le voulions.

□

Définition 7.247.
Une distance d sur un espace vectoriel topologique V est dite ***compatible*** *avec la topologie si la topologie induite*[104] *de d est celle de V.*

104. Définition 7.108.

Définition 7.248.
Une distance d sur un espace vectoriel V est dite ***invariante*** *si pour tout $x, y, a \in V$ nous avons*

$$d(x+a, y+a) = d(x, y). \tag{7.241}$$

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.

Lemme 7.249 ([1]).
Soit un espace vectoriel muni d'une distance invariante. Alors

$$B(a, r) + x = B(a + x, r). \tag{7.242}$$

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 $d(y - x, a) = d(y - x + x, a + x) = d(y, a + x) < r$. □

<++>

Une version plus complète du lemme suivant sera dans la proposition 11.134 et ce qui suit.

Lemme 7.250.
Nous introduisons l'ensemble $\mathbb{D}_2$ des suites finies dans $\{0, 1\}$ [105].

L'application

$$\begin{aligned} \varphi\colon \mathbb{D}_2 &\to [0, 1[\\ x &\mapsto \sum_{i=1}^{l(x)} \frac{x_i}{2^i}. \end{aligned} \tag{7.243}$$

où $l(x)$ est la longueur de la suite finie x est injective.

Démonstration. Le lemme 1.468 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,

$$x \leqslant \sum_{i=1}^{n} \left(\frac{1}{2}\right)^i = \frac{1 - (1/2)^{n+1}}{1/2} - 1 = 1 - (1/2)^{n+1} < 1. \tag{7.244}$$

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 :

$$0 = \frac{1}{2^{n_0}} + \sum_{i=n_0+1}^{N} \frac{x_i - y_i}{2^i}. \tag{7.245}$$

105. C'est en gros ce qui se fera dans 11.132 pour les développements de nombres dans une base donnée, sauf qu'ici nous n'avons pas besoin de subtilités sur les queues de suites.

Le deuxième terme est majoré de la façon suivante :

$$|\sum_{i=n_0+1}^{N}\frac{x_i-y_i}{2^i}| \leqslant \sum_{i=n_0+1}^{N}\frac{|x_i-y_i|}{2^i} \tag{7.246a}$$

$$\leqslant \sum_{i=n_0+1}^{N}\frac{1}{2^i} \tag{7.246b}$$

$$= \sum_{i=1}^{N}\left(\frac{1}{2}\right)^i-\sum_{i=1}^{n_0}\left(\frac{1}{2}\right)^i \tag{7.246c}$$

$$= \frac{1-(1/2)^{N+1}}{1/2}-\frac{1-(1/2)^{n_0+1}}{1/2} \tag{7.246d}$$

$$= \frac{1}{2^{n_0}}-\frac{1}{2^N} \tag{7.246e}$$

$$< \frac{1}{2^{n_0}}. \tag{7.246f}$$

L'égalité (7.245) 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. □

Toujours avec l'application φ du lemme 7.250 nous avons ceci.

Lemme 7.251.
Soient $r,s\in\varphi(\mathbb{D}_2)$ tels que $r+s<1$. Alors $r+s\in\varphi(\mathbb{D}_2)$.

Lemme 7.252.
Soient $r,s\in\varphi(\mathbb{D}_2)$ tels que $r+s<1$. Nous posons $u=\varphi^{-1}(r)$, $v=\varphi^{-1}(s)$ et $w=\varphi^{-1}(r+s)$. Si k est le plus petit entier tel que $w_k\neq u_k+v_k$, alors $u_k=v_k=0$ et $w_k=1$.

Théorème 7.253 (Espace topologique métrisable[212, 1])**.**
Si V est un espace vectoriel topologique. Nous supposons :

(1) Tout point admet une base dénombrable de topologie[106]*.*

(2) Le singleton $\{0\}$ est fermé[107]*.*

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 : $\{A_i\}_{i\in\mathbb{N}}$.

(i) **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 7.174 donne un ouvert symétrique équilibré dans A_0. Nous le nommons U_0 :

$$U_0\subset A_0. \tag{7.247}$$

Pour les suivants, U_{k+1} est un ouvert symétrique équilibré dans $U_k\cap A_k$ vérifiant

$$U_{k+1}+U_{k+1}+U_{k+1}+U_{k+1}\subset A_k\cap U_k. \tag{7.248}$$

Le fait est que $A_k\cap U_k$ est un ouvert autour de 0 ; donc la proposition 7.174 permet de construire un ouvert symétrique et équilibré U_{k+1} autour de 0 ayant la propriété demandée.

(ii) **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 7.2 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.

106. Définition 7.2.
107. Attention : dans [212], cela fait partie de la définition d'un espace vectoriel topologique et n'est donc pas listé dans les hypothèses de ce théorème.

(iii) **Quelques inclusions** Notons au passage quelques inclusions. Pour tout $n \in \mathbb{N}$ nous avons

$$U_{n+1} + U_{n+1} + U_{n+1} + U_{n+1} \subset U_n. \tag{7.249}$$

À fortiori nous avons

$$U_{n+1} \subset U_n \tag{7.250}$$

et pour tout $n, k \in \mathbb{N}$, nous obtenons alors

$$U_{n+1} + U_{n+2} + \cdots + U_{n+(k-1)} + U_{n+k} \subset U_{n+1} + U_{n+1} \subset U_n. \tag{7.251}$$

(iv) **L'ensemble D** Nous considérons l'ensemble $\mathbb{D}_2$ et l'application φ du lemme 7.250. 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 $r \in D$.

(v) **La fonction ϕ** Nous définissons maintenant une fonction à valeurs dans la topologie τ_V de V :

$$\begin{aligned} \phi\colon D \cup [1, +\infty[&\to \tau_V \\ r &\mapsto \begin{cases} V & \text{si } r \geqslant 1; \\ \sum_i \varphi^{-1}(r)_i U_i & \text{si } r \in D. \end{cases} \end{aligned} \tag{7.252}$$

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.

(i) **Une égalité facile** Si je ne me trompe pas d'un off-by-one, nous avons

$$\phi(1/2^N) = U_N. \tag{7.253}$$

(ii) **$0 \in \phi(r)$ pour tout r** En effet, $\phi(r)$ n'est jamais vide, c'est toujours un voisinage de 0.

(iii) **$\phi(r) + \phi(s) \subset \phi(r+s)$** 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.

(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 :

$$\phi(r+s) = \sum_i w_i U_i = \sum_i u_i U_i + \sum_i v_i U_i = \phi(r) + \phi(s); \tag{7.254}$$

(ii) **Second cas** Sinon, posons k le plus petit entier tel que $w_k \neq u_k + v_k$. Alors le lemme 7.252 dit que $u_k = v_k = 0$ et $w_k = 1$. Nous avons d'abord

$$\phi(r) = \sum_{i=1}^{k-1} u_i U_i + \sum_{i=k+1}^{n} u_i U_i \subset \sum_{i=1}^{k-1} u_i U_i + U_{k+1} + U_{k+1} \tag{7.255}$$

où nous avons utilisé (7.250) pour tous les derniers termes. De même nous avons :

$$\phi(s) = \sum_{i=1}^{k-1} v_i U_i + \sum_{i=k+1}^{n} v_i U_i \subset \sum_{i=1}^{k-1} v_i U_i + U_{k+1} + U_{k+1}. \tag{7.256}$$

En combinant, et en utilisant (7.249),

$$\phi(r)+\phi(s)=\sum_{i=1}^{k-1}u_iU_i+\sum_{i=1}^{k-1}v_iU_i+\underbrace{U_{k+1}+U_{k+1}+U_{k+1}+U_{k+1}}_{\subset U_k} \tag{7.257a}$$

$$\subset\sum_{i=1}^{k-1}w_iU_i+U_k \tag{7.257b}$$

$$=\sum_{i=1}^{k}w_iU_i \tag{7.257c}$$

$$\subset\phi(r+s). \tag{7.257d}$$

Pour (7.257c) nous avons utilisé le fait que $w_k=1$. Au final nous avons bien $\phi(r)+\phi(s)\subset\phi(r+s)$.

(iv) ϕ **est croissante** Dans notre contexte « croissante » signifie que si $r<s$ alors $\phi(r)\subset\phi(s)$. Il suffit d'écrire

$$\phi(r)\subset\phi(r)+\phi(s-r)\subset\phi(s). \tag{7.258}$$

(iv) **Définition de la distance (enfin !)** Nous définissons l'application

$$\begin{aligned}f\colon V&\to\mathbb{R}\\ x&\mapsto\inf\{r\text{ tel que }x\in\phi(r)\},\end{aligned} \tag{7.259}$$

et ensuite ce qui va être notre distance :

$$d(x,y)=f(y-x). \tag{7.260}$$

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.

(v) d **est invariante par translation** Il s'agit seulement d'écrire $d(x+a,y+a)$ et de remarquer que $(y+a)-(x+a)=y-x$.

(v) $d(x,x)=0$ Oui, car 0 est dans $\phi(r)$, pour tout r, puisque les U_i sont des voisinages de 0.

(vi) $d(x,y)=0$ **implique** $x=y$ Nous montrons que $f(x)\neq0$ dès que $x\neq0$. Rappellez-vous que nous avons posé l'hypothèse que $\{0\}$ est un fermé dans V. Vu que $\{x\}$ est un compact [108], la proposition 7.246 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

$$x\notin U_k \tag{7.261}$$

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

$$\phi(\epsilon)\subset U_k \tag{7.262}$$

et donc $x\notin\phi(\epsilon)$. Donc

$$f(x)\geqslant\frac{1}{2^k}>0 \tag{7.263}$$

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.

(vii) $d(x,y)=d(y,x)$ Oui, car tous les voisinages considérés sont symétriques. Donc $x-y\in\phi(r)$ si et seulement si $y-x\in\phi(r)$.

108. Les singletons sont toujours des compacts dans les espaces topologiques.

(viii) $d(x,z) \leqslant d(x,y) + d(y,z)$ 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 1.428, il existe r et s dans $\varphi(\mathbb{D}_2)$ tels que :

$$d(x,y) < r < d(x,y) + \frac{\epsilon}{2} \quad \text{et} \quad d(y,z) < s < d(y,z) + \frac{\epsilon}{2}. \tag{7.264}$$

En sommant :

$$d(x,y) + d(y,z) < r + s < d(x,y) + d(y,z) + \epsilon. \tag{7.265}$$

Vu que ϕ est croissante, on a $y - x \in \phi(r)$ et $z - y \in \phi(s)$; donc

$$z - x = (y - x) + (z - y) \in \phi(r) + \phi(s) \subset \phi(r + s) \tag{7.266}$$

Ainsi, pour tout $\epsilon > 0$, on a

$$d(x,z) \leqslant r + s < d(x,y) + d(y,z) + \epsilon. \tag{7.267}$$

(ix) **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 7.2.

(i) **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

$$U_n \subset \mathcal{O} - x. \tag{7.268}$$

Nous avons alors

$$B(0, \frac{1}{2^n}) \subset U_n \subset \mathcal{O} - x. \tag{7.269}$$

Nous utilisant le lemme 7.249 pour additionner x dans toutes les inclusions :

$$B(x, \frac{1}{2^n}) = B(0, \frac{1}{2^n}) + x \subset \mathcal{O}. \tag{7.270}$$

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.

(ii) **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

$$U_n \subset B(0,r). \tag{7.271}$$

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.

□

7.13.4 Équivalence entre Cauchy et $\tau-$Cauchy

Lemme 7.254.
Soit un espace vectoriel topologique[109] V *et une distance* $d\colon V \times V \to \mathbb{R}^+$ *compatible*[110] *avec la topologie de* V. *Si* d *est invariante*[111], *alors les suites de Cauchy pour* d *et les suites* τ*-Cauchy sont les mêmes.*

Démonstration. Nous avons deux implications à prouver.

109. Définition 7.158.
110. Définition 7.247.
111. Définition 7.248.

(i) **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

$$d(0,x_m-x_n)<\epsilon, \tag{7.272}$$

c'est-à-dire $x_m-x_n\in B(0,\epsilon)\subset U$. La suite (x_n) est donc τ-Cauchy.

(ii) **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.

Théorème-Définition 7.255.
Soit V un espace vectoriel topologique métrisable[112]*, 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 7.253. Vu qu'elle est invariante par translation, les suites d-Cauchy sont exactement les suites τ-Cauchy par le lemme 7.254. □

Remarque 7.256.
Même si V est métrisable, si on choisit la métrique n'importe comment, on ne peut rien espérer.

7.257.
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 1.438 qui en est un lemme indispensable mais qui parle de notions différentes, bien que très liées.

Théorème 7.258 (Complétude de $\mathbb{R}$, critère de Cauchy[17])**.**
Nous avons :

(1) L'espace métrique $(\mathbb{R},d)$ est complet (définition 7.239).

(2) Une suite dans $\mathbb{R}$ est convergente (définition 7.13) si et seulement si elle est de Cauchy (définition 7.255).

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 1.367).

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 1.438 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. □

112. Voir la proposition 7.253 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 1.438 en remplaçant partout $\mathbb{Q}$ par $\mathbb{R}$, et aussi en remplaçant les $|x-y|$ par $d(x,y)$.

7.259.
Nous pouvons également mettre une structure d'espace métrique sur $\mathbb{C}$ en posant

$$d(z,z') = |z-z'|. \tag{7.273}$$

Proposition 7.260.
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

$$|x_k-x_l| = |\operatorname{Re}(z_k-z_l)| \leqslant |z_k-z_l|. \tag{7.274}$$

Vu que (z_k) est de Cauchy, il existe un N tel que si $k,l\geqslant N$,

$$|x_k-x_l| \leqslant |z_k-z_l| \leqslant \epsilon. \tag{7.275}$$

Donc la suite des parties réelles converge par la complétude de $(\mathbb{R},d)$ du théorème 7.258. 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,

$$|z_k-(x+iy)| = \big|\operatorname{Re}(z_k)-x+i(\operatorname{Im}(z_k)-y)\big| \leqslant |x_k-x|+|y_k-y| \leqslant \epsilon. \tag{7.276}$$

□

7.14 Norme, espace vectoriel normé

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 10.78 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

$$|x-a|\leqslant\delta \Rightarrow |f(x)-f(a)|\leqslant\varepsilon. \tag{7.277}$$

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 :

$$\text{taille de } (a,b) = \sqrt{a^2+b^2}. \tag{7.278}$$

Nous pouvons introduire une notion de distance entre les éléments de $\mathbb{R}^2$ de façon similaire :

$$d\big((a_x,a_y),(b_x,b_y)\big) = \sqrt{(a_x-b_x)^2+(a_y-b_y)^2}. \tag{7.279}$$

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.

7.14.0.1 Critère de Cauchy

Théorème 7.261 (Bolzano-Weierstrass, thème 32)**.**
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 7.73 de la compactié). Nous avons donc des points $a_1,\dots,a_n$ tels que

$$K \subset \bigcup_{i=1}^{n} \mathcal{O}_{a_i} \tag{7.280}$$

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 1.116 qui dit que $\mathbb{N}$ est infini. □

Corolaire 7.262 ([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 7.261). Par hypothèse, cette sous-sous-suite doit converger vers a, ce qui est impossible.

Contradiction et le corolaire est prouvé. □

Lemme 7.263.
Une suite de Cauchy[113] *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

113. Définition 7.238.

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

$$\|a_k - \ell\| \leqslant \|a_k - a_n\| + \|a_n - \ell\| \leqslant 2\epsilon. \tag{7.281}$$

□

Dans le cas des espaces de dimension finie, le fait d'être complet est automatique, comme le montre la proposition suivante.

Proposition 7.264.
Soit $\big(E, \|.\|\big)$ un espace vectoriel normé de dimension finie sur un corps $\mathbb{K}$ qui est complet[114]*. Alors E est complet*[115]*.*

Pour rappel, la complétude de l'espace métrique $\mathbb{R}$ est la proposition 1.390.

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

$$\|f_n - f_m\| = \|\sum_\alpha (a_{n\alpha} - a_{m\alpha}) e_\alpha\| = \sum_\alpha |a_{n\alpha} - a_{m\alpha}|^2. \tag{7.282}$$

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

$$\sum_\alpha |a_{n\alpha} - a_{m\alpha}|^2 < \epsilon. \tag{7.283}$$

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

$$\|f_n - f\| = \|\sum_\alpha (a_{n\alpha} - a_\alpha) e_\alpha\|, \tag{7.284}$$

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. □

Proposition 7.265.
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 7.195.

Démonstration. Nous allons prouver que $f(K)$ est fermée et bornée.

(i) **$f(K)$ 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 7.261). 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

$$f(a) = \lim f(x'_n) = \lim y_n. \tag{7.285}$$

Cela prouve que la limite de (y_n) est dans $f(K)$ et par conséquent que $f(K)$ est fermé.

114. La définition est 1.367, 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 $\mathbb{C}$.
115. Définition 7.239.

(ii) $f(K)$ **est borné** Si $f(K)$ n'est pas borné, nous pouvons trouver une suite (x_n) dans K telle que

$$\|f(x_n)\|_W > n \tag{7.286}$$

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

$$\|f(a)\|_W = \lim \|f(x'_n)\|_W. \tag{7.287}$$

La suite $f(x'_n)$ est alors une suite bornée, ce qui n'est pas possible au vu de la condition (7.286) imposée à la suite de départ (x_n).

□

Corolaire 7.266.
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 7.265 montre que $f(K)$ est compact et donc borné. □

7.15 Espaces métriques

7.15.1 Espaces métrisables

Définition 7.267.
*Un espace topologique est **métrisable** si il est homéomorphe à un espace métrique.*

Proposition 7.268.
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

$$\begin{aligned} \tilde{f}\colon E &\to Y \\ a &\mapsto f\big(\phi^{-1}(a)\big). \end{aligned} \tag{7.288}$$

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

$$\tilde{f}(a_k) = f\big(\phi^{-1}(a_k)\big), \tag{7.289}$$

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

$$\lim_{k\to\infty} \tilde{f}(a_k) = \lim_{k\to\infty} f\big(\phi^{-1}(a_k)\big) = f\big(\phi^{-1}(a)\big) = \tilde{f}(a). \tag{7.290}$$

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 7.231. L'application $f = \tilde{f} \circ \phi$ est donc continue en tant que composée d'applications continues. □

7.15.2 Fonctions continues

La propriété suivante donne des caractérisations importantes de la continuité dans le cas des espaces métriques.

Proposition 7.269 (Continuité, ouverts et voisinages et limite[231]).
Soient $f : E \to F$ une application entre espaces métriques et $a \in E$. Alors nous avons équivalence entre les choses suivantes :

(1) f est continue en a,

(2) Pour tout voisinage ouvert W de $f(a)$, il existe un voisinage ouvert V de a tel que $f(V) \subset W$.

(3) Pour toute boule $W' = B\big(f(a), \epsilon\big)$, il existe une boule $V' = B(a, \delta)$ telle que $f(V) \subset W'$.

(4) $\forall \epsilon > 0$, $\exists \delta > 0$ tel que $f\big(B(a, \delta)\big) \subset B\big(f(a), \epsilon\big)$.

(5) $\lim_{x \to a} f(x) = f(a)$ où la limite est donnée par la définition 7.101,

(6) Pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que $\|x - a\| < \delta$ implique $\|f(x) - f(a)\| < \epsilon$.

La proposition 7.307 nous montrera que ces équivalences tiennent encore lorsque l'espace a une topologie de seminormes.

Démonstration. L'équivalence (1) ⇔ (2) est la définition 7.32. 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 [116], 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 7.32 de la continuité en un point couplée à l'unicité de la limite due à la proposition 7.104 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. □

Voici un théorème qui parle de fermés emboîtés dans un espace métrique. Le corolaire 7.87 parle du cas $\cap_i A_i = \varnothing$ dans un compact.

Théorème 7.270 (Théorème [232]).
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.

(i) **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.

(ii) **Condition nécessaire** Soit (x_n) un suite de Cauchy. Nous considérons les ensembles

$$F_n = \overline{\{x_i \text{ tel que } i \geqslant n\}}. \tag{7.291}$$

Le fait que la suite soit de Cauchy implique que $\operatorname{diam}(F_n) \to 0$. Par hypothèse, nous avons alors

$$\bigcap_{n \in \mathbb{N}} F_n = \{a\}. \tag{7.292}$$

116. Cela est le théorème-définition 7.108 des ouverts dans un espace métrique, à ne pas confondre avec le théorème 7.8.

Pour s'assurer que a est bien la limite de (x_n), il suffit de remarquer que

$$d(x_n, a) \leqslant \operatorname{diam} F_n \to 0. \tag{7.293}$$

□

Proposition 7.271.
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 7.244(1).

Par la caractérisation séquentielle des fermés (un fermé contient les limites de toutes ses suites, proposition 7.228), la suite (x_k) étant dans F, la limite est dans F. Donc $x \in F$. □

Lemme 7.272.
Soit A_n une suite décroissante de fermés dans un espace métrique[117] *compact K. Alors*

$$C = \bigcap_{n\in\mathbb{N}} A_n \tag{7.294}$$

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 7.90), 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 7.134. Une queue de la suite y_n est dans A_2 et nous considérons donc une sous-suite convergente dans A_2 donnée par

$$z_n = y_{\sigma_2(n)} = x_{\sigma_1\sigma_2(n)}. \tag{7.295}$$

En continuant ainsi nous construisons une suite convergente dans A_k. Nous considérons enfin la suite

$$y_n = x_{\sigma_1\ldots\sigma_n(n)}. \tag{7.296}$$

Pour tout k, une queue de cette suite est une sous-suite de $x_{\sigma_1\ldots\sigma_k(n)}$ et par conséquent cette suite converge dans A_k. La limite de cette suite est donc dans l'intersection demandée. □

Remarque 7.273.
Cette propriété est fausse pour les ouverts. Par exemple

$$\bigcap_{n>1}]0, \frac{1}{n}[= \varnothing. \tag{7.297}$$

Lemme 7.274.
Si K est un compact dans un espace métrique et F un fermé disjoint de K, alors $d(K, F) > 0$.

Démonstration. La fonction

$$\begin{aligned} K &\to \mathbb{R} \\ x &\mapsto d(x, F) \end{aligned} \tag{7.298}$$

est une fonction continue sur K, et donc atteint son minimum par le théorème de Weierstrass 7.136. 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. □

117. L'hypothèse métrique provient de l'utilisation de Bolzano-Weierstrass, lequel est vrai pour les espaces séquentiellement compacts, dont les espaces métriques.

Proposition 7.275 ([208]).
Une isométrie d'un espace métrique compact sur lui-même est une bijection.

Démonstration. Soient X un espace métrique compact et $f\colon X \to X$ une isométrie. Le fait que f soit injective est obligatoire (sinon il y a des images dont la distance est nulle). Il faut montrer que f est surjective.

Soit $x \in X$ hors de $f(X)$. Le lemme 7.274 appliqué au fermé $\{x\}$ et au compact $f(K)$ donne un $r > 0$ tel que

$$d\big(x, f(K)\big) > r. \tag{7.299}$$

Soit la suite $u_n = f^n(x)$; c'est une suite dans K et possède donc une sous-suite convergente (Bolzano-Weierstrass7.134) que l'on nomme (y_n). Vu que f est une isométrie,

$$d(y_n, y_{n+1}) = d(x, y_m) > r \tag{7.300}$$

pour un certain $m \leqslant n+1$. Cela signifie que pour tout n, nous avons $d(y_n, y_{n+1}) > r$, ce qui contredit le fait que la suite (y_n) converge. □

Proposition 7.276.
Soient (X, d) un espace métrique compact et (u_n) une suite de X telle que

$$\lim_{n\to\infty} d(u_n, u_{n+1}) = 0. \tag{7.301}$$

Alors l'ensemble des points d'accumulation[118] *de (u_n) est connexe.*

Démonstration. Nous notons Γ l'ensemble des points d'accumulation de la suite.

(i) **Γ est compact** Nous notons $A_p = \{u_n \text{ tel que } n \geqslant p\}$ et nous avons

$$\Gamma = \bigcap_{p\in\mathbb{N}} \overline{A_p} \tag{7.302}$$

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 7.6). En tant que fermé dans un compact, Γ est compact (lemme 7.90).

(ii) **Recouvrement par deux compacts** Supposons que Γ ne soit[119] pas connexe. Nous pouvons alors considérer S et O, deux ouverts disjoints recouvrant Γ et intersectant tous deux Γ. Nous posons alors

$$A = S \cap \Gamma \tag{7.303a}$$
$$B = O \cap \Gamma, \tag{7.303b}$$

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[120].

118. Définition 7.30.
119. est-ce qu'il faut vraiment un subjonctif ici ?
120. Lemme 7.90.

(iii) **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 7.274. Nous notons

$$A'=\{x\in X \text{ tel que } d(x,A)<\frac{\alpha}{3}\} \tag{7.304a}$$
$$B'=\{x\in X \text{ tel que } d(x,B)<\frac{\alpha}{3}\} \tag{7.304b}$$

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

$$K=X\backslash(A'\cup B') \tag{7.305}$$

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).

(iv) **Sous-suites de (u_n)** L'hypothèse sur la suite (u_n) nous indique qu'il existe un N_0 tel que $\forall n\geqslant N_0$,

$$d(u_n,u_{n+1})<\frac{\alpha}{3}. \tag{7.306}$$

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 (7.306) 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

$$\begin{aligned}d(u_{n_0},B)&\geqslant d(u_{n_0-1},B)-d(u_{n_0-1},u_{n0})\\&\geqslant d(A,B)-d(u_{n_0-1},A)-d(u_{n_0-1},u_{n_0})\\&\geqslant\alpha-\frac{\alpha}{3}-\frac{\alpha}{3}\\&=\frac{\alpha}{3}.\end{aligned} \tag{7.307}$$

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.

Proposition 7.277.
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. □

Lemme-Définition 7.278 ([233])**.**
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 $z \in K_n$, $B(z, \delta_n) \subset K_{n+1}$.
(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

$$V_n = \{z \in E \text{ tel que } |z|\} \cup \bigcup_{a \notin \Omega} B(a, \frac{1}{n}), \tag{7.308}$$

et nous définissons $K_n = V_n^c$. Vérifions que ces ensembles vérifient tout ce qu'il faut.

(i) $\underline{K_n \subset \Omega}$ Si $a \notin \Omega$ alors a est dans tous les V_n et donc dans aucun des K_n ; nous avons donc bien $K_n \subset \Omega$.

(ii) $\underline{\bigcup_{n=0}^{\infty} K_n = \Omega}$ 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 $\Omega \subset \bigcup_{n=0}^{\infty} K_n$.

(iii) $\underline{K_n \subset \text{Int}(K_{n+1})}$ 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

$$\frac{1}{n+1} < \delta < \frac{1}{n} \tag{7.309}$$

alors $B(z, \delta) \subset K_{n+1}$.

(iv) $\underline{\textbf{Les } K_n \textbf{ sont compacts}}$ Enfin, les K_n sont tous compacts. En effet ils sont bornés parce que $K_n \subset B(0, n)$ 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

$$\Omega = \bigcup_{n=0}^{\infty} K_n \subset \bigcup_{n=0}^{\infty} \text{Int}(K_{n+1}) \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \tag{7.310}$$

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

$$K \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \tag{7.311}$$

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

$$\frac{1}{n+1} < \delta_n < \frac{1}{n}. \tag{7.312}$$

Lemme 7.279 ([234]).
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 7.8). Autrement dit, il existe $r(x) > 0$ tel que

$$\overline{B\big(x, r(x)\big)} \subset \Omega_{k(x)}. \tag{7.313}$$

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 [121]. Soient donc $x_1,\dots,x_m \in K$ tels que

$$K \subset \bigcup_{i=1}^m B\big(x_i, r(x_i)\big). \tag{7.314}$$

Pour chaque $j = 1,\dots,n$, nous posons

$$A_j = \big\{l \in \{1,\dots,m\} \text{ tel que } k(x_l) = j\big\}. \tag{7.315}$$

Et enfin nous définisssons, pour $j = 1,\dots,n$ les parties

$$K_j = \bigcup_{l\in A_j} \overline{B\big(x_l, r(x_l)\big)} \tag{7.316}$$

et il nous reste à prouver que ces ensembles répondent bien à la question.

(i) $\bigcup_{j=1}^n A_j = \{1,\dots,m\}$ **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 $\{1,\dots,m\}$.

(ii) $K_j \subset \Omega_j$ Nous avons

$$K_j = \bigcup_{l\in A_j} \overline{B\big(x_l, r(x_l)\big)} \subset \bigcup_{l\in A_j} \Omega_{k(x_l)} = \bigcup_{l\in A_j} \Omega_j = \Omega_j. \tag{7.317}$$

(iii) $K \subset \bigcup_{i=1}^n K_i$. Par (7.314), et vu que $\{1,\dots,m\} = \bigcup_{j=1}^n A_j$,

$$K \subset \bigcup_{i=1}^m B\big(x_i, r(x_i)\big) \tag{7.318a}$$

$$= \bigcup_{j=1}^n \bigcup_{l\in A_j} B\big(x_l, r(x_l)\big) \tag{7.318b}$$

$$= \bigcup_{j=1}^n \underbrace{\bigcup_{l\in A_j} \overline{B\big(x_l, r(x_l)\big)}}_{K_j} \tag{7.318c}$$

$$= \bigcup_{j=1}^n K_j. \tag{7.318d}$$

121. C'est la définition 7.73 d'un compact.

□

Théorème 7.280 (Tykhonov)**.**
Un produit quelconque d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

Nous n'allons donner la preuve que dans le cas d'un produit fini dans le théorème 7.286.

7.15.3 Ensembles enchainés

Soit (X, d) un espace métrique.

Définition 7.281.
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 7.282.
Les rationnels dans $\mathbb{R}$ sont bien enchainés.

Démonstration. Soient p et q des rationnels avec $p < q$, ainsi que $\epsilon > 0$. Le lemme 1.424 nous permet de considérer un rationnel δ vérifiant $0 < \delta < \epsilon$. Et nous définissons les rationnels

$$r_k = p + k\delta. \tag{7.319}$$

Vu que $\mathbb{Q}$ est archimédien [122], 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

$$|r_n - r_{n-1}| = \delta < \epsilon, \tag{7.320}$$

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

$$0 \leqslant q - r_N \leqslant r_{N+1} - r_N = \delta \leqslant \epsilon. \tag{7.321}$$

Donc ok aussi pour ce dernier pas. □

Proposition 7.283 ([235, 1])**.**
Un espace métrique connexe [123] 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 7.8.

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

$$B = \bigcup_{k \in I \setminus \{i_0\}} [x_k]. \tag{7.322}$$

Ce sont deux ouverts disjoints qui recouvrent X qui n'est donc pas connexe. □

122. Proposition 1.383.
123. Définition 7.63.

Proposition 7.284.
La fermeture d'un ensemble bien enchainé dans un espace métrique compact (X, d) est connexe.

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 7.276 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

$$\bigcup_{x \in \bar{A}} C_{a,x} = \bar{A}. \tag{7.323}$$

Vu que le membre de gauche est une union de connexes, c'est un connexe par la proposition 7.69. □

Corolaire 7.285.
Un espace métrique compact est connexe si et seulement si il est bien enchainé.

Démonstration. Dans le sens direct, c'est la proposition 7.283. Dans l'autre sens, si X est compact, alors X est fermé par le lemme 7.90(2). Et vu qu'il est fermé et bien enchainé, la proposition 7.284 implique qu'il est connexe. □

7.15.4 Produit fini d'espaces métriques

Pour rappel, la distance sur un espace produit est donnée par la définition 7.201.

Théorème 7.286 ([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 (7.201) (attention : chacun des K_i peut être de dimension infinie) :

$$d(\alpha, \beta) = \max\{d_i(\alpha_i, \beta_i)\} \tag{7.324}$$

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 7.134). 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

$$d_i\big((\alpha_p)_i, \ell_i\big) \leqslant \epsilon. \tag{7.325}$$

En prenant $N = \max_k N_k$ et $n > N$ nous avons

$$d\big(\alpha_n, (\ell_1, \ldots, \ell_n)\big) \leqslant \epsilon. \tag{7.326}$$

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

$$\mathcal{P}_i = \mathcal{O}_i \times K_2 \times \ldots \times K_n, \tag{7.327}$$

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 7.287 ([236]).
Soient (E_n, d_n) des espaces métriques. Sur l'ensemble produit $E = \prod_{i=1}^{\infty} E_i$ nous définissons la métrique

$$d(x,y) = \sum_{k=1}^{\infty} \frac{1}{2^k} d'_k(x_i, y_i) \tag{7.328}$$

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.

Théorème 7.288 (Tykhonov dénombrable[236]).
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 7.280.

7.15.5 Équicontinuité

Définition 7.289 ([1, 237, 238]).
*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*

$$h(U) \subset h(a) + V \tag{7.329}$$

pour tout $h \in H$.

Nous disons que H est équicontinue si elle est équicontinue en tout point.

Lemme 7.290 ([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 7.289 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

$$\|h(x) - h(a)\| = \|h(x-a)\| = d(x,a) < r, \tag{7.330}$$

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. □

Lemme 7.291 ([238]).
Soit une famille de fonctions $f_i \colon X \to E$ indexée par un ensemble I où X est un espace topologique

et E un espace métrique. Cette famille est équicontinue[124] *en $x \in X$ si pour tout $\epsilon > 0$, il existe un voisinage V de x tel que*

$$\|f_i(x) - f_i(y)\| < \epsilon \tag{7.331}$$

pour tout i dès que $y \in V$.

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 12.414.

Proposition 7.292 ([1, 238])**.**
Soit une suite équicontinue (f_i) de fonctions qui converge simplement vers f, alors f est continue.

Démonstration. Soit une suite équicontinue $f_i : X \to E$ 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

$$|f(x) - f(a)| \leqslant |f(x) - f_i(x)| + |f_i(x) - f_i(a)| + |f_i(a) - f(a)|. \tag{7.332a}$$

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

$$|f(x) - f(a)| \leqslant 3\epsilon. \tag{7.333}$$

□

¡¡ Avertissement/question au lecteur !! 7.293
Je n'ai pas du tout vérifié si le lemme 7.294 est correct. Sinon, il faudra trouver autre chose dans la preuve de la proposition 21.90.

Lemme 7.294 ([1])**.**
Si A est une partie fermée de $\mathbb{R}^3$, alors $\texttt{proj}_{\mathbb{R}^+}(A)$ est fermé dans $\mathbb{R}$.

7.15.6 Continuité uniforme

Définition 7.295 ([239])**.**
*Soient deux espaces métriques (E, d) et (E', d'). Une application $f : E \to E'$ 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 12.7.

7.16 Ensembles nulle part denses

Nous allons nous limiter au cas de $\mathbb{R}$, mais je crois que ça se généralise sans trop de peine aux espaces métriques, voire plus. Voir aussi la section 7.18 sur les espaces de Baire.

Définition 7.296.
*Un ensemble est dit **nulle part dense** si il n'est dense dans aucun intervalle.*

*Un ensemble dans $\mathbb{R}$ est de **première catégorie** ou **maigre** si il est une union dénombrable d'ensembles nulle part dense (c'est-à-dire d'ensembles denses sur aucun intervalle).*

124. Définition 7.289.

Théorème 7.297 (Baire[240]).
Une réunion dénombrable d'ensembles nulle part denses est d'intérieur vide.

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

$$B(x_1, r_1) \cap A_1 = \varnothing. \tag{7.334}$$

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 [125] 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. □

7.17 Topologie des seminormes

Les principaux espaces topologiques construit avec des seminormes seront les espaces de fonctions de la définition 30.14. Nous verrons également la topologie $*$-faible sur $\mathscr{D}'(\Omega)$ en la définition 30.24.

7.17.1 Seminorme

Définition 7.298.
*Si E est un espace vectoriel sur le corps $\mathbb{K} = \mathbb{R}, \mathbb{C}$, une **seminorme** sur E est une application $p\colon E \to \mathbb{R}$ telle que*

(1) $p(x) \geqslant 0$,
(2) $p(\lambda x) = |\lambda| p(x)$
(3) $p(x+y) \leqslant p(x) + p(y)$

pour tout $x, y \in E$ et pour tout $\lambda \in \mathbb{K}$.

La seule différence avec une norme est qu'une seminorme peut s'annuler en des éléments non-nuls de l'espace.

Lemme 7.299 ([241]).
Si p est une seminorme [126] nous avons

$$|p(x) - p(y)| \leqslant p(x-y). \tag{7.335}$$

Démonstration. 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,

$$-p(h) \leqslant p(x+h) - p(x) \leqslant p(h) \tag{7.336}$$

ou encore

$$|p(x+h) - p(x)| \leqslant p(h) \tag{7.337}$$

qui donne le résultat demandé en posant $h = y - x$. □

125. Par la proposition 1.390
126. Définition 7.298.

Définition 7.300 ([242]).
*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 $m \in M$.*

Lemme 7.301 ([242]).
Une application linéaire est dominée par une seminorme si et seulement si sa partie réelle est dominée par le dessus[127].

Démonstration. Soit une application linéaire $f : X \to \mathbb{C}$. Nous la décomposons en parties réelles et imaginaires par

$$f(x) = u(x) + iv(x) \tag{7.338}$$

où u et v sont des application à valeurs réelles.

(i) $\Rightarrow$ Nous supposons que $|f(x)| \leqslant p(x)$ pour tout $x \in X$. Nous avons les majorations

$$u(x) \leqslant |u(x)| \leqslant |f(x)| \leqslant p(x). \tag{7.339}$$

(ii) $\Leftarrow$ 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[128]

$$f(\frac{|z|}{z}x) = \frac{|z|}{z}f(x) = |z|. \tag{7.340}$$

En particulier $f(\frac{|z|}{z}x)$ est réel et est donc donné par u :

$$f(\frac{|z|}{z}x) = u(\frac{|z|}{z}x). \tag{7.341}$$

Nous avons alors le calcul

$$r = f(\frac{|z|}{z}x) = u(\frac{|z|}{z}x) \leqslant p(\frac{|z|}{z}x) = |\frac{|z|}{z}|p(x) = p(x). \tag{7.342}$$

□

7.17.2 Topologie des seminormes

Soit $(p_i)_{i\in I}$ une famille de seminormes sur E. Nous construisons alors une topologie sur E de la façon suivante.

Proposition-Définition 7.302 (Topologie et seminormes[243, 244]).
*Soient des seminormes $\{p_i\}_{i\in I}$. Pour tout J fini dans I nous définissons les **boules ouvertes***

$$B_J(x, r) = \{y \in E \text{ tel que } p_j(y - x) < r \; \forall j \in J\}. \tag{7.343}$$

*La **topologie** sur E donnée par la famille de seminorme est définie en disant que $\mathcal{O} \subset E$ est ouvert si et seulement si chaque point de $\mathcal{O}$ est dans une boule contenue dans $\mathcal{O}$.*

Cela définit une topologie.

Proposition 7.303.
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 $i \in I$,

$$p_i(x - x_n) \to 0. \tag{7.344}$$

127. Définition 7.300.
128. 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 18.64 n'arrive que dans longtemps.

Démonstration. Si la suite (x_n) converge[129] 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 $x_n \in B_j(x, \epsilon)$.

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 $x_n \in B_J(x, r)$. □

¡¡ Avertissement/question au lecteur !! 7.304
Je n'ai pas vérifié si la proposition 7.305 est correcte. D'ailleurs je même pas trouvé l'énoncé ; et j'avoue n'avoir pas trop cherché.

La preuve serait sans doute similaire à ce qu'on a pour le lemme 7.203.

Proposition 7.305 ([1]).
Soient des espaces vectoriels munis de seminormes $\big(E, \{p_i\}_{i\in I}\big)$ et $\big(F, \{q_j\}_{j\in J}\big)$. Nous posons

$$\begin{aligned} r_{ij} \colon E \times F &\to \mathbb{R} \\ (x, y) &\mapsto \max\big\{p_i(x), q_j(y)\big\}. \end{aligned} \tag{7.345}$$

Alors :

(1) Les r_{ij} sont des seminormes.

(2) La topologie induite sur $E \times F$ par ces seminormes est la topologie produit.

Proposition 7.306 ([245, 1]).
Un espace vectoriel muni de seminormes sur un corps valué est un espace vectoriel topologique[130].

Démonstration. Soit un espace vectoriel E muni des seminormes $\{p_i\}_{i\in I}$. Sa topologie est donnée par la définition 7.302. Sur le corps $\mathbb{K}$, nous avons la topologie métrique 7.168.

(i) **Somme** Nous commençons par prouver que

$$\begin{aligned} f \colon E \times E &\to E \\ (x, y) &\mapsto x + y \end{aligned} \tag{7.346}$$

est continue. Soit un ouvert $\mathcal{O}$ de E ; nous allons prouver que $f^{-1}(\mathcal{O})$ est ouvert en prouvant qu'il contient une boule ouverte autour de chacun de ses points (théorème 7.8). Notez que $f^{-1}(\mathcal{O}) \subset E \times E$; la topologie sur cet ensemble est celle est seminormes r_{ij} données en (7.345). Nous allons en particulier utiliser la seminorme $q_i = r_{ii}$ donnée par

$$\begin{aligned} q_i \colon E \times E &\to \mathbb{R} \\ (x, y) &\mapsto \max\big\{p_i(x), p_i(y)\big\}. \end{aligned} \tag{7.347}$$

Soit $(a, b) \in f^{-1}(\mathcal{O})$. Vu que $a + b \in \mathcal{O}$ et que $\mathcal{O}$ est ouvert, la partie $\mathcal{O}$ contient une boule ouverte autour de $a + b$ (définition 7.302). Soit $i \in I$ et $r > 0$ tels que

$$B_i(a + b, r) \subset \mathcal{O}. \tag{7.348}$$

Nous allons prouver qu'il existe un $s > 0$ tel que $B_i\big((a, b), s\big) \subset f^{-1}(\mathcal{O})$, et plus précisément que

$$f\Big(B_i\big((a, b), s\big)\Big) \subset B_i(a + b, r). \tag{7.349}$$

À gauche, B_i est la boule dans $E \times E$ pour la seminorme (7.347). Soit $(x, y) \in B_i\big((a, b), s\big)$, c'est-à-dire

$$q_i\big((a, b) - (x, y)\big) \leqslant s. \tag{7.350}$$

129. Définition 7.13.
130. Définition 7.158.

Pour savoir si $f(x,y) \in B_i(a+b,r)$, nous posons $x = a+h$ et $y = b+k$ et nous calculons

$$\begin{aligned}
p_i\big(f(x,y) - (a+b)\big) &= p_i(x+y-a-b) && (7.351a)\\
&= p_i(h+k) && (7.351b)\\
&\leqslant p_i(h) + p_i(k) && (7.351c)\\
&\leqslant 2\max\{p_i(h), p_i(k)\} && (7.351d)\\
&= 2q_i(h,k) && (7.351e)\\
&\leqslant 2s \qquad \text{par (7.350).} && (7.351f)
\end{aligned}$$

En posant $s = r/2$, nous avons bien $f(x,y) \in \mathcal{O}$, et donc $f^{-1}(\mathcal{O})$ est un ouvert ; f est alors continue.

(ii) **Produit** Nous nommons $\mathbb{K}$ le corps de l'espace vectoriel E. Nous devons voir que l'application

$$\begin{aligned} f\colon \mathbb{K} \times E &\to E \\ (\lambda, x) &\mapsto \lambda x \end{aligned} \tag{7.352}$$

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

$$\begin{aligned} q_i\colon \mathbb{K} \times E &\to \mathbb{R} \\ (\lambda, x) &\mapsto \max\{|\lambda|, p_i(x)\}. \end{aligned} \tag{7.353}$$

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 $i \in I$ 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

$$f\Big(B_i\big((\lambda,a),s\big)\Big) \subset B_i(\lambda a, r). \tag{7.354}$$

Ici encore, à gauche B_i est la boule pour la seminorme q_i donnée en (7.353). Soit $(\mu, x) \in B_i\big((\lambda,a),s\big)$, c'est-à-dire

$$q_i\big((\mu,x) - (\lambda,a)\big) = \max\{|\lambda-\mu|, p_i(a-x)\} < s. \tag{7.355}$$

En particulier nous avons les deux inégalités

$$\begin{cases} |\lambda - \mu| < s, & (7.356a)\\ p_i(a-x) < s. & (7.356b) \end{cases}$$

Nous avons le calcul suivant :

$$\begin{aligned}
p_i\big(f(\mu,x), \lambda a\big) &= p_i(\mu x - \lambda a) && (7.357a)\\
&= p_i(\mu x - \lambda x + \lambda x - \lambda a) && (7.357b)\\
&\leqslant p_i\big((\mu-\lambda)x\big) + |\lambda| p_i(x-a) && (7.357c)\\
&= |\mu - \lambda| p_i(x) + |\lambda| p_i(x-a) && (7.357d)\\
&\leqslant s p_i(x) + |\lambda| s. && (7.357e)
\end{aligned}$$

C'est le moment de chercher une majoration pour $p_i(x)$:

$$p_i(x) = p_i\big(a + (x-a)\big) \leqslant p_i(a) + p_i(x-a) \leqslant p_i(a) + s. \tag{7.358}$$

Nous pouvons continuer la majoration (7.357) tout en ne nous posant pas de questions sur le sens de l'inégalité parce que nous cherchons $s > 0$:

$$\begin{aligned} p_i\big(f(\mu,x),\lambda a\big) &\leqslant sp_i(x) + |\lambda|s && (7.359a)\\ &\leqslant s\big(p_i(a)+s\big) + |\lambda|s && (7.359b)\\ &= s^2 + \big(|\lambda| + p_i(a)\big)s. && (7.359c)\end{aligned}$$

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

$$s^2 + \big(|\lambda| + p_i(a)\big)s - r < 0. \tag{7.360}$$

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 7.269.

Proposition 7.307.
Soit $f\colon \mathbb{R} \to (E, p_i)_{i\in I}$ une application. Nous avons équivalence entre

(1) la fonction f est continue en $t_0 \in \mathbb{R}$,

(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 $f(V) \subset W$,

(3) pour tout $i \in I$ et $\epsilon > 0$ il existe $\delta > 0$ tel que

$$f\big(B(t_0,\delta)\big) \subset B_i\big(f(t_0),\epsilon\big). \tag{7.361}$$

Démonstration. L'équivalence (1) ⇔ (2) est la définition 7.32.

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

$$f\big(B(t_0,\delta)\big) \subset f(V) \subset B_i\big(f(t_0),\epsilon\big). \tag{7.362}$$

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

$$f\big(B(t_0,\delta)\big) \subset B_i\big(f(t_0),\epsilon\big) \subset W. \tag{7.363}$$

□

Lorsqu'on a un espace E muni d'une quantité dénombrable de seminormes $\{p_k\}_{k\in I}$ nous définissons l'écart [131]

$$d(x,y) = \sup_{k\geqslant 1} \min\Big\{\frac{1}{k}, p_k(x-y)\Big\}. \tag{7.364}$$

Notons que cet écart est invariant par translation au sens où pour tout x, y, h dans E nous avons

$$d(x+h,y+h) = \sup_{k\geqslant 1} \min\Big\{\frac{1}{k}, p_k(x-y)\Big\} = d(x,y). \tag{7.365}$$

Proposition 7.308.
Si X est un espace topologique dont la topologie est donnée par une famille dénombrable de seminormes, alors il est métrisable.

131. 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.

Proposition 7.309 ([241]).
La topologie donnée par les boules

$$B_k(a,r) = \{x \in E \text{ tel que } \forall\, k \leqslant \frac{1}{r}, p_k(x-a) < r\} \tag{7.366}$$

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 (7.366) et par P celle des seminormes : P-continue, d-ouvert, etc.

D'abord nous avons

$$B(a,r) = \bigcap_{k \leqslant \frac{1}{k}} B_k(a,r). \tag{7.367}$$

Si $\mathcal{O}$ est un d-ouvert, il contient une d-boule autour de chacun de ses points. Or d'après la formule (7.367), 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

$$\begin{aligned} |p_k(y) - p_k(x)| &\leqslant p_k(x-y) && \text{(7.368a)}\\ &= \min\{\frac{1}{k}, p_k(x-y)\} && \text{(7.368b)}\\ &\leqslant d(x,y) && \text{(7.368c)}\\ &\leqslant \epsilon. && \text{(7.368d)} \end{aligned}$$

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 inclue à $B_k(a,r)$. Pour cela prenons $y \in B(x,\epsilon)$; nous avons

$$\big|p_k(a-x) - p_k(a-y)\big| \leqslant d(x,y) \leqslant \epsilon. \tag{7.369}$$

Par conséquent le nombre $p_k(a-y)$ est dans l'intervalle

$$p_k(a-x) \pm \epsilon \tag{7.370}$$

et il suffit de prendre $\epsilon < \frac{r - p_k(a-x)}{2}$. □

7.17.2.1 Norme induite sur la topologie quotient

Proposition-Définition 7.310 (Norme quotient[246]).
Soient un espace vectoriel topologique normé E, et un sous-espace M. Pour $\alpha \in E/M$ nous posons

$$\|\alpha\|_{E/M} = d(\alpha, M) \tag{7.371}$$

où $d(\alpha, M)$ est la distance entre la partie α et la partie M.

Nous avons :

(1) La formule $\|\alpha\| = \inf_{u \in \alpha} \|u\|_E$.

(2) L'opération $\|.\|$ est une seminorme[132] *sur l'espace vectoriel E/M.*

(3) C'est une norme si et seulement si M est fermé.

Nous parlons de ***(semi)norme quotient****.*

132. Définition 7.298.

Démonstration. Point par point.

(i) **Pour (1)** La définition de $\|\alpha\|$ est $\|\alpha\| = d(\alpha, M) = \inf_{\substack{u\in\alpha\\ v\in M}} \|u - v\|$. Mais

$$\{u - v \text{ tel que } u \in \alpha, v \in M\} = \alpha, \tag{7.372}$$

donc

$$d(\alpha, M) = \inf_{u\in\alpha} \|u\|. \tag{7.373}$$

(ii) **Pour (2)** Nous devons vérifier les propriétés de la définition 7.298. D'abord en tant que distance, nous avons $\|\alpha\| \geqslant 0$ pour tout α.

Si $\lambda \in \mathbb{R}$ nous avons aussi

$$\|\lambda\alpha\| = \inf_{u\in\lambda\alpha} \|u\| = \inf_{u\in\alpha} \|\lambda u\| = |\lambda| \inf_{u\in\alpha} \|u\| = |\lambda|\|\alpha\|. \tag{7.374}$$

Enfin si $\alpha, \beta \in E/M$, nous avons

$$\inf_{u\in\alpha+\beta} \|u\| \leqslant \inf_{\substack{u\in\alpha\\ v\in\beta}} \|u + v\| \leqslant \inf_{\substack{u\in\alpha\\ v\in\beta}} \big(\|u\| + \|v\|\big) = \inf_{u\in\alpha} \|u\| + \inf_{v\in\beta} \|v\| = \|\alpha\| + \|b\|. \tag{7.375}$$

(iii) **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

$$\alpha = \{x - v \text{ tel que } v \in M\} \tag{7.376}$$

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

$$0 = \|\alpha\| = d(\alpha, M) = \inf_{u\in\alpha} \|u\| = \inf_{v\in M} \|x - v\|. \tag{7.377}$$

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 7.228 nous indique que la limite doit être dans M. Autrement dit : $x \in M$. Par définition des classes nous avons alors $\alpha = [x] = 0$.

(iv) **Pour (3) en supposant que $\|.\|$ est une norme** Supposons que M n'est pas fermé. Il ne contient donc pas son adhérence. Soit $a \in \text{Adh}(M)\backslash M$. 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 !! 7.311
Je ne suis pas certain de la proposition 7.312. Peut-être qu'il faut ajouter l'hypothèse que M est fermé.

Proposition 7.312.
Soient un espace vectoriel topologique normé E, et un sous-espace M. La topologie quotient[133] *sur E/M est la même que celle de la seminorme induite*[134].

133. Topologie quotient, définition 7.43.
134. Voir la définition 7.310.

7.17.3 Espace dual

Nous parlerons plus en détail d'espace dual d'un espace normé en la section 11.15.

Lemme-Définition 7.313.
Soient F un espace métrique et E un espace topologique vectoriel. Pour chaque $v \in E$, l'application

$$\begin{aligned} p_v\colon \mathcal{L}(E,F) &\to \mathbb{R} \\ T &\mapsto \|T(v)\|_F \end{aligned} \tag{7.378}$$

est une seminorme.

*La **topologie $*$-faible** sur $\mathcal{L}(E,F)$ est la topologie des ces seminormes.*

7.314.
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 30.24.

La proposition suivante indique qu'elle est un peu la topologie de la convergence ponctuelle.

Proposition 7.315.
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 :

$$T_n \xrightarrow{*} T \tag{7.379a}$$
$$p_v(T_n - T) \to 0 \; \forall v \in E \qquad \text{proposition 7.303} \tag{7.379b}$$
$$\|T_n(v) - T(v)\|_F \to 0 \; \forall v \in E \tag{7.379c}$$
$$T_n(v) \xrightarrow{E} T(v). \tag{7.379d}$$

□

7.17.4 Espace $C^k(\mathbb{R}, E')$

Nous revenons à nos histoires de limites de la définition 7.13.

Proposition 7.316 (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 7.313. 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 $\mathbb{R}$) :

$$\lim_{t\to t_0} u_t(x) = T(x). \tag{7.380}$$

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

$$\lim_{t\to t_0} u_t(x) = T'(x). \tag{7.381}$$

Par unicité de la limite dans $\mathbb{R}$ nous devons alors avoir $T(x) = T'(x)$ pour tout x, c'est-à-dire $T = T'$. □

Proposition 7.317.
Soit $u\colon \mathbb{R} \to E'$ une fonction continue. Alors

(1) pour tout $x \in E$ la fonction $t \mapsto u_t(x)$ est continue,

(2) pour tout $x \in E$ nous avons la limite dans $\mathbb{R}$

$$\lim_{t\to t_0} u_t(x) = u_{t_0}(x), \tag{7.382}$$

(3) nous avons la limite dans E'

$$\lim_{t\to t_0} u_t = u_{t_0}. \tag{7.383}$$

Démonstration. Soient $x \in E$ et $\epsilon > 0$. Par la proposition 7.307 la continuité de u donne un $\delta > 0$ tel que

$$u_{B(t_0,\delta)} \subset B_x(u_{t_0}, \epsilon). \tag{7.384}$$

C'est-à-dire que si $|t - t_0| \leqslant \delta$ nous avons

$$\big|u_{t_0}(x) - u_t(x)\big| < \epsilon, \tag{7.385}$$

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 (7.382).

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

$$u_{B(t_0,\delta)} \subset B_i(u_{t_0}, \epsilon) \subset \mathcal{O}. \tag{7.386}$$

Cela signifie bien que

$$|t - t_0| \leqslant \delta \Rightarrow u_t \in \mathcal{O}, \tag{7.387}$$

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 7.101 de la limite et le résultat d'unicité 7.316. □

Définition 7.318.
*Si nous avons une application $u\colon \mathbb{R} \to E'$ nous considérons sa **dérivée** donnée par la limite*

$$u'_{t_0} = \lim_{t\to t_0} \frac{u_t - u_{t_0}}{t - t_0}. \tag{7.388}$$

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 30.4.

7.18 Espaces de Baire

Définition 7.319.
*Un **espace de Baire** est un espace topologique dans lequel toute intersection dénombrable d'ouverts denses est dense.*

Lemme 7.320 ([247])**.**
Un espace topologique est de Baire si et seulement si toute union dénombrable de fermés d'intérieur vides est d'intérieur vide.

Théorème 7.321 (Théorème de Baire[247])**.**
Les espaces suivants sont de Baire :

(1) les espaces topologiques localement compacts,

(2) les espaces métriques complets (donc ceux de Banach en particulier),

(3) tout ouvert d'un espace de Baire.

Démonstration. (i) **Espaces topologiques localement compacts**

(ii) **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

$$\bigcap_{n\in\mathbb{N}} U_n \cap V \tag{7.389}$$

contient l'intersection des B_n. Par le théorème 7.270 des fermés emboîtés (que nous utilisons parce que E est métrique et complet), cette intersection est non vide.

(iii) **Ouvert d'un espace de Baire**

□

Parmi les applications du théorème de Baire, nous avons

— Le théorème de Banach-Steinhaus 11.141.

— Le théorème de l'application ouverte 11.150.

Chapitre 8

Espaces affines

8.1 Vecteurs agissant sur un espace

Définition 8.1.
Soit E, un espace vectoriel. Un ***espace affine modelé sur*** *E est un ensemble $\mathcal{E}$ sur lequel le groupe $(E,+)$ agit à droite transitivement et librement*[1].

Étant donné que E est un groupe commutatif, l'action peut être vue indifféremment à gauche ou à droite. Si $M \in \mathcal{E}$ et si $x \in E$ nous notons $M + x$ au lieu de $x \cdot M$ le résultat de l'action de x sur M.

8.2.
Lorsque nous écrivons « $M + x$ », le symbole plus n'est pas une loi de composition interne de $\mathcal{E}$, mais une action.

Proposition-Définition 8.3.
Soient $N, M \in \mathcal{E}$. Il existe un unique $x \in E$ tel que $M + x = N$.
Nous noterons $\overrightarrow{MN}$ ce vecteur.

Démonstration. La transitivité de l'action assure l'existence et la liberté assure l'unicité. □

Lemme 8.4.
Pour tout élément A nous avons $A + 0 = A$.

Démonstration. Soit $B \in \mathcal{E}$. Nous avons :

$$B + 0 = B + (0 + 0) = (B + 0) + 0 \tag{8.1}$$

parce que le $+$ dénote une action.
En appliquant cette égalité à l'élément $B = A - 0$ nous trouvons l'égalité demandée. □

Proposition 8.5.
Soit un espace affine $\mathcal{E}$ modelé sur l'espace vectoriel E. Soient $A, B, C \in \mathcal{E}$. Nous avons les égalités suivantes dans E :

(1) $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$ *(relations de Chasles),*
(2) $\overrightarrow{AA} = 0$,
(3) $\overrightarrow{BA} = -\overrightarrow{AB}$.

Démonstration. Point par point.

1. Définition 2.45.

(i) **Pour (1)** Nous avons, par définition 8.3 les égalités

$$\begin{cases} C = A + \overrightarrow{AC} & \text{(8.2a)} \\ B = A + \overrightarrow{AB} & \text{(8.2b)} \\ C = B + \overrightarrow{BC} & \text{(8.2c)} \end{cases}$$

En substituant les deux premières dans la troisième, nous trouvons $A+\overrightarrow{AB}+\overrightarrow{BC} = A+\overrightarrow{AC}$. Par liberté de l'action, nous pouvons « simplifier » par A et trouver la relation de Chasles.

(ii) **Pour (2)** Nous avons $A + \overrightarrow{AA} = A$, mais aussi $A + 0 = A$. Par unicité nous avons $\overrightarrow{AA} = 0$.

(iii) **Pour (3)** Nous avons $B + \overrightarrow{BA} = A$ et $A + \overrightarrow{AB} = B$. En mettant bout à bout,

$$B + \overrightarrow{BA} + \overrightarrow{AB} = B. \tag{8.3}$$

Donc $\overrightarrow{BA} + \overrightarrow{AB} = 0$.

□

8.6.
Si E est un espace vectoriel, le groupe $(E, +)$ agit sur E par l'action $t_y(x) = y + x$. Utilisant cette action nous construisons l'**espace affine canonique** de E. En particulier nous notons $\mathcal{E}_n(\mathbb{K})$ l'espace affine canonique de $\mathbb{K}^n$ vu comme espace vectoriel sur $\mathbb{K}$.

— En tant qu'ensembles, $\mathcal{E}_n(\mathbb{K}) = \mathbb{K}^n$.

— Sur cet espace en particulier, si $M, N \in \mathcal{E}_n(\mathbb{K})$, nous avons $\overrightarrow{MN} = N - M$ où à droite, la différence est la différence vectorielle dans $\mathbb{K}^n$.

Ces deux points se généralisent immédiatement à un espace vectoriel E au lieu de $\mathbb{K}^n$.

8.2 Repères cartésiens affines

Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $\mathcal{E}$ un espace affine construit sur E.

Définition 8.7.
*Un multiplet $(A, e_1, \dots, e_n)$ où A est un point de $\mathcal{E}$ et $\{e_i\}$ est une base de E est un **repère cartésien** de $\mathcal{E}$.*

*Nous disons que $\{e_i\}$ est la **base associée** au repère.*

Proposition 8.8.
Si $\mathcal{E}$ est un espace affine modelé sur l'espace vectoriel E de dimension n sur le corps $\mathbb{K}$, et si $\big(A, \{e_i\}_{i=1,\dots,n}\big)$ est un repère cartésien, alors

$$\begin{aligned} \phi\colon \mathbb{K}^n &\to \mathcal{E} \\ (x_1, \dots, x_n) &\mapsto A + \sum_i x_i e_i. \end{aligned} \tag{8.4}$$

est une bijection.

*Ces nombres x_i sont les **coordonnées** du point $A + \sum_i x_i e_i$ dans le repère (A, e_i).*

Démonstration. L'application ϕ est surjective parce que l'action de E sur $\mathcal{E}$ est transitive et injective parce que l'action est libre. □

8.3 Classification affine des coniques

Soit une conique $f(x, y) = 0$ avec

$$f(x, y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f \tag{8.5}$$

dans le repère $R = (A, e_i)$.

Lemme 8.9.
La signature de la quadratique

$$q(x,y) = ax^2 + 2bxy + cy^2 \tag{8.6}$$

ne dépend pas de la base choisie et un changement de variables

$$\begin{cases} \tilde{x} = \alpha x + \beta y & \text{(8.7a)} \\ \tilde{y} = \gamma x + \delta y & \text{(8.7b)} \end{cases}$$

peut nous amener dans trois cas :

$$q(x,y) = \begin{cases} \tilde{x}^2 + \tilde{y}^2 & \text{genre ellipse} \\ \tilde{x}^2 - \tilde{y}^2 & \text{genre hyperbole} \\ \tilde{x}^2 & \text{genre parabole.} \end{cases} \tag{8.8}$$

Dans le troisième cas, la matrice de q est de rang 1.

Nous cherchons maintenant à savoir si un point $I = (x_0, y_0)$ est un centre de symétrie de $f(x,y) = 0$. Pour cela nous choisissons le repère centré en I, c'est-à-dire que nous posons

$$\begin{cases} x = x_0 + \tilde{x} & \text{(8.9a)} \\ y = y_0 + \tilde{y}. & \text{(8.9b)} \end{cases}$$

Un peu de calcul montre qu'alors la conique s'écrit

$$f(x_0,y_0) + q(\tilde{x},\tilde{y}) + (2ax_0 + 2by_0 + 2d)\tilde{x} + (2bx_0 + 2cy_0 + 2e)\tilde{y} = 0. \tag{8.10}$$

Lemme 8.10.
Le point I sera un centre de symétrique si les termes linéaires en $\tilde{x}$ et $\tilde{y}$ s'annulent, c'est-à-dire si

$$\begin{cases} ax_0 + by_0 + d = 0 & \text{(8.11a)} \\ bx_0 + cy_0 + e = 0. & \text{(8.11b)} \end{cases}$$

Nous supposons que $(d,e) \neq (0,0)$, sinon la conique de départ serait déjà centrée. Le déterminant du système (8.11) est

$$\delta = ac - b^2. \tag{8.12}$$

Si ce dernier est différent de zéro, le système possède une unique solution et la conique aura alors un unique centre de symétrie.

Si le déterminant du système est nul, il y a soit aucun centre de symétrie, soit une infinité. Dans le premier cas nous sommes en présence d'une parabole, et dans le second cas de deux droites parallèles.

Exemple 8.11.
Soit

$$f(x,y) = x^2 + 2xy - y^2 - 6x + 2y - 1 = 0 \tag{8.13}$$

donnée dans le repère affine $R = (A, \{e_i\})$. Nous commençons par étudier la signature de $q(x,y) = x^2 + 2xy - y^2$ dont la matrice symétrique est

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{8.14}$$

Son polynôme caractéristique est $\lambda^2 - 2$ dont les racines sont $\pm\sqrt{2}$. La signature est donc $(1,1)$ et nous sommes en présence d'une conique de genre hyperbole. Nous cherchons le centre en suivant le lemme 8.10. Nous posons $x = \tilde{x} + x_0$, $y = \tilde{y} + y_0$, et nous cherchons à résoudre le système

$$\begin{cases} x_0 + y_0 - 3 = 0 & \text{(8.15a)} \\ x_0 - y_0 + 1 = 0. & \text{(8.15b)} \end{cases}$$

L'unique solution est $(x_0, y_0) = (1, 2)$. Nous considérons le repère centré en (x_0, y_0), c'est-à-dire le repère

$$R' = (I, \{e_i\}) \tag{8.16}$$

avec $I = A + x_0 e_1 + y_0 e_2$ où A est l'origine du repère dans lequel l'équation (8.13) était donnée.

Par construction dans ce repère nous avons la conique

$$f(x_0, y_0) + q(\tilde{x}, \tilde{y}) = 0, \tag{8.17}$$

c'est-à-dire

$$\tilde{x}^2 + 2\tilde{x}\tilde{y} - \tilde{y}^2 - 2 = 0. \tag{8.18}$$

Maintenant, nous avons une quadrique centrée que nous voulons mettre sous une forme plus canonique :

$$\left(\frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y})\right)^2 - \tilde{y}^2 - 1 = 0. \tag{8.19}$$

Nous posons donc

$$\begin{cases} X = \frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y}) & \text{(8.20a)} \\ Y = \tilde{y}, & \text{(8.20b)} \end{cases}$$

pour trouver l'hyperbole

$$X^2 - Y^2 - 1 = 0. \tag{8.21}$$

Cherchons le changement de base correspondant. Pour trouver les coordonnées de e'_1 dans la base (e_1, e_2) nous cherchons pour quelles valeurs de x, y nous avons $e'_1 = xe_1 + ye_2$. Le point e'_1 étant caractérisé par $X = 1$, $Y = 0$ nous avons à résoudre

$$\begin{cases} \frac{1}{\sqrt{2}}(x + y) = 1 & \text{(8.22a)} \\ y = 0, & \text{(8.22b)} \end{cases}$$

ce qui donne $x = \sqrt{2}$ et $y = 0$. Donc

$$e'_1 = \sqrt{2}e_1. \tag{8.23}$$

Pour trouver e'_2, c'est le même raisonnement en posant $X = 0$ et $Y = 1$. Le résultat est :

$$e'_2 = -e_1 + e_2. \tag{8.24}$$

Résumons :

$$\begin{cases} e'_1 = \sqrt{2}e_1 & \text{(8.25a)} \\ e'_2 = -e_1 + e_2. & \text{(8.25b)} \end{cases}$$

Il y a un dicton qui dit que les vecteurs de base se transforment avec la matrice inverse des coefficients. Prenons la matrice M donnée par

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} = M \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} \tag{8.26}$$

Calculons la matrice inverse.

```
sage: M=matrix([  [1/sqrt(2), 1/sqrt(2)],[0,1]  ])
sage: M
[1/2*sqrt(2) 1/2*sqrt(2)]
[           0            1]
sage: M.inverse()
[sqrt(2)      -1]
[       0       1]
```

tex/sage/sageSnip023.sage

Nous voyons que les colonnes de la matrice M^{-1} donnent les coordonnées des vecteurs e'_1 et e'_2.

△

8.4 Applications affines

Voici la définition d'une application affine entre deux espaces affines. La définition 9.154 donnera le définition d'une application affine entre espaces vectoriels.

Définition 8.12.
Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines sur les espaces vectoriels E et E' (sur le même corps $\mathbb{K}$). Une application $f\colon \mathcal{E} \to \mathcal{E}'$ est dite ***affine*** *si pour tout $M \in \mathcal{E}$, il existe une application linéaire*[2] *$u_M\colon E \to E'$ telle que*

$$f(M+x) = f(M) + u_M(x) \tag{8.27}$$

pour tout $x \in E$.

La définition suivante permet de décomposer une application affine en une partie linéaire et une translation. À partir de là, la proposition 8.62 nous donnera une structure de groupe sur $\mathrm{Aff}(\mathbb{R}^n)$.

Lemme-Définition 8.13 (partie linéaire d'une application affine[1])**.**
Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines sur les espaces vectoriels E et E' (sur le même corps $\mathbb{K}$). Nous considérons une application affine $f\colon \mathcal{E} \to \mathcal{E}'$.

Il existe une unique application linéaire $u\colon E \to E'$ telle que

$$f(M+x) = f(M) + u(x) \tag{8.28}$$

pour tout $x \in E$ et pour tout $M \in \mathcal{E}$.

Cette application linéaire est appelée ***partie linéaire*** *de f. Pour varier les notations, nous noterons souvent $f = \alpha \circ \tau_v$ pour une application linéaire α et la translation τ_v de vecteur v.*

Démonstration. En plusieurs étapes.

(i) **Unicité** Supposons que u_1 et u_2 vérifient la propriété, alors pour tout $x \in E$ et tout $M \in \mathcal{E}$ nous avons $f(M+x) = f(M) + u_1(x)$ et $f(M+x) = f(M) + u_2(x)$. Cela suffit à nous convaincre que $u_1 = u_2$.

(ii) $u_M = u_N$ Avant de prouver l'existence, nous considérons $M, N \in \mathcal{E}$ et les applications linéaires u_M et u_N vérifiant l'équation (8.27) pour M et N respectivement. Prouvons que $u_M = u_N$.
Posons

$$f(M+x) = f(M) + u_M(x) \tag{8.29a}$$
$$f(N+y) = f(N) + u_N(y). \tag{8.29b}$$

Définissons $a \in E$ par $N = M + a$; nous avons d'une part

$$f(N+y) = f(M+y+a) = f(M) + u_M(y+a), \tag{8.30}$$

et d'autre part

$$f(N+y) = f(M+a) + u_N(y) = f(M) + u_M(a) + u_N(y). \tag{8.31}$$

Par conséquent $u_M(y+a) = u_M(a) + u_N(y)$. Par linéarité $u_N = u_M$.

(iii) **Existence** Soit $M \in \mathcal{E}$. Nous affirmons que u_M fait l'affaire. En effet, soient $N \in \mathcal{E}$ et $x \in E$. Puisque $u_M = u_N$ nous avons

$$f(N+x) = f(N) + u_N(x) = f(N) + u_M(x). \tag{8.32}$$

Donc effectivement u_M peut être utilisé en tout point de $\mathcal{E}$.

□

Ce lemme est important car il permet de démontrer qu'une application est affine en prouvant la linéarité des u_M séparément sans devoir prouver qu'elles sont égales.

2. Définition 4.28.

8.4.1 Autres propriétés

Lemme 8.14 ([1]).
Soient $M \in \mathcal{E}$ et $A, B \in \mathcal{E}$ deux points donnés par $A = M + x_a$, $B = M + x_b$. Soit encore une application affine f sur $\mathcal{E}$. Alors

$$\overrightarrow{f(A)f(B)} = u_f(x_b - x_a). \tag{8.33}$$

Démonstration. En appliquant f à $A = M + x_a$ et $B = M + x_b$,

$$f(A) = f(M) + u_f(x_a) \tag{8.34a}$$
$$f(B) = f(M) + u_f(x_b). \tag{8.34b}$$

Donc $f(B) = f(A) - u_f(x_a) + u_f(x_b)$ ou encore

$$f(B) = f(A) + u_f(x_b - x_a). \tag{8.35}$$

□

Remarque 8.15.
La condition (8.27) pour tout $M \in \mathcal{E}$ est équivalente à demander

$$f \circ t_x = t_{u(x)} \circ f \tag{8.36}$$

pour tout $x \in E$.

Proposition 8.16 ([1]).
Soit une application affine $f : \mathcal{E} \to \mathcal{E}'$.

(1) Il existe une unique application linéaire u_f telle que $f(M + x) = f(M) + u_f(x)$ pour tout $M \in \mathcal{E}$ et tout $x \in E$.

(2) L'application u_f est injective si et seulement si f est injective.

(3) L'application u_f est surjective si et seulement si f est surjective.

Démonstration. En plein de parties.

(i) **Pour (1)** La partie (1) est le lemme 8.13.

(ii) **Si u_f est injective** Soient $M, N \in \mathcal{E}$ tels que $f(M) = f(N)$. Nous avons

$$f(M) = f(N) = f\big(M + (N - M)\big) = f(M) + u_f(N - M), \tag{8.37}$$

donc $u_f(N - M) = 0$. Vu que u_f est injective, nous déduisons que $N - M = 0$.

(iii) **Si f est injective** Soient $x, y \in E$ tels que $u_f(x) = u_f(y)$. Soit M quelconque dans $\mathcal{E}$; nous avons

$$f(M + x) = f(M) + u_f(x) = f(M) + u_f(y) = f(M + y). \tag{8.38}$$

L'injectivité de f nous indique alors que $M + x = M + y$ et donc que $x = y$ parce que l'action de E sur $\mathcal{E}$ est libre.

(iv) **Si u_f est surjective** Soit $M \in \mathcal{E}$. Nous allons trouver un élément de $\mathcal{E}$ dont l'image par f est M. Soient $N \in \mathcal{E}$ et $x \in E$ tels que $u_f(x) = M - f(N)$.
Alors nous avons $f(N + x) = f(N) + u_f(x) = M$.

(v) **Si f est surjective** Soit $a \in E$. Nous voulons $x \in E$ tel que $u_f(x) = a$. Soit $M \in E$. Vu que f est surjective, il existe $N \in \mathcal{E}$ tel que $f(N) = f(M) + a$.
Posons $x = N - M$. Nous avons d'une part

$$f(M + x) = f(M) + u_f(x) \tag{8.39}$$

et d'autre part

$$f(M + x) = f\big(M + (N - M)\big) = f(N) = f(M) + a. \tag{8.40}$$

En égalisant nous trouvons $u_f(x) = a$.

□

Proposition 8.17.
Soient des espaces affines $\mathcal{E}$ et $\mathcal{E}'$ de même dimension. Une application affine $f\colon \mathcal{E} \to \mathcal{E}'$ est injective si et seulement si elle est surjective.

Démonstration. Nous allons utiliser les équivalences de la proposition 8.16, ainsi que le corolaire 4.48 pour la partie linéaire. Nous avons les équivalences :

$$f \text{ est injective} \Leftrightarrow u_f \text{ est injective} \Leftrightarrow u_f \text{ est surjective} \Leftrightarrow f \text{ est surjective.} \tag{8.41}$$

□

Exemple 8.18.
L'espace $\mathbb{R}^n$ est très particulier parce qu'il agit sur lui-même ; il est donc un espace affine à lui tout seul : $\mathcal{E} = E = \mathbb{R}^n$.

Dans le cas de $\mathbb{R}^n$, en posant $M = 0$ dans la condition (8.27), si f est une application affine il existe une application linéaire α et un vecteur v tel que $f = \tau_v \circ \alpha$.

Notons que ça n'a pas de sens de poser $M = 0$, et la décomposition $f = \tau_v \circ \alpha$ n'a aucun sens en général. En particulier, nous ne pouvons pas appliquer une application linéaire à un élément d'un espace affine général. △

Proposition 8.19.
Si $f\colon \mathcal{E} \to \mathcal{E}'$ et $g\colon \mathcal{E}' \to \mathcal{E}''$ sont des applications affines, alors $g \circ f\colon \mathcal{E} \to \mathcal{E}''$ est affine et $u_{g\circ f} = u_g \circ u_f$.

Démonstration. Si $M \in \mathcal{E}$ et $x \in E$ nous avons

$$\begin{aligned}(g \circ f)(M + x) &= g\big(f(M) + u_f(x)\big)\\ &= g\big(f(M)\big) + u_g\big(u_f(x)\big)\\ &= (g \circ f)(M) + (u_g \circ u_f)(x).\end{aligned} \tag{8.42}$$

□

Théorème 8.20.
Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines de dimensions finies p et q sur $\mathbb{K}$. Soient les repères cartésiens $R = (O, \{e_i\})$ et $R' = (O', \{e'_i\})$. Une application $f\colon \mathcal{E} \to \mathcal{E}'$ est affine si et seulement si il existe une matrice $a \in \mathbb{M}_{p,q}(\mathbb{K})$ et $b \in \mathbb{K}^q$ tels que[3]

$$f(x) = b + ax. \tag{8.43}$$

8.5 Isomorphismes

Définition 8.21.
*Un **isomorphisme** entre les espaces affines $\mathcal{E}$ et $\mathcal{E}'$ est une application affine $f\colon \mathcal{E} \to \mathcal{E}'$ inversible dont l'inverse est affine.*

Proposition 8.22.
Une application affine bijective est un isomorphisme. Si f est un isomorphisme d'espaces affines, alors $u_{f^{-1}} = (u_f)^{-1}$.

Proposition 8.23.
Un espace affine de dimension finie n sur un corps $\mathbb{K}$ est isomorphe à l'espace affine canonique $\mathcal{E}_n(\mathbb{K})$.

3. L'équation (8.43) est écrite en utilisant un abus de notation entre le vecteur $x \in \mathbb{K}^p$ et le point de $\mathcal{E}$ qui est représenté par x dans le repère $(A, \{e_i\})$.

Démonstration. Si nous considérons le repère $R = (A, \{e_i\})$ de l'espace affine $\mathcal{E}$ alors l'application

$$\begin{aligned} \varphi\colon \mathbb{K}^n &\to \mathcal{E} \\ (x_1, \ldots, x_n) &\mapsto A + \sum_i x_i e_i \end{aligned} \tag{8.44}$$

est un isomorphisme. □

8.6 Sous espaces affines

Définition 8.24.
Soit $\mathcal{E}$ un espace affine sur l'espace vectoriel E. Un ***sous-espace affine*** *de $\mathcal{E}$ est une orbite de l'action d'un sous-espace vectoriel de E.*

Si $\mathcal{F}$ est un sous-ensemble de $\mathcal{E}$, il sera un sous-espace affine de $\mathcal{E}$ si et seulement si l'ensemble

$$F = \{AB \text{ tel que } A, B \in \mathcal{F}\} \tag{8.45}$$

est un sous-espace vectoriel de E. Dans ce cas nous disons que F est la **direction** de $\mathcal{F}$. Si $A \in \mathcal{F}$, alors l'orbite de A sous F est $\mathcal{F}$. La **dimension** de $\mathcal{F}$ est la dimension de sa direction.

Si $\mathcal{F}$ et $\mathcal{G}$ sont des sous-espaces affines de $\mathcal{E}$ de directions F et G, nous disons que $\mathcal{F}$ est **parallèle** à $\mathcal{G}$ si $F \subset G$.

Proposition 8.25.
Soit $\mathcal{F}$ un sous-espace affine de dimension k dans l'espace affine $\mathcal{E}$ de dimension n. Alors il existe une application affine $f\colon \mathcal{E} \to \mathbb{K}^{n-k}$ telle que $\mathcal{F} = f^{-1}(0)$.

Démonstration. Soient F la direction de $\mathcal{F}$ et $A \in \mathcal{F}$. Nous considérons une base $\{e_i\}$ adaptée à F au sens $\{e_1, \ldots, e_k\}$ est une base de F. Nous considérons maintenant le repère cartésien $(A, \{e_i\})$ et nous construisons l'application affine

$$\begin{aligned} f\colon \mathcal{E} &\to \mathbb{K}^{n-k} \\ A + \sum_{i=1}^{n} x_i e_i &\mapsto \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}. \end{aligned} \tag{8.46}$$

Par construction nous avons $f(M) = 0$ si et seulement si $M \in \mathcal{F}$. □

Proposition 8.26 ([57])**.**
Soit σ une partie de l'espace affine $\mathcal{E}$.

(1) L'intersection de tous les sous-espaces affines contenant σ est un sous-espace affine, noté $\mathcal{F}$.

(2) Si $A \in \sigma$, alors la direction de $\mathcal{F}$ est le sous-espace vectoriel

$$F = \operatorname{Span}\{\overrightarrow{AM} \text{ tel que } M \in \sigma\}. \tag{8.47}$$

Le sous-espace affine donné par la proposition 8.26 est le sous-espace affine **engendré** par la partie σ, et il est noté $\operatorname{eae}(\sigma)$.

Proposition 8.27.
Soit $\mathcal{E}$ un espace affine de dimension n sur $\mathbb{K}$, soit $f\colon \mathcal{E} \to \mathbb{K}^r$ une fonction affine. Pour tout $a = (a_1, \ldots, a_r) \in \mathbb{K}^r$, l'ensemble $f^{-1}(a)$ est un sous-espace affine[4] *de dimension* $\dim \ker(u_f)$.

4. Définition 8.24.

Démonstration. Nous considérons le repère $(A, \{e_i\})$ de $\mathcal{E}$. Étant donné que f est affine nous avons

$$f\big(A + \sum_i x_i e_i\big) = f(A) + u_f\big(\sum_i x_i e_i\big). \tag{8.48}$$

Nous avons donc $f\big(A + \sum_i x_i e_i\big) = a$ lorsque

$$u_f(\sum_i x_i e_i) = a - f(A). \tag{8.49}$$

En utilisant le lemme 4.39, nous avons donc

$$f^{-1}(a) = A + (u_f)^{-1}\big(a - f(A)\big) = A + m + \ker(u_f) \tag{8.50}$$

où m est n'importe que élément de $u_f^{-1}\big(a - f(A)\big)$. □

Proposition 8.28.
Soit un espace vectoriel normé[5] $(V, \|.\|)$. *Pour tout* $a \in V$ *et* $r > 0$, *la boule* $B(a, r)$ *est convexe*[6]. *La boule fermée* $\overline{B(a, r)}$ *également.*

Démonstration. En deux parties.

(i) **La boule centrée en zéro** Soient $x, y \in B(0, r)$ et $\lambda \in]0, 1[$. Alors

$$\|\lambda x + (1 - \lambda)y\| \leqslant |\lambda|\|x\| + |1 - \lambda|\|y\| < (|\lambda| + |1 - \lambda|)r \leqslant r \tag{8.51}$$

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.

(ii) **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

$$\lambda(x - a) + (1 - \lambda)(y - a) \in B(0, r) \tag{8.52}$$

par la première partie. En développant et simplifiant,

$$\lambda x + (1 - \lambda)y - a \in B(0, r), \tag{8.53}$$

ce qui signifie que $\lambda x + (1 - \lambda)y \in B(a, r)$.

□

Proposition 8.29.
Soit A *un ensemble convexe*[7] *dans un espace vectoriel et* $v_1, \dots, v_n$ *des éléments de* A. *Alors toute combinaison*

$$a_1 v_1 + \cdots + a_n v_n \tag{8.54}$$

telle que $a_1 + \cdots + a_n = 1$ *et* $a_i \in [0, 1]$ *appartient à* A.

Démonstration. Nous prouvons la proposition pour $n = 3$. Nous devons trouver des nombres $t_1, t_2 \in [0, 1]$ tels que

$$t_2\big(t_1 v_1 + (1 - t_1)v_2\big) + (1 - t_2)v_3 = a v_1 + b v_2 + c v_3. \tag{8.55}$$

La réponse est immédiatement donnée par

$$t_2 a = 1 - c \tag{8.56a}$$
$$t_1 = a/t_2. \tag{8.56b}$$

Étant donné que $c \in [0, 1]$ nous avons $t_2 \in [0, 1]$. En ce qui concerne t_1 nous avons

$$t_1 = \frac{a}{t_2} \leqslant \frac{1 - c}{1 - c} = 1. \tag{8.57}$$

□

5. Définition 7.146.
6. Définition 7.144.
7. Définition 7.144.

8.7 Barycentre

Soit $\mathcal{E}$ un espace affine sur le $\mathbb{K}$-espace vectoriel E. Un couple (A, λ) avec $A \in \mathcal{E}$ et $\lambda \in \mathbb{K}$ est un **point pondéré**.

Lemme-Définition 8.30 ([248]).
Soit une famille de points pondérés $\{(A_i, \lambda_i)\}_{i=1\ldots r}$. Si $\sum_i \lambda_i \neq 0$, alors il existe un unique $G \in \mathcal{E}$ tel que

$$\sum_{i=1}^{r} \lambda_i \overrightarrow{GA_i} = 0. \tag{8.58}$$

*Le point G donné par le lemme 8.30 est le **barycentre** des points pondérés (A_i, λ_i).*

Notons que l'on peut toujours supposer que $\sum_i \lambda_i = 1$ parce que le barycentre ne change pas lorsque tous les λ_i sont multipliés par un même nombre.

Définition 8.31 (Combinaison convexe).
*Des nombres positifs ou nuls $\lambda_1, \ldots, \lambda_n$ vérifiant $\sum_i \lambda_i = 1$ forment une **combinaison convexe**.*

Le théorème suivant donne quelques caractérisations équivalentes du barycentre.

Théorème 8.32 ([248]).
Soient $\{(A_i, \lambda_i)\}_{i=1,\ldots,r}$ une famille de points pondérés. Les conditions suivantes sur le point $G \in \mathcal{E}$ sont équivalentes.

(1) Le point G est le barycentre de la famille.
(2) Pour tout $\alpha \in \mathbb{R}^*$, $\sum_i (\alpha\lambda_i)\overrightarrow{GA_i} = 0$.
(3) Il existe $A \in \mathcal{E}$ tel que $\left(\sum_i \lambda_i\right)\overrightarrow{AG} = \sum_i \lambda_i \overrightarrow{AA_i}$.
(4) Pour tout $B \in \mathcal{E}$, nous avons $\left(\sum_i \lambda_i\right)\overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}$.

Définition 8.33.
*Si $A, B \in \mathcal{E}$, le **segment** $[AB]$ est l'ensemble des barycentres de A et B pondérés par des poids positifs (ouvert ou fermé suivant que l'on accepte que l'un ou l'autre des poids soit nul).*

Lorsque tous les λ_i sont égaux, nous parlons d'**isobarycentre**. Autrement dit, l'isobarycentre des points A_i est le barycentre des points pondérés $(A_i, 1)$.

8.7.1 Sous-espaces affines

Proposition 8.34.
Une partie $\mathcal{F}$ de $\mathcal{E}$ est un sous-espace affine si et seulement si elle est stable par barycentrisation.

Démonstration. Soit $\mathcal{F}$ un sous-espace affine de direction F et $A_1, \ldots, A_n$ des points de $\mathcal{F}$. Nous devons voir que le barycentre des points A_i pondérés de n'importe quelles masses appartient à $\mathcal{F}$. Pour ce faire nous faisons appel à la caractérisation (4) du théorème 8.32 : pour tout $B \in \mathcal{F}$,

$$\overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}. \tag{8.59}$$

Puisque B et A_i sont dans $\mathcal{F}$, nous avons $\overrightarrow{BA_i} \in F$ et donc $\overrightarrow{BG} \in F$. Mais comme $B \in \mathcal{F}$, le point G est à son tour dans $\mathcal{F}$.

Réciproquement, nous supposons que $\mathcal{F}$ est stable par barycentrisme. Nous voudrions montrer que l'ensemble

$$F = \{\overrightarrow{AB} \text{ tel que } A, B \in \mathcal{F}\} \tag{8.60}$$

est un sous-espace vectoriel. Soit $A \in \mathcal{F}$. Nous commençons par prouver que les vecteurs de la forme $\overrightarrow{AX}$ ($X \in \mathcal{F}$) forment un espace vectoriel. Considérons $\overrightarrow{AX} + \overrightarrow{AY}$ qui est un élément de E ; il existe donc $V \in \mathcal{E}$ tel que

$$\overrightarrow{AV} = \overrightarrow{AX} + \overrightarrow{AY}. \tag{8.61}$$

Par les relations de Chasles,

$$\overrightarrow{AV} = \overrightarrow{AV} + \overrightarrow{VX} + \overrightarrow{AV} + \overrightarrow{VY}, \tag{8.62}$$

donc

$$0 = \overrightarrow{VX} - \overrightarrow{VA} + \overrightarrow{VY}, \tag{8.63}$$

ce qui prouve que V est un barycentre de X, A, Y, et donc que $V \in \mathcal{F}$. De la même manière si $W \in \mathcal{E}$ est défini par $\overrightarrow{AW} = \mu\overrightarrow{AX}$, alors

$$\overrightarrow{AW} = \mu\overrightarrow{AX} = \mu(\overrightarrow{AW} + \overrightarrow{WX}), \tag{8.64}$$

ce qui signifie que

$$(1-\mu)\overrightarrow{AW} + \mu\overrightarrow{XW} = 0 \tag{8.65}$$

et que W est un barycentre.

Afin de montrer que (8.60) est bien un espace vectoriel, nous devons considérer $A, B, X, Y \in \mathcal{F}$ et prouver que $\overrightarrow{AX} + \overrightarrow{BY} \in F$. Nous avons

$$\begin{aligned}
\overrightarrow{AX} + \overrightarrow{BY} &= \overrightarrow{AX} + \overrightarrow{BA} + \overrightarrow{AY} && && \text{(8.66a)}\\
&= \overrightarrow{AV} + \overrightarrow{BA} && V \text{ est celui donné plus haut} && \text{(8.66b)}\\
&= \overrightarrow{AV} - \overrightarrow{AB} && && \text{(8.66c)}\\
&= \overrightarrow{AV} + \overrightarrow{AW} && W \text{ est donné par } \mu = -1. && \text{(8.66d)}\\
&= \overrightarrow{AV'}. && && \text{(8.66e)}
\end{aligned}$$

□

Proposition 8.35 ([248]).
Soient $A_0, \dots, A_r$ des points de $\mathcal{E}$. L'ensemble des barycentres de ces points (avec des masses de somme 1) est le sous-espace affine engendré par les A_i que nous nommons $\mathcal{F}$.

Démonstration. Soit G le barycentre associé aux poids λ_i. Nous avons

$$G = A_0 + \overrightarrow{A_0G} = A_0 + \sum_{i=1}^{r} \lambda_i \overrightarrow{A_0A_i}. \tag{8.67}$$

Notons que les vecteurs $\overrightarrow{A_0A_i}$ sont dans la direction du sous-espace affine engendré par les A_i par (8.47). Donc G est bien dans $\mathcal{F}$.

Inversement si X est dans $\mathcal{F}$, on a

$$X = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i} \tag{8.68}$$

parce que $\sum_i \lambda_i \overrightarrow{A_0A_i}$ est un élément général de la direction de $\mathcal{F}$. Donc

$$\overrightarrow{A_0X} = \sum_i \lambda_i \overrightarrow{A_0A_i}, \tag{8.69}$$

et en utilisant la relation de Chasles sur chacun des $\overrightarrow{A_0A_i}$,

$$\overrightarrow{A_0X} = \sum_i \lambda_i \big(\overrightarrow{A_0X} + \overrightarrow{XA_i}\big). \tag{8.70}$$

De là nous concluons que

$$\big(1 - \sum_i \lambda_i\big)\overrightarrow{A_0X} + \sum_i \lambda_i \overrightarrow{A_iX} = 0, \tag{8.71}$$

ce qui signifie précisément que X est un barycentre des A_i. □

Proposition 8.36.
Soient $r+1$ point $A_0, \dots, A_r$ dans $\mathcal{E}$. Le sous-espace affine engendré par les A_i est au plus de dimension r.

Démonstration. La direction de l'espace engendré $\text{Aff}\{A_i\}$ est l'espace

$$\text{Span}\{\overrightarrow{A_0A_i}_{i=1,\dots,r}\} \tag{8.72}$$

qui est engendré par r vecteurs et donc est au plus de dimension r. □

En deux mots, la proposition suivante signifie que le barycentre des barycentres est le barycentre.

Proposition 8.37 (Associativité des barycentres[249])**.**
Soit une partition $J_0, \dots, J_r$ de $I = \{0, 1, \dots, n\}$. Soient des points $a_0, \dots, a_n \in \mathcal{E}$ et $\lambda_0, \dots, \lambda_n$ des nombres tels que $\sum_i \lambda_i \neq 0$. Nous supposons que $\mu_k = \sum_{i\in J_k} \lambda_i \neq 0$ pour tout k, et enfin nous nommons b_k le barycentre de la famille $\{(a_i, \lambda_i), i \in J_k\}$.

Alors le barycentre de la famille $\{(b_k, \mu_k)\}_{k=1,\dots,r}$ est le barycentre de la famille $\{(a_i, \lambda_i)\}_{i\in I}$.

Démonstration. Nous nommons b le barycentre des b_k pondérés par les μ_k, donc par définition

$$0 = \sum_{k=0}^{r} \mu_k \overrightarrow{bb_k} \tag{8.73a}$$

$$= \sum_k \sum_{i\in J_k} \lambda_i \overrightarrow{bb_k} \tag{8.73b}$$

$$= \sum_{k=0}^{r} \sum_{i\in J_k} \lambda_i (\overrightarrow{ba_i} + \overrightarrow{a_ib_k}) \tag{8.73c}$$

$$= \sum_{k=0}^{r} \sum_{i\in J_k} \lambda_i \overrightarrow{ba_i} + \sum_{k=0}^{r} \underbrace{\sum_{i\in J_k} \lambda_i \overrightarrow{a_ib_k}}_{=0} \tag{8.73d}$$

$$= \sum_{i\in I} \lambda_i \overrightarrow{ba_i}. \tag{8.73e}$$

Donc b est bien barycentre des a_i avec les poids λ_i. □

8.7.2 Enveloppe convexe

Définition 8.38.
*Soit A une partie d'un espace vectoriel E. L'**enveloppe convexe** de A, notée $\mathcal{C}\text{onv}(A)$ est l'intersection de tous les convexes contenant A.*

L'enveloppe convexe est un convexe. En effet soit C un convexe contenant A et $x, y \in \mathcal{C}\text{onv}(A)$; alors x et y sont dans C et par conséquent le segment $[x, y]$ est inclus dans C. Ce segment étant inclus dans tout convexe contenant A, il est inclus dans $\mathcal{C}\text{onv}(A)$.

Proposition 8.39 ([250])**.**
Soit C un convexe dans l'espace affine $\mathcal{E}$ et une famille de points pondérés $\{(a_i, \lambda_i)\}_{i=1,\dots,r}$ dont tous les poids sont positifs (et non tous nuls). Alors le barycentre est aussi dans C.

En d'autre termes, un convexe est stable par barycentrage à poids positifs[8]*.*

Démonstration. Nous prouvons par récurrence. D'abord pour $r = 2$. Le barycentre des points pondérés (a_1, λ_1), (a_2, λ_2) est le point b tel que

$$\lambda_1 \overrightarrow{ba_1} + \lambda_2 \overrightarrow{ba_2} = 0. \tag{8.74}$$

8. Sauf si on prend tous les poids nuls ; mais contre ce genre d'idées, on ne peut rien faire.

Par définition, ce qui est noté $\overrightarrow{ab}$ n'est rien d'autre que $b-a$; en déballant (8.74), nous trouvons

$$\lambda_1(a_1-b)+\lambda_2(a_2-b)=0 \tag{8.75}$$

et donc

$$b=\frac{\lambda_1}{\lambda_1+\lambda_2}a_1+\frac{\lambda_2}{\lambda_1+\lambda_2}a_2, \tag{8.76}$$

qui est bien un point du segment $[a_1,a_2]$ parce que c'est une combinaison à coefficients positifs de somme 1.

Nous passons maintenant à la vraie récurrence avec un ensemble de points pondérés

$$A_r=\{(a_1,\lambda_1),\dots,(a_r,\lambda_r)\} \tag{8.77}$$

de masse totale non nulle ; et en vous laissant deviner ce que va désigner A_{r-1}. Si une des masses est nulle (disons λ_r), alors le barycentre de A_r est le même que celui de A_{r-1} et l'hypothèse de récurrence nous enseigne que ledit barycentre est dans C. Nous supposons donc que $\lambda_i\neq 0$ pour tout i. Dans ce cas le théorème d'associativité des barycentres 8.37 dit que le barycentre de A_r est le barycentre entre le barycentre de A_{r-1} et (a_r,λ_r), qui sont deux points de C par hypothèse de récurrence. □

Si E est un espace vectoriel et si $x_i\in E$ et $\lambda_i\in\mathbb{R}$, alors le barycentre des couples (x_i,λ_i) est le point g tel que $\sum_i\lambda_i\overrightarrow{gx_i}$, c'est-à-dire $\sum_i\lambda_i(x_i-g)=0$ ou encore

$$\sum_i\lambda_i x_i=\sum_i\lambda_i g. \tag{8.78}$$

Donc, quitte à diviser tous les λ_i par la somme, nous pouvons supposer que la somme des poids est 1. C'est pourquoi lorsque nous parlerons de barycentre dans un espace vectoriel sans contexte affine, nous allons toujours supposer $\sum_i\lambda_i=1$ et avoir le barycentre

$$g=\sum_i\lambda_i x_i. \tag{8.79}$$

Proposition 8.40.
Soit E, un espace vectoriel et $A\subset E$. L'enveloppe convexe $\mathcal{C}\mathrm{onv}(A)$ est l'ensemble des barycentres de familles finies de points affublés de masses positives.

Démonstration. Nous notons $\mathcal{B}$ l'ensemble des dits barycentres. Par la proposition 8.39, ces barycentres sont dans l'enveloppe convexe et donc $\mathcal{B}\subset\mathcal{C}\mathrm{onv}(A)$. A contrario, si nous prouvons que $\mathcal{B}$ était convexe, alors nous aurions $\mathcal{C}\mathrm{onv}(A)\subset\mathcal{B}$ parce que l'enveloppe convexe est l'intersection des convexes contenant A.

Soient $a,b\in\mathcal{B}$, c'est-à-dire que l'on a $a_0,\dots,a_n$ et $b_0,\dots,b_m$ dans A ainsi que les nombres strictement positifs $\lambda_0,\dots,\lambda_n$ et $\mu_0,\dots,\mu_m$ tels que

$$a=\sum_i\lambda_i a_i \qquad \sum_{i=1}^{n}\lambda_i=1 \tag{8.80a}$$

$$b=\sum_j\mu_j b_j \qquad \sum_{j=1}^{n}\mu_j=1 \tag{8.80b}$$

Un point du segment $[a,b]$ est de la forme $p=ta+(1-t)b$ avec $t\in[0,1]$. En développant,

$$p=\sum_{i=0}^{n}(t\lambda_i)a_i+\sum_{j=0}^{m}(1-t)\mu_j b_j. \tag{8.81}$$

C'est le barycentre de la famille $\{(a_i,\lambda_i),(b_j,\mu_j)\}$, parce que la somme des coefficients vaut bien 1 :

$$\sum_i(t\lambda_i)+\sum_j(1-t)\mu_j=t+(1-t)=1. \tag{8.82}$$

□

Théorème 8.41 (Carathéodory[102]).
Dans un espace affine de dimension n, l'enveloppe convexe[9] *de A est l'ensemble des barycentres à coefficients positifs ou nuls de familles de $n+1$ points.*

Démonstration. Soit $x \in \mathcal{C}\text{onv}(A)$; on sait par la proposition 8.40 que x est barycentre de points de A avec des coefficients positifs :

$$x = \sum_{k=1}^{p} \lambda_k x_k \tag{8.83}$$

avec $\sum_k \lambda_k = 1$. Nous supposons que $p > n+1$ (sinon le théorème est réglé), et nous allons faire une récurrence à l'envers en montrant qu'on peut aussi écrire x sous forme d'un barycentre de strictement moins de p points.

Étant donné que $p-1 > n$, la famille $\{x+i-x_1\}_{i=2,\dots,p}$ est liée et il existe donc $\alpha_1, \dots, \alpha_p \in \mathbb{R}$ tels que $\sum_{i=2}^{p} \alpha_i(x_i - x_1) = 0$, c'est-à-dire telle que

$$\sum_{i=2}^{p} \alpha_i x_i = \sum_{i=2}^{p} \alpha_i x_1. \tag{8.84}$$

Nous posons $\alpha_1 = -\sum_{i=2}^{p} \alpha_1$. Remarquons qu'alors $\sum_{i=1}^{p} \alpha_i x_i = 0$ parce que

$$\sum_{i=1}^{p} \alpha_i x_i = \alpha_1 x_1 + \sum_{i=2}^{p} \alpha_i x_i = \alpha_1 x_1 + \sum_{i=2}^{p} \alpha_i x_1 = \sum_{i=1}^{p} \alpha_i x_1 = 0. \tag{8.85}$$

Par conséquent ça ne coûte rien de récrire (8.83) sous la forme

$$x = \sum_{i=1}^{p} (\lambda_i + t\alpha_i) x_i. \tag{8.86}$$

Les α_i ne sont pas tous nuls, mais leur somme est nulle, donc il y en a au moins un négatif. Nous notons

$$\tau = \min\{-\frac{\lambda_i}{\alpha_i} \text{ tel que } \alpha_i < 0\}, \tag{8.87}$$

et J l'ensemble de i pour lesquels ce minimum est atteint. Nous considérons aussi les nombres $\mu_i = \lambda_i + \tau\alpha_i$. Plusieurs remarques.

(1) Si $j \in J$, alors $\mu_j = 0$

(2) Si $\alpha_i > 0$ alors $\mu_i \geqslant 0$, mais si $\alpha_i < 0$ alors

$$\lambda_i + \tau\alpha_i \geqslant \lambda_i + (-\frac{\lambda_i}{\alpha_i})\alpha_i = 0 \tag{8.88}$$

donc $\mu_i \geqslant 0$ quand même.

(3) $\sum_{i=1}^{p} \mu_i = 1$, toujours parce que $\sum_{i=1}^{p} \alpha_i = 0$.

Avec tout ça, nous avons

$$\sum_{i \notin J} \mu_i x_i = \sum_{i=1}^{p} \mu_i x_i = x. \tag{8.89}$$

Et voilà, nous avons écrit x comme un barycentre à coefficients positifs de moins de p éléments parce que J n'est pas vide. □

Corolaire 8.42.
Dans un espace affine de dimension finie, l'enveloppe convexe d'un compact est compacte.

9. Définition 8.38.

Démonstration. Soit A une partie compacte de l'espace vectoriel E, et $\mathcal{C}\text{onv}(A)$ son enveloppe convexe. Nous allons montrer que toute suite dans $\mathcal{C}\text{onv}(A)$ admet une sous-suite convergente en écrivant un point de $\mathcal{C}\text{onv}(A)$ comme le théorème de Carathéodory 8.41 nous le suggère. Pour cela nous considérons le simplexe

$$\Lambda = \left\{ \lambda \in \mathbb{R}^{n+1} \text{ tel que } \sum_{k=1}^{n+1} \lambda_k = 1 \text{ et } \lambda_k \geqslant 0 \forall k \right\}. \tag{8.90}$$

Montrons en passant que Λ est compact. Si $\lambda_k \in \Lambda$ est une suite, alors chacun des λ_k est un $(n+1)$-uple de nombres dans $[0,1]$:

$$k \mapsto (\lambda_k)_i \tag{8.91}$$

est une suite qui possède une sous-suite convergente. En passant $n+1$ fois à une sous-suite, nous tombons sur une suite convergente vers $\lambda \in \Lambda$, grâce à la convergence composante par composante. De plus pour chaque k nous avons $\sum_{i=1}^{n+1}(\lambda_k)_i = 1$, et en passant à la limite, la somme étant une application continue, $\sum_i \lambda_i = 1$.

Considérons l'application

$$\begin{aligned} f\colon \Lambda \times A^{n+1} &\to \mathcal{C}\text{onv}(A) \\ (\lambda, x) &\mapsto \sum_{k=1}^{n+1} \lambda_k x_k. \end{aligned} \tag{8.92}$$

C'est une application continue parce qu'elle est bilinéaire en dimension finie ; son image est contenue dans $\mathcal{C}\text{onv}(A)$ par la proposition 8.39, et elle est surjective par le théorème de Carathéodory 8.41. Bref, $\mathcal{C}\text{onv}(A) = f(\Lambda \times A^{n+1})$ est donc l'image d'un compact par une application continue ; elle est donc compacte par le théorème 7.195. □

Notons que sans le théorème de Carathéodory, peut être que le nombre de points utiles pour décomposer les différents a_k n'était pas borné ; dans ce cas nous aurions du prendre une infinité de sous-suites et rien n'aurait été sûr.

8.7.3 Applications affines et barycentre

Proposition 8.43 ([251]).
Une application $f\colon \mathcal{E} \to \mathcal{E}'$ entre deux espaces affines est affine si et seulement si pour tout système $\{(A_i, \lambda_i)\}_{i=1,\dots,k}$ de barycentre G et de poids total non nul, le point $f(G)$ est barycentre du système $\{\big(f(A_i), \lambda_i\big)\}$.

Démonstration. En deux parties.

(i) **Si f est affine** Par définition d'un barycentre,

$$\sum_i \lambda_i \overrightarrow{GA_i} = 0. \tag{8.93}$$

Nous considérons un point arbitraire $O \in \mathcal{E}$ et nous écrivons $A_i = O + x_i$, $G = O + x_g$. Ensuite nous utilisons le lemme 8.14 pour le calcul suivant :

$$\begin{aligned} \sum_i \lambda_i \overrightarrow{f(G)f(A_i)} &= \sum_i \lambda_i u_f(x_i - x_g) && \text{(8.94a)} \\ &= u_f\big(\sum_i \lambda_i (x_i - x_g)\big) && \text{(8.94b)} \\ &= u_f\big(\sum_i \lambda_i \overrightarrow{GA_i}\big) && \text{(8.94c)} \\ &= u_f(0) = 0. && \text{(8.94d)} \end{aligned}$$

Donc $f(G)$ est bien le barycentre du nouveau système.

(ii) **Si f conserve les barycentres** Nous définissons u par $f(O+x) = f(O) + u(x)$. À priori, ce u dépend de O et n'est pas linéaire.

(i) **u est linéaire** Soient $M, N \in \mathcal{E}$ et les éléments $x_m, x_n \in E$ tels que $\overrightarrow{OM} = x_m$ et $\overrightarrow{ON} = x_n$. Nous définissons enfin P par

$$\overrightarrow{OP} = \alpha\overrightarrow{OM} + \beta\overrightarrow{ON}, \tag{8.95}$$

et $P = O + x_p$. En décomposant $\overrightarrow{MO}$ et $\overrightarrow{NO}$ par les relations de Chasles de la proposition 8.5(1) nous avons

$$(\alpha + \beta - 1)\overrightarrow{PO} - \alpha\overrightarrow{PM} - \beta\overrightarrow{PN} = 0 \tag{8.96}$$

et donc P est barycentre du système

$$\{(O, \alpha + \beta - 1), (M, \alpha), (N, \beta)\}. \tag{8.97}$$

Le point $f(P)$ sera barycentre du système

$$\Big\{\big(f(O), \alpha + \beta - 1\big), \big(f(M), \alpha\big), \big(f(N), \beta\big)\Big\}. \tag{8.98}$$

Cela signifie que

$$(\alpha + \beta - 1)\overrightarrow{f(P)f(O)} - \alpha\overrightarrow{f(P)f(M)} - \beta\overrightarrow{f(P)f(N)} = 0. \tag{8.99}$$

En y substituant $\overrightarrow{f(P)f(O)} = u(-x_p)$, $\overrightarrow{f(P)f(M)} = u(x_m - x_p)$ et $\overrightarrow{f(P)f(N)} = u(x_n - x_p)$ ainsi que $x_p = \alpha x_m + \beta x_b$ nous trouvons

$$u(\alpha x_m + \beta x_n) = \alpha u(x_m) + \beta u(x_n). \tag{8.100}$$

Donc u est linéaire.

(ii) **u ne dépend pas du point O** Il n'est pas besoin de démontrer cela parce que la définition 8.12 ne le demande pas. Note : c'est le lemme 8.13 qui dit que c'est par ailleurs vrai.

□

8.8 Repères, coordonnées cartésiennes et barycentriques

Définition 8.44.
*On dit que les points $A_0, \dots, A_r \in \mathcal{E}$ sont **affinement indépendants** si le sous-espace affine engendré est de dimension r.*

Proposition 8.45 ([248]).
Pour $r+1$ points $A_0, \dots, A_r$ dans $\mathcal{E}$, les propriétés suivantes sont équivalentes.

(1) Les A_i sont affinement indépendants.

(2) Pour tout $i = 0, \dots, r$, le point A_i n'est pas dans $\mathrm{Aff}\{A_0, \dots, A_{i-1}, A_{i+1}, \dots, A_r\}$.

(3) Les points $A_0, \dots, A_{r-1}$ sont affinement indépendants et $A_r \notin \mathrm{Aff}\{A_0, \dots, A_{r-1}\}$.

(4) Il existe i tel que les vecteurs $\overrightarrow{A_kA_i}$ $(k \neq i)$ sont linéairement indépendants.

(5) Pour tout $i \in \{1, \dots, r\}$, les vecteurs $\overrightarrow{A_kA_i}$ $(k \neq i)$ sont linéairement indépendants.

Notons à propos de la condition (3) que l'existence d'un i pour lequel A_i n'est pas dans $\mathrm{Aff}\{A_0, \dots, A_{i-1}, A_{i+1}, \dots, A_r\}$ n'implique pas l'indépendance des $r+1$ points. En effet dans $\mathbb{R}^2$ nous considérons les 4 points $A_0 = (0,0)$, $A_1 = (1,0)$, $A_2 = (2,0)$ et $A_3 = (0,1)$. Évidemment le point A_3 n'est pas dans l'espace engendré par les trois autres ; il n'empêche que ces points ne sont pas affinement indépendants parce que la direction est de dimension 2 au lieu de 3.

Définition 8.46.
Soit $\mathcal{E}$ un espace affine de dimension n et $\mathcal{F}$ un sous-espace affine de dimension k. Un ***repère affine*** *de $\mathcal{F}$ est la donnée de $k+1$ points affinement indépendants de $\mathcal{F}$.*

Si $\{A_0, \ldots, A_n\}$ est un repère affine, le point A_0 est l'**origine**. C'est un choix complètement arbitraire ; et c'est bien cet arbitraire qui nous amènera à considérer les coordonnées barycentriques au lieu des coordonnées cartésiennes.

Soit $M \in \mathcal{E}$; par définition nous avons

$$M = A_0 + \overrightarrow{A_0M}. \tag{8.101}$$

Mais nous savons que les vecteurs $\overrightarrow{A_0A_i}$ forment une base de E, nous avons donc des nombres λ_i tels que

$$\overrightarrow{A_0M} = \sum_{i=1}^{n} \lambda_i \overrightarrow{A_0A_i}. \tag{8.102}$$

Les nombres λ_i ainsi construits sont les **coordonnées cartésiennes** du point M dans le repère $\{A_0, \ldots, A_n\}$ d'origine A_0.

À partir de ces coordonnées, le point $M \in \mathcal{E}$ se retrouve par la formule

$$M = A_0 + \sum_{i=1}^{n} \lambda_i \overrightarrow{A_0A_i}. \tag{8.103}$$

Proposition 8.47 ([1])**.**
La paire $\big(O, \{e_1, \ldots, e_n\}\big)$ est un repère cartésien de $\mathcal{E}$ si et seulement si $\{O, O+e_1, \ldots, O+e_n\}$ est un repère affine.

Démonstration. En deux parties.

(i) **Sens direct** Vue la proposition 8.45, il suffit de prouver que les vecteurs $\overrightarrow{O(O+e_i)}$ sont linéairement indépendants. Mais $\overrightarrow{O(O+e_i)} = e_i$, donc oui, ils sont linéairement indépendants.

(ii) **Sens inverse** Il s'agit d'utiliser la même proposition 8.45 qui est encore applicable parce que c'est une équivalence.

□

8.48.
Soient (A, e_i) et (A', e'_i) deux repères cartésiens pour l'espace affine $\mathcal{E}$. Soit (s_{ij}) la matrice de changement de base entre $\{e_i\}$ et $\{e'_i\}$ dans E. Nous voudrions trouver les x_i en termes des x'_i.

Pour cela nous considérons un point M dans $\mathcal{E}$ et nous l'écrivons dans les deux bases. Cela fournit l'égalité

$$A + \sum_i x_i e_i = A' + \sum_i x'_i e'_i. \tag{8.104}$$

Nous considérons les coordonnées (a_i) de A' dans le repère (A, e_i), c'est-à-dire

$$A' = A + \sum_i a_i e_i. \tag{8.105}$$

En substituant $e'_i = \sum_k s_{jk} e_k$ et (8.105) dans (8.104) nous trouvons

$$\sum_k x_k e_k = \sum_k a_k e_k + \sum_{jk} s_{jk} x'_j e_k, \tag{8.106}$$

et par conséquent

$$x_k = a_k + \sum_j s_{jk} x'_j. \tag{8.107}$$

Les coordonnées barycentriques sont données par la proposition suivante.

Proposition 8.49 ([248]).
Soient $A_0, \dots, A_r$ des points affinement indépendants dans $\mathcal{E}$ et $\mathcal{F} = \text{Aff}\{A_0, \dots, A_r\}$. Tout point $M \in \mathcal{F}$ s'écrit de façon unique comme barycentre[10] *des A_i affectés de poids λ_i tels que $\sum_{i=0}^{r} \lambda_i = 1$.*

Démonstration. Nous avons vu plus haut (définition 8.46) que l'affine indépendance des points A_i assurait que $(A_0, \dots, A_r)$ était un repère de $\mathcal{F}$.

En ce qui concerne l'existence de l'écriture de M comme barycentre, nous savons que les sous-espace affines sont exactement les ensembles de barycentres (proposition 8.35), c'est-à-dire que si on a des points dans un sous-espace affine, alors les barycentres de ces points est encore dans le sous-espace affine.

L'unicité est comme suit. Si M est barycentre des A_i avec poids λ_i, nous écrivons la caractérisation (4) du théorème 8.32 avec $B = A_0$:

$$\overrightarrow{A_0M} = \sum_{i=1}^{r} \lambda_i \overrightarrow{A_0A_i} \tag{8.108}$$

où la somme à droite s'étend à priori de 0 à r, mais comme $\overrightarrow{A_0A_0} = 0$, nous l'avons limitée à 1. Si M s'écrit comme barycentre de deux façons différentes, nous aurions

$$\overrightarrow{A_0M} = \sum_{i=1}^{r} \lambda_i \overrightarrow{A_0A_i} = \sum_{i=1}^{r} \mu_i \overrightarrow{A_0A_i} \tag{8.109}$$

avec $\sum_i \lambda_i = \sum_i \mu_i = 1$. Étant donné que les points $A_0, \dots, A_r$ forment un repère, les vecteurs $\overrightarrow{A_0A_i}$ sont linéairement indépendants (point (5) de la proposition 8.45) et donc $\lambda_i = \mu_i$ pour $i = 1, \dots, r$. La condition de somme des poids égale à 1 impose alors immédiatement $\lambda_0 = \mu_0$. □

Définition 8.50.
Soit un espace affine $\mathcal{E}$ de dimension n. Soient des points affinement indépendants $A_1, \dots, A_n$. Pour $M \in \mathcal{E}$, la proposition 8.49 indique qu'il existe un unique choix de λ_i tel que

$$\begin{cases} \sum_i \lambda_i = 1 & \text{(8.110a)} \\ \sum_i \lambda_i \overrightarrow{MA_i} = 0. & \text{(8.110b)} \end{cases}$$

Ces λ_i sont les ***coordonnées barycentriques*** *de M dans le repère $\{A_i\}_{i=1,\dots,n}$.*

8.51.
Soit $\mathbb{R}^2$ et les points non alignés A, B, C. Les coordonnées barycentriques (α, β, γ) dans ce système correspondent à l'unique $X \in \mathbb{R}^2$ tel que

$$\alpha\overrightarrow{XA} + \beta\overrightarrow{XB} + \gamma\overrightarrow{XC} = 0. \tag{8.111}$$

Exemple 8.52.
Soient les points $A = (3, 1)$, $B = (-1, 2)$ et $C = (0, -1)$ dans $\mathbb{R}^2$. Nous allons montrer qu'il forment un repère affine de $\mathbb{R}^2$. L'espace engendré par ces trois points est l'espace des

$$A + \alpha\overrightarrow{AB} + \beta\overrightarrow{AC}, \tag{8.112}$$

et la direction correspondante est l'espace vectoriel donné par $\alpha\overrightarrow{AB} + \beta\overrightarrow{AC}$ qui est de dimension deux. Donc l'espace affine engendré par A, B et C est de dimension 2. △

Exemple 8.53.
Dans le repère (A, B, C), quel est le point de coordonnées barycentriques $(\frac{1}{6}, \frac{1}{3}, \frac{1}{2})$? D'abord nous vérifions que

$$\frac{1}{6} + \frac{1}{3} + \frac{1}{2} = 1. \tag{8.113}$$

10. Définition 8.30.

Ensuite nous cherchons $X \in \mathbb{R}^2$ tel que

$$\frac{1}{6}\overrightarrow{AX} + \frac{1}{3}\overrightarrow{BX} + \frac{1}{2}\overrightarrow{CX} = 0, \tag{8.114}$$

c'est-à-dire

$$\frac{1}{6}\begin{pmatrix} x-3 \\ y-1 \end{pmatrix} + \frac{1}{3}\begin{pmatrix} x+1 \\ y-2 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} x \\ y+1 \end{pmatrix} = 0. \tag{8.115}$$

Nous trouvons immédiatement $x = 1/6$ et $y = 1/3$. Le point cherché est donc le point $\begin{pmatrix} 1/6 \\ 1/3 \end{pmatrix}$. △

Lemme 8.54 ([1]).
Une application affine $f : \mathcal{E} \to \mathcal{E}$ qui préserve les points d'une base affine de $\mathcal{E}$ est l'identité.

Démonstration. Une base affine de $\mathcal{E}$ consiste en $n+1$ points $\{A_0, \dots, A_n\}$ affinement indépendants. Nous utilisons la proposition 8.47 pour dire que $\big(A_0, \{\overrightarrow{A_0A_i}\}_{i=1,\dots,n}\big)$ est un repère cartésien.

En utilisant la formule du lemme 8.13,

$$f(A_i) = f(A_0 + \overrightarrow{A_0A_i}) = f(A_0) + u(\overrightarrow{A_0A_i}). \tag{8.116}$$

Donc $A_i = A_0 + u(\overrightarrow{A_0A_i})$, ce qui signifie que

$$u(\overrightarrow{A_0A_i}) = \overrightarrow{A_0A_i} \tag{8.117}$$

Par ailleurs, tout point M[11] de $\mathcal{E}$ peut être écrit sous la forme

$$M = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i}. \tag{8.118}$$

En appliquant f, et en utilisant (8.117),

$$f(M) = f(A_0) + \sum_i \lambda_i u(\overrightarrow{A_0A_i}) = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i} = M. \tag{8.119}$$

Donc tout point de $\mathcal{E}$ est fixé par f, ce qui signifie que f est l'identité. □

8.8.1 Équation de droite

Proposition-Définition 8.55.
Soit $\mathcal{E}$ un espace affine de dimension trois muni d'un repère barycentrique[12] *(A_1, A_2, A_3). Nous notons $D(a, b, c)$ l'ensemble des éléments de $\mathcal{E}$ dont les coordonnées barycentriques (normalisées) (x, y, z) vérifient $ax + by + cz = 0$, c'est-à-dire l'ensemble des $M \in \mathcal{E}$ tels que*

$$\begin{cases} x + y + z = 1 & \text{(8.120a)} \\ x\overrightarrow{MA_1} + y\overrightarrow{MA_2} + \overrightarrow{MA_3} = 0. & \text{(8.120b)} \end{cases}$$

Alors L'ensemble $D(a, b, c)$ est un sous-espace de dimension 1 de $\mathcal{E}$.

*Nous nommons **droite affine** une telle partie de $\mathcal{E}$.*

Idée de preuve : ne pas oublier la condition $x + y + z = 1$ parce que la somme des coordonnées barycentriques doit valoir 1.

Exemple 8.56.
La droite $D(1, 1, 1)$ n'existe pas parce que ce serait $x + y + z = 0$, qui est incompatible avec $x + y + z = 1$. △

11. Même les points qui ne s'appellent pas « M » en fait.
12. Définition 8.50.

Les droites $D(a,b,c)$ et $D(a',b',c')$ s'intersectent selon les solutions du système

$$\begin{cases} x+y+z=1 & (8.121a)\\ ax+by+cz=0 & (8.121b)\\ a'x+b'y+c'z=0 & (8.121c)\end{cases}$$

Donc deux droites affines ont un unique point d'intersection si et seulement si

$$d=\begin{vmatrix}1 & 1 & 1\\ a & b & c\\ a' & b' & c'\end{vmatrix}\neq 0. \tag{8.122}$$

Elles seront parallèles ou confondues si et seulement si $d=0$.

8.8.2 Associativité, coordonnées barycentriques dans un triangle

Lemme 8.57 ([252])**.**
Soient trois points non alignés A, B, C ainsi que des nombres α, β, γ tels que $\alpha+\beta\neq 0$ et $\alpha+\beta+\gamma\neq 0$.

Soit H le barycentre du système $\{(A,\alpha),(B,\beta)\}$ et G le barycentre de $\{(A,\alpha),(B,\beta),(C,\gamma)\}$.

Alors G est barycentre de $\{(H,\alpha+\beta),(C,\gamma)\}$.

Démonstration. Vues les définitions de H et G nous avons

$$\alpha\overrightarrow{HA}+\beta\overrightarrow{HB}=0 \tag{8.123a}$$
$$\alpha\overrightarrow{GA}+\beta\overrightarrow{GB}+\gamma\overrightarrow{GC}=0. \tag{8.123b}$$

En utilisant les relations de Chasles nous introduisons H dans la seconde relation :

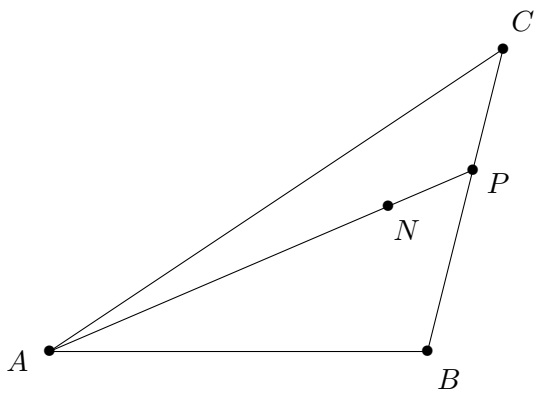
$$\alpha(\overrightarrow{GH}+\overrightarrow{HA})+\beta(\overrightarrow{GH}+\overrightarrow{HB})+\gamma\overrightarrow{GC}=0 \tag{8.124a}$$
$$(\alpha+\beta)\overrightarrow{GH}+\underbrace{\alpha\overrightarrow{HA}+\beta\overrightarrow{HB}}_{=0}+\gamma\overrightarrow{GC}=0 \tag{8.124b}$$
$$(\alpha+\beta)\overrightarrow{GH}+\gamma\overrightarrow{GC}=0. \tag{8.124c}$$

□

Les coordonnées barycentriques dans un triangle (et plus généralement en fait) permettent de faire des projections.

Proposition 8.58.
Soient trois points non alignés A, B, C ainsi qu'un point N de coordonnées barycentriques (α,β,γ) dans le système (A,B,C). Si P est l'intersection $(AN)\cap(BC)$ alors les coordonnées de P sont $(0,\beta,\gamma)$.

Démonstration. Un dessin de la situation :



Dire que les coordonnées de N sont (α,β,γ) signifie que

$$\alpha\overrightarrow{NA}+\beta\overrightarrow{NB}+\gamma\overrightarrow{NC}=0. \tag{8.125}$$

Nous voudrions montrer que le point P est bien le point de coordonnées $(0,\beta,\gamma)$. Soit donc le point P tel que

$$\beta\overrightarrow{PB}+\gamma\overrightarrow{PC}=0 \tag{8.126}$$

et montrons que ce point est l'intersection $(BC)\cap(NA)$.

D'abord la relation (8.126) nous dit immédiatement que P est sur la droite (BC). Ensuite, en utilisant les relations de Chasles pour introduire N :

$$\beta(\overrightarrow{PN}+\overrightarrow{NB})+\gamma(\overrightarrow{PN}+\overrightarrow{NC})=0. \tag{8.127}$$

Nous remplaçons $\beta\overrightarrow{NB}+\gamma\overrightarrow{NC}$ par $-\alpha\overrightarrow{NA}$ pour obtenir :

$$(\beta+\gamma)\overrightarrow{PN}-\alpha\overrightarrow{NA}=0. \tag{8.128}$$

Cela montre que les vecteurs $\overrightarrow{PN}$ et $\overrightarrow{NA}$ sont colinéaires, et donc que P, N et A sont alignés. □

8.9 Applications affines sur $\mathbb{R}^n$

Soit $v\in\mathbb{R}^n$; nous notons $\tau_v\colon\mathbb{R}^n\to\mathbb{R}^n$ la translation donnée par $\tau_v(x)=x+v$. Le groupe de toutes les translations de $\mathbb{R}^n$ est noté $T(n)$ et est isomorphe au groupe abélien $(\mathbb{R}^n,+)$.

Nous avons déjà discuté de la structure d'un espace vectoriel (en particulier $\mathbb{R}^n$) comme espace affine en 8.6.

Lemme 8.59.
Décomposition d'une application affine.

(1) *Une application $f\colon E\to E$ est affine si et seulement si il existe $v\in E$ et une application linéaire α sur E telle que $f=\tau_v\circ\alpha$.*
(2) *Dans ce cas, le choix de (v,α) est unique.*
(3) *Si f est bijective, alors α est bijective.*

Démonstration. Nous supposons d'abord que f est affine. Alors il existe une application linéaire u_f sur E telle que

$$f(M+x)=f(M)+u_f(x)=(\tau_{f(M)}\circ u_f)(x) \tag{8.129}$$

pour tout x et M. De plus l'application u_f ne dépend ni de M ni de x (c'est la proposition 8.16(1)). En posant $M=0$ nous avons :

$$f(x)=(\tau_{f(0)}\circ u_f)(x). \tag{8.130}$$

Dans l'autre sens nous supposons avoir $v\in E$ et α linéaire sur E telles que

$$f(M)=(\tau_v\circ\alpha)(M). \tag{8.131}$$

Notons qu'il y a un abus de notation entre α qui est linéaire sur l'espace *vectoriel* E et l'application α qui est une application sur l'espace *affine* E. Cet abus est légitime parce que les deux espaces sont identiques en tant qu'ensembles. Ce qui est vraiment abuser par contre, c'est de se poser ce genre de questions.

Nous avons :

$$\begin{aligned}f(M+x)=\tau_v\big(\alpha(M+x)\big)&=\alpha(M+x)+v=\alpha(M)+v+\alpha(x)\\&=(\tau_v\circ\alpha)(M)+\alpha(x)=f(M)+\alpha(x).\end{aligned} \tag{8.132}$$

Donc la fonction f vérifie la définition 8.12. La partie (1) est prouvée.

Pour prouver l'unicité de la partie (2), nous supposons que $\tau_v\circ\alpha=\tau_w\circ\alpha$. En appliquant cela à 0 nous trouvons $v=w$. Nous avons donc $\tau_v\circ\alpha=\tau_v\circ\beta$. Comme τ_v est inversible, nous en déduisons $\alpha=\beta$.

Enfin le point (3) est relativement évident du fait que τ_v, elle, est surement bijective. □

Corolaire 8.60.
Une application affine qui conserve l'origine est linéaire.

Démonstration. Conserver l'origine demande de poser $v = 0$ dans l'expression du lemme 8.59. □

Proposition 8.61.
Soit une application affine $f : \mathbb{R}^n \to \mathbb{R}^n$. L'ensemble des points fixes

$$\mathrm{Fix}(f) = \{x \in \mathbb{R}^n \text{ tel que } f(x) = x\} \tag{8.133}$$

est soit vide soit un sous-espace affine de $\mathbb{R}^n$.

Démonstration. Soit $f = \tau_v \circ \alpha$; nous avons $x \in \mathrm{Fix}(f)$ si et seulement si

$$x = \tau_v\big(\alpha(x)\big) = \alpha(x) + v, \tag{8.134}$$

autrement dit, en considérant l'application linéaire $\beta = \mathrm{Id} - \alpha$, si et seulement si $\beta(x) = v$. Nous écrivons $\mathrm{Fix}(f) = \beta^{-1}(v)$. Supposons que cet ensemble soit non vide et considérons $x_0 \in \beta^{-1}(v)$. Nous avons

$$\begin{aligned}
\beta^{-1}(v) &= \{x \in \mathbb{R}^n \text{ tel que } \beta(x) = \beta(x_0)\} && \text{(8.135a)}\\
&= \{x \text{ tel que } \beta(x - x_0) = 0\} && \text{(8.135b)}\\
&= \{x \text{ tel que } x - x_0 \in \ker(\beta)\} && \text{(8.135c)}\\
&= \ker(\beta) + x_0 && \text{(8.135d)}\\
&= \tau_{x_0}\big(\ker(\beta)\big). && \text{(8.135e)}
\end{aligned}$$

Mais comme $\ker(\beta)$ est un sous-espace vectoriel, $\beta^{-1}(v)$ est le translaté d'un sous-espace vectoriel, c'est-à-dire un sous-espace affine. □

8.9.1 Structure de groupe pour les applications affines

Proposition-Définition 8.62 ([1])**.**
L'ensemble des applications affines bijectives de $\mathbb{R}^n$ forment un groupe pour la composition. Les lois de groupe sont données par les formules suivantes :

(1) Le neutre est l'identité.

(2) Le produit est donné par

$$(\tau_v \circ \alpha)(\tau_w \circ \beta) = \tau_{\alpha(w)+v} \circ \alpha\beta. \tag{8.136}$$

(3) L'inverse est donné par

$$(\tau_v \circ \alpha)^{-1} = \tau_{-\alpha^{-1}(v)} \circ \alpha^{-1}. \tag{8.137}$$

Ce groupe est noté $\mathrm{Aff}(\mathbb{R}^n)$.

Démonstration. Pour l'identité, oui, composer par l'identité est neutre.

Le fait que la formule (8.136) soit vraie est un simple calcul :

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta)(x) = (\alpha\beta)(x) + \alpha(w) + v = \big(\tau_{\alpha(w)+v} \circ \alpha\beta\big)x. \tag{8.138}$$

Le fait que la formule (8.136) donne bien un produit pour tous les éléments de $\mathrm{Aff}(\mathbb{R}^n)$ est le lemme 8.59.

En ce qui concerne l'inverse, c'est un calcul :

$$\begin{aligned}
(\tau_{-\alpha^{-1}(v)}\alpha^{-1})(\tau_v\alpha)(x) &= (\tau_{-\alpha^{-1}(v)}\alpha^{-1})\big(\alpha(x) + v\big) && \text{(8.139a)}\\
&= \tau_{-\alpha^{-1}(v)}\big(x + \alpha^{-1}(v)\big) && \text{(8.139b)}\\
&= x. && \text{(8.139c)}
\end{aligned}$$

□

Si $f\colon \mathbb{R}^n \to \mathbb{R}^n$ est une application affine, la proposition 8.59 affirme qu'il existe une application linéaire u telle que

$$f(x+y) = f(x) + u(y). \tag{8.140}$$

En écrivant cela pour $x = 0$,

$$f(y) = f(0) + u(y), \tag{8.141}$$

ou encore $f = \tau_{f(0)} \circ u$.

Proposition 8.63.
L'ensemble $\mathrm{Aff}(\mathbb{R}^n)$ *est isomorphe au produit semi-direct*[13]

$$\mathrm{Aff}(\mathbb{R}^n) \simeq T(n) \times_{\boldsymbol{Ad}} \mathrm{GL}(n,\mathbb{R}) \tag{8.142}$$

où $\boldsymbol{Ad}$ *est l'action adjointe, c'est-à-dire*

$$\begin{aligned} \boldsymbol{Ad}\colon \mathrm{GL}(n,\mathbb{R}) &\to \mathrm{Aut}\big(T(n)\big) \\ \alpha &\mapsto \big(\tau_v \mapsto \alpha \circ \tau_v \circ \alpha^{-1}\big). \end{aligned} \tag{8.143}$$

Démonstration. En plusieurs points.

(i) **Égalité d'ensembles** Il faut que $\mathrm{Aff}(\mathbb{R}^n)$ soit en bijection avec $T(n) \times \mathrm{GL}(n,\mathbb{R})$. En effet si $f \in \mathrm{Aff}(\mathbb{R}^n)$, la décomposition $f = \tau_v \circ \alpha$ est unique. D'abord en appliquant à 0, $f(0) = \tau_v\big(\alpha(v)\big) = v$. Donc v est fixé par la valeur de $f(0)$. Ensuite $\alpha = f \circ \tau_v^{-1}$, donc α fixé.

(ii) **L'action adjointe fonctionne** Il faut vérifier que $\alpha \circ \tau_v \circ \alpha^{-1}$ est bien dans $T(n)$. Pour cela, en agissant sur $x \in \mathbb{R}^n$ nous trouvons

$$\alpha\tau_v\alpha^{-1}(x) = \alpha\big(\alpha^{-1}(x) + v\big) = x + \alpha(v) = \tau_{\alpha(v)}(x). \tag{8.144}$$

Le fait que $\mathbf{Ad}(\alpha)$ soit un automorphisme est toujours correct.

(iii) **Morphisme** Nous montrons que

$$\begin{aligned} \psi\colon T(n) \times \mathrm{GL}(n,\mathbb{R}) &\to \mathrm{Aff}(\mathbb{R}^n) \\ (\tau_v, \alpha) &\mapsto \tau_v \circ \alpha \end{aligned} \tag{8.145}$$

est un isomorphisme de groupes. D'abord la loi de groupe sur $\mathrm{Aff}(\mathbb{R}^n)$ est donnée par

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta) = \tau_{v+\alpha(w)} \circ (\alpha \circ \beta). \tag{8.146}$$

Ensuite la loi de groupe du produit semi-direct est donnée par

$$(\tau_v, \alpha) \cdot (\tau_w, \beta) = \big(\tau_v\, \mathbf{Ad}(\alpha)\tau_w, \alpha\beta\big) = \big(\tau_v\tau_{\alpha(w)}, \alpha\beta\big) = \big(\tau_{\alpha(w)+v}, \alpha\beta\big). \tag{8.147}$$

Nous avons donc bien

$$\psi\big((\tau_v,\beta)\cdot(\tau_w,\beta)\big) = \psi(\tau_v,\beta) \circ \psi(\tau_w,\beta). \tag{8.148}$$

□

8.10 Isométries

Définition 8.64 (Isométrie d'espace affine)**.**
Si $\mathcal{E}$ *est un espace affine muni d'une distance* d*, une isométrie de* $\mathcal{E}$ *est une application* $f\colon \mathcal{E} \to \mathcal{E}$ *préservant* d*, c'est-à-dire telle que*

$$d(x,y) = d\big(f(x), f(y)\big). \tag{8.149}$$

13. Définition 2.47.

Notons que toutes les applications affines ne sont pas des isométries : par exemple les homothéties.

Proposition 8.65.
Si $\mathcal{E}$ est modelé sur un espace euclidien $(E, \|.\|)$ alors la formule

$$d(A,B) = \|\overrightarrow{AB}\| \tag{8.150}$$

définit une distance[14] *sur $\mathcal{E}$.*

Démonstration. Étant donné la proposition 8.3, la formule a un sens parce qu'à A et B donnés dans $\mathcal{E}$, il est associé un unique vecteur $\overrightarrow{AB} \in E$.

Pour vérifier que d est une distance, nous vérifions les points de la définition 7.106 et nous utilisons les propriétés correspondantes dans la définition 7.146 d'une norme.

(1) $d(A,B) = \|\overrightarrow{AB}\| \geqslant 0$.

(2) Si $d(A,B) = 0$, alors $\|\overrightarrow{AB}\| = 0$, ce qui implique que $\overrightarrow{AB} = 0$. Nous avons donc

$$\begin{aligned} B &= A + \overrightarrow{AB} && \text{proposition 8.3} && (8.151a)\\ &= A + 0 && && (8.151b)\\ &= A && \text{lemme 8.4.} && (8.151c) \end{aligned}$$

(3) En utilisant la proposition 8.5(3),

$$d(A,B) = \|\overrightarrow{AB}\| = \|-\overrightarrow{BA}\| = \|\overrightarrow{BA}\| = d(B,A) \tag{8.152}$$

(4) En utilisant les relation de Chasles 8.5(1) ainsi que l'inégalité triangulaire 7.146(4)

$$d(A,B) = \|\overrightarrow{AB}\| = \|\overrightarrow{AC} + \overrightarrow{CB}\| \leqslant \|\overrightarrow{AC}\| + \|\overrightarrow{CB}\| = d(A,C) + d(C,B). \tag{8.153}$$

□

Nous parlons d'isométries affines ou linéaires dans le thème 77.

14. Définition 7.106.

Chapitre 9

Espaces vectoriels (encore)

9.1 Déterminants

9.1.1 Formes multilinéaires alternées

Définition 9.1.
Soit E, un $\mathbb{K}$-espace vectoriel. Une forme multilinéaire ***alternée*** *sur E est une application k-linéaire $f\colon E^k \to \mathbb{K}$ telle que $f(v_1,\dots,v_k)=0$ dès que $v_i=v_j$ pour certains $i\neq j$.*

Définition 9.2.
Soit E, un $\mathbb{K}$-espace vectoriel. Une forme multilinéaire $f\colon E^k\to\mathbb{K}$ est ***antisymétrique*** *telle que*

$$f(x_1,\dots,x_i,\dots,x_j,\dots,x_k)=-f(x_1,\dots,x_j,\dots,x_i,\dots,x_k) \tag{9.1}$$

pour tout couple (i,j).

Lemme 9.3 ([253])**.**
Une forme k-linéaire alternée est antisymétrique[1]*. Si $\mathbb{K}$ est de caractéristique différente de 2, alors une forme antisymétrique est alternée*[2]*.*

Démonstration. Soit f une forme alternée ; quitte à fixer toutes les autres variables, nous pouvons travailler avec une 2-forme et simplement montrer que $f(x,y)=-f(y,x)$. Pour ce faire nous écrivons

$$0=f(x+y,x+y)=f(x,x)+f(x,y)+f(y,x)+f(y,y)=f(x,y)+f(y,x). \tag{9.2}$$

Pour la réciproque, si f est antisymétrique, alors $f(x,x)=-f(x,x)$. Cela montre que $f(x,x)=0$ lorsque $\mathbb{K}$ est de caractéristique différente de deux. □

Proposition 9.4 ([254])**.**
Soit E, un $\mathbb{K}$-espace vectoriel de dimension n, où la caractéristique de $\mathbb{K}$ n'est pas deux. L'espace des n-formes multilinéaires alternées sur E est de $\mathbb{K}$-dimension 1.

Démonstration. Soient $\{e_i\}$, une base de E, une n-forme linéaire alternée $f\colon E\to\mathbb{K}$ ainsi que des vecteurs $(v_1,\dots,v_n)$ de E. Nous pouvons les écrire dans la base

$$v_j=\sum_{i=1}^{n}\alpha_{ij}e_i \tag{9.3}$$

1. Antisymétrique, définition 9.2.
2. Définition 9.1.

et alors exprimer f par

$$f(v_1,\dots,v_n) = f\Big(\sum_{i_1=1}^{n}\alpha_{1i_1}e_{i_1},\dots,\sum_{i_n=1}^{n}\alpha_{ni_n}e_{i_n}\Big) \tag{9.4a}$$

$$= \sum_{i_1,\dots,i_n}\alpha_{1i_1}\dots\alpha_{ni_n}f(e_{i_1},\dots,e_{i_n}). \tag{9.4b}$$

Étant donné que f est alternée, les seuls termes de la somme sont ceux dont les i_k sont tous différents, c'est-à-dire ceux où $\{i_1,\dots,i_n\} = \{1,\dots,n\}$. Il y a donc un terme par élément du groupe des permutations S_n et

$$f(v_1,\dots,v_n) = \sum_{\sigma\in S_n}\alpha_{\sigma(1)1}\dots\alpha_{\sigma(n)n}f(e_{\sigma(1)},\dots,e_{\sigma(n)}). \tag{9.5}$$

En utilisant encore une fois le fait que la forme f soit alternée, $f = f(e_1,\dots,e_n)\Pi$ où

$$\Pi(v_1,\dots,v_n) = \sum_{\sigma\in S_n}\epsilon(\sigma)\alpha_{\sigma(1)1}\dots\alpha_{\sigma(n)n}. \tag{9.6}$$

Pour rappel, la donnée des v_i est dans les nombres α_{ij}.

L'espace des n-formes alternées est donc *au plus* de dimension 1. Pour montrer qu'il est exactement de dimension 1, il faut et suffit de prouver que Π est alternée. Par le lemme 9.3, il suffit de prouver que cette forme est antisymétrique [3].

Soient donc $v_1,\dots,v_n$ tels que $v_i = v_j$. En posant $\tau = (1i)$ et $\tau' = (2j)$ et en sommant sur $\sigma\tau\tau'$ au lieu de σ, nous pouvons supposer que $i = 1$ et $j = 2$. Montrons que $\Pi(v,v,v_3,\dots,v_n) = 0$ en tenant compte que $\alpha_{i1} = \alpha_{i2}$:

$$\Pi(v,v,v_3,\dots,v_n) = \sum_{\sigma\in S_n}\epsilon(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\alpha_{\sigma(3)3}\dots\alpha_{\sigma(n)n} \tag{9.7a}$$

$$= \sum_{\sigma\in S_n}\epsilon(\sigma\tau)\alpha_{\sigma\tau(1)1}\alpha_{\sigma\tau(2)2}\alpha_{\sigma\tau(3)3}\dots\alpha_{\sigma\tau(n)n} \qquad \text{où } \tau = (12) \tag{9.7b}$$

$$= -\sum_{\sigma\in S_n}\epsilon(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\alpha_{\sigma(3)3}\dots\alpha_{\sigma(n)n} \tag{9.7c}$$

$$= -\Pi(v,v,v_3,\dots,v_n). \tag{9.7d}$$

□

9.1.2 Déterminant d'une famille de vecteurs

Nous considérons un corps $\mathbb{K}$ et l'espace vectoriel E de dimension n sur $\mathbb{K}$.

Définition 9.5 (Déterminant d'une famille de vecteurs[10])**.**
*Le **déterminant** de la famille de vecteurs $(v_1,\dots,v_n)$ dans la base $B = \{b_1,\dots,b_n\}$ est l'élément de $\mathbb{K}$*

$$\det_{(b_1,\dots,b_n)}(v_1,\dots,v_n) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n}b^*_{\sigma(i)}(v_i) \tag{9.8}$$

où

- *la somme porte sur le groupe symétrique,*
- *le nombre $\epsilon(\sigma)$ est la signature [4] de la permutation σ,*
- *les éléments $\{b_i^*\}$ sont la base duale [5] de $\{b_i\}$.*

3. C'est ici que joue l'hypothèse sur la caractéristique de $\mathbb{K}$.
4. Définition 1.290.
5. Définition 4.124.

9.6.
La base $\{e_i\}$ est la base canonique de $\mathbb{K}^n$, et l'élément e_k^* est la forme linéaire définie par

$$\begin{aligned} e_k^* \colon \mathbb{K}^n &\to \mathbb{K} \\ \sum_i x_i e_i &\mapsto x_k. \end{aligned} \tag{9.9}$$

Il n'est pas sous-entendu que $\mathbb{K}^n$ ait un produit scalaire. Il n'est donc pas autorisé de dire que $\{e_i\}$ est une base orthonormée et que $e_k^*(x) = \langle e_k, x \rangle$. Ce genre d'égalités sont vraies dans le cas $\mathbb{K} = \mathbb{R}$, mais n'ont pas de sens en général.

Le lemme 11.5 va un peu parler du cas où $\mathbb{K}^n$ est muni d'une base orthonormée.

Lemme 9.7 ([10])**.**
Les propriétés du déterminant. Soit B une base de E.

(1) L'application $\det_B \colon E^n \to \mathbb{K}$ est n-linéaire.

(2) L'application $\det_B \colon E^n \to \mathbb{K}$ est n-linéaire est antisymétrique et alternée[6]*.*

(3) Pour toute base, $\det_B(B) = 1$.

(4) Le déterminant ne change pas si on remplace un vecteur par une combinaison linéaire des autres :

$$\det_B(v_1, \dots, v_n) = \det_B\big(v_1 + \sum_{s=2}^{n} a_s v_s, v_2, \dots, v_n\big). \tag{9.10}$$

(5) Si on permute les vecteurs,

$$\det_B(v_1, \dots, v_n) = \epsilon(\sigma) \det_B(v_{\sigma(1)}, \dots, v_{\sigma(n)}). \tag{9.11}$$

(6) Si B' est une autre base :

$$\det_B = \det_B(B') \det_{B'} \tag{9.12}$$

(7) Nous avons aussi la formule $\det_B(B') \det_{B'}(B) = 1$.

(8) Les vecteurs $\{v_1, \dots, v_n\}$ forment une base si et seulement si $\det_B(v_1, \dots, v_n) \neq 0$.

Démonstration. Point par point.

(i) **(1)** En posant $v_1 = x_1 + \lambda x_2$ nous avons

$$\det_B(x_1 + \lambda x_2, v_2, \dots, v_n) = \sum_\sigma \epsilon(\sigma) \prod_{i=1}^{n} e_{\sigma(i)}^*(v_i) \tag{9.13a}$$

$$= \sum_\sigma \epsilon(\sigma) \Big(e_{\sigma(1)}^*(x_1 + \lambda x_2) \Big) \prod_{i=2}^{n} e_{\sigma(i)}^*(v_i). \tag{9.13b}$$

À partir de là, la linéarité de $e_{\sigma(1)}^*$ montre que $\det_B$ est linéaire en son premier argument. Pour les autres arguments, le même calcul tient.

(ii) **(2)** Nous prouvons à présent que det est alternée. Si votre corps est de caractéristique différente de deux, vous pouvez lire la proposition 9.8.

Supposons $v_k = v_l$, et considérons la permutation $\beta = (k, l)$. Nous savons par la proposition 5.46 que $S_n = A_n \cup A_n\beta$. Cela nous permet de décomposer la somme sur S_n en deux parties :

$$\sum_{\sigma \in S_n} (-1)^\sigma \prod_i \epsilon_{\sigma(i)}^*(v_i) = \sum_{\sigma \in A_n} (-1)^\sigma \prod_i \epsilon_{\sigma(i)}^*(v_i) + \sum_{\sigma \in A_n} (-1)^{\sigma\beta} \prod_i \epsilon_{(\sigma\beta)(i)}^*(v_i). \tag{9.14}$$

6. Alternée, définition 9.1. En caractéristique 2, alternée n'est pas équivalent à symétrique.

D'abord $(-1)^{\sigma}=1$ et $(-1)^{\sigma\beta}=-1$. Ensuite, pour un $\sigma\in A_n$ donné, nous avons

$$\prod_i \epsilon^*_{(\sigma\beta)(i)}(v_i) = \epsilon^*_{(\sigma\beta)(k)}(v_k)\epsilon^*_{(\sigma\beta)(l)}(v_l)\prod_{\substack{i\neq k\\ i\neq l}}\epsilon^*_{(\sigma\beta)(i)}(v_i) \tag{9.15a}$$

$$= \epsilon^*_{\sigma(l)}(v_k)\epsilon^*_{\sigma(k)}(v_l)\prod_{\substack{i\neq k\\ i\neq l}}\epsilon^*_{\sigma(i)}(v_i) \tag{9.15b}$$

$$= \epsilon^*_{\sigma(l)}(v_l)\epsilon^*_{\sigma(k)}(v_k)\prod_{\substack{i\neq k\\ i\neq l}}\epsilon^*_{\sigma(i)}(v_i) \tag{9.15c}$$

$$= \prod_i \epsilon^*_{\sigma(i)}(v_i). \tag{9.15d}$$

Donc les deux termes de la somme (9.14) ne diffèrent que par un signe. Elle est donc nulle, et la forme déterminant est alternée.

La fonction det est antisymétrique parce que alternée, voir le lemme 9.3.

(iii) **(3)** Nous avons

$$\det_B(B) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n}\underbrace{e^*_{\sigma(i)}(e_i)}_{=\delta_{\sigma(i),i}}. \tag{9.16}$$

Si σ n'est pas l'identité, le produit contient forcément un facteur nul. Il ne reste de la somme que $\sigma=\mathrm{Id}$ et le résultat est 1.

(iv) **(4)** Vu que $\det_B$ est linéaire en tous ses arguments,

$$\det_B\left(v_1+\sum_{s=2}^{n}a_sv_s,v_2,\dots,v_n\right)=\det_B(v_1,\dots,v_n)+\sum_{s=2}^{n}a_s\det_B(v_s,v_2,\dots,v_n). \tag{9.17}$$

Chacun des termes de la somme est nul parce qu'il y a répétition de v_s parmi les arguments alors que la forme est alternée.

(v) **(5)** Nous devons calculer $\det_B(v_{\sigma(1)},\dots,v_{\sigma(n)})$, et pour y voir plus clair nous posons $w_i=v_{\sigma(i)}$. Alors :

$$\det_B(v_{\sigma(1)},\dots,v_{\sigma(n)}) = \sum_{\sigma'}\epsilon(\sigma')\prod_{i=1}^{n}e^*_{\sigma'(i)}(w_i) \tag{9.18a}$$

$$= \sum_{\sigma'}\epsilon(\sigma')\prod_{i=1}^{n}e^*_{\sigma'(i)}(v_{\sigma(i)}) \tag{9.18b}$$

$$= \sum_{\sigma'}\epsilon(\sigma')\prod_{i=1}^{n}e^*_{\sigma^{-1}\sigma'(i)}(v_i) \tag{9.18c}$$

$$= \sum_{\sigma'}\epsilon(\sigma\sigma')\prod_{i=1}^{n}e^*_{\sigma'(i)}(v_i) \tag{9.18d}$$

$$= \epsilon(\sigma)\det_B(v_1,\dots,v_n). \tag{9.18e}$$

Justifications : nous avons d'abord modifié l'ordre des éléments du produit et ensuite l'ordre des éléments de la somme. Nous avons ensuite utilisé le fait que $\epsilon\colon S_n\to\{0,1\}$ était un morphisme de groupe (proposition 1.293).

(vi) **(6)** Étant donné que l'espace des formes multilinéaires alternées est de dimension 1, il existe un $\lambda\in\mathbb{K}$ tel que $\det_B=\lambda\det_{B'}$. Appliquons cela à B' :

$$\det_B(B')=\lambda\det_{B'}(B'), \tag{9.19}$$

donc $\lambda=\det_B(B')$.

(vii) (7) Il suffit d'appliquer l'égalité précédente à B en nous souvenant que $\det_B(B) = 1$.

(viii) (8) Si $B' = \{v_1, \dots, v_n\}$ est une base alors $\det_B(B') \neq 0$, sinon il n'est pas possible d'avoir $\det_B(B') \det_{B'}(B) = 1$.

À l'inverse, si B' n'est pas une base, c'est que $\{v_1, \dots, v_n\}$ est liée par la proposition 4.18. Il y a donc moyen de remplacer un des vecteurs par une combinaison linéaire des autres. Le déterminant s'annule alors.

□

Proposition 9.8.
Si la caractéristique du corps de base n'est pas deux, le déterminant est antisymétrique et alterné.

Démonstration. Si la caractéristique du corps de base n'est pas deux, une forme antisymétrique est alternée (lemme 9.3).

Pour prouver que le déterminant est antisymétrique, remarquez que permuter v_k et v_l revient à calculer le nombre $\det_B(v_{\sigma_{kl}(1)}, \dots, v_{\sigma_{kl}(n)})$ au lieu de $\det_B(v_1, \dots, v_n)$. Cela revient à changer la somme $\sum_\sigma$ en $\sum_{\sigma\circ\sigma_{kl}}$. Cela multiplie $\epsilon(\sigma)$ par -1 parce qu'on ajoute une permutation.

Donc le déterminant est antisymétrique. Nous en déduisons qu'il est alterné parce que, en permutant trivialement v_1 et v_1, nous obtenons $\det_B(v_1, v_1) = -\det_B(v_1, v_1)$. Si le corps est de caractéristique différente de deux, cela implique que $\det_B(v_1, v_1) = 0$. □

D'après la proposition 9.4, il existe une unique forme n-linéaire alternée égale à 1 sur B, et c'est $\det_B : E^n \to \mathbb{K}$.

9.1.3 Déterminant d'un endomorphisme

L'interprétation géométrique du déterminant en termes d'aires et de volumes est donnée après le théorème 14.289.

Lemme-Définition 9.9.
Si $f : E \to E$ est un endomorphisme, et si les parties B et B' sont deux bases, alors[7]

$$\det_B\big(f(B)\big) = \det_{B'}\big(f(B')\big). \tag{9.20}$$

Ce nombre, indépendant de la base choisie est nommé le ***déterminant*** *de f et est noté* $\det(f)$.

Démonstration. L'application

$$\begin{aligned} \varphi : E^n &\to \mathbb{K} \\ v_1, \dots, v_n &\mapsto \det_B\big(f(v_1), \dots, f(v_n)\big) \end{aligned} \tag{9.21}$$

est n-linéaire et alternée ; il existe donc $\lambda \in \mathbb{K}$ tel que $\varphi = \lambda \det_B$. En appliquant cela à B :

$$\det_B\big(f(B)\big) = \lambda \det_B(B) = \lambda. \tag{9.22}$$

Nous avons donc déjà prouvé que $\lambda = \det_B\big(f(B)\big)$, c'est-à-dire

$$\det_B\big(f(v)\big) = \det_B\big(f(B)\big) \det_B(v). \tag{9.23}$$

Nous allons maintenant introduire B' là où il y a du v en utilisant les formules (9.12) :

$$\det_B\big(f(v)\big) = \det_B(B') \det_{B'}\big(f(v)\big) \tag{9.24a}$$

$$\det_B(v) = \det_B(B') \det_{B'}(v). \tag{9.24b}$$

Nous obtenons

$$\det_{B'}\big(f(v)\big) = \det_B\big(f(B)\big) \det_{B'}(v). \tag{9.25}$$

7. Définition de $\det_B(B')$, 9.5.

Et on applique cela à $v = B'$:

$$\det_{B'}\big(f(B')\big) = \det_B\big(f(B)\big)\underbrace{\det_{B'}(B')}_{=1}. \tag{9.26}$$

□

Proposition 9.10.
Principales propriétés géométriques du déterminant d'un endomorphisme.

(1) *Si f et g sont des endomorphismes, alors* $\det(f\circ g) = \det(f)\det(g)$.
(2) *L'endomorphisme f est un automorphisme*[8] *si et seulement si* $\det(f)\neq 0$.
(3) *Si* $\det(f)\neq 0$ *alors* $\det(f^{-1}) = \det(f)^{-1}$.
(4) *L'application* $\det\colon \mathrm{GL}(E)\to\mathbb{K}\backslash\{0\}$ *est un morphisme de groupe.*

Démonstration. Point par point.

(1) Nous considérons l'application

$$\begin{aligned}\varphi\colon E^n &\to \mathbb{K}\\ v &\mapsto \det_B\big(f(v)\big).\end{aligned} \tag{9.27}$$

Comme d'habitude nous avons $\varphi(v) = \lambda\det_B(v)$. En appliquant à B et en nous souvenant que $\det_B(B) = 1$ nous avons $\det_B\big(f(B)\big) = \lambda$. Autrement dit :

$$\lambda = \det(f). \tag{9.28}$$

Calculons à présent $\varphi\big(g(B)\big)$: d'une part,

$$\varphi\big(g(B)\big) = \det_B\big((f\circ g)(B)\big) \tag{9.29}$$

et d'autre part,

$$\varphi\big(g(B)\big) = \lambda\det_B\big(g(B)\big) = \lambda\det(g) \tag{9.30}$$

En égalisant et en reprenant la la valeur déjà trouvée de λ,

$$\det\big((f\circ g)(B)\big) = \det(f)\det(g), \tag{9.31}$$

ce qu'il fallait.

(2) Supposons que f soit un automorphisme. Alors si B est une base, $f(B)$ est une base. Par conséquent $\det(f) = \det_B\big(f(B)\big)\neq 0$ parce que $f(B)$ est une base (lemme 9.7(8)).
Réciproquement, supposons que $\det(f)\neq 0$. Alors si B est une base quelconque nous avons $\det_B\big(f(B)\big)\neq 0$, ce qui est uniquement possible lorsque $f(B)$ est une base. L'application f transforme donc toute base en une base et est alors un automorphisme d'espace vectoriel.
(3) Vu que le déterminant de l'identité est 1 et que f est inversible, $1 = \det(f\circ f^{-1}) = \det(f)\det(f^{-1})$.

□

Proposition 9.11.
Soient deux espaces vectoriels E et F de dimension finies n et m sur le corps $\mathbb{K}$ munis de bases $\{e_i\}$ et $\{f_\alpha\}$. À une matrice $A\in\mathbb{M}(m\times n,\mathbb{K})$ nous associons l'application linéaire[9]

$$f_A(x) = \sum_{i\alpha} A_{\alpha i}x_i f_\alpha. \tag{9.32}$$

Alors, en ce qui concerne les déterminants[10]*, nous avons*

8. Endomorphisme inversible, définition 4.35.
9. Dont nous avons déjà beaucoup parlé entre autres dans la proposition 4.72.
10. Définition 9.9 pour les applications linéaires et 4.76 pour les matrices.

(1) $\det(f_A) = \det(A)$

(2) $\det(f_{AB}) = \det(f_A)\det(f_B)$

Démonstration. Nous devons étudier la formule

$$\det(f_A) = \sum_{\sigma\in S_n} \epsilon(\sigma) \prod_{i=1}^{n} e^*_{\sigma(i)}\big(f_A(e_i)\big). \tag{9.33}$$

En premier lieu nous avons

$$f_A(e_i) = \sum_{jk} A_{jk}(e_i)_k e_j = \sum_j A_{ji} e_j. \tag{9.34}$$

Nous avons alors

$$e^*_{\sigma(i)}\big(f_A(e_i)\big) = \sum_j A_{ji} \underbrace{e^*_{\sigma(i)}(e_j)}_{\delta_{j\sigma(i)}} = A_{\sigma(i)i}. \tag{9.35}$$

Au final,

$$\det(f_A) = \sum_\sigma \epsilon(\sigma) \prod_{i=1}^{n} A_{\sigma(i)i} = \det(A^t) = \det(A) \tag{9.36}$$

où la dernière égalité est autorisée par le lemme 4.78.

Cela prouve la formule $\det(f_A) = \det(A)$.

En ce qui concerne la seconde formule, il s'agit de se souvenir de la proposition 4.72 qui donne $f_{AB} = f_A \circ f_B$, et ensuite de la proposition 9.10(1) qui donne $\det(f_A \circ f_B) = \det(f_A)\det(f_B)$. □

9.1.4 Déterminant de Vandermonde

Proposition 9.12 ([111]).
*Le **déterminant de Vandermonde** est le polynôme en n variables donné par*

$$V(T_1,\dots,T_n) = \det\begin{pmatrix} 1 & 1 & \dots & 1 \\ T_1 & T_2 & \dots & T_n \\ \vdots & \ddots & \ddots & \vdots \\ T_1^{n-1} & T_2^{n-1} & \dots & T_n^{n-1} \end{pmatrix} = \prod_{1\leqslant i<j\leqslant n} (T_j - T_i). \tag{9.37}$$

Notez que l'inégalité du milieu est stricte (sinon d'ailleurs l'expression serait nulle).

Démonstration. Nous considérons le polynôme

$$f(X) = V(T_1,\dots,T_{n-1},X) \in \big(\mathbb{K}[T_1,\dots,T_{n-1}]\big)[X]. \tag{9.38}$$

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 [11] 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

$$f = \alpha \prod_{i=1}^{n-1} (X - T_i). \tag{9.39}$$

Nous trouvons α en écrivant $f(0)$. D'une part la formule (9.39) nous donne

$$f(0) = \alpha(-1)^{n-1} T_1 \dots T_{n-1}. \tag{9.40}$$

11. Proposition 3.118.

D'autre part la définition donne

$$f(0) = \det \begin{pmatrix} 1 & \cdots & 1 & 1 \\ T_1 & & T_{n-1} & 0 \\ \vdots & & \vdots & \vdots \\ T_1^{n-1} & \cdots & T_{n-1}^{n-1} & 0 \end{pmatrix} \tag{9.41a}$$

$$= (-1)^{n-1} \det \begin{pmatrix} T_1 & \ldots & T_{n-1} \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \ldots & T_{n-1}^{n-1} \end{pmatrix} \tag{9.41b}$$

$$= (-1)^{n-1} T_1 \ldots T_{n-1} \det \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \cdots & T_{n-1}^{n-1} \end{pmatrix} \tag{9.41c}$$

$$= (-1)^{n-1} T_1 \ldots T_{n-1} V(T_1, \ldots, T_{n-1}) \tag{9.41d}$$

En égalisant avec (9.40), nous trouvons $\alpha = V(T_1, \ldots, T_{n-1})$, et donc

$$f = V(T_1, \ldots, T_{n-1}) \prod_{j \leqslant n-1} (X - T_j) \tag{9.42}$$

Enfin, une récurrence montre que

$$V(T_1, \ldots, T_n) = f(T_n) \tag{9.43a}$$

$$= V(T_1, \ldots, T_{n-1}) \prod_{j \leqslant n-1} (T_n - T_j) \tag{9.43b}$$

$$= \prod_{k \leqslant n} \prod_{j \leqslant k-1} (T_k - T_j) \tag{9.43c}$$

$$= \prod_{1 \leqslant j < k \leqslant n} (T_i - T_j). \tag{9.43d}$$

□

Exemple 9.13.
Le déterminant de Vandermonde (proposition 9.12) est alterné, semi-symétrique et non symétrique. Le fait qu'il soit alterné est le fait qu'il soit un déterminant. Étant donné qu'il est alterné, il est semi-symétrique parce que sur A_n, nous avons $\epsilon = 1$. Étant donné qu'il est alterné, il change de signe sous l'action des éléments impairs de S_n et n'est donc pas symétrique. △

Proposition 9.14.
Un polynôme semi-symétrique $f \in \mathbb{K}[T_1, \ldots, T_n]$ se décompose de façon unique en

$$f = P + VQ \tag{9.44}$$

où P et Q sont deux polynômes symétriques.

Démonstration. Nous commençons par prouver l'unicité en montrant que si $f = P + VQ$ avec P et Q symétrique, alors P et Q sont donnés par des formules explicites en termes de f.

Si σ_1 et σ_2 sont deux permutations impaires de $\{1, \ldots, n\}$, alors $\sigma_1 \cdot f = \sigma_2 \cdot f$ parce que l'élément $\sigma_2^{-1}\sigma_1$ est pair (proposition 1.293), de telle sorte que $\sigma_2^{-1}\sigma_1 \cdot f = f$. Nous posons donc $g = \tau \cdot f$ où τ est une permutation impaire quelconque – par exemple une transposition.

Vu que V est alternée et que τ est une transposition nous avons

$$g = \tau \cdot f = P - VQ. \tag{9.45}$$

Donc $f + g = 2P$ et $f - g = 2VQ$. Cela donne P et Q en termes de f et g, et donc l'unicité.

Attention : cela ne donne pas un moyen de prouver l'existence parce que rien ne prouve pour l'instant que $f-g$ peut effectivement être écrit sous la forme VQ, c'est-à-dire que $f-g$ soit divisible par V. C'est cela que nous allons nous atteler à démontrer maintenant.

Nous commençons par prouver que $f+g$ est symétrique et $f-g$ alterné. Si σ est une transposition,

$$\sigma \cdot (f+g) = \sigma \cdot f + \sigma\tau \cdot f = g + f \tag{9.46}$$

parce que $\sigma\tau$ est pair. De la même façon,

$$\sigma \cdot (f-g) = g - f = \epsilon(\sigma)(f-g). \tag{9.47}$$

Dans les deux cas nous concluons en utilisant le fait que toute permutation est un produit de transpositions (proposition 1.288) et que ϵ est un homomorphisme.

Soient maintenant deux entiers $h<k$ dans $\{1,\dots,n\}$ et l'anneau

$$\big(\mathbb{K}[T_1,\dots,\hat{T}_k,\dots,T_n]\big)[T_k]. \tag{9.48}$$

Cet anneau contient le polynôme T_k-T_h où T_k est la variable et T_h est un coefficient. Nous faisons la division euclidienne de $f-g$ par T_k-T_h parce que nous avons dans l'idée de faire arriver le déterminant de Vandermonde et donc le produit de toutes les différences T_k-T_h :

$$f-g = (T_k-T_h)q + r \tag{9.49}$$

où $\deg_{T_k} r < 1$, c'est-à-dire que r ne dépends pas de T_k. Nous revoyons maintenant l'égalité (9.49) dans $\mathbb{K}[T_1,\dots,T_n]$ et nous y appliquons la transposition τ_{kh}. Nous savons que $\tau_{kh}(f-g) = -(f-g)$ et $\tau_{kh}(T_k-T_h) = -(T_k-T_h)$, et donc

$$-(f-g) = -(T_k-T_h)\tau_{kh} \cdot q + \tau_{kh} \cdot r \tag{9.50}$$

où $\tau_{kh} \cdot r$ ne dépend pas de T_h. Nous appliquons à (9.50) l'application

$$\begin{aligned} t\alpha\colon \mathbb{K}[T_1,\dots,T_n] &\to \mathbb{K}[T_1,\dots,\hat{T}_k,\dots,T_n] \\ \alpha(PT_1,\dots,\hat{T}_k,\dots,T_n) &= P(T_1,\dots,T_h,\dots,T_n). \end{aligned} \tag{9.51}$$

Cette application vérifie $\alpha\big(\tau_{kh} \cdot r\big) = \alpha(r)$ et nous avons

$$-\alpha(f-g) = \alpha(r). \tag{9.52}$$

Puis en appliquant α à la relation $f-g = (T_k-T_h)q + r$, nous trouvons

$$\alpha(f-g) = \alpha(r), \tag{9.53}$$

et par conséquent $\alpha(r) = 0$. Ici nous utilisons l'hypothèse de caractéristique différente de deux. Dire que $\alpha(r) = 0$, c'est dire que r est divisible par T_k-T_h, mais r étant de degré zéro en T_k, nous avons $r=0$. Par conséquent T_k-T_h divise $f-g$ pour tout $h<k$, et nous pouvons définir un polynôme Q par

$$f-g = 2Q\prod_{h<k}\prod_{k\leqslant n}(T_k-T_h) = 2Q(T_1,\dots,T_n)V(T_1,\dots,T_n), \tag{9.54}$$

où nous avons utilisé la formule du déterminant de Vandermonde de la proposition 9.12.

Étant donné que $f+g$ est un polynôme symétrique, nous allons aussi poser $f+g = 2P$ avec P symétrique.

Montrons à présent que Q est un polynôme symétrique. Soit $\sigma \in S_n$; vu que nous savons déjà que $f-g$ est alternée, nous avons

$$\sigma \cdot (f-g) = \epsilon(\sigma)(f-g) = \epsilon(\sigma)2QV, \tag{9.55}$$

Mais en appliquant σ à l'équation (9.54),

$$\sigma \cdot (f-g) = 2(\sigma \cdot V)(T_1,\dots,,T_n)(\sigma \cdot Q)(T_1,\dots,T_n) \tag{9.56a}$$
$$= 2\epsilon(\sigma)V(T_1,\dots,T_n)(\sigma \cdot Q)(T_1,\dots,T_n). \tag{9.56b}$$

Nous égalisons cela avec (9.55) et nous souvenant que l'anneau $\mathbb{K}[T_1,\dots,T_n]$ est intègre par le théorème 3.99. Ensuite nous simplifions par $2\epsilon(\sigma)V$ pour obtenir

$$Q = \sigma \cdot Q, \tag{9.57}$$

c'est-à-dire que Q est symétrique.

Au final nous avons $f+q = 2P$ et $f-g = 2VQ$ avec P et Q symétriques. En faisant la somme,

$$f = P + VQ. \tag{9.58}$$

□

9.1.5 Déterminant de Gram

Si $x_1,\dots,x_r$ sont des vecteurs d'un espace vectoriel, alors le **déterminant de Gram** est le déterminant

$$G(x_1,\dots,x_r) = \det\big(\langle x_i, x_j\rangle\big). \tag{9.59}$$

Notons que la matrice est une matrice symétrique.

Proposition 9.15.
Si F est un sous-espace vectoriel de base $\{x_1,\dots,x_n\}$ et si x est un vecteur, alors le déterminant de Gram est un moyen de calculer la distance entre x et F par

$$d(x,F)^2 = \frac{G(x,x_1,\dots,x_n)}{G(x_1,\dots,x_n)}. \tag{9.60}$$

9.1.6 Déterminant de Cauchy

Soient des nombres a_i et b_i $(i=1,\dots,n)$ tels que $a_i+b_j \neq 0$ pour tout couple (i,j). Le **déterminant de Cauchy** est

$$D_n = \det\left(\frac{1}{a_i+b_j}\right). \tag{9.61}$$

Proposition 9.16 ([255]).
Le déterminant de Cauchy est donné par la formule

$$D_n = \frac{\prod_{i<j}(a_j-a_i)\prod_{i<j}(b_j-b_i)}{\prod_{ij}(a_i+b_j)}. \tag{9.62}$$

9.1.7 Matrice de Sylvester

Définition 9.17 (Matrice de Sylvester, résultant[256]).
Soient P et Q deux polynômes non nuls, de degrés respectifs n et m :

$$P(x) = p_0 + p_1x + \cdots + p_nx^n \tag{9.63a}$$
$$Q(x) = q_0 + q_1x + \cdots + q_mx^m. \tag{9.63b}$$

*La **matrice de Sylvester** associée à P et Q est la matrice carrée $m+n \times m+n$ définie ainsi :*

(1) la première ligne est formée des coefficients de P, suivis de 0 :

$$\begin{pmatrix} p_n & p_{n-1} & \cdots & p_1 & p_0 & 0 & \cdots & 0 \end{pmatrix}; \tag{9.64}$$

(2) la seconde ligne s'obtient à partir de la première par permutation circulaire vers la droite ;

(3) les $(m-2)$ lignes suivantes s'obtiennent en répétant la même opération ;

(4) la ligne $(m+1)$ est formée des coefficients de Q, suivis de 0 :

$$\begin{pmatrix} q_m & q_{m-1} & \cdots & q_1 & q_0 & 0 & \cdots & 0 \end{pmatrix}; \tag{9.65}$$

(5) les $(n-1)$ lignes suivantes sont formées par des permutations circulaires.

Le déterminant de la matrice de Sylvester associée à P et Q est appelé le ***résultant*** *de P et Q et noté* $\operatorname{res}(P,Q)$.

Ainsi dans le cas $n=4$ et $m=3$, la matrice obtenue est

$$S_{p,q} = \begin{pmatrix} p_4 & p_3 & p_2 & p_1 & p_0 & 0 & 0 \\ 0 & p_4 & p_3 & p_2 & p_1 & p_0 & 0 \\ 0 & 0 & p_4 & p_3 & p_2 & p_1 & p_0 \\ q_3 & q_2 & q_1 & q_0 & 0 & 0 & 0 \\ 0 & q_3 & q_2 & q_1 & q_0 & 0 & 0 \\ 0 & 0 & q_3 & q_2 & q_1 & q_0 & 0 \\ 0 & 0 & 0 & q_3 & q_2 & q_1 & q_0 \end{pmatrix}. \tag{9.66}$$

Attention : si P est de degré n et Q de degré m, il y a m lignes pour P et n pour Q dans le déterminant du résultant (et non le contraire).

Lemme 9.18 ([257])**.**
Si P et Q sont deux polynômes de degrés n et m à coefficients dans l'anneau $\mathbb{A}$, alors pour tout $\lambda \in \mathbb{A}$,

$$\operatorname{res}(\lambda P, Q) = \lambda^m \operatorname{res}(P,Q) \tag{9.67a}$$
$$\operatorname{res}(P, \lambda Q) = \lambda^n \operatorname{res}(P,Q). \tag{9.67b}$$

Démonstration. Cela est simplement un comptage du nombre de lignes. Il y a m lignes contenant les coefficients de P ; donc prendre λP revient à multiplier m lignes dans un déterminant et donc le multiplier par λ^m. □

L'équation de Bézout (6.114) peut être traitée avec une matrice de Sylvester. Soient P et Q, deux polynômes donnés et à résoudre l'équation

$$xP + yQ = 0 \tag{9.68}$$

par rapport aux polynômes inconnus x et y dont les degrés sont $\deg(x) < \deg(Q)$ et $\deg(y) < \deg(P)$. Si nous notons $\tilde{x}$ et $\tilde{y}$ la liste des coefficients de x et y (dans l'ordre décroissant de degré), nous pouvons récrire l'équation (9.68) sous la forme

$$S_{PQ}^t \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} = 0. \tag{9.69}$$

Pour s'en convaincre, écrivons pour les polynômes de l'exemple (9.66) :

$$\begin{pmatrix} p_4 & 0 & 0 & q_3 & 0 & 0 & 0 \\ p_3 & p_4 & 0 & q_2 & q_3 & 0 & 0 \\ p_2 & p_3 & p_4 & q_1 & q_2 & q_3 & 0 \\ p_1 & p_2 & p_3 & q_0 & q_1 & q_2 & q_3 \\ p_0 & p_1 & p_2 & 0 & q_0 & q_1 & q_2 \\ 0 & p_0 & p_1 & 0 & 0 & q_0 & q_1 \\ 0 & 0 & p_0 & 0 & 0 & 0 & q_0 \end{pmatrix} \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_2p_4 + y_3q_3 \\ p_3x_2 + p_4x_1 + q_2y_3 + q_3y_2 \\ \\ \\ \vdots \end{pmatrix} \tag{9.70}$$

Nous voyons que sur la ligne numéro k (en partant du bas et en numérotant de à partir de zéro) nous avons les produits p_ix_j et q_iy_j avec $i+j=k$. La colonne de droite représente donc bien les coefficients du polynôme $xP + yQ$.

Proposition 9.19.
Le résultant de deux polynômes est non nul si et seulement si les deux polynômes sont premiers entre eux.

Un polynôme P a une racine double en a si et seulement si P et P' ont a comme racine commune, ce qui revient à dire que P et P' ne sont pas premiers entre eux.

Une application importante de ces résultats sera le théorème de Rothstein-Trager 20.101 sur l'intégration de fractions rationnelles.

Exemple 9.20.
Si nous prenons $P = aX^2 + bX + c$ et $P' = 2aX + b$ alors la taille de la matrice de Sylvester sera $2 + 1 = 3$ et

$$S_{P,P'} = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}. \tag{9.71}$$

Le résultant est alors

$$\operatorname{res}(P, P') = -a(b^2 - 4ac). \tag{9.72}$$

Donc un polynôme du second degré a une racine double si et seulement si $b^2 - 4ac = 0$. Cela est un résultat connu depuis longtemps mais qui fait toujours plaisir à revoir. △

La matrice de Sylvester permet aussi de récrire l'équation de Bézout pour les polynômes ; voir le théorème 6.47 et la discussion qui s'ensuit.

Une proposition importante du résultant est qu'il peut s'exprimer à l'aide des racines des polynômes.

Proposition 9.21.
Si

$$P(X) = a_p \prod_{i=1}^{p} (X - \alpha_i) \tag{9.73a}$$

$$Q(X) = b_q \prod_{j=1}^{q} (X - \beta_i) \tag{9.73b}$$

alors nous avons les expressions suivantes pour le résultant :

$$\operatorname{res}(P, Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\beta_j - \alpha_i) = b_q^p \prod_{j=1}^{q} P(\beta_j) = (-1)^{pq} a_p^q \prod_{i=1}^{p} Q(\alpha_i). \tag{9.74}$$

Démonstration. Si P et Q ne sont pas premiers entre eux, d'une part la proposition 9.19 nous dit que $\operatorname{res}(P, Q) = 0$ et d'autre part, P et Q ont un facteur irréductible en commun, ce qui signifie que nous devons avoir un des $X - \alpha_i$ égal à un des $X - \beta_j$. Autrement dit, nous avons $\alpha_i = \beta_j$ pour un couple (i, j). Par conséquent tous les membres de l'équation (9.74) sont nuls.

Nous supposons donc que P et Q sont premiers entre eux. Nous commençons par supposer que les polynômes P et Q sont unitaires, c'est-à-dire que $a_p = b_q = 1$. Nous considérons alors l'anneau

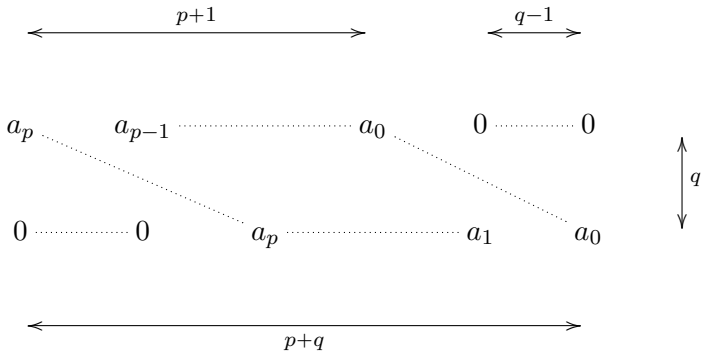
$$\mathbb{A} = \mathbb{Z}[\alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_q]. \tag{9.75}$$

Dans cet anneau, l'élément $\beta_j - \alpha_i$ est irréductible (tout comme $X - Y$ est irréductible dans $\mathbb{Z}[X, Y]$). Le résultant $R = \operatorname{res}(P, Q)$ est un élément de $\mathbb{A}$ parce que tous leurs coefficients peuvent être exprimés à l'aide des α_i et des β_j. Dans $\mathbb{A}$, l'élément $\beta_j - \alpha_i$ divise R. En effet lorsque $\beta_j = \alpha_i$, le déterminant définissant le résultant est nul, ce qui signifie que $\beta_j - \alpha_i$ est un facteur irréductible de R.

Par conséquent il existe un polynôme $T \in \mathbb{A}$ tel que

$$R = T(\alpha_1, \dots, \beta_q) \prod_{i=1}^{p} \prod_{j=1}^{r} (\beta_j - \alpha_i). \tag{9.76}$$

Comptons les degrés. Pour donner une idée de ce calcul de degré, voici comment se présente, au niveau des dimensions, le déterminant :



(9.77)

si les a_i sont les coefficients de P. Mais chacun des a_i est de degré 1 en les α_i, donc le déterminant dans son ensemble est de degré q en les α_i, parce que R contient q lignes telles que (9.77). Le même raisonnement montre que R est de degré p en les β_j. Par ailleurs le polynôme $\prod_{i=1}^{p}\prod_{j=1}^{r}(\beta_j-\alpha_i)$ est de degré p en les β_j et q en les α_i. Nous en déduisons que T doit être un polynôme ne dépendant pas de α_i ou de β_j.

Nous pouvons donc calculer la valeur de T en choisissant un cas particulier. Avec $P(X)=X^p$ et $Q(X)=X^q+1$, il est vite vu que $R(P,Q)=1$ et donc que $T=1$.

Si les polynômes P et Q ne sont pas unitaires, le lemme 9.18 nous permet de conclure.

□

9.1.8 Théorème de Kronecker

Nous considérons K_n l'ensemble des polynômes de $\mathbb{Z}[X]$

(1) unitaires de degré n,

(2) dont les racines dans $\mathbb{C}$ sont de modules plus petits ou égaux à 1,

(3) et qui ne sont pas divisés par X.

Un tel polynôme s'écrit sous la forme

$$P=X^n+\sum_{k=0}^{n-1}a_kX^k. \tag{9.78}$$

Théorème 9.22 (Kronecker[102]).
Les racines des éléments de K_n sont des racines de l'unité.

Démonstration. Vu que $\mathbb{C}$ est algébriquement clos nous pouvons considérer les racines $\alpha_1,\dots,\alpha_n$ de P dans $\mathbb{C}$. Nous les considérons avec leurs multiplicités.

Soit $R=X^n+\sum_{k=0}^{n-1}b_kX^k$ un élément de K_n dont nous notons $\beta_1,\dots,\beta_n$ les racines dans $\mathbb{C}$. Les relations coefficients-racines stipulent que

$$b_k=\sum_{1\leqslant i_1<\dots<i_{n-k}\leqslant n}\prod_{j=1}^{n-k}\beta_{i_j}. \tag{9.79}$$

En prenant le module et en se souvenant que $|\beta_l|\leqslant 1$ pour tout l, nous trouvons que

$$|b_k|\leqslant\binom{n}{n-k}. \tag{9.80}$$

Mais comme $b_k\in\mathbb{Z}$, nous avons

$$b_k\in\Big\{-\binom{n}{n-k},-\binom{n}{n-k}+1,\dots,0,\dots,\binom{n}{n-k}\Big\} \tag{9.81}$$

qui est de cardinal $2\binom{n}{n-k}+1$. Nous avons donc

$$\text{Card}(K_n) \leqslant \prod_{k=0}^{n-1}\left(1+\binom{n}{n-k}\right) < \infty. \tag{9.82}$$

La conclusion jusqu'ici est que K_n est un ensemble fini.

Pour chaque $k \in \mathbb{N}^*$ nous considérons les polynômes

$$P_k = \prod_{i=1}^{n}(X-\alpha_i^k) \tag{9.83a}$$

$$Q_k = X^k - Y \in \mathbb{Z}[X,Y], \tag{9.83b}$$

et puis nous considérons le résultant $R_k = \text{res}_X(P,Q_k) \in \mathbb{Z}[Y]$:

$$R_k = \text{res}_X(P,Q_k) = \begin{pmatrix} 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & & & \\ 0 & \cdots & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 \\ 1 & 0 & \ldots & 0 & -Y & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & -Y & 0 & \ldots & 0 \\ & & \ddots & & & \ddots & \ddots & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y \end{pmatrix} \tag{9.84}$$

Cela est un polynôme en Y dont le terme de plus haut degré est $(-1)^nY^n$. Les petites formules de la proposition 9.21 nous permettent d'exprimer $R_k(Y)$ en termes des racines de P :

$$R_k(Y) = \prod_{i=1}^{n}Q_k(\alpha_i) = \prod_{i=1}^{n}(\alpha_i^k - Y) = (-1)^n\prod_{i=1}^{n}(Y-\alpha_i^k) = (-1)^nP_k(Y). \tag{9.85}$$

Vu que $P \in K_n$ nous savons que les α_i ne sont pas tous nuls ; donc $P_k \in K_n$. Cependant nous avons vu que K_n est un ensemble fini ; donc parmi les P_k, il y a des doublons (et pas un peu) [12]. Nous regardons même l'ensemble des P_{2^n} dans lequel nous pouvons en trouver deux les mêmes. Soit $l > k$ tels que $P_{2^k} = P_{2^l}$. Si α est racine de P_{2^k}, alors il est de la forme $\alpha = \beta^{2^k}$ pour une certaine racines β de P. Par conséquent

$$\alpha^{2^l/2^k} = \alpha^{2^{l-k}} \tag{9.86}$$

est racine de P_{2^l}. Notons que dans cette expression il n'y a pas de problèmes de définition d'exposant fractionnaire dans $\mathbb{C}$ parce que $l > k$. Vu que (9.86) est racine de P_{2^l}, il est aussi racine de P_{2^k}. Donc

$$\left(\alpha^{2^{l-k}}\right)^{2^{l-k}} = \alpha^{2^{2(l-k)}} \tag{9.87}$$

est racine de P_{2^l} et donc de P_{2^k}. Au final nous savons que tous les nombres de la forme $\alpha^{2^{n(l-k)}}$ sont racines de P_{2^k}. Mais comme P_{2^k} a un nombre fini de racines, nous pouvons en trouver deux égales. Si nous avons

$$\alpha^{2^{n(l-k)}} = \alpha^{2^{m(l-k)}} \tag{9.88}$$

pour certains entiers $m > n$, alors

$$\alpha^{2^{n(l-k)}-2^{m(l-k)}} = 1, \tag{9.89}$$

ce qui prouve que α est une racine de l'unité. Nous avons donc prouvé que toutes les racines de P_{2^k} sont des racines de l'unité et donc que les racines de P sont racines de l'unité. □

12. Ici dans [102], il déduit qu'on a un k tel que $P_k = P_1 = P$. Moi je vois pourquoi on a un k et un l tels que $P_k = P_l$, mais pourquoi on peut en trouver un spécialement égal au premier ? Une réponse à cette question permettrait de solidement réduire la lourdeur de la suite de la preuve.

9.2 Orientation

9.2.1 Cas vectoriel

Proposition-Définition 9.23 ([258]).
Soient deux bases $\mathcal{B}$ et $\mathcal{B}'$ d'un espace vectoriel réel E. Nous définissons la relation $\mathcal{B} \sim \mathcal{B}'$ si et seulement si $\det_{\mathcal{B}}(\mathcal{B}') > 0$ [13].

Cela est une relation d'équivalence [14] *sur l'ensemble des bases de E, et les classes sont les* ***orientations*** *de E.*

Démonstration. Tout est dans le lemme 9.7. D'abord quand $\mathcal{B}$ et $\mathcal{B}'$ sont des bases, $\det_{\mathcal{B}}(\mathcal{B}') \neq 0$ ensuite, nous passons en revue les points qu'il faut pour être une relation d'équivalence.

(1) $\mathcal{B} \sim \mathcal{B}$ parce que $\det_{\mathcal{B}}(\mathcal{B}) = 1 > 0$.

(2) Vu que $\det_{\mathcal{B}}(\mathcal{B}') = \frac{1}{\det_{\mathcal{B}'}(\mathcal{B})}$, les deux sont positifs en même temps ou pas du tout.

(3) Si $\mathcal{B} \sim \mathcal{B}'$ et $\mathcal{B}' \sim \mathcal{B}''$, alors en utilisant la formule

$$\det_{\mathcal{B}}(\mathcal{B}'') = \det_{\mathcal{B}}(\mathcal{B}') \det_{\mathcal{B}'}(\mathcal{B}''), \tag{9.90}$$

nous voyons que $\det_{\mathcal{B}}(\mathcal{B}'') > 0$.

□

Lemme 9.24.
Soit un espace vectoriel réel E. L'ensemble des bases de E possède exactement deux orientations [15]

Démonstration. Nous considérons une base $\mathcal{B} = (e_1, \dots, e_n)$ [16] à partir de laquelle nous définissons une autre base : $\mathcal{B}' = (-e_1, e_2, \dots, e_n)$. Nous allons prouver que ces deux bases ne sont pas équivalentes, et que toute base de E est équivalente soit à $\mathcal{B}$ soit à $\mathcal{B}'$.

(i) **Au moins deux classes** Le fait que $\det_{\mathcal{B}}(\mathcal{B}') = -1$ vient du fait que $\det_{\mathcal{B}}(\mathcal{B}) = 1$ et que l'application $\det_{\mathcal{B}}$ est n-linéaire ; en multipliant par -1 le premier argument, la valeur du déterminant est multipliée par -1.

Donc les bases $\mathcal{B}$ et $\mathcal{B}'$ ne sont pas équivalentes et il existe au moins deux classes.

(ii) **Au plus deux classes** Nous montrons à présent que toute base est équivalente soit à $\mathcal{B}$ soit à $\mathcal{B}'$. Supposons que $\mathcal{B}''$ ne soit pas équivalente à $\mathcal{B}$, c'est-à-dire que $\det_{\mathcal{B}}(\mathcal{B}'') < 0$. Nous utilisons encore la formule (9.12),

$$\underbrace{\det_{\mathcal{B}}(\mathcal{B}'')}_{<0} = \underbrace{\det_{\mathcal{B}}(\mathcal{B}')}_{<0} \det_{\mathcal{B}'}(\mathcal{B}''), \tag{9.91}$$

et nous déduisons que $\det_{\mathcal{B}'}(\mathcal{B}'') > 0$.

□

9.25.
Vu qu'il n'y a que deux classes d'équivalence parmi les bases, nous pouvons utiliser le vocable « avoir la même orientation que » ou « avoir l'orientation contraire de ». Ce n'est pas ambigu.

Proposition 9.26 ([258]).
Si $\mathcal{B}$ est une base de l'espace vectoriel E de dimension n, et si τ est une transposition [17] *de S_n, alors la base $\tau(\mathcal{B})$ est de sens contraire.*

13. Définition 9.5.
14. Définition 1.30.
15. Définition 9.23.
16. Nous notons (e_1, e_2) et non $\{e_1, e_2\}$ parce que l'ordre est important.
17. Définition 1.286.

Démonstration. Le lemme 9.7(2) dit que $\det_{\mathcal{B}}$ est une forme anti-symétrique ; donc

$$\det_{\mathcal{B}}(\mathcal{B}') = -\det_{\mathcal{B}}\big(\tau(\mathcal{B})'\big). \tag{9.92}$$

Si l'un est positif, l'autre est négatif. Elles ont donc des orientations contraires. □

Corolaire 9.27.
Si $\mathcal{B}$ est une base de l'espace vectoriel E de dimension n, et si $\sigma \in S_n$, la base $\sigma(\mathcal{B})$ a même orientation que $\mathcal{B}$ si et seulement si $\sigma \in A_n$.

Démonstration. Notons c_1 la classe d'orientation de $\mathcal{B}$ et c_2 l'autre classe. La permutation σ se décompose en produit de transpositions dont la parité est fixée (proposition 1.289). Posons $\sigma = \tau_k \dots \tau_1$.

En posant $\mathcal{B}_0 = \mathcal{B}$ et $\mathcal{B}_{l+1} = \tau_{l+1}(\mathcal{B}_l)$, pour tout l, la base $\mathcal{B}_l$ est d'orientation contraire à celle de la base $\mathcal{B}_{l-1}$. Une base sur deux a l'orientation de $\mathcal{B}$ et l'autre sur deux a l'orientation contraire.

Donc $\sigma(\mathcal{B})$ a la même orientation que $\mathcal{B}$ si et seulement si k est pair. Mais $\sigma \in A_n$ si et seulement si k est pair. C'est bon. □

Proposition-Définition 9.28 ([258])**.**
Soit un espace vectoriel réel, et un endomorphisme f de E. Deux définitions.

*(1) L'endomorphisme f est **direct** si sont déterminant est strictement positif.*

*(2) L'endomorphisme **préserve l'orientation** si il transforme toutes base de E en une base de même orientation.*

Un endomorphisme est direct si et seulement si il préserve l'orientation.

Démonstration. En deux sens.

(i) **Direct implique préserve l'orientation** Soit une base $\mathcal{B}$ de E et un endomorphisme direct u. D'abord, u est inversible du fait que son déterminant est non nul par la proposition 9.10(2). Donc u transforme une base en une base par le lemme 4.8.

La définition 9.9 du déterminant de u est que

$$\det(u) = \det_{\mathcal{B}}\big(u(\mathcal{B})\big) > 0. \tag{9.93}$$

Donc $\mathcal{B}$ et $u(\mathcal{B})$ ont même orientation.

(ii) **Préserve l'orientation implique direct** Le fait que u préserve l'orientation signifie en particulier qu'il transforme une base en une base et qu'il est inversible par le lemme 4.8.

Donc si $\mathcal{B}$ est une base, $u(\mathcal{B})$ est encore une base et nous avons, parce que $\mathcal{B}$ et $u(\mathcal{B})$ ont même orientation,

$$0 < \det_{\mathcal{B}}\big(u(\mathcal{B})\big) = \det(u). \tag{9.94}$$

□

9.2.2 Cas affine

Définition 9.29.
Soit un espace affine $\mathcal{E}$ modelé sur E. Les repères cartésiens[18] *$(O, \mathcal{B})$ et $(O', \mathcal{B}')$ ont **même orientation** si les bases $\mathcal{B}$ et $\mathcal{B}'$ ont même orientation.*

Les classes d'équivalence (il y en a deux) sont les orientations de $\mathcal{E}$.

*Une application affine $f : \mathcal{E} \to \mathcal{E}$ **préserve l'orientation** si sa partie linéaire*[19] *préserve l'orientation.*

18. Définition 8.7.
19. Définition 8.13.

9.3 Hermitien, orthogonal, adjoint

9.30.
Une des choses à retenir de la définition de l'opérateur adjoint est que la notion de A^* dépend du produit scalaire considéré.

Il se fait que le plus souvent, sur $\mathbb{R}^n$, nous considérons le produit scalaire usuel et la base canonique. De ce fait, les notions d'opérateur adjoint et d'opérateur transposés se confondent avec la notion de matrice transposée. Ce sont pourtant, en général, trois notions distinctes.

Proposition-Définition 9.31 (Définition de la transposée[1])**.**
Soient deux espaces vectoriels euclidiens ou hermitiens E et F et une application linéaire $A\colon E \to F$.

(1) Il existe une unique application linéaire $B\colon F \to E$ telle que

$$\langle Ax, y\rangle_F = \langle x, By\rangle_E \tag{9.95}$$

pour tout $x \in E$ et $y \in F$.

(2) Si $\{e_i\}$ est une base orthonormée de E et $\{f_\alpha\}$ est une base orthonormée de F, alors la matrice de A et B pour ces bases sont liées par

$$B_{i\alpha} = A_{\alpha i}. \tag{9.96}$$

*L'application B ainsi définie set nommée **adjoint** de A et sera notée $B = A^*$.*

Démonstration. Pour l'unicité, nous écrivons la condition avec $x = e_j$ pour obtenir :

$$\langle Ae_j, y\rangle = \langle e_j, By\rangle = (By)_j \tag{9.97}$$

c'est-à-dire que les coefficients $B(y)_j$ de $B(y)$ dans la base canonique sont fixés par la condition.

Pour l'existence, il suffit de vérifier que poser

$$B(y) = \sum_j \langle Ae_j, y\rangle e_j \tag{9.98}$$

fonctionne. Pour cela il faut utiliser la bilinéarité du produit scalaire et le fait que $\langle x, e_j\rangle = x_j$. Nous avons :

$$\langle x, B(y)\rangle = \langle x, \sum_j \langle A(e_j), y\rangle e_j\rangle \tag{9.99a}$$

$$= \sum_j \langle A(e_j), y\rangle\langle x, e_j\rangle \tag{9.99b}$$

$$= \sum_j \langle A(x_j e_j), y\rangle \tag{9.99c}$$

$$= \langle A(x), y\rangle. \tag{9.99d}$$

En ce qui concerne la matrice de l'application B ainsi définie, nous écrivons la condition (9.95) avec $y = e'_\alpha$ et $x = e_i$, de telle sorte que

$$A(x) = A(e_i) = \sum_\beta A_{\beta i} e'_\beta \tag{9.100}$$

et

$$B(y) = B(e'_\alpha) = \sum_j B_{j\alpha} e_j. \tag{9.101}$$

Alors nous avons :

$$\sum_\beta A_{\beta i}\langle e'_\beta, e'_\alpha\rangle = \sum_j B_{j\alpha}\langle e_i, e_j\rangle, \tag{9.102}$$

donc

$$A_{\alpha i} = B_{i\alpha}. \tag{9.103}$$

□

9.32.
À cause de l'expression (9.96) pour la matrice de A^*, cette application est souvent appelé **transposé** de A et noté A^t. Nous allons cependant voir plus tard (définition9.183) que la transposée de A est une application $A^t\colon F^* \to E^*$. Il nous arrivera cependant d'écrire des égalités comme $\langle Ax, y\rangle = \langle x, A^t y\rangle$.

Proposition 9.33.
En ce qui concerne le déterminant,

$$\det(A^*) = \det(A)^* \tag{9.104}$$

où l'étoile à droite dénote la conjugaison complexe dans $\mathbb{C}$.

Démonstration. Écrivons l'expression explicite (9.8) du déterminant. Le tout avec la base canonique :

$$\det(A) = \det_{(e_1,\dots,e_n)}(Ae_1,\dots,Ae_n) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n} e^*_{\sigma(i)}(Ae_i). \tag{9.105}$$

Mais nous pouvons développer :

$$e^*_{\sigma(i)}(Ae_i) = \langle e_{\sigma(i)}, Ae_i\rangle = \langle A^*e_{\sigma(i)}, e_i\rangle = \langle e_i, A^*e_{\sigma(i)}\rangle^* = e_i^*(A^*e_{\sigma(i)})^*. \tag{9.106}$$

Notez que dans la dernière expression, les trois * ont trois significations différentes. Par conséquent,

$$\det(A) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n} e_i^*(A^*e_{\sigma(i)})^*. \tag{9.107}$$

Mais $e_i^*(A^*e_{\sigma(i)}) = e^*_{\sigma(j)}(A^*e_j)$ pour $j = \sigma(i)$, donc le produit ne change pas si on déplace le σ :

$$\det(A) = \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n} e^*_{\sigma(i)}(A^*e_i)^* = \det(A^*)^*. \tag{9.108}$$

Nous avons donc $\det(A) = \det(A^*)^*$, c'est-à-dire $\det(A)^* = \det(A^*)$. Pour information, la dernière étoile est la conjugaison complexe. □

Proposition 9.34 ([1])**.**
Si $A\colon E_2 \to E_3$ et $B\colon E_1 \to E_2$ sont des applications linéaires, alors

$$(AB)^* = B^*A^* \tag{9.109}$$

où la « multiplication » est la composition.

Démonstration. L'existence de $(AB)^*$, de A^* et de B^* ne donne pas lieu à débat parce que la proposition 9.31 ne souffre pas de discussions. La propriété que $(AB)^*$ est unique a avoir est que

$$\langle ABx, y\rangle = \langle x, (AB)^*y\rangle \tag{9.110}$$

pour tout $x \in E_1$ et $y \in E_3$. Or l'application B^*A^* possède également cette propriété parce que

$$\langle x, B^*A^*y\rangle = \langle Bx, A^*y\rangle = \langle ABx, y\rangle. \tag{9.111}$$

La partie unicité de la proposition 9.31 nous impose donc d'accepter que les applications $(AB)^*$ et B^*A^* sont en réalité les mêmes [20]. □

9.35.
Un grand moment d'utilisation de la notion d'adjoint pour un opérateur non carré sera la définition d'une intégrale sur une variété ; en particulier dans la proposition 20.9.

20. Et ce même si vous croyez les avoir déjà vu ensemble dans la même pièce.

Lemme 9.36.
Si E est un espace euclidien, un endomorphisme $f: E \to E$ est autoadjoint si et seulement si pour tout $x, y \in E$ nous avons $\langle x, f(y)\rangle = \langle f(x), y\rangle$.

Démonstration. Dans le sens direct, nous avons

$$\langle f(x), y\rangle = \langle x, f^*(y)\rangle = \langle x, f(y)\rangle. \tag{9.112}$$

La première égalité est la définition de f^* et la seconde est l'hypothèse $f = f^*$.

Dans l'autre sens, l'hypothèse est que l'endomorphisme f vérifie $\langle x, f(y)\rangle = \langle f(x), y\rangle$. Mais la proposition 9.31(1) spécifie que f^* est l'unique endomorphisme à satisfaire cette égalité. Donc $f = f^*$. □

9.3.1 Opérateur orthogonal, matrice orthogonale

Définition 9.37.
*Un opérateur est **orthogonal** lorsque $A^* = A^{-1}$ où A^* est l'adjoint de A définit en 9.31.*

Définition 9.38.
*Une matrice U est **orthogonale** si $U^t = U^{-1}$. Le **groupe orthogonal** noté $\mathrm{O}(n)$ est l'ensemble des matrices orthogonales $n \times n$.*

Lemme 9.39.
Soit un opérateur $A: \mathbb{R}^n \to \mathbb{R}^n$ muni du produit scalaire usuel. Il est orthogonal si et seulement si sa matrice dans la base canonique est orthogonale[21].

Démonstration. Soit la base canonique $\{e_i\}_{i=1,\dots,n}$ de $\mathbb{R}^n$. Nous avons

$$\langle AA^*e_i, e_j\rangle = \langle e_i, e_j\rangle = \delta_{ij}, \tag{9.113}$$

donc $\big((AA^*)e_i\big)_j = \delta_{ij}$, ou encore $(AA^*)_{ij} = \delta_{ij}$, ce qui signifie que la matrice AA^* est l'identité. □

Proposition 9.40 (Thème 77)**.**
À propos de matrices orthogonales.

(1) L'ensemble des matrices réelles orthogonales forme un groupe noté $\mathrm{O}(n, \mathbb{R})$.

(2) Si A est une matrice orthogonale, alors $\det(A) = \pm 1$.

(3) Le groupe $\mathrm{O}(n)$ est le groupe des isométries linéaires[22] *de $\mathbb{R}^n$.*

Démonstration. Commençons par prouver que $\mathrm{O}(n, \mathbb{R})$ est un groupe. La matrice $\mathbb{1}$ est orthogonale. De plus si A et B sont orthogonale, la matrice produit AB est orthogonale :

$$(AB)(AB)^t = ABB^tA^t = A\mathbb{1}A^t = \mathbb{1}. \tag{9.114}$$

Nous avons donc bien un groupe.

En ce qui concerne le déterminant, $AA^t = \mathbb{1}$ donne $\det(A)\det(A^t) = 1$, mais la proposition 9.33 dit que $\det(A) = \det(A^t)$, donc $\det(A)^2 = 1$. D'où le fait que $\det(A) = \pm 1$.

D'autre part si A est une isométrie de $\mathbb{R}^n$ alors pour tout $x, y \in \mathbb{R}^n$ nous avons $\langle Ax, Ay\rangle = \langle x, y\rangle$. En particulier,

$$\langle A^tAx, y\rangle = \langle x, y\rangle \tag{9.115}$$

pour tout $x, y \in \mathbb{R}^n$. En prenant $y = e_i$ nous trouvons

$$(A^tAx)_i = x_i, \tag{9.116}$$

ce qui signifie que pour tout x, $A^tAx = x$, ou encore que A^tA est l'identité.

21. Définition 9.38.

22. Au sens où, parmi les applications linéaires, les isométries sont les éléments de $\mathrm{O}(n)$. À part ça, il y a aussi les translations, mais c'est une autre histoire qui vous sera contée une autre fois.

Réciproquement si A^tA est l'identité nous avons

$$\langle x, y\rangle = \langle A^tAx, y\rangle = \langle Ax, Ay\rangle, \tag{9.117}$$

ce qui prouve que A est une isométrie. □

En ce qui concerne les valeurs propres des matrices de $\mathrm{O}(n)$ ainsi que leurs formes canoniques (avec des fonctions trigonométriques) pour $\mathrm{O}(3)$ et $\mathrm{SO}(3)$, ce sera pour la proposition 18.222 et ce qui s'ensuit.

Définition 9.41.
Le sous-groupe des matrices orthogonales de déterminant 1 *est le groupe* ***spécial orthogonal*** *noté* $\mathrm{SO}(n)$.

9.4 Topologie

9.4.1 Boules et sphères

Un espace vectoriel normé (définition 7.146) vient avec sa topologie métrique (théorème 7.108). Sphères et boules fermées viennent dans la définition 7.124.

Définition 9.42.
Une partie A de V est dite ***bornée*** *si il existe un réel R tel que $A \subset B(0_V, R)$.*

Une partie est donc bornée si elle est contenue dans une boule de rayon fini.

Exemple 9.43.
Dans $\mathbb{R}$, les boules sont les intervalles ouverts et fermés tandis que la sphère est donnée par les points extrêmes des intervalles :

$$\begin{aligned} B(a,r) &=]a-r, a+r[, \\ \bar{B}(a,r) &= [a-r, a+b], \\ S(a,r) &= \{a-r, a+r\}. \end{aligned} \tag{9.118}$$

△

Exemple 9.44.
Si nous considérons $\mathbb{R}^2$, la situation est plus riche parce que nous avons plus de normes. Essayons de voir les sphères de centre $(0,0) \in \mathbb{R}^2$ et de rayon r pour les normes $\|.\|_1$, $\|.\|_2$ et $\|.\|_\infty$.

Pour la norme $\|.\|_1$, la sphère de rayon r est donnée par l'équation

$$|x| + |y| = r. \tag{9.119}$$

Pour la norme $\|.\|_2$, l'équation de la sphère de rayon r est

$$\sqrt{x^2 + y^2} = r, \tag{9.120}$$

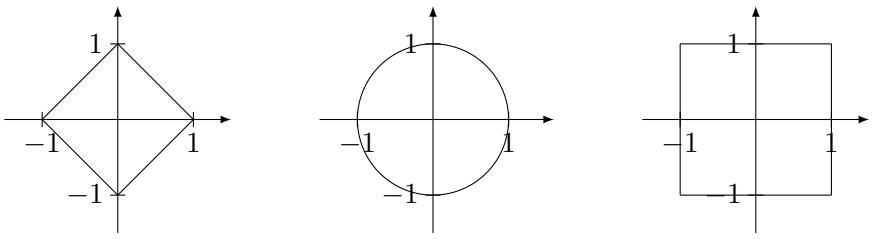
et pour la norme supremum, la sphère de rayon r a pour équation

$$\max\{|x|, |y|\} = r. \tag{9.121}$$

Elles sont dessinées sur la figure 9.1

△

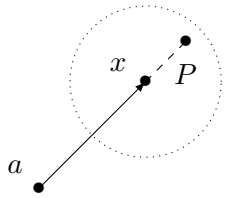
Proposition 9.45.
Soient V un espace vectoriel normé, a dans V et x tel que $d(a,x) = r$, c'est-à-dire $x \in S(a,r)$. Dans ce cas, toute boule centrée en x contient un point P tel que $d(P,a) > r$ et un point Q tel que $d(Q,a) < r$.



(a) La sphère unité pour la norme $\|.\|_1$ (b) La sphère unité pour la norme $\|.\|_2$ (c) La sphère unité pour la norme $\|.\|_\infty$

FIGURE 9.1 – Les sphères de rayon 1 pour les trois normes classiques.

Démonstration. Soit une boule de rayon δ autour de x. Le but est de trouver un point P tel que $d(P,a) > r$ et $d(P,x) < \delta$. Pour cela, nous prenons P sur la même droite que x (en partant de a), mais juste « un peu plus loin », comme sur la figure suivante :



Plus précisément, nous considérons le point

$$P = x + \frac{v}{N} \tag{9.122}$$

où $v = x - a$ et N est suffisamment grand pour que $d(x,P)$ soit plus petit que δ. Cela est toujours possible parce que

$$d(P,x) = \|P - x\| = \frac{\|v\|}{N} \tag{9.123}$$

peut être rendu aussi petit que l'on veut par un choix approprié de N. Montrons maintenant que $d(a,P) > d(a,x)$:

$$\begin{aligned} d(a,P) &= \|a - x - \frac{v}{N}\| \\ &= \|a - x + \frac{a}{N} - \frac{x}{N}\| \\ &= \|\big(1 + \frac{1}{N}\big)(a - x)\| \\ &> \|a - x\| = d(a,x). \end{aligned} \tag{9.124}$$

Nous laissons en exercice le soin de trouver un point Q tel que $d(Q,a) < r$ et $d(Q,x) < \delta$. □

9.4.2 Ouverts, fermés, intérieur et adhérence

Définition 9.46.
*Soit $(V, \|.\|)$ un espace vectoriel normé et A, une partie de V. Un point a est dit **intérieur** à A si il existe une boule ouverte centrée en a et contenue dans A.*

*On appelle **l'intérieur** de A l'ensemble des points qui sont intérieurs à A. Nous notons* $\mathrm{Int}(A)$ *l'intérieur de A.*

Notons que $\mathrm{Int}(A) \subset A$ parce que si $a \in \mathrm{Int}(A)$, nous avons $B(a,r) \subset A$ pour un certain r et en particulier $a \in A$.

Exemple 9.47.
Trouver l'intérieur d'un intervalle dans $\mathbb{R}$ consiste à « ouvrir là où c'est fermé ».

(1) $\mathrm{Int}\big([0,1[\big) =]0,1[$.
Prouvons d'abord que $]0,1[\subset \mathrm{Int}([0,1[)$. Si $a \in]0,1[$, alors a est strictement supérieur à 0 et strictement inférieur à 1. Dans ce cas, la boule de centre a et de rayon $\frac{\min\{a,1-a\}}{2}$ est contenue dans $]0,1[$ (voir figure 9.2). Cela prouve que a est dans l'intérieur de $[0,1[$.

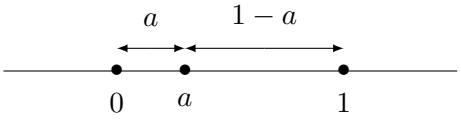


FIGURE 9.2 – Trouver le rayon d'une boule autour de a. Une boule qui serait centrée en a avec un rayon strictement plus petit à la fois de a et de $1-a$ est entièrement contenue dans le segment $]0,1[$.

Prouvons maintenant que $\mathrm{Int}\big([0,1[\big) \subset]0,1[$. Vu que l'intérieur d'un ensemble est inclus dans l'ensemble, nous savons déjà que $\mathrm{Int}\big([0,1[\big) \subset [0,1[$. Nous devons donc seulement montrer que 0 n'est pas dans l'intérieur de $[0,1[$. C'est le cas parce que toute boule du type $B(0,r)$ contient le point $-r/2$ qui n'est pas dans $[0,1[$.

(2) $\mathrm{Int}\Big(\big[0,\infty\big[\Big) =]0,\infty[$.

(3) $\mathrm{Int}\big(]2,3[\big) =]2,3[$.

△

Exemple 9.48.
Les intérieurs des boules et sphères sont importantes à savoir.

(1) $\mathrm{Int}\big(B(a,r)\big) = B(a,r)$. Si $x \in B(a,r)$, nous avons $d(a,x) < r$. Alors la boule $B\big(x, r-d(x,a)\big)$ est incluse à $B(a,r)$, et donc x est dans l'intérieur de $B(a,r)$. Conseil : faire un dessin.

(2) $\mathrm{Int}\big(\bar{B}(a,r)\big) = B(a,r)$. Par le point précédent, la boule $B(a,r)$ est certainement dans l'intérieur de la boule fermée. Il reste à montrer que les points de $\bar{B}(a,r)$ qui ne sont pas dans $B(a,r)$ ne sont pas dans l'intérieur. Ces points sont ceux dont la distance à a est *égale* à r. Le résultat découle alors de la proposition 9.45.

(3) $\mathrm{Int}\big(S(a,r)\big) = \varnothing$. Si $x \in S(a,r)$, toute boule centrée en a contient des points qui ne sont pas à distance r de a.
Notez que la sphère est un exemple d'ensemble non vide mais d'intérieur vide.

△

Définition 9.49.
Une partie A de l'espace vectoriel normé $(V, \|.\|)$ est dite ***ouverte*** *si chacun de ses points est intérieur. La partie A est donc ouverte si $A \subset \mathrm{Int}(A)$. Par convention, nous disons que l'ensemble vide $\varnothing$ est ouvert.*

Une partie est dite ***fermée*** *si son complémentaire est ouvert. La partie A est donc fermée si $V \backslash A$ est ouverte.*

Remarque : un ensemble A est ouvert si et seulement si $\mathrm{Int}(A) = A$.

Définition 9.50.
Une partie A de l'espace vectoriel normé V est dite ***compacte*** *si elle est fermée et bornée.*

Nous verrons tout au long de ce cours que les ensembles compacts, et les fonctions définies sur ces ensembles ont de nombreuses propriétés agréables.

Exemple 9.51.
En ce qui concerne les intervalles de $\mathbb{R}$,

— $]1,2[$ est ouvert ;

— $[3,4]$ est fermé ;

— $[5, 6[$ n'est ni ouvert ni fermé ;

Les intervalles fermés de $\mathbb{R}$ sont toujours compacts. △

Proposition 9.52.
Soit V un espace vectoriel normé.

(1) L'ensemble V lui-même et le vide sont à la fois fermés et ouverts.

(2) Toute union d'ouverts est ouverte.

(3) Toute intersection finie *d'ouverts est ouverte.*

(4) Le vide et V sont les seules parties de V à être à la fois fermées et ouvertes.

Démonstration. L'ingrédient principal de cette démonstration est que si a est un point d'un ouvert $\mathcal{O}$, alors il existe une boule autour de a contenue dans $\mathcal{O}$ parce que a doit être dans l'intérieur de $\mathcal{O}$.

(1) Nous avons déjà dit que, par définition, l'ensemble vide est ouvert. Cela implique que V lui-même est fermé (parce que son complémentaire est le vide). De plus, V est ouvert parce que toutes les boules sont inclues à V. Le vide est alors fermé (parce que son complémentaire est V).

(2) Soit une famille $(\mathcal{O}_i)_{i\in I}$ d'ouverts[23], et l'union

$$\mathcal{O} = \bigcup_{i\in I} \mathcal{O}_i. \tag{9.125}$$

Soit maintenant $a \in \mathcal{O}$. Nous devons prouver qu'il existe une boule centrée en a entièrement contenue dans $\mathcal{O}$. Étant donné que $a \in \mathcal{O}$, il existe $i \in I$ tel que $a \in \mathcal{O}_i$ (c'est-à-dire que a est au moins dans un des $\mathcal{O}_i$). Par hypothèse l'ensemble $\mathcal{O}_i$ est ouvert et donc tous ses points (en particulier a) sont intérieurs ; il existe donc une boule $B(a, r)$ centrée en a telle que $B(a, r) \subset \mathcal{O}_i \subset \mathcal{O}$.

(3) Soit une famille finie d'ouverts $(\mathcal{O}_k)_{k\in\{1,\dots,n\}}$, et $a \in \mathcal{O}$ où

$$\mathcal{O} = \bigcap_{k=1}^{n} \mathcal{O}_k. \tag{9.126}$$

Vu que a appartient à chaque ouvert $\mathcal{O}_k$, nous pouvons trouver, pour chacun de ces ouverts, une boule $B(a, r_k)$ contenue dans $\mathcal{O}_k$. Chacun des r_k est strictement positif, et nous n'en avons qu'un nombre fini, donc le nombre $r = \min\{r_1, \dots, r_n\}$ est strictement positif. La boule $B(a, r)$ est inclue dans toutes les autres (parce que $B(a, r) \subset B(a, r')$ lorsque $r \leqslant r'$), par conséquent

$$B(a, r) \subset \bigcap_{k=1}^{n} B(a, r_k) \subset \bigcap_{k=1}^{n} \mathcal{O}_k = \mathcal{O}, \tag{9.127}$$

c'est-à-dire que la boule de rayon r est une boule centrée en a contenue dans $\mathcal{O}$, ce qui fait que a est intérieur à $\mathcal{O}$.

(4) Nous acceptons ce point sans démonstration.

□

La proposition dit que toute intersection *finie* d'ouvert est ouverte. Il est faux de croire que cela se généralise aux intersections infinies, comme le montre l'exemple suivant :

$$\bigcap_{i=1}^{\infty}]-\frac{1}{n}, \frac{1}{n}[= \{0\}. \tag{9.128}$$

Chacun des ensembles $]-\frac{1}{n}, \frac{1}{n}[$ est ouvert, mais le singleton $\{0\}$ est fermé (pourquoi ?).

Nous reportons à la proposition 1.442 la preuve du fait que tout ensemble borné de $\mathbb{R}$ possède un infimum et un supremum.

23. L'ensemble I avec lequel nous « numérotons » les ouverts $\mathcal{O}_i$ est *quelconque*, c'est-à-dire qu'il peut être $\mathbb{N}$, $\mathbb{R}$, $\mathbb{R}^n$ ou n'importe quel autre ensemble, fini ou infini.

Définition 9.53.
L'ensemble des ouverts de V est la ***topologie*** *de V. La topologie dont nous parlons ici est dite* ***induite*** *par la norme $\|.\|$ de V (parce que cette norme définit la notion de boule et qu'à son tour la notion de boule définit la notion d'ouverts). Un* ***voisinage*** *de a dans V est un ensemble contenant un ouvert contenant a.*

Il existe de nombreuses topologies sur un espace vectoriel donné, mais certaines sont plus fameuses que d'autres. Dans le cas de $V = \mathbb{R}^n$, la topologie **usuelle** est celle induite par la norme euclidienne. Lorsque nous parlons de boules, de fermés, de voisinages ou d'autres notions topologiques (y compris de convergence, voir plus bas) dans $\mathbb{R}^n$, nous sous-entendons toujours la topologie de la norme euclidienne.

Exemple 9.54.
Les ensembles suivants sont des voisinages de 3 dans $\mathbb{R}$:

— $]1, 5[$;
— $[0, 10]$;
— $\mathbb{R}$.

Les ensembles suivants ne sont pas des voisinages de 3 dans $\mathbb{R}$:

— $]1, 3[$;
— $]1, 3]$;
— $[0, 5[\backslash\{3\}$.

△

Proposition 9.55.
Dans un espace vectoriel normé,

(1) toute intersection de fermés est fermée ;
(2) toute union finie *de fermés est fermée.*

Encore une fois, l'hypothèse de finitude de l'intersection est indispensable comme le montre l'exemple suivant :

$$\bigcup_{n=1}^{\infty} [-1 + \frac{1}{n}, 1 - \frac{1}{n}] =]-1, 1[. \tag{9.129}$$

Chacun des intervalles dont on prend l'union est fermé tandis que l'union est ouverte.

Lemme 9.56.
Soit A, une partie de l'espace vectoriel normé V. Un point $a \in V$ est adhérent[24] *à A dans V si et seulement si pour tout $\varepsilon > 0$,*

$$B(a, \varepsilon) \cap A \neq \varnothing. \tag{9.130}$$

Un point peut être adhérent à A sans faire partie de A, et nous avons toujours $A \subset \mathrm{Adh}(A)$.

Exemple 9.57.
La terminologie « fermeture » de A pour désigner $\bar{A}$ provient de deux origines.

(1) L'ensemble $\bar{A}$ est le plus petit fermé contenant A. Cela signifie que si B est un fermé qui contient A, alors $\bar{A} \subset B$. Cela est fondamentalement le sens de la définition 7.19.
(2) Pour les intervalles dans $\mathbb{R}$, trouver $\bar{A}$ revient à fermer les extrémités qui sont ouvertes, comme on en a parlé dans l'exemple 9.51.

△

24. Définition 7.19.

Exemple 9.58.
Dans $\mathbb{R}$, l'infimum et le supremum d'un ensemble sont des points adhérents. En effet si M est le supremum de $A \subset \mathbb{R}$, pour tout ε, il existe un $a \in A$ tel que $a > M - \varepsilon$, tandis que $M > a$. Cela fait que $a \in B(M, \varepsilon)$, et en particulier que pour tout rayon ε, nous avons $B(M, \varepsilon) \cap A \neq \varnothing$.

Le même raisonnement montre que l'infimum est également dans l'adhérence de A. △

Exemple 9.59.
Il ne faut pas conclure de l'exemple précédent qu'un point limite ou adhérent est automatiquement un minimum ou un maximum. En effet, si nous regardons l'ensemble formé par les points de la suite $x_n = (-1)^n/n$, le nombre zéro est un point adhérent et une limite, mais pas un infimum ni un maximum. △

Lemme 9.60.
Si B est une partie fermée de V, alors $B = \bar{B}$.

Démonstration. Supposons qu'il existe $a \in \bar{B}$ tel que $a \notin B$. Alors il n'y a pas d'ouverts autour de a qui soit contenu dans $\complement B$. Cela prouve que $\complement B$ n'est pas ouvert, et par conséquent que B n'est pas fermé. Cela est une contradiction qui montre que tout point de $\bar{B}$ doit appartenir à B lorsque B est fermé. □

Exemple 9.61.
Au niveau des intervalles dans $\mathbb{R}$, prendre l'adhérence consiste à « fermer là où c'est ouvert ». Attention cependant à ne pas fermer l'intervalle en l'infini.

(1) $\overline{[0, 2[} = [0, 2]$.
(2) $\overline{]3, \infty[} = [3, \infty[$.

Si au lieu de travailler dans $\mathbb{R}$, vous travaillez dans une extension comme le compactifié d'Alexandrov $\hat{\mathbb{R}}$ (définition 7.97) ou dans la droite réelle achevée (définition 12.27), vous devez un peu réfléchir avant de décider si il faut fermer les intervalles en $\pm\infty$ ou en ω. Bref, ne faites rien mécaniquement et posez vous des questions de topologie quand vous cherchez des fermetures. △

Proposition 9.62.
Soit V un espace vectoriel normé et $a \in V$. Les trois conditions suivantes sont équivalentes :

(1) $a \in \bar{A}$;
(2) il existe une suite d'éléments x_n dans A qui converge vers a ;
(3) $d(a, A) = 0$.

Notez que dans cette proposition, nous ne supposons pas que a soit dans A.

Proposition 9.63.
Pour toute partie A d'un espace vectoriel normé nous avons

(1) $V \backslash \bar{A} = \operatorname{Int}(V \backslash A)$,
(2) $V \backslash \operatorname{Int}(A) = \overline{V \backslash A}$.

En utilisant les notations du complémentaire (1.1.5), les deux points de la proposition se récrivent

(1) $\complement \bar{A} = \operatorname{Int}(\complement A)$,
(2) $\complement \operatorname{Int}(A) = \overline{\complement A}$.

Démonstration. Nous avons $a \in V \backslash \bar{A}$ si et seulement si $a \notin \bar{A}$. Or ne pas être dans $\bar{A}$ signifie qu'il existe un rayon ε tel que la boule $B(a, \varepsilon)$ n'intersecte pas A. Le fait que la boule $B(a, \varepsilon)$ n'intersecte pas A est équivalent à dire que $B(a, \varepsilon) \subset V \backslash A$. Or cela est exactement la définition du fait que a est à l'intérieur de $V \backslash A$. Nous avons donc montré que $a \in V \backslash \bar{A}$ si et seulement si $a \in \operatorname{Int}(V \backslash A)$. Cela prouve la première affirmation.

Pour prouver la seconde affirmation, nous appliquons la première au complémentaire de A : $\complement(\overline{\complement A}) = \text{Int}(\complement\complement A)$. En prenant le complémentaire des deux membres nous trouvons successivement

$$\begin{aligned} \complement\complement(\overline{\complement A}) &= \complement\,\text{Int}(\complement\complement A), \\ \overline{\complement A} &= \complement\,\text{Int}(A), \end{aligned} \tag{9.131}$$

ce qu'il fallait démontrer. □

Attention à ne pas confondre $\complement\bar{A}$ et $\overline{\complement A}$. Ces deux ensembles ne sont pas égaux. En effet, en tant que complément d'un fermé, l'ensemble $\complement\bar{A}$ est certainement ouvert, tandis que, en tant que fermeture, l'ensemble $\overline{\complement A}$ est fermé. Pouvez-vous trouver des exemples d'ensembles A tels que $\complement\bar{A} = \overline{\complement A}$?

Proposition 9.64.
Soient A et B deux parties de l'espace vectoriel normé V.

(1) Pour les inclusions, si $A \subset B$, alors $\text{Int}(A) \subset \text{Int}(B)$ et $\bar{A} \subset \bar{B}$.

(2) Pour les unions, $\overline{A \cup B} = \overline{A} \cup \overline{B}$ et $\overline{A \cap B} \subset \bar{A} \cap \bar{B}$.

(3) Pour les intersections, $\text{Int}(A) \cap \text{Int}(B) = \text{Int}(A \cap B)$ et $\text{Int}(A) \cup \text{Int}(B) \subset \text{Int}(A \cup B)$.

Démonstration. (1) Si a est dans l'intérieur de A, il existe une boule autour de a contenue dans A. Cette boule est alors contenue dans B et donc est une boule autour de a contenue dans B, ce qui fait que a est dans l'intérieur de B. Si maintenant a est dans l'adhérence de A, toute boule centrée en a contient un élément de A et donc un élément de B, ce qui prouve que a est dans l'adhérence de B.

(2) Nous avons $A \subset A \cup B$ et donc, en utilisant le premier point, $\bar{A} \subset \overline{A \cup B}$. De la même manière, $\bar{B} \subset \overline{A \cup B}$. En prenant l'union, $\bar{A} \cup \bar{B} \subset \overline{A \cup B}$.
Réciproquement, soit $a \in \overline{A \cup B}$ et montrons que $a \in \bar{A} \cup \bar{B}$. Supposons par l'absurde que a ne soit ni dans $\bar{A}$ ni dans $\bar{B}$. Il existe donc des rayons ε_1 et ε_2 tels que

$$\begin{aligned} B(a, \varepsilon_1) \cap A &= \varnothing, \\ B(a, \varepsilon_2) \cap B &= \varnothing. \end{aligned} \tag{9.132}$$

En prenant $r = \min\{\varepsilon_1, \varepsilon_2\}$, la boule $B(a, r)$ est inclue aux deux boules citées et donc n'intersecte ni A ni B. Donc $a \notin \overline{A \cup B}$, d'où la contradiction.

(3) Si nous appliquons le second point à $\complement A$ et $\complement B$, nous trouvons

$$\overline{\complement A \cup \complement B} = \overline{\complement A} \cup \overline{\complement B}. \tag{9.133}$$

En utilisant les propriétés du lemme 1.27, le membre de gauche devient

$$\overline{\complement A \cup \complement B} = \overline{\complement(A \cap B)} = \complement\,\text{Int}(A \cap B), \tag{9.134}$$

tandis que le membre de droite devient

$$\overline{\complement A} \cup \overline{\complement B} = \complement\,\text{Int}(A) \cup \complement\,\text{Int}(A) = \complement\Big(\text{Int}(A) \cap \text{Int}(B)\Big). \tag{9.135}$$

En égalisant le membre de droite de (9.134) avec celui de (9.135) et en passant au complémentaire nous trouvons

$$\text{Int}(A \cap B) = \text{Int}(A) \cap \text{Int}(B), \tag{9.136}$$

comme annoncé.
La dernière affirmation provient du fait que $\text{Int}(A) \subset \text{Int}(A \cup B)$ et de la propriété équivalente pour B.

□

Remarque 9.65.
Nous avons prouvé que $\overline{A\cap B}\subset\bar{A}\cap\bar{B}$. Il arrive que l'inclusion soit stricte, comme dans l'exemple suivant. Si nous prenons $A=[0,1]$ et $B=]1,2]$, nous avons $A\cap B=\varnothing$ et donc $\overline{A\cap B}=\varnothing$. Par contre nous avons $\bar{A}\cap\bar{B}=\{1\}$.

Définition 9.66.
*La **frontière** d'un sous-ensemble A de l'espace vectoriel normé V est l'ensemble des points $a\in V$ tels que*

$$\begin{aligned}B(a,r)\cap A\neq\varnothing,\\ B(a,r)\cap\complement A\neq\varnothing,\end{aligned}\tag{9.137}$$

pour tout rayon r. En d'autres termes, toute boule autour de a contient des points de A et des points de $\complement A$. La frontière de A se note ∂A.

Proposition 9.67.
La frontière d'une partie A d'un espace vectoriel normé V s'exprime sous la forme

$$\partial A=\bar{A}\backslash\operatorname{Int}(A).\tag{9.138}$$

Démonstration. Le fait pour un point a de V d'appartenir à $\bar{A}$ signifie que toute boule centrée en a intersecte A. De la même façon, le fait de ne pas appartenir à $\operatorname{Int}(A)$ signifie que toute boule centrée en a intersecte $\complement A$. □

La description de la frontière donnée par la proposition 9.67 est celle qu'en pratique nous utilisons le plus souvent. Dans certains textes, elle est prise comme définition de la frontière.

Lemme 9.68.
La frontière de A peut également s'exprimer des façons suivantes :

$$\partial A=\bar{A}\cap\complement\operatorname{Int}(A)=\bar{A}\cap\overline{\complement A},\tag{9.139}$$

Démonstration. En partant de $\partial A=\bar{A}\backslash\operatorname{Int}(A)$, la première égalité est une application de la propriété (2) du lemme 1.27. La seconde égalité est alors la proposition 9.63. □

Exemple 9.69.
Dans $\mathbb{R}$, la frontière d'un intervalle est la paire constituée des points extrêmes. En effet

$$\partial[a,b[=\overline{[a,b[}\backslash\operatorname{Int}\big([a,b[\big)=[a,b]\backslash]a,b[=\{a,b\}.\tag{9.140}$$

Toujours dans $\mathbb{R}$ nous avons

$$\partial\mathbb{R}=\bar{\mathbb{R}}\backslash\operatorname{Int}(\mathbb{R})=\mathbb{R}\backslash\mathbb{R}=\varnothing,\tag{9.141}$$

et

$$\partial\mathbb{Q}=\bar{\mathbb{Q}}\backslash\operatorname{Int}(\mathbb{Q})=\mathbb{R}\backslash\varnothing=\mathbb{R}.\tag{9.142}$$

△

Exemple 9.70.
Dans $\mathbb{R}^n$, nous avons

$$\partial B(a,r)=\partial\bar{B}(a,r)=S(a,r).\tag{9.143}$$

Cela est un boulot pour la proposition 9.45. Si $x\in S(a,r)$ alors tout boule autour de x contient des points à distance strictement plus grande et plus petite que $d(a,x)$, c'est-à-dire des points dans $B(a,r)$ et hors de $B(a,r)$. Cela prouve que les points de $S(a,r)$ font partie de $\partial B(a,r)$, c'est-à-dire que $S(a,r)\subset\partial B(a,r)$; et idem pour $\bar{B}(a,r)$.

Pour prouver l'inclusion inverse, soit $x\in\partial B(a,r)$. Vu que toute boule autour de x contient des points intérieurs à $B(a,r)$, pour tout $\epsilon>0$, $d(a,x)-\epsilon<r$, c'est-à-dire que $d(a,x)\leqslant r$. De la même manière toute boule autour de x contient des points hors de $B(a,r)$ signifie que pour tout ϵ, $d(a,x)+\epsilon>r$ ou encore que $d(a,x)\geqslant r$. Nous avons donc $d(a,x)=r$. △

Remarque 9.71.
Il serait toutefois faux de croire que $\partial A = \partial \bar{A}$ pour toute partie A de $\mathbb{R}^n$. En effet si $A = \mathbb{R}\backslash\{0\}$ nous avons $\partial A = \{0\}$ et $\bar{A} = \mathbb{R}$, donc $\partial \bar{A} = \varnothing$.

9.4.3 Point isolé, point d'accumulation

Lemme 9.72.
Soit un espace vectoriel normé V ainsi qu'une partie D de V.

(1) Un point $a \in D$ est dit isolé[25] *dans D relativement à V si il existe un $\varepsilon > 0$ tel que*

$$B(a, \varepsilon) \cap D = \{a\}. \tag{9.144}$$

(2) Un point $a \in V$ point d'accumulation[26] *de D si pour tout $\varepsilon > 0$,*

$$\Big(B(a, \varepsilon)\backslash\{a\}\Big) \cap D \neq \varnothing. \tag{9.145}$$

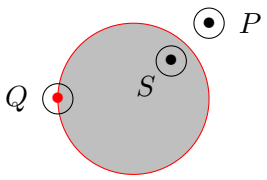


FIGURE 9.3 – L'ensemble décrit par l'équation (9.146). Le point P est un point isolé de D, tandis que les points S et Q sont des points d'accumulation.

Exemple 9.73.
Considérons la partie suivante de $\mathbb{R}^2$:

$$D = \{(x, y) \text{ tel que } x^2 + y^2 < 1\} \cup \{(1, 1)\}. \tag{9.146}$$

Comme on peut le voir sur la figure 9.3, le point $P = (1, 1)$ est un point isolé de D parce qu'on peut tracer une boule autour de P sans inclure d'autres points de D que P lui-même. Le point $Q = (-1, 0)$ est un point d'accumulation de D parce que toute boule autour de Q contient des points de D.

Le point S, étant un point intérieur, est un point d'accumulation : toute boule autour de S intersecte D.

Notez cependant que le point Q lui-même n'est pas dans D parce que l'inégalité qui définit D est stricte. △

Remarque 9.74.
À propos de la position des points d'accumulation et des points isolés.

(1) Les points intérieurs sont tous des points d'accumulation.
(2) Les points isolés ne sont jamais intérieurs.
(3) Certains points d'accumulation ne font pas partie de l'ensemble. Par exemple le point 1 est un point d'accumulation de $E =]0, 1[$.
(4) Les points de la frontière sont soit d'accumulation soit isolés.

Exemple 9.75.
Tous les points de $\mathbb{R}$ sont des points d'accumulation de $\mathbb{Q}$ parce que dans toute boule autour d'un réel, on peut trouver un nombre rationnel. △

Remarque 9.76.
L'ensemble des points d'accumulation d'un ensemble n'est pas exactement son adhérence. En effet, un point isolé dans A est dans l'adhérence de A, mais n'est pas un point d'accumulation de A.

25. Définition 7.31.
26. Définition 7.30.

9.4.4 Des exemples

Exemple 9.77.
Nous considérons l'ensemble.

$$A_1 = \{(x,y) \in \mathbb{R}^2 \mid x^2 - 5x + 6 < y \leqslant 2\}. \tag{9.147}$$

Si un point $(x,y) \in \mathbb{R}^2$ est tel que $x^2 - 5x + 6 < y$, alors dans une boule centrée en (x,y) (de rayon r_1), l'inégalité reste vraie (parce que la fonction $x^2 - 5x + 6 - y$ est une fonction continue). De la même manière, si nous avons $y < 2$ en (x,y), alors nous avons encore l'inégalité dans une boule de rayon r_2. En prenant $r = \min\{r_1, r_2\}$, les deux inégalités restent vraies dans la boule de rayon r.

Donc les points (x,y) tels que $x^2 - 5x + 6 < y < 2$ sont dans l'intérieur de A_1.

Pour les mêmes raisons, autour d'un point (x,y) tel que $x^2 - 5x + 6 > y$, nous pouvons trouver une boule dans laquelle l'inégalité reste stricte. Ces points ne sont donc pas dans l'adhérence de A_1. Un point qui vérifie $x^2 - 5x + 6 = y = 2$ est par contre dans l'adhérence parce que dans toute boule, on pourra trouver un x tel que $x^2 - 5x + 6 < y$, et un y. L'adhérence est donc donnée par les inéquations

$$\bar{A}_1 \equiv x^2 - 5x + 6 \leqslant y \leqslant 2. \tag{9.148}$$

La frontière est donnée par les points de l'adhérence qui ne sont pas dans l'intérieur de A_1. Attention : **ne pas dire** que la frontière est alors donnée simplement en remplaçant les inégalités par des égalités : $\partial A_1 \equiv x^2 - 5x + 6 = y = 2$. Quel est cet ensemble ?

Trouver la frontière demande un peu plus de travail. Le point marqué sur la figure 9.4 est sur la frontière parce que toute boule intersecte l'intérieur et l'extérieur. Cela est dû au fait que, sur ce point, nous ayons $x^2 - 5x + 6 = y$ en même temps que $y < 2$. Donc si on prend une boule assez petite, on conserve $y < 2$, mais on obtient des points tels que $x^2 - 5x + 6 < y$.

En voyant le dessin, la chose à faire pour écrire la frontière est de trouver les deux points d'intersection entre la parabole et la droite horizontale. Ces points sont les points (x,y) qui satisfont au système

$$\begin{cases} x^2 - 5x + 6 = y & \text{(9.149a)} \\ y = 2. & \text{(9.149b)} \end{cases}$$

En substituant la seconde équation dans la première, il vient $x^2 - 5x + 6 = 2$, ce qui nous donne à résoudre le polynôme du second degré $x^2 - 5x + 4 = 0$. Les éventuelles solutions entières sont les diviseurs de 4. Par chance[27], on voit que $x = 1$ et $x = 4$ sont des solutions. Le théorème 3.125 nous assure qu'il n'y a pas d'autres racines. Les deux points d'intersection sont les points $P = (1,2)$ et $Q = (4,2)$. Les points de la frontière de A_1 sont donc donnés par

$$\begin{aligned} \partial A_1 = &\{(x,y) \in \mathbb{R}^2 \text{ tels que } x^2 - 5x + 6 = y \text{ et } 1 \leqslant x \leqslant 4\} \\ &\cup \{(x,y) \in \mathbb{R}^2 \text{ tels que } y = 2 \text{ et } 1 \leqslant x \leqslant 4\}. \end{aligned} \tag{9.150}$$

Notez que les points de la parabole qui sont sur la frontière ne font pas partie de l'ensemble A_1 lui-même, tandis que ceux de la frontière qui sont sur la droite horizontale en font partie sauf $(4,2)$ et $(1,2)$.

L'intérieur de A_1 n'étant pas égal à A_1, cet ensemble n'est pas ouvert ; de la même manière, vu que $\bar{A}_1 \neq A_1$, l'ensemble n'est pas fermé. L'ensemble A_1 est par contre borné parce qu'il est contenu par exemple dans la boule de centre $(0,0)$ et de rayon 5. Les points d'accumulation de A_1 sont les points de sa fermeture. △

Exemple 9.78.
Nous étudions

$$A_2 = \{(x,y) \in \mathbb{R}^2 \mid x + 1 < y < 2x\}. \tag{9.151}$$

Pour les mêmes raisons que dans l'exemple 9.77 l'intérieur est donné par

$$\text{Int}(A_2) \equiv x + 1 < y < 2x; \tag{9.152}$$

27. Sinon, il aurait fallu utiliser la proposition 10.108.

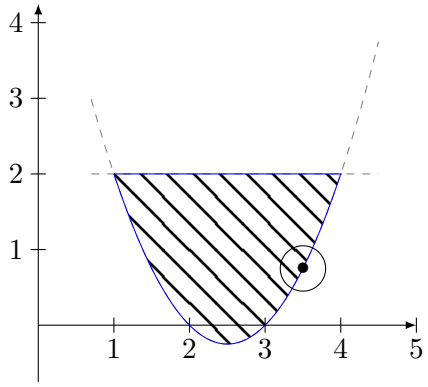


FIGURE 9.4 – En hachuré : l'intérieur ; en trait plein : la frontière. L'adhérence est l'union des deux. Exemple9.77.

L'adhérence est donnée par

$$\overline{A_2} \equiv x + 1 \leqslant y \leqslant 2x, \tag{9.153}$$

Pour la frontière, les deux droites dont il est question dans la définition de A_2 (les droites $y = x+1$ et $y = 2x$) se coupent en $x = 1$ (refaire soi-même le dessin de la figure 9.5). Lorsque $x < 1$, les conditions $x + 1 < y$ et $y < 2x$ sont incompatibles : aucun point de A_2 n'est dans la partie $x < 1$ du plan. Lorsque $x > 1$, alors les points situés *entre* les deux droites font partie de A_2. La frontière est donc donnée par ces deux droites pour $x \geqslant 1$.

Étant donné que $\text{Int}(A_2) = A_2$, cet ensemble est ouvert (et donc pas fermé par la proposition 9.52(4)). Il n'est par contre pas borné parce qu'il contient des point (x, y) avec des x arbitrairement grands. △

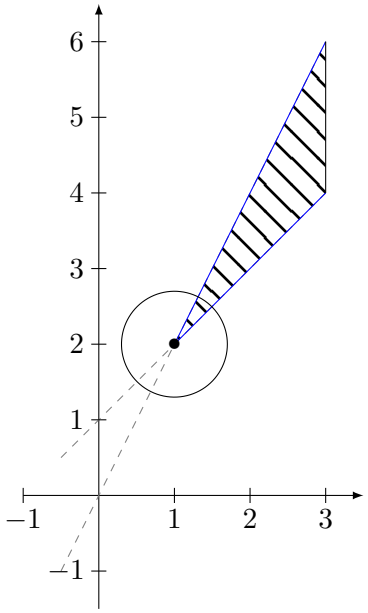


FIGURE 9.5 – Notez que le point d'angle fait partie de la frontière, mais pas de l'ensemble. Exemple 9.78.

Proposition 9.79 ([259]).
Tout partie de $\mathbb{R}$ sans point d'accumulation est dénombrable.

Démonstration. Soit une partie S de $\mathbb{R}$ ne contenant pas de points d'accumulation. Pour chaque $s \in S$, il existe un $\epsilon_s > 0$ tel que

$$B(s, \epsilon_s) \cap S = \{s\}. \tag{9.154}$$

Rien ne garantit cependant que $B(s,\epsilon_s)\cap B(t,\epsilon_t)=\varnothing$, alors que nous en aurons besoin pour la suite.

Le nombre

$$\inf\{|s-v| \text{ tel que } v\in S\backslash\{s\}\} \tag{9.155}$$

est au moins égal à ϵ_s et est don strictement positif. Nous posons

$$r_s=\frac{\inf\big\{|s-v| \text{ tel que } v\in S\backslash\{s\}\big\}}{4}, \tag{9.156}$$

et

$$I_s=B(s,r_s). \tag{9.157}$$

Nous avons maintenant $I_s\cap I_t=\varnothing$. Soit en effet $u\in I_s\cap I_t$. Alors

$$\begin{aligned}|s-t|&\leqslant |s-u|+|u-t| &(9.158a)\\ &\leqslant r_s+t_t &(9.158b)\\ &\leqslant 2r_s &(9.158c)\end{aligned}$$

où nous avons supposé $r_s\geqslant r_t$. Si ce n'est pas le cas, changer s et t dans ce qui suit ; les deux point ont des rôles symétrique. Nous avons donc

$$|s-t|\leqslant 2r_s=\frac{\inf\big\{|s-v| \text{ tel que } v\in S\backslash\{s\}\big\}}{2}\leqslant\frac{|s-t|}{2}. \tag{9.159}$$

Donc $|s-t|=0$ et $s=t$.

Cela pour dire que I_s ne possède d'intersection avec I_t que si $s=t$.

Nous définissons alors une application

$$\begin{aligned}\varphi\colon S&\to\mathbb{Q}\\ s&\mapsto q_s\end{aligned} \tag{9.160}$$

où q_s est un choix de rationnel dans I_s. C'est le lemme 1.424 qui nous permet de choisir un tel rationnel.

La construction des intervalles I_s garantit que φ est une injection. Le fait qu'il existe une injection de $\mathbb{Q}$ vers S et le fait que $\mathbb{Q}$ est dénombrable impliquent que S est au plus dénombrable. □

9.5 Valeur propre et vecteur propre

9.5.1 Généralités

Nous savons qu'une application *linéaire* $A\colon\mathbb{R}^3\to\mathbb{R}^3$ est complètement définie par la donnée de son action sur les trois vecteurs de base, c'est-à-dire par la donnée de

$$Ae_1,\quad Ae_2\quad\text{et}\quad Ae_3. \tag{9.161}$$

La matrice d'une application A se forme en mettant simplement les vecteurs Ae_1, Ae_2 et Ae_3 en colonne. Donc la matrice

$$A=\begin{pmatrix}3&0&0\\0&0&1\\0&1&0\end{pmatrix} \tag{9.162}$$

signifie que l'application linéaire A envoie le vecteur e_1 sur $\begin{pmatrix}3\\0\\0\end{pmatrix}$, le vecteur e_2 sur $\begin{pmatrix}0\\0\\1\end{pmatrix}$ et le vecteur e_3 sur $\begin{pmatrix}0\\1\\0\end{pmatrix}$. Pour savoir comment A agit sur n'importe quel vecteur, on applique la règle

de produit vecteur×matrice :

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x + 2y + 3z \\ 4x + 5y + 6z \\ 7x + 8y + 9z \end{pmatrix}. \tag{9.163}$$

Une chose intéressante est de savoir quelles sont les directions invariantes de la transformation linéaire. Par exemple, on peut lire sur la matrice (9.162) que la direction $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ est invariante : elle est simplement multipliée par 3. Dans cette direction, la transformation est juste une dilatation. Afin de savoir si v est un vecteur d'une direction conservée, il faut voir si il existe un nombre λ tel que $Av = \lambda v$, c'est-à-dire voir si v est simplement dilaté.

L'équation $Av = \lambda v$ se récrit $(A - \lambda\mathbb{1})v = 0$, c'est-à-dire qu'il faut résoudre l'équation

$$(A - \lambda\mathbb{1}) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \tag{9.164}$$

Nous savons qu'une telle équation ne peut avoir de solutions que si $\det(A - \lambda\mathbb{1}) = 0$. La première étape est donc de trouver les λ qui vérifient cette condition.

9.5.2 Dans le vif du sujet

Définition 9.80.
*Soit un $\mathbb{K}$-espace vectoriel E et un endomorphisme $T : E \to E$. Un **vecteur propre** de T est un vecteur $v \neq 0$ tel que $T(v) = \lambda v$ pour un certain $\lambda \in \mathbb{K}$. Dans ce cas, λ est la **valeur propre** de v.*

*L'**espace propre** de T pour la valeur λ[28] est l'ensemble des vecteurs propres de T pour la valeur propre λ, et le vecteur nul.*

Définition 9.81.
*L'ensemble des valeurs propres de l'endomorphisme T est son **spectre** et est noté* $\mathrm{Spec}(T)$.

Remarque 9.82.
Le nombre zéro peut être une valeur propre ; c'est le vecteur zéro qui ne peut pas être vecteur propre. La matrice nulle est une matrice diagonalisable.

Lemme 9.83 ([260])**.**
Le spectre d'une matrice est égal au spectre de sa transposée : $\mathrm{Spec}(T) = \mathrm{Spec}(T^t)$.

Démonstration. Nous savons que T est inversible si et seulement si T^t l'est parce que si $TS = \mathbb{1}$ alors $S^tT^t = \mathbb{1}$. Nous avons équivalence entre les énoncés suivants :

- λ est une valeur propre de T
- il existe v tel que $(T - \lambda\mathbb{1})v = 0$
- $T - \lambda\mathbb{1}$ n'est pas inversible
- $(T^t - \lambda\mathbb{1})$ n'est pas inversible
- il existe w tel que $T^tw = \lambda w$.
- λ est valeur propre de T^t.

□

Lemme 9.84.
Soient un espace vectoriel E, un endomorphisme $T \in \mathrm{End}(E)$, ainsi que ses sous-espaces propres $\{E_\lambda\}_{\lambda \in \mathrm{Spec}(T)}$. Toute somme finie de la forme

$$E_{\lambda_1} + \ldots + E_{\lambda_p} \tag{9.165}$$

28. Nous laissons au lecteur le soin de vérifier que c'est bien un sous-espace vectoriel de E.

est directe[29].

Démonstration. Nous utilisons le lemme 4.137. Soient $v_i \in E_{\lambda_i}$ un choix de vecteurs tels que

$$\sum_{i=1}^{p} v_i = 0. \tag{9.166}$$

Soit un entier j_0 entre 1 et p. Nous allons montrer que $v_{j_0} = 0$. Pour cela nous remarquons d'abord que, pour tout $i \neq j_0$,

$$\prod_{k\neq j_0} (\lambda_i - \lambda_k) = 0. \tag{9.167}$$

Nous appliquons l'opérateur $\prod_{k\neq j_0}(T - \lambda_k \mathbb{1})$ à l'égalité (9.166) :

$$0 = \sum_{i=1}^{p} \prod_{k\neq j_0} (T - \lambda_k)v_i \tag{9.168a}$$

$$= \sum_{i=1}^{p} \prod_{k\neq j_0} (\lambda_i - \lambda_k)v_i \tag{9.168b}$$

$$= \prod_{k\neq j_0} (\lambda_{j_0} - \lambda_k)v_{j_0}. \tag{9.168c}$$

Justifications.

— Pour (9.168b). Pour chaque k et i nous avons $(T - \lambda_k)v_i = Tv_i - \lambda_k v_i = \lambda_i v_i - \lambda_k v_i$ parce que v_i est un vecteur propre de T pour la valeur propre λ_i.

— Pour (9.168c). Dans la somme, seul le terme $i = j_0$ est non nul, à cause de (9.167).

Donc $v_{j_0} = 0$ parce que le produit $\prod_{k\neq j_0}(\lambda_{j_0} - \lambda_k)$, lui, est non nul. □

9.6 Polynômes d'endomorphismes

Soit A un anneau commutatif et $\mathbb{K}$, un corps commutatif. L'injection canonique $A \to A[X]$ se prolonge en une injection

$$\mathbb{M}(A) \to \mathbb{M}\big(A[X]\big). \tag{9.169}$$

9.6.1 Polynômes d'endomorphismes

Soit $u \in \mathrm{End}(E)$ où E est un $\mathbb{K}$-espace vectoriel. Nous considérons l'application

$$\begin{aligned} \varphi_u \colon \mathbb{K}[X] &\to \mathrm{End}(E) \\ P &\mapsto P(u). \end{aligned} \tag{9.170}$$

L'image de φ_u est un sous-espace vectoriel. En effet si $A = \varphi_u(P)$ et $B = \varphi_u(Q)$, alors $A + B = \varphi_u(P + Q)$ et $\lambda A = (\lambda P)(u)$. En particulier c'est un espace fermé.

Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E et P, un polynôme. Nous disons que P est un polynôme **annulateur** de u si $P(u) = 0$ en tant qu'endomorphisme de E.

Lemme 9.85.
Si P et Q sont des polynômes dans $\mathbb{K}[X]$ et si u est un endomorphisme d'un $\mathbb{K}$-espace vectoriel E, nous avons

$$(PQ)(u) = P(u) \circ Q(u). \tag{9.171}$$

29. Définition 4.135.

Démonstration. Si $P = \sum_i a_i X^i$ et $Q = \sum_j b_j X^j$, alors le coefficient de X^k dans PQ est

$$\sum_l a_l b_{k-l}. \tag{9.172}$$

Par conséquent $(PQ)(u)$ contient $\sum_l a_l b_{k-l} u^k$. Par ailleurs $P(u) \circ Q(u)$ est donné par

$$\sum_i a_i u^i \left(\sum_j b_j u^j \right)(x) = \sum_{ij} a_i b_j u^{i+j}(x). \tag{9.173}$$

Le coefficient du terme en u^k est bien le même que celui donné par (9.172). □

Théorème 9.86 (Décomposition des noyaux ou lemme des noyaux[261])**.**
Soit u un endomorphisme du $\mathbb{K}$-espace[30] *vectoriel E. Soit $P \in \mathbb{K}[X]$ un polynôme tel que $P(u) = 0$. Nous supposons que P s'écrive comme le produit $P = P_1 \dots P_n$ de polynômes deux à deux étrangers*[31]*. Alors*

(1)
$$E = \ker P_1(u) \oplus \dots \oplus \ker P_n(u). \tag{9.174}$$

(2) En posant $Q_i = \prod_{j \neq i} P_j$, il existe des polynômes R_i tels que $R_1 Q_1 + \dots + R_n Q_n = 1$

(3) Les projecteurs sur $\ker\big(P_j(u)\big)$ sont donnés par

$$\texttt{proj}_{\ker(P_i(i))} = (R_i Q_i)(u). \tag{9.175}$$

Démonstration. Dans ce qui suit, nous allons beaucoup utiliser le fait que $\mathbb{K}[X]$ soit commutatif (lemme 1.357). Nous posons

$$Q_i = \prod_{j \neq i} P_j. \tag{9.176}$$

(i) **Utilisation de Bézout** Par le lemme 6.48 ces polynômes sont étrangers entre eux et le théorème de Bézout (théorème 6.47) donne l'existence de polynômes R_i tels que

$$R_1 Q_1 + \dots + R_n Q_n = 1. \tag{9.177}$$

(ii) **Une première somme, pas directe** Si nous appliquons cette égalité à u et ensuite à $x \in E$ nous trouvons

$$\sum_{i=1}^{n} (R_i Q_i)(u)(x) = x, \tag{9.178}$$

et en particulier si nous posons $E_i = \text{Image}\big(R_i Q_i(u)\big)$ nous avons

$$E = \sum_{i=1}^{n} E_i. \tag{9.179}$$

Cette dernière somme n'est éventuellement pas une somme directe.

(iii) **$Q_i Q_j$ est multiple de P** Si $i \neq j$, en utilisant la commutativité de $\mathbb{K}[X]$,

$$Q_i Q_j = \left(\prod_{k \neq i} P_k \right) \left(\prod_{l \neq j} P_l \right) = \Big(\prod_{\substack{k \neq i \\ k \neq j}} P_k \Big) P_j \left(\prod_{l \neq j} P_l \right) = \prod_{\substack{k \neq i \\ k \neq j}} P_k \prod_k P_l = S_{ij} P, \tag{9.180}$$

où S_{ij} est un polynôme. Nous voyons que $Q_i Q_j$ est multiple de P.

30. Le corps $\mathbb{K}$ est commutatif comme tous les corps dans le Frido.
31. Définition 3.106.

(iv) **Une somme directe** Toujours avec $i \neq j$, en utilisant le lemme 9.85,

$$(R_iQ_i)(u) \circ (R_jQ_j)(u) = \big(R_iQ_iR_jQ_j\big)(u) = \big(R_iR_j \underbrace{Q_iQ_j}_{=S_{ij}P}\big)(u) = (R_iR_jS_{ij})(u) \circ P(u) = 0 \tag{9.181}$$

Nous pouvons voir E comme un $\mathbb{K}$-module et appliquer le théorème 1.337. Les opérateurs $R_iQ_i(u)$ ont l'identité comme somme et sont orthogonaux, et nous avons donc la décomposition en somme directe :

$$E = \bigoplus_{i=1}^{n} R_iQ_i(u)E. \tag{9.182}$$

(v) $R_iQ_i(u)E \subset \ker P_i(u)$ Attention : utilisation massive du lemme 9.85. Un élément de $R_iQ_i(u)E$ est de la forme $(R_iQ_i)(u)x$ avec $x \in E$. Nous appliquons l'endomorphisme $P_i(u)$ à cet élément, et nous vérifions que nous obtenons zéro :

$$\begin{aligned}
P_i(u)\big((R_iQ_i)(u)x\big) &= (P_iR_iQ_i)(u)x && \text{(9.183a)}\\
&= (R_i \underbrace{P_iQ_i}_{=P})(u)x && \text{(9.183b)}\\
&= (R_iP)(u)x && \text{(9.183c)}\\
&= \big(R_i(u) \circ \underbrace{P(u)}_{=0}\big)x && \text{(9.183d)}\\
&= 0. && \text{(9.183e)}
\end{aligned}$$

Par conséquent $\text{Image}(R_iQ_i(u)) \subset \ker P_i(u)$.

(vi) **Et la somme qu'il nous fallait** Le fait que la somme (9.182) soit directe n'est en fait pas crucial. En effet, vu que chacun des termes est inclus dans $\ker P_i(u)$, nous avons la somme (pas directe à priori)

$$E = \sum_{i=1}^{n} R_iQ_i(u)E \subset \sum_{i=1}^{n} \ker P_i(u). \tag{9.184}$$

Mais cette fois, nous prouvons qu'elle est directe en utilisant la caractérisation du lemme 4.137(4). Supposons que, pour un certain k,

$$x \in \ker P_k(u) \cap \Big(\sum_{j\neq k} \ker P_j(u)\Big). \tag{9.185}$$

Nous allons montrer que $x = 0$.

(i) $Q_i(u)x = 0$ **si** $i \neq k$ Si $i \neq k$, nous avons

$$Q_i(u)x = \Big(\prod_{\substack{j\neq i\\ j\neq k}} P_j\Big)P_k(u)x = 0 \tag{9.186}$$

parce que $x \in \ker P_k(u)$.

(ii) $Q_k(u)x = 0$ Nous savons qu'il existe $z_l \in \ker P_l(u)$ tel que $x = \sum_{l\neq k} z_l$. Nous avons alors

$$Q_k(u)x = \Big(\prod_{j\neq k} P_j\Big)\sum_{l\neq k} z_l = \sum_{l\neq k}\Big(\prod_{j\neq k} P_j(u)\Big)z_l = 0 \tag{9.187}$$

parce que parmi les $P_j(u)$ $(j \neq k)$, il y a $P_l(u)$ qui annule z_l.

(iii) **Et finalement** Nous avons prouvé que $Q_i(u)x = 0$ pour tout i. La formule de Bézout (9.177) donne alors

$$\sum_i R_i \subset Q_i(u)x_{=0} = x \tag{9.188}$$

et donc $x = 0$.

(vii) **Les projecteurs**

□

9.87.
Ce résultat est utilisé pour prouver que toute représentation est décomposable en représentations irréductibles, proposition 16.10 ainsi que pour le théorème 9.211 qui dit que si le polynôme minimal d'un endomorphisme est scindé à racine simple alors il est diagonalisable.

Corolaire 9.88.
Soit E, un $\mathbb{K}$-espace vectoriel de dimension finie et f, un endomorphisme semi-simple dont la décomposition du polynôme minimal μ_f en facteurs irréductibles sur $\mathbb{K}[X]$ est $\mu_f = M_1^{\alpha_1}\cdots M_r^{\alpha_r}$. Si F est un sous-espace stable par f, alors

$$F = \bigoplus_{i=1}^{r} \ker M_i^{\alpha_i}(f) \cap F \tag{9.189}$$

Démonstration. Nous posons $E_i = \ker M_i^{\alpha_i}(f)$ et $F_i = E_i \cap F$. Les polynômes $M_i^{\alpha_i}$ sont deux à deux étrangers et $\mu_f(f) = 0$, donc le lemme des noyaux (9.86) s'applique et

$$E = E_1 \oplus \ldots \oplus E_r. \tag{9.190}$$

Nous pouvons décomposer $x \in F$ en termes de cette somme :

$$x = x_1 + \cdots + x_r \tag{9.191}$$

avec $x_i \in E_i$. Toujours selon le lemme des noyaux, les projections sur les espaces E_i sont des polynômes en f. Par conséquent F est stable sous toutes ces projections $\texttt{proj}_i\colon E \to E_i$, et en appliquant $\texttt{proj}_i$ à (9.191), $\texttt{proj}_i(x) = x_i$. Puisque $x \in F$, le membre de gauche est encore dans F et $x_i \in E_i \cap F$. Nous avons donc

$$F \subset \bigoplus_{i=1}^{r} F_i. \tag{9.192}$$

L'inclusion inverse est immédiate parce que $F_i \subset F$ pour chaque i. □

Lemme 9.89.
Si x est un vecteur propre de valeur propre λ pour l'endomorphisme u et si P est un polynôme, alors x est vecteur propre de $P(u)$ pour la valeur propre $P(\lambda)$.

Démonstration. C'est un simple calcul de $P(u)x$ en ayant noté [32] $P(X) = \sum_{k=0}^{n} c_k X^n$:

$$P(u)x = \sum_{k=0}^{n} c_k u^k(x) = \sum_{k=0}^{n} c_k \lambda^k x = P(\lambda)x. \tag{9.193}$$

□

9.6.2 Polynôme minimal et minimal ponctuel

Nous avons déjà vu la définition de polynôme minimal en 6.64. Le lemme suivant permet de parler de polynôme minimal d'endomorphisme.

Lemme 9.90 ([1])**.**
Si E est un $\mathbb{K}$-espace vectoriel, l'ensemble $\mathrm{End}(E)$ des endomorphismes de E est une extension du corps $\mathbb{K}$.

32. En complète violation de ce qu'on disait dans 1.358.

Lemme 9.91.
Soit un endomorphisme $f : E \to E$ d'un $\mathbb{K}$-espace vectoriel de dimension finie. Il existe un unique polynôme annulateur unitaire de degré minimum[33].

Tout endomorphisme de $\mathbb{K}$-espace vectoriel de dimension finie possède un polynôme minimal[34].

Démonstration. Pour l'unicité, soient P et Q deux polynômes annulateurs de f de même degré minimum N et ayant tous deux 1 comme coefficient de x^N. Alors $P-Q$ est de degré $N-1$ tout en étant encore annulateur. Vu que nous avions dit que N était le degré minimum, le seul polynôme annulateur de degré $N-1$ est le polynôme nul. Donc $P-Q=0$.

Pour l'existence, les endomorphismes Id, f, f^2, ...ne peuvent pas être tous linéairement indépendants parce que la dimension de $\mathrm{End}(E)$ est finie. Il existe donc un nombre N et des coefficients a_k tels que $\sum_{k=0}^{N} a_k f^k = 0$. Le polynôme $P(X) = \sum_{k=0}^{N} a_k X^k$ est donc annulateur de f.

Une autre façon de le dire est que l'application linéaire $\varphi : \mathbb{K}[X] \to \mathrm{End}(E)$ donnée par $\varphi(P) = P(f)$ est un endomorphisme d'un espace vectoriel de dimension infinie vers un espace vectoriel de dimension finie. Il ne peut donc pas être injectif et possède donc un noyau non réduit à zéro.

L'existence d'un polynôme minimal est maintenant seulement dû au fait que, avec les notations de la définition 6.64, l'idéal I_f n'est pas réduit à $\{0\}$. □

Remarque 9.92.
La preuve donnée ci-dessus montre que $\deg(\mu) \leqslant \dim(E)^2$. Comme conséquence du théorème de Cayley-Hamilton 9.115 nous verrons qu'en réalité le degré du polynôme minimal est majoré par la dimension de l'espace.

Proposition 9.93 (Exemple en dimension infinie[1])**.**
L'endomorphisme de dérivation sur l'espace des fonctions dérivables $\mathbb{R} \to \mathbb{R}$ n'a pas de polynôme minimal.

Dans la suite, l'endomorphisme f du $\mathbb{K}$-espace vectoriel E de dimension n est fixé. Pour $x \in E$ nous notons

$$E_x = \{P(f)x \text{ tel que } P \in \mathbb{K}[X]\}. \tag{9.194}$$

Nous considérons le morphisme d'algèbres

$$\begin{aligned} \varphi : \mathbb{K}[X] &\to \mathrm{End}(E) \\ P &\mapsto P(f) \end{aligned} \tag{9.195}$$

et si $x \in E$ est donné nous considérons le morphisme de $\mathbb{K}$-espaces vectoriels

$$\begin{aligned} \varphi_x : \mathbb{K}[X] &\to E \\ P &\mapsto P(f)x. \end{aligned} \tag{9.196}$$

Les noyaux de ces applications sont des idéaux, entre autres par le lemme 9.85. Ils ont donc un unique générateur unitaire (chacun) par le théorème 6.43. En termes de vocabulaire, l'ensemble

$$\ker(\varphi) = \{P \in \mathbb{K}[X] \text{ tel que } P(f) = 0\} \tag{9.197}$$

est l'**idéal annulateur** de f et un polynôme P tel que $P(f) = 0$ est un polynôme annulateur de f.

Proposition-Définition 9.94.
La partie $\ker(\varphi_x)$ est un idéal de $\mathbb{K}[X]$ qui possède un unique générateur unitaire.

Le générateur unitaire de $\ker(\varphi_x)$ est le ***polynôme minimal ponctuel*** *de f en x. Il sera noté $\mu_{f,x}$ ou μ_x lorsque la dépendance en f est claire dans le contexte.*

33. Degré minimum au sens où il existe peut-être d'autres polynômes annulateurs, mais ils seront de degré plus élevé.
34. Définition 6.64.

Nous notons μ le générateur unitaire du noyau de φ et μ_x celui de φ_x. Puisque $\mu \in \ker(\varphi_x)$ pour tout x nous avons $\mu_x \mid \mu$ pour tout x.

Exemple 9.95 (Pas en dimension infinie)**.**
En dimension infinie, il n'y a pas toujours de polynôme annulateur. Si E est un espace vectoriel de dimension infinie ayant une base dénombrable $\{e_i\}_{i\in\mathbb{N}}$ alors l'opérateur donné par $f(e_i) = e_{i+1}$ n'a pas de polynôme annulateur. Même pas ponctuel en quel que point que ce soit.

De même l'opérateur donné par $g(e_1) = 0$ et $g(e_i) = e_{i-1}$ si $i \neq 1$ n'a pas de polynôme annulateur, mais il a un polynôme annulateur ponctuel évident en $x = e_1$. L'exemple 15.90 donnera un habillage à peine subtil à cet exemple. △

Proposition 9.96.
Si P est un polynôme tel que $P(f) = 0$, alors le polynôme minimal μ_f divise P. Autrement dit, le polynôme minimal engendre l'idéal des polynômes annulateurs.

Démonstration. L'ensemble $\ker(\varphi) = \{Q \in \mathbb{K}[X] \text{ tel que } Q(f) = 0\}$ est un idéal par le lemme 9.85. Le polynôme minimal de f est un élément de degré plus bas dans I et par conséquent $I = (\mu_f)$ par le théorème 6.43. Nous concluons que μ_f divise tous les éléments de I. □

La proposition suivante permet de caractériser le polynôme minimal.

Proposition 9.97 ([127])**.**
Soit une application linéaire f sur un $\mathbb{K}$-espace vectoriel. Il existe un unique polynôme unitaire[35] *$P \in \mathbb{K}[X]$ tel que*

(1) $P(f) = 0$;

(2) l'application

$$\begin{aligned}\varphi\colon \frac{\mathbb{K}[X]}{(P)} &\to \mathrm{End}(E)\\ \bar{Q} &\mapsto Q(f)\end{aligned} \tag{9.198}$$

est injective.

Démonstration. En ce qui concerne l'existence, il existe le polynôme minimal de f qui satisfait les conditions. Pour l'unicité nous y travaillons maintenant.

Supposons que l'application (9.198) soit injective. Alors pour tout $Q \in \mathbb{K}[X]$ tel que $Q(f) = 0$ nous avons $\bar{Q} = 0$, c'est-à-dire $Q = PR$ pour un certain $R \in \mathbb{K}[X]$. Autrement dit : P est un générateur unitaire de l'idéal annulateur de f. Le théorème 6.43(3) nous dit alors que $P = \mu$ parce que μ est également générateur unitaire. □

Lemme 9.98 ([262])**.**
Soit $f\colon E \to E$ un endomorphisme de l'espace vectoriel E. Il existe un élément $x \in E$ tel que $\mu_{f,x} = \mu_f$.

Démonstration. Soit une décomposition en irréductibles du polynôme minimal $\mu = P_1^{\alpha_1} \dots P_r^{\alpha_r}$. Nous notons $E_i = \ker\big(P_i^{\alpha_i}(f)\big)$. Les polynômes P_i sont étrangers deux à deux (un diviseur commun aurait a fortiori été un diviseur et aurait contredit l'irréductibilité). Le lemme des noyaux 9.86 nous donne la somme directe

$$E = \bigoplus_{i=1}^{r} \ker\big(P_i^{\alpha_i}(f)\big). \tag{9.199}$$

Si $x_i \in E_i$ alors μ_{x_i} est une puissance de P_i. En effet $\mu_{x_i} \mid \mu$ et est donc un produit des puissances des P_j. Or si $(QP_j)(f)x_i = 0$ alors $(P_jQ)(f)x_i = 0$, ce qui donne $Q(f)x_i \in E_j \cap E_i = \{0\}$ si $j \neq i$. Donc μ_{x_i} n'est pas de la forme QP_j pour $j \neq i$. Nous en déduisons que μ_{x_i} est une puissance de P_i dès que $x_i \in E_i$. Nous choisissons $x_i \in E_i$ tel que $\mu_{x_i} = P_i^{\alpha_i}$.

35. À mon avis, « unitaire » manque dans [127].

Nous posons enfin $a = x_1 + \cdots + x_r$; par définition du polynôme annulateur μ_a, nous avons

$$0 = \mu_a(f)a = \mu_a(f)x_1 + \cdots + \mu_a(f)x_r. \tag{9.200}$$

Mais $\mu_a(f)x_i \in E_i$, et la somme des E_i est directe, donc l'annulation de la somme (9.200) implique l'annulation de chacun des termes : $\mu_a(f)x_i = 0$ pour tout i. Cela prouve que $\mu_{x_i} \mid \mu_a$. Mais comme les μ_{x_i} sont premiers deux à deux (parce que ce sont les $P_i^{\alpha_i}$), nous concluons que le produit divise encore μ_a :

$$\prod_{i=1}^{r} \mu_{x_i} \mid \mu_a, \tag{9.201}$$

c'est-à-dire $\mu \mid \mu_a$. Comme nous avons aussi $\mu_a \mid \mu$, nous déduisons $\mu_a = \mu$. □

Définition 9.99 (Matrices, endomorphismes et vecteurs cycliques)**.**
Une matrice est ***cyclique*** *si elle est semblable à une matrice compagnon. Un endomorphisme $f : E \to E$ est* ***cyclique*** *si il existe un vecteur $x \in E$ tel que $\{f^k(x)\}_{k=0,\dots,n-1}$ est une base de E. Un vecteur ayant cette propriété est un* ***vecteur cyclique*** *pour f.*

Lemme 9.100.
Soit E un espace vectoriel de dimension finie et un endomorphisme cyclique[36] *f de E. Soit un vecteur cyclique v de f, alors le polynôme minimal de f est égal au polynôme minimal de f au point v : $\mu_f = \mu_{f,v}$.*

Démonstration. Montrons que $\mu_{f,v}$ est un polynôme annulateur de f, ce qui prouvera que μ_f divise $\mu_{f,v}$ par la proposition 9.96. Étant donné que v est cyclique, tout élément de E s'écrit sous la forme $x = Q(f)v$. Prenons un polynôme P annulateur de f en v : $P(f)v = 0$. Nous montrons que P est alors un polynôme annulateur de f. En effet, nous avons

$$P(f)x = \big(P(f) \circ Q(f)\big)v = \big(Q(f) \circ P(f)\big)v = 0 \tag{9.202}$$

où nous avons utilisé le lemme 9.85. □

Lemme 9.101 ([262])**.**
Soit $a \in E$ un vecteur cyclique pour f, tel que $\mu_a = \mu$. Alors E_a est un sous-espace stable par f pour lequel il existe un supplémentaire stable.

Démonstration. Soit $l = \deg(\mu) = \deg(\mu_a)$. L'espace E_a étant engendré par les $f^k(a)$ nous savons que $e_1 = a$, $e_2 = f(a)$,..., $e_l = f^{l-1}(a)$ forment une base de E_a. Nous pouvons la compléter en une base $\{e_1, \dots, e_n\}$ de E. Et nous posons[37]

$$G = \{x \in E \text{ tel que } e_l^*\big(f^k(x)\big) = 0, \forall k \geqslant 0\} \tag{9.203a}$$
$$= \bigcap_{k \geqslant 0} \ker\{e_l^* \circ f^k\} \tag{9.203b}$$
$$= \bigcap_{k=0}^{l-1} \ker(e_l^* \circ f^k). \tag{9.203c}$$

La dernière égalité est due au fait que l soit le degré de μ. Du coup f^l est une combinaison linéaire des f^i avec $i \leqslant l-1$.

Nous avons $f(G) \subset G$ et de plus $E_a \cap G = \{0\}$ parce qu'un élément de E_a est une combinaison linéaire d'éléments de la forme $f^j(a)$ $(j \leqslant l)$. Après application de f^{l-j}, ces éléments obtiennent une composante $f^l(a) = e_l$. De plus G est un sous-espace vectoriel du fait que $e_l^* \circ f^i$ est une application linéaire.

36. Voir la définition 9.99.
37. ici, comme presque partout, e_l^* est le dual de e_l, c'est-à-dire l'application linéaire sur E donnée par $e_l^*(e_i) = \delta_{li}$, voir la définition 4.124.

Montrons enfin que $\dim(G) = n - l$. Pour cela nous remarquons que G est une intersection d'hyperplans, et nous montrons que les équations définissant ces hyperplans sont linéairement indépendantes. Soit donc

$$\sum_{j=0}^{l-1} \lambda_j \big(e_l^* \circ f^j\big) = 0 \tag{9.204}$$

et montrons que $\lambda_j = 0$ pour tout j est l'unique solution. Soit $x \in E$ et appliquons l'opération (9.204) au vecteur $f^i(x)$; le résultat est zéro :

$$0 = \sum_{j=0}^{l-1} \lambda_j (e_l^* \circ f^i \circ f^j) = (e_l^* \circ f^i) P(u) \tag{9.205}$$

où nous avons posé $P(X) = \sum_{j=0}^{l-1} \lambda_j X^j$. Appliquons cela à a : pour tout i nous avons

$$(e_l^* \circ f^i)\big(P(f)a\big) = 0. \tag{9.206}$$

Mais par définition de E_a, l'élément $P(f)a$ est dans E_a. Nous en déduisons que

$$P(f)a \in G \cap E_a = \{0\}, \tag{9.207}$$

c'est-à-dire que P est un polynôme annulateur de a. Mais P est de degré $l-1$ alors que le polynôme minimal de a est de degré l. Par conséquent $P = 0$ et $\lambda_j = 0$ pour tout j. □

Définition 9.102.
*L'endomorphisme f d'un espace vectoriel est **semi-simple** si tout sous-espace stable par f possède un supplémentaire stable.*

Lemme 9.103.
Si le polynôme minimal d'un endomorphisme est irréductible, alors cet endomorphisme est semi-simple[38].

Démonstration. Soit f, un endomorphisme dont le polynôme minimal est irréductible et F, un sous-espace stable par f. Nous devons en trouver un supplémentaire stable. Si $F = E$, il n'y a pas de problème. Sinon nous considérons $u_1 \in E \backslash F$ et

$$E_{u_1} = \{P(f)u_1 \text{ tel que } P \in \mathbb{K}[X]\}, \tag{9.208}$$

qui est un espace stable par f.

Montrons que $E_{u_1} \cap F = \{0\}$. Pour cela nous étudions l'idéal

$$I_{u_1} = \{P \in \mathbb{K}[X] \text{ tel que } P(f)u_1 = 0\}. \tag{9.209}$$

C'est un idéal non réduit à $\{0\}$ parce que le polynôme minimal de f par exemple est dans I_{u_1}. Soit P_{u_1} un générateur unitaire de I_{u_1}. Étant donné que $\mu_f \in I_{u_1}$, nous avons P_{u_1} divise μ_f et donc, $P_{u_1} = \mu_f$, parce que μ_f est irréductible par hypothèse.

Soit $y \in E_{u_1} \cap F$. Par définition il existe $P \in \mathbb{K}[X]$ tel que $y = P(f)u_1$ et si $y \neq 0$, cela signifie que $P \notin I_{u_1}$, c'est-à-dire que P_{u_1} ne divise pas P. Étant donné que P_{u_1} est irréductible cela implique que P_{u_1} et P sont premiers entre eux (ils n'ont pas d'autre pgcd que 1).

Nous utilisons maintenant des coefficient de Bézout (théorème 6.47) $A, B \in \mathbb{K}[X]$ tels que

$$AP + BP_{u_1} = 1. \tag{9.210}$$

Nous appliquons cette égalité à f et puis à u_1 :

$$u_1 = A(f) \circ \underbrace{P(f)u_1}_{=y} + B(f) \circ \underbrace{P_{u_1}(f)u_1}_{=0} = A(f)y. \tag{9.211}$$

38. Définition 9.102.

Mais $y \in F$, donc $A(f)y \in F$. Nous aurions donc $u_1 \in F$, ce qui est impossible par choix. Nous savons maintenant que l'espace $E_{u_1} \oplus F$ est stable sous f. Si cet espace est E alors nous arrêtons. Sinon nous reprenons le raisonnement avec $E_{u_1} \oplus F$ en guise de F et en prenant $u_2 \in E\backslash(E_{u_1} \oplus F)$. Étant donné que E est de dimension finie, ce procédé s'arrête à un certain moment et nous aurons

$$E = F \oplus E_{u_1} \oplus \ldots \oplus E_{u_k} \tag{9.212}$$

où chacun des E_{u_i} sont stables. □

Théorème 9.104.
Un endomorphisme est semi-simple si et seulement si son polynôme minimal est produit de polynômes irréductibles distincts deux à deux.

Démonstration. Supposons que f soit semi-simple et que son polynôme minimal soit donné par $\mu_f = M_1^{\alpha_1} \ldots M_r^{\alpha_r}$ où les M_i sont des polynômes irréductibles deux à deux distincts. Nous devons montrer que $\alpha_i = 1$ pour tout i. Soit i tel que $\alpha_i \geqslant 1$ et $N \in \mathbb{K}[X]$ tel que $\mu_f = M^2N$ où l'on a noté $M = M_i$. Nous étudions l'espace

$$F = \ker M(f) \tag{9.213}$$

qui est stable par f, et qui possède donc un supplémentaire S également stable par f. Nous allons montrer que MN est un polynôme annulateur de f.

D'abord nous prenons $x \in S$. Étant donné que F est le noyau de $M(f)$,

$$M(f)\big(MN(f)x\big) = \mu_f(f)x = 0, \tag{9.214}$$

ce qui signifie que $MN(f)x \in F$. Mais puisque S est stable par f nous avons aussi $MN(f)x \in S$. Finalement $MN(f)x \in F \cap S = \{0\}$. Autrement dit, $MN(f)$ s'annule sur S.

Prenons maintenant $y \in F$. Nous avons

$$MN(f) = N(f)\big(M(f)y\big) = 0 \tag{9.215}$$

parce que $y \in F = \ker M(f)$.

Nous avons prouvé que $MN(f)$ s'annule partout et donc que $MN(f)$ est un polynôme annulateur de f, ce qui contredit la minimalité de $\mu_f = M^2N$.

Nous passons au sens inverse. Soit $m_f = M_1 \ldots M_r$ une décomposition du polynôme minimal de l'endomorphisme f en irréductibles distincts deux à deux. Soit F un sous-espace vectoriel stable par f. Nous notons

$$E_i = \ker(M_i(f)) \tag{9.216}$$

et $f_i = f|_{E_i}$. Par le lemme 9.88 nous avons

$$F = \bigoplus_{i=1}^{r}(F \cap E_i). \tag{9.217}$$

Les espaces E_i sont stables par f et étant donné que M_i est irréductible, il est le polynôme minimal de f_i. En effet, M_i est annulateur de f_i, ce qui montre que le polynôme minimal de f_i divise M_i. Mais M_i étant irréductible, M_i est le polynôme minimal. Étant donné que $\mu_{f_i} = M_i$, l'endomorphisme f_i est semi-simple par le lemme 9.103.

L'espace $F \cap E_i$ étant stable par l'endomorphisme semi-simple f_i, il possède un supplémentaire stable que nous notons S_i :

$$E_i = S_i \oplus (F \cap E_i). \tag{9.218}$$

Étant donné que sur chaque S_i nous avons $f|_{S_i} = f_i$, l'espace $S = S_1 \oplus \ldots \oplus S_r$ est stable par f. Par conséquent, nous avons

$$\begin{aligned}
E &= E_1 \oplus \ldots \oplus E_r && \text{(9.219a)}\\
&= \big(S_1 \oplus (F \cap E_1)\big) \oplus \ldots \oplus \big(S_r \oplus (F \cap E_r)\big) && \text{(9.219b)}\\
&= \big(\bigoplus_{i=1}^{r} S_i\big) \oplus \big(\bigoplus_{i=1}^{r} F \cap E_i\big) && \text{(9.219c)}\\
&= S \oplus F, && \text{(9.219d)}
\end{aligned}$$

ce qui montre que F a bien un supplémentaire stable par f et donc que f est semi-simple. □

Exemple 9.105 (L'espace engendré par $\mathbb{1}$, A, A^2,...).
Soit A une matrice, et

$$E = \text{Span}\{A^k \text{ tel que } k \in \mathbb{N}\}. \tag{9.220}$$

Nous montrons que $\dim(E)$ est le degré du polynôme minimal de A.

D'abord l'idéal annulateur de A est engendré par le polynôme minimal[39] que nous notons $\mu = \sum_{k=0}^{p} a_k X^k$. La partie $\{\mathbb{1}, \dots, A^{p-1}\}$ est libre parce qu'une combinaison linéaire nulle de ces éléments serait un polynôme annulateur en A de degré plus petit que p. Donc $\dim(E) \geqslant p$.

La partie $\{\mathbb{1}, A, \dots, A^p\}$ est liée à cause du polynôme minimal. Isoler A^p dans $\mu(A) = 0$ donne un polynôme f de degré $p-1$ tel que $A^p = f(A)$.

Nous allons montrer à présent que la famille $\{\mathbb{1}, A, \dots, A^{p-1}\}$ est génératrice (alors $\dim(E) \leqslant p$). Soit un entier $q \geqslant p$ et de division euclidienne[40] $np + r = q$ avec $r < p$. Nous avons $A^q = A^{np}A^r$. D'une part

$$A^{np} = (A^p)^n = f(A)^n \tag{9.221}$$

est de degré $n(p-1)$. Par conséquent

$$A^q = f(A)^n A^r \tag{9.222}$$

qui est de degré $n(p-1)+r = q-n$. Autrement dit il existe un polynôme g_1 de degré $q-n$ tel que $A^q = g_1(A)$. Si $q-n > p-1$ alors nous pouvons recommencer et obtenir un polynôme g_2 de degré strictement inférieur à celui de g_1 tel que $A^q = g_2(A)$. Au bout du compte, il existe un polynôme g de degré au maximum $p-1$ tel que $A^q = g(A)$. Cela prouve que la partie $\{\mathbb{1}, A, \dots, A^{p-1}\}$ est génératrice de E.

La dimension de E est donc p, le degré du polynôme minimal. △

Proposition 9.106.
Soit f un endomorphisme d'un espace vectoriel de dimension finie. Nous avons l'isomorphisme d'espace vectoriel

$$\mathbb{K}[f] \simeq \frac{\mathbb{K}[X]}{(\mu_f)} \tag{9.223}$$

La dimension en est $\deg(\mu_f)$.

Démonstration. Notons avant de commencer que (μ) est l'idéal engendré par μ. Les classes dont il est question dans le quotient $\mathbb{K}[X]/(\mu)$ sont

$$\bar{P} = \{P + S\mu\}_{S \in \mathbb{K}[X]}. \tag{9.224}$$

Nous allons montrer que l'application suivante fournit l'isomorphisme :

$$\begin{aligned} \psi\colon \frac{\mathbb{K}[X]}{(\mu)} &\to \mathbb{K}[f] \\ \bar{P} &\mapsto P(f). \end{aligned} \tag{9.225}$$

(i) **ψ est bien définie** Si $Q \in \bar{P}$ alors $Q = P + S\mu$ pour un certain $S \in \mathbb{K}[X]$. Du coup nous avons

$$\psi(\bar{Q}) = P(f) + (S\mu)(f). \tag{9.226}$$

Mais $\mu(f) = 0$ donc le deuxième terme est nul. Donc $\psi(\bar{P})$ est bien défini.

(ii) **Injectif** Si $\psi(\bar{P}) = 0$ nous avons $P(f) = 0$, ce qui signifie que $P = S\mu$ pour un polynôme S. Par conséquent $P \in (\mu)$ et donc $\bar{P} = 0$.

(iii) **Surjectif** Soit $P \in \mathbb{K}[X]$. L'élément $P(f)$ de $\mathbb{K}[f]$ est dans l'image de ψ parce que c'est $\psi(\bar{P})$.

En ce qui concerne la dimension, le corolaire 6.44 en parle déjà : une base est donnée par les projections de $1, X, \dots, X^{\deg(\mu_f)-1}$. □

39. Proposition 9.96.
40. Théorème 1.215.

9.6.3 Polynôme caractéristique

Définition 9.107.
Soit un anneau commutatif A. Si $u \in \mathbb{M}(n, A)$, nous définissons le ***polynôme caractéristique de*** *u :*

$$\chi_u(X) = \det(u - X\mathbb{1}_n). \tag{9.227}$$

Nous définissons de même le polynôme caractéristique d'un endomorphisme $u\colon E \to E$.

Remarque 9.108.
Quelques remarques à propos du signe[41].

- Certains auteurs définissent le polynôme caractéristique par $\det(X-u)$ au lieu de $\det(u-X)$.
- Wikipédia francophone[263] prend la définition $\det(X-u)$ (donc opposée de la notre). Allez lire la page de discussion.
- Sur les wikipédias en d'autres langues, ça varie.
- Un avantage de $\det(u-X)$ est que $\det(u) = \chi_u(0)$.
- Un avantage de $\det(X-u)$ est qu'il est unitaire.

Lemme 9.109.
Le polynôme caractéristique χ_u est unitaire en dimension paire et a pour degré la dimension de l'espace vectoriel E.

Théorème 9.110.
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et un endomorphisme $u \in \mathrm{End}(E)$. Alors

(1) Le polynôme caractéristique divise $(\mu_u)^n$ dans $\mathbb{K}[X]$.
(2) Les polynômes caractéristiques et minimaux ont mêmes facteurs irréductibles dans $\mathbb{K}[X]$.
(3) Les polynômes caractéristiques et minimaux ont mêmes racines dans $\mathbb{K}[X]$.
(4) Le polynôme caractéristique est scindé si et seulement si le polynôme minimal est scindé.

Théorème 9.111.
Soit $u \in \mathrm{End}(E)$ et $\lambda \in \mathbb{K}$. Les conditions suivantes sont équivalentes

(1) $\lambda \in \mathrm{Spec}(u)$
(2) $\chi_u(\lambda) = 0$
(3) $\mu_u(\lambda) = 0$.

Démonstration. (1) $\Leftrightarrow$ (2). Dire que λ est dans le spectre de u signifie que l'opérateur $u - \lambda\mathbb{1}$ n'est pas inversible, ce qui est équivalent à dire que $\det(u - \lambda\mathbb{1})$ est nul par la proposition 9.10(1) ou encore que λ est une racine du polynôme caractéristique de u.

(2) $\Leftrightarrow$ (3). C'est une application directe du théorème 9.110 qui précise que le polynôme caractéristique a les mêmes racines dans $\mathbb{K}$ que le polynôme minimal. □

Exemple 9.112.
Sur $\mathbb{R}^2$, nous considérons la matrice $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ qui a pour polynôme caractéristique[42] le polynôme $\chi_A = (X-1)^2$. Le nombre $\lambda = 1$ est une racine double de ce polynôme, et pourtant il n'y a qu'une seule dimension d'espace propre :

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{9.228}$$

entraine $x = 0$.

Ici la multiplicité algébrique est différente de la multiplicité géométrique. △

41. Attention : je crois qu'il y a des incohérences dans le Frido à propos de ce choix
42. Définition 9.107.

La proposition suivante donne une utilisation amusante de la notion de polynôme caractéristique[43].

Proposition 9.113 ([264]).
Soit un espace vectoriel E de dimension finie pour lequel il existe un endomorphisme $f\colon E\to E$ tel que $(f\circ f)(x)=-x$ pour tout $x\in E$. Alors la dimension de E est paire.

Démonstration. Cherchons les valeurs propres de f en résolvant l'équation $f(x)=\lambda x$. Nous appliquons f à cette égalité :

$$-x=\lambda f(x)=\lambda^2 x. \tag{9.229}$$

Donc λ ne peut pas être réel. Nous avons montré que f n'a pas de valeur propre réelle. Or le polynôme caractéristique de f est de degré égal à la dimension. Si la dimension est impaire, le polynôme caractéristique est de degré impair, et possède donc une racine réelle. Autrement dit, l'absence de racines réelles au polynôme caractéristique indique une dimension paire. □

Une autre preuve possible est d'utiliser le déterminant : si la dimension de E est n nous avons :

$$\det(f^2)=\det(-\mathrm{Id})=(-1)^n. \tag{9.230}$$

Donc $(-1)^n$ est positif, ce qui montre que n est pair.

Proposition 9.114 ([265]).
Soit f, un endomorphisme de E et $x\in E$. Alors

(1) L'espace $E_{f,x}$ est stable par f.

(2) L'espace $E_{f,x}$ est de dimension

$$p_{f,x}=\dim E_{f,x}=\deg(\mu_{f,x}) \tag{9.231}$$

où $\mu_{f,x}$ est le générateur unitaire de $I_{f,x}$.

(3) Le polynôme caractéristique de $f|_{E_{f,x}}$ est $\mu_{f,x}$.

(4) Nous avons

$$\chi_{f|_{E_{f,x}}}(f)x=\mu_{f,x}(f)x=0. \tag{9.232}$$

Démonstration. Le fait que $E_{f,x}$ soit stable par f est classique. Le point (4) est une application du point (3). Les deux gros morceaux sont donc les points (2) et (3).

Étant donné que $\mu_{f,x}$ est de degré minimal dans $I_{f,x}$, l'ensemble

$$B=\{f^k(x)\text{ tel que }0\leqslant k\leqslant p_{f,x}-1\} \tag{9.233}$$

est libre. En effet une combinaison nulle des vecteurs de B donnerait un polynôme en f de degré inférieur à $p_{f,x}$ annulant x. Nous écrivons

$$\mu_{f,x}(X)=X^{p_{f,x}}-\sum_{i=0}^{p_{f,x}-1}a_iX^i. \tag{9.234}$$

Étant donné que $\mu_{f,x}(f)x=0$ et que la somme du membre de droite est dans $\mathrm{Span}(B)$, nous avons $f^{p_{f,x}}(x)\in\mathrm{Span}(B)$. Nous prouvons par récurrence que $f^{p_{f,x}+k}(x)\in\mathrm{Span}(B)$. En effet en appliquant f^k à l'égalité

$$0=f^{p_{f,x}}(x)-\sum_{i=0}^{p_{f,x}-1}a_if^i(x) \tag{9.235}$$

nous trouvons

$$f^{p_{f,x}+k}(x)=\sum_{i=0}^{p_{f,x}-1}a_if^{i+k}(x), \tag{9.236}$$

43. Définition 9.107.

alors que par hypothèse de récurrence le membre de droite est dans $\text{Span}(B)$. L'ensemble B est alors générateur de $E_{f,x}$ et donc une base d'icelui. Nous avons donc bien $\dim(E_{f,x}) = p_{f,x}$.

Nous montrons maintenant que $\mu_{f,x}$ est annulateur de f au point x. Nous savons que

$$\mu_{f,x}(f)x = 0. \tag{9.237}$$

En y appliquant f^k et en profitant de la commutativité des polynômes sur les endomorphismes (proposition 9.85), nous avons

$$0 = f^k\big(\mu_{f,x}(f)x\big) = \mu_{f,x}(f)f^k(x), \tag{9.238}$$

de telle sorte que $\mu_{f,x}(f)$ est nul sur B et donc est nul sur $E_{f,x}$. Autrement dit,

$$\mu_{f,x}\big(f|_{E_{f,x}}\big) = 0. \tag{9.239}$$

Montrons que $\mu_{f,x}$ est même minimal pour $f|_{E_{f,x}}$.

Supposons avoir Q, un polynôme non nul de degré $p_{f,x} - 1$ annulant $f|_{E_{f,x}}$. En particulier $Q(f)x = 0$. Cela signifie que B est un système lié, alors que nous avons montré que c'était un système libre. Contradiction. Nous concluons que $\mu_{f,x}$ est le polynôme minimal de $f|_{E_{f,x}}$. □

Cette histoire de densité permet de donner une démonstration alternative du théorème de Cayley-Hamilton.

Théorème 9.115 (Cayley-Hamlilton)**.**
Le polynôme caractéristique est un polynôme annulateur.

Une démonstration plus simple via la densité des diagonalisables est donnée en théorème 13.25.

Démonstration. Nous devons prouver que $\chi_f(f)x = 0$ pour tout $x \in E$. Pour cela nous nous fixons un $x \in E$, nous considérons l'espace $E_{f,x}$ et $\chi_{f,x}$, le polynôme caractéristique de $f|_{E_{f,x}}$. Étant donné que $E_{f,x}$ est stable par f, le polynôme caractéristique de $f|_{E_{f,x}}$ divise χ_f, c'est-à-dire qu'il existe un polynôme Q_x tel que

$$\chi_f = Q_x\chi_{f,x}, \tag{9.240}$$

et donc aussi

$$\chi_f(f)x = Q_x(f)\big(\chi_{f,x}(f)x\big) = 0 \tag{9.241}$$

parce que la proposition 9.114 nous indique que $\chi_{f,x}$ est un polynôme annulateur de $f|_{E_{f,x}}$. □

Corolaire 9.116.
Le degré du polynôme minimal est majoré par la dimension de l'espace.

Démonstration. Le polynôme minimal divise le polynôme caractéristique parce qu'il engendre l'idéal des polynômes annulateurs par la proposition 9.96. Or le degré du polynôme caractéristique est la dimension de l'espace par le lemme 9.109. □

Exemple 9.117 (Calcul de l'inverse d'un endomorphisme)**.**
Le théorème de Cayley-Hamilton donne un moyen de calculer l'inverse d'un endomorphisme inversible pourvu que l'on connaisse son polynôme caractéristique. En effet, supposons que

$$\chi_f(X) = \sum_{k=0}^{n} a_k X^k. \tag{9.242}$$

Nous aurons alors

$$0 = \chi_f(f) = \sum_{k=0}^{n} a_k f^k. \tag{9.243}$$

Nous appliquons f^{-1} à cette dernière égalité en sachant que $f^{-1}(0) = 0$:

$$0 = a_0 f^{-1} + \sum_{k=1}^{n} a_k f^{k-1}, \tag{9.244}$$

et donc

$$f^{-1} = -\frac{1}{\det(f)} \sum_{k=1}^{n} a_k f^{k-1} \tag{9.245}$$

où nous avons utilisé le fait que $a_0 = \chi_f(0) = \det(f)$. △

Proposition 9.118.
Si $(X-z)^l$ ($l \geqslant 1$) est la plus grande puissance de $(X-z)$ dans le polynôme caractéristique d'un endomorphisme f alors

$$1 \leqslant \dim(E_z) \leqslant l. \tag{9.246}$$

C'est-à-dire que nous avons au moins un vecteur propre pour chaque racine du polynôme caractéristique.

Démonstration. Si $(X-z)$ divise χ_f alors en posant $\chi_f = (X-z)P(X)$ nous avons

$$\det(f - X\mathbb{1}) = (X-z)P(X), \tag{9.247}$$

ce qui, évalué en $X = z$, donne $\det(f - z\mathbb{1}) = 0$. L'annulation du déterminant étant équivalente à l'existence d'un noyau non trivial, nous avons $v \neq 0$ dans E tel que $(f - z\mathbb{1})v = 0$. Cela donne $f(v) = zv$ et montre que v est vecteur propre de f pour la valeur propre z. Et aussi que $\dim(E_z) \geqslant 1$.

Si $\dim(E_z) = k$ alors le théorème de la base incomplète 4.13 nous permet d'écrire une base de E dont les k premiers vecteurs forment une base de E_z. Dans cette base, la matrice de f est de la forme

$$\begin{pmatrix} z & & & * \\ & \ddots & & \vdots \\ & & z & * \\ & & & * \end{pmatrix} \tag{9.248}$$

où les étoiles représentent des blocs à priori non nuls. En tout cas, sous cette forme, il est visible que $(X-z)^k$ divise χ_f. □

9.7 Formes bilinéaires et quadratiques

Plus à propos de formes bilinéaires dans le thème 16.

Définition 9.119 ([266]).
*Soient trois espaces vectoriels E, F et V sur le même corps commutatif $\mathbb{K}$. Une application $b\colon E \times F \to V$ est **bilinéaire** si elle est séparément linéaire en ses deux variables, c'est-à-dire si*

(1) $b(u_1 + u_2, v) = b(u_1, v) + b(u_2, v)$,

(2) $b(u, v_1 + v_2) = b(u, v_1) + b(u, v_2)$

(3) $b(\lambda u, v) = b(u, \lambda v) = \lambda b(u, v)$

pour tout $u, u_1, u_2 \in E$, $v, v_1, v_2 \in F$ et pour tout $\lambda \in \mathbb{K}$.

*(1) Dans le cas $E = F$ et $V = \mathbb{K}$, nous parlons de **forme bilinéaire** sur E.*

*(2) Nous parlons de forme bilinéaire **symétrique** si de plus $b(u, v) = b(v, u)$.*

Définition 9.120 ([267]).
*Soit un espace vectoriel E et $\mathbb{F}$ un corps de caractéristique différente de 2. Une **forme quadratique** sur E est une application $q\colon E \to \mathbb{F}$ pour laquelle il existe une forme bilinéaire symétrique $b\colon E \times E \to \mathbb{F}$ satisfaisant $q(x) = b(x, x)$ pour tout $x \in E$.*

L'ensemble des formes quadratiques réelles sur E est noté $Q(E)$.

La topologie sur $Q(E)$ sera la topologie métrique donnée dans le lemme 9.135.

Définition 9.121 (Application bilinéaire définie positive, thème 38)**.**
Si b est une application bilinéaire[44] *sur un espace vectoriel E nous disons qu'elle est*

(1) ***définie positive*** *si $b(x,x) \geqslant 0$ pour tout $x \in E$ et $b(x,x) = 0$ si et seulement si $x = 0$.*

(2) ***semi-définie positive*** *si $b(x,x) \geqslant 0$ pour tout $x \in E$. Nous dirons aussi parfois qu'elle est simplement « positive ».*

9.122.
Une application bilinéaire $E \times E \to \mathbb{K}$ n'est pas une application linéaire ; la distinction est importante. La linéarité est

$$b(\lambda u, \lambda v) = b\big(\lambda(u,v)\big) = \lambda b(u,v) \tag{9.249}$$

et la bilinéarité est

$$b(\lambda u, v) = b(u, \lambda v) = \lambda b(u,v). \tag{9.250}$$

En réalité la seule forme qui soit à la fois linéaire et bilinéaire est la forme identiquement nulle : la condition

$$b(\lambda u, \lambda v) = \lambda^2 b(u,v) = \lambda b(u,v) \tag{9.251}$$

pour tout $\lambda \in \mathbb{K}$ implique $b(u,v) = 0$.

Exemple 9.123 ([268])**.**
L'application

$$\begin{aligned} b\colon \mathbb{M}(n,\mathbb{K}) \times \mathbb{M}(n,\mathbb{K}) &\to \mathbb{K} \\ (A,B) &\mapsto \operatorname{Tr}(AB) \end{aligned} \tag{9.252}$$

est une forme bilinéaire symétrique.

La vérification est un calcul :

$$\operatorname{Tr}(BA) = \sum_i (BA)_{ii} = \sum_{ik} B_{ik}A_{ki} = \sum_{ik} A_{ki}B_{ik} = \sum_k (AB)_{kk} = \operatorname{Tr}(AB). \tag{9.253}$$

△

9.7.1 Dégénérescence d'une forme bilinéaire

Soit b, une forme bilinéaire symétrique non dégénérée sur l'espace vectoriel E de dimension n sur $\mathbb{K}$ où $\mathbb{K}$ est un corps de caractéristique différente de 2. Nous notons q la forme quadratique associée.

Définition 9.124.
Une forme bilinéaire est ***non dégénérée*** *si $b(x,z) = 0$ pour tout z implique $x = 0$.*

Lemme 9.125.
Soit b une forme bilinéaire non dégénérée. Si x et y sont tels que $b(x,z) = b(y,z)$ pour tout z, alors $x = y$.

Démonstration. C'est immédiat du fait de la linéarité en le premier argument et de la non-dégénérescence : si $b(x,z) - b(y,z) = 0$ alors

$$b(x-y,z) = 0 \tag{9.254}$$

pour tout z, ce qui implique $x - y = 0$. □

44. Définition 9.119.

9.7.2 Orthogonal pour une forme bilinéaire

Définition 9.126.
Soit in espace vectoriel E et une forme bilinéaire symétrique b. Si $A \subset E$ nous notons

$$A^\perp = \{z \in E \text{ tel que } b(z,x) = 0 \, \forall x \in A\}. \tag{9.255}$$

*C'est l'**orthogonal** de A par rapport à la forme b.*

Définition 9.127.
*Soit in espace vectoriel E et une forme bilinéaire symétrique b. Le **noyau** est la partie*

$$\ker(b) = \{z \in E \text{ tel que } b(z,x) = 0 \forall x \in E\}. \tag{9.256}$$

Proposition 9.128 ([269]).
Soit un espace vectoriel E sur le corps $\mathbb{K}$. Soit une forme bilinéaire symétrique b sur E. Si A et B sont des parties de E nous avons :

(1) $A^\perp$ est un sous-espace vectoriel.
(2) Si $A \subset B$ alors $B^\perp \subset A^\perp$.
(3) $A^\perp = \text{Span}(A)^\perp$.

Démonstration. Point par point.

(i) **Pour (1)** Soient $x, y \in A^\perp$, $a \in A$ et $\lambda \in \mathbb{K}$. Nous avons alors

$$b(x + \lambda y, a) = b(x,a) + \lambda b(y,a) = 0 \tag{9.257}$$

(ii) **Pour (2)** Soient $x \in B^\perp$ et $a \in A$. Nous avons $b(x,a) = 0$ parce que $a \in A \subset B$ et $x \in B^\perp$.

(iii) **Pour (3)** Deux inclusions à prouver.

(i) **Première inclusion** Nous avons $A \subset \text{Span}(A)$, donc le point (2) montre que $\text{Span}(A)^\perp \subset A^\perp$.

(ii) **Deuxième inclusion** Soit $x \in A^\perp$ et $y \in \text{Span}(A)$. Nous avons $y = \sum_i \lambda_i a_i$ pour certains $a_i \in A$ et $\lambda_i \in \mathbb{K}$. Alors

$$b(x,y) = \sum_i \lambda_i b(x, a_i) = 0. \tag{9.258}$$

□

Proposition 9.129 ([269]).
Soit un espace vectoriel E sur le corps $\mathbb{K}$. Soit une forme bilinéaire symétrique b sur E. Si V est un sous-espace de E, alors :

(1) Si $b_V : V \times V \to \mathbb{K}$ est la restriction de b, alors $V \cap V^\perp = \ker(b_V)$[45].
(2) $(V + W)^\perp = V^\perp \cap W^\perp$.
(3) $V \subset (V^\perp)^\perp$.

Démonstration. En plusieurs parties.

(i) **Pour (1)** En deux parties.

(i) $V \cap V^\perp \subset \ker(b_V)$ Soit $x \in V \cap V^\perp$. Si $v \in V$, nous avons $b(x,v) = 0$ parce que $x \in V^\perp$.

(ii) $\ker(b_V) \subset V \cap V^\perp$ Soit $x \in \ker(b_V)$. Nous avons $x \in V$ parce que $x \in \ker(b_V) \subset V$. Pour montrer que $x \in V^\perp$ nous considérons $y \in V$ et nous remarquons que $b(x,y) = 0$ parce que $x \in V^\perp$.

(ii) **Pour (2)** En deux parties.

45. Définition du noyau de b, définition 9.127.

(i) $\underline{(V+W)^\perp \subset V^\perp \cap W^\perp}$ Soit $x \in (V+W)^\perp$. Si $v \in V$, alors $v \in V+W$, donc $f(x,v)=0$. Cela prouve que $x \in V^\perp$. Nous prouvons que $x \in W^\perp$ de même.

(ii) $\underline{V^\perp \cap W^\perp \subset (V+W)^\perp}$ Un élément de $V+W$ est de la forme $v+w$ avec $v \in V$ et $w \in W$. Nous avons

$$b(x, v+w) = b(x,v) + b(x,w) = 0. \tag{9.259}$$

(iii) **Pour (3)** Si $x \in V$, alors $b(x,z)=0$ pour tout $V^\perp$.

□

Proposition 9.130.
Soit une forme bilinéaire non dégénérée b sur l'espace vectoriel E de dimension finie. L'application

$$\begin{aligned} \varphi_b \colon E &\to E^* \\ x &\mapsto b(x,.) \end{aligned} \tag{9.260}$$

est un isomorphisme d'espaces vectoriels.

Démonstration. En plusieurs parties.

(i) **Linéaire** Le fait que φ_b soit linéaire est une conséquence de la bilinéarité de b.

(ii) **Injectif** Si $\varphi_b(v) = \varphi_b(w)$, alors pour tout $x \in E$ nous avons $\varphi_b(v)x = \varphi_b(w)x$, c'est-à-dire

$$b(v-w, x) = 0. \tag{9.261}$$

Vu que b est non dégénérée, cela implique $v-w=0$.

(iii) **Isomorphisme** Nous savons que $\dim(E) = \dim(E^*)$ par le lemme 4.124. Une application linéaire injective entre espaces de même dimension est toujours une bijection par le corolaire 4.48.

□

Lemme 9.131 ([270]).
Soit une forme bilinéaire non dégénérée b sur l'espace vectoriel E de dimension finie. Soit un sous-espace vectoriel V. Nous avons

$$\dim(E) = \dim(V) + \dim(V^\perp). \tag{9.262}$$

Démonstration. Nous considérons les applications

$$\begin{aligned} \varphi_b \colon E &\to E^* \\ x &\mapsto b(x,.). \end{aligned} \tag{9.263}$$

et l'application de restriction

$$\begin{aligned} r \colon E^* &\to V^* \\ \alpha &\mapsto \alpha|_F \end{aligned} \tag{9.264}$$

(i) **Théorème du rang** Nous appliquons le théorème du rang 4.50 à l'application r :

$$\mathrm{rk}(r) + \dim\big(\ker(r)\big) = \dim(E). \tag{9.265}$$

(ii) $\underline{\mathrm{rk}(r) = \dim(V)}$ Étant donné que r est surjective, $\mathrm{rk}(r) = \dim(V^*) = \dim(V)$. La seconde égalité est l'égalité des dimensions du lemme 4.124.

(iii) $\underline{\varphi_b(V^\perp) \subset \ker(r)}$ Soit $x \in V^\perp$. Pour tout $v \in V$ nous avons

$$r\big(\varphi_b(x)\big)v = \varphi_b(x)v = b(x,v) = 0. \tag{9.266}$$

Donc $\varphi_b(x) \in \ker(r)$.

(iv) $\varphi_b\colon V^\perp \to \ker(r)$ **est surjective** Soit $\alpha \in \ker(r)$. Vu que φ_b est une bijection, il existe $x \in E$ tel que $\alpha = \varphi_b(x)$, c'est-à-dire $\alpha = b(x, \cdot\,)$. Nous avons $\alpha(y) = 0$ pour tout $y \in V$, c'est à dire $b(x, y) = 0$ pour tout $y \in V$, ce qui signifie que $x \in V^\perp$. Donc $\alpha \in \varphi_b(V^\perp)$.

(v) $\dim(V^\perp) = \dim\big(\ker(r)\big)$ L'application φ_b étant globalement injective, elle est une bijection entre $V^\perp$ et $\ker(r)$. Donc ces deux ont la même dimension.

(vi) **Conclusion** Nous pouvons reprendre l'équation (9.265) et y mettre nos découvertes : $\mathrm{rk}(r) = \dim(V)$ et $\dim\big(\ker(r)\big) = \dim(V^\perp)$. Cela donne la formule demandée

$$\dim(V) + \dim(V^\perp) = \dim(E). \tag{9.267}$$

□

Lemme 9.132.
Si V est un sous-espace de E de dimension finie, alors

$$(V^\perp)^\perp = V. \tag{9.268}$$

Démonstration. Nous avons déjà vu dans la proposition 9.129 que $V \subset (V^\perp)^\perp$.

Nous écrivons maintenant la formule (9.262) pour V, et pour $V^\perp$ (qui est un sous-espace vectoriel par la proposition 9.128(1)) :

$$\dim(V) + \dim(V^\perp) = \dim(E) \tag{9.269a}$$
$$\dim(V^\perp) + \dim\Big((V^\perp)^\perp\Big) = \dim(E). \tag{9.269b}$$

En soustrayant ces deux équations membre à membres, nous trouvons $\dim(V) = \dim\Big((V^\perp)^\perp\Big)$. Vu que V s'injecte (par l'identité) dans $(V^\perp)^\perp$ et qu'ils ont la même dimension, ils sont égaux. □

9.7.3 Formes quadratiques

Lemme 9.133 ([271]).
Soit une forme quadratique Q sur E. Si F est un sous-espace de E, alors

$$\dim(F) + \dim(F^\perp) \geqslant n \tag{9.270}$$

où $F^\perp$ est l'orthogonal par rapport à Q.

Démonstration. Nous posons $p = \dim(F)$. Nous considérons une base $\{f_i\}_{i=1,\dots,n}$ de E telle que $\{f_i\}_{i=1,\dots,p}$ est une base de F [46]. Nous posons

$$\begin{aligned} \phi\colon E &\to F \\ x &\mapsto \sum_{i=1}^{p} B(x, f_i) f_i \end{aligned} \tag{9.271}$$

où B est la forme bilinéaire associée à Q. Ce ϕ est une application linéaire à qui nous appliquons le théorème du rang (4.50) :

$$\dim(E) = \mathrm{rk}(\phi) + \dim\big(\ker(\phi)\big). \tag{9.272}$$

Mais vu que l'image de ϕ est dans F, nous avons $\mathrm{rk}(\phi) \leqslant \dim(F)$. De plus, $\ker(\phi) = F^\perp$. Donc (9.272) devient

$$\dim(E) \leqslant \dim(F) + \dim(F^\perp). \tag{9.273}$$

□

46. Théorème de la base incomplète, 4.24.

Lemme 9.134 ([271])**.**
Soit un espace vectoriel E de dimension finie et un sous-espace F sur lequel la forme quadratique Q est strictement définie positive ou négative. Alors

$$E = F \oplus F^{\perp}. \tag{9.274}$$

Démonstration. D'abord nous montrons que $F \cap F^{\perp} = \{0\}$. Si $v \neq 0$ est dans F, alors $Q(v) > 0$, et donc v n'est pas dans $F^{\perp}$. Donc $F \cap F^{\perp} \subset \{0\}$. L'inclusion inverse est immédiate.

Nous avons vu dans le lemme 9.133 que

$$\dim(E) \leqslant \dim(F) + \dim(F^{\perp}). \tag{9.275}$$

Vu que F et $F^{\perp}$ n'ont pas d'intersection autre que $\{0\}$, nous avons

$$\dim(E) \geqslant \dim(F \oplus F^{\perp}) = \dim(F) + \dim(F^{\perp}) \geqslant \dim(E). \tag{9.276}$$

Toutes ces inégalités sont donc des égalités et $\dim(E) = \dim(F) + \dim(F^{\perp})$. □

Lemme 9.135.
La topologie considérée sur $Q(E)$[47] *est celle de la norme L'application*

$$\begin{aligned} N\colon Q(E) &\to \mathbb{R} \\ q &\mapsto \sup_{\|x\|_E=1} |q(x)|, \end{aligned} \tag{9.277}$$

est une norme.

L'application

$$\begin{aligned} N\colon S(n,\mathbb{R}) &\to \mathbb{R} \\ A &\mapsto \sup_{\|x\|_E=1} |x \cdot Ax| \end{aligned} \tag{9.278}$$

est une norme. À droite, nous trouvons le produit scalaire usuel sur $\mathbb{R}^n$ et la valeur absolue usuelle sur $\mathbb{R}$.

Ces normes sont celles que nous considérons pour la topologie sur $Q(E)$ et $S(n,\mathbb{R})$.

Proposition 9.136.
*Soit une forme bilinéaire b et la forme quadratique associée q. Alors nous avons l'**identité de polarisation** :*

$$b(x,y) = \frac{1}{2}\big(q(x) + q(y) - q(x-y)\big). \tag{9.279}$$

Démonstration. Il suffit de substituer dans le membre de droite $q(x) = b(x,x)$ et d'utiliser la bilinéarité :

$$\begin{aligned} q(x) + q(y) - q(x-y) &= b(x,x) + b(y,y) - b(x-y,x-y) && \text{(9.280a)} \\ &= b(x,x) + b(y,y) - b(x,x) + b(x,y) + b(y,x) - b(y,y) && \text{(9.280b)} \\ &= 2b(x,y) && \text{(9.280c)} \end{aligned}$$

où nous avons utilisé le fait que b est symétrique : $b(x,y) = b(y,x)$. □

Proposition 9.137 (Matrice associée à une forme bilinéaire)**.**
Soit $\{e_i\}$ une base de E. L'application

$$\begin{aligned} \phi\colon Q(E) &\to S(n,\mathbb{R}) \\ q &\mapsto \big(b(e_i,e_j)\big)_{i,j} \end{aligned} \tag{9.281}$$

où b est forme bilinéaire associée à q est une bijection linéaire et continue[48].

47. $Q(E)$ sont les formes quadratiques réelles sur E, définition 9.120.
48. Pour les topologies des normes données dans le lemme 9.135.

Démonstration. Si $\phi(q) = \phi(q')$; alors

$$q(x) = \sum_{i,j} \phi(q)_{ij} x_i x_j = \sum_{i,j} \phi(q')_{ij} x_i x_j = q'(x). \tag{9.282}$$

Donc $q = q'$. L'application ϕ est donc injective

De plus elle est surjective parce que si $B \in S(n, \mathbb{R})$ alors la forme quadratique

$$q(x) = \sum_{i,j} B_{ij} x_i x_j \tag{9.283}$$

a évidemment B comme matrice associée. L'application ϕ est donc surjective.

Notre application ϕ est de plus linéaire parce que l'association d'une forme quadratique à la forme bilinéaire associée est linéaire.

En ce qui concerne la continuité, nous la prouvons en zéro en considérant une suite convergente $q_n \xrightarrow{Q(E)} 0$. C'est-à-dire que

$$\sup_{\|x\|=1} |q_n(x)| \to 0. \tag{9.284}$$

Nous rappelons l'identité de polarisation [49] :

$$b_n(x, y) = \frac{1}{2}\big(q_n(x - y) - q_n(x) - q_n(y)\big). \tag{9.285}$$

En ce qui concerne deux des trois termes, il n'y a pas de problèmes :

$$\big|\phi(q_n)_{ij}\big| = \big|b_n(e_i, e_j)\big| \leqslant \frac{1}{2}\big|q_n(e_i - e_j)\big| + \frac{1}{2}\big|q_n(e_i)\big| + \frac{1}{2}\big|q_n(e_j)\big|. \tag{9.286}$$

Si n est assez grand, nous avons tout de suite

$$\big|\phi(q_n)_{ij}\big| \leqslant \frac{1}{2}\big|q_n(e_i - e_j)\big| + \epsilon. \tag{9.287}$$

Nous définissons e_{ij} et α_{ij} de telle sorte que $e_i - e_j = \alpha_{ij} e_{ij}$ avec $\|e_{ij}\| = 1$. Si $\alpha = \max\{\alpha_{ij}, 1\}$ alors nous avons

$$q_n(e_i - e_j) = \alpha_{ij}^2 q_n(e_{ij}) \leqslant \alpha^2 q_n(e_{ij}). \tag{9.288}$$

Il suffit maintenant de prendre n assez grand pour avoir $\sup_{\|x\|=1} |q_n(x)| \leqslant \frac{\epsilon}{\alpha^2}$ pour avoir

$$\big|\phi(q_n)_{ij}\big| \leqslant \frac{\epsilon}{2} + \frac{\epsilon}{\alpha^2}. \tag{9.289}$$

□

9.7.4 Isotropie

Définition 9.138 (Isotropie[272])**.**
Quelques définitions.

(1) Un vecteur est ***isotrope*** *pour b si il est perpendiculaire à lui-même. En d'autres termes, x est isotrope si et seulement si $b(x, x) = 0$.*

(2) Un sous-espace $W \subset E$ est ***isotrope*** *si $W \cap W^\perp \neq \varnothing$.*

(3) Un sous-espace $W \subset E$ est ***totalement isotrope*** *si pour tout $x, y \in W$, nous avons $b(x, y) = 0$.*

Le ***cône isotrope*** *de b est l'ensemble de ses vecteurs isotropes :*

$$C(b) = \{x \in E \text{ tel que } b(x, x) = 0\}. \tag{9.290}$$

49. Proposition 9.136.

Nous introduisons quelques notations. D'abord pour $y \in E$ nous notons

$$\begin{aligned} \Phi_y \colon E &\to \mathbb{R} \\ x &\mapsto b(x,y) \end{aligned} \tag{9.291}$$

et ensuite

$$\begin{aligned} \Phi \colon E &\to E^* \\ y &\mapsto \Phi_y. \end{aligned} \tag{9.292}$$

Définition 9.139.
*Le fait pour une forme bilinéaire b d'être dégénérée signifie que l'application Φ n'est pas injective. Le **noyau** de la forme bilinéaire est celui de Φ, c'est-à-dire*

$$\ker(b) = \{z \in E \text{ tel que } b(z,y) = 0 \, \forall y \in E\}. \tag{9.293}$$

Autrement dit, $\ker(b) = E^\perp$ où le perpendiculaire est pris par rapport à b.

Notons tout de même que nous utilisons la notation $\perp$ même si b est dégénérée et éventuellement pas positive ; c'est-à-dire même si la formule $(x,y) \mapsto b(x,y)$ ne fournit pas un produit scalaire.

Lemme 9.140.
Si E est de dimension finie, et si V est un sous-espace non isotrope[50] *de E, alors $V^\perp$ est également non-isotrope.*

Démonstration. En dimension finie, le lemme 9.132 nous indique que $(V^\perp)^\perp = V$. Si $V^\perp$ était isotrope nous aurions $V^\perp \cap (V^\perp)^\perp \neq \varnothing$. Cela donne alors immédiatement $V^\perp \cap V \neq \varnothing$, qui serait que V est isotrope. □

9.8 Formes bilinéaires et quadratiques

Plus à propos de formes bilinéaires dans le thème 16.

Lemme 9.141.
Si q est une forme quadratique, il existe une unique forme bilinéaire b telle que $q(x) = b(x,x)$.

Démonstration. L'existence n'est pas en cause : c'est la définition d'une forme quadratique. Pour l'unicité, étant donné une forme quadratique, la forme bilinéaire b doit forcément vérifier l'identité de polarisation de la proposition 9.136. Elle est donc déterminée par q. □

Notons la division par 2 qui est le pourquoi de la demande de la caractéristique différente de 2 pour $\mathbb{F}$ dans la définition de forme quadratique.

Définition 9.142.
*Soit une forme quadratique q sur E. Nous disons que $v, w \in E$ sont **q-orthogonaux** si $b(v,w) = 0$ la forme bilinéaire b associée à q par le lemme 9.141.*

9.8.1 Matrice associée à une forme bilinéaire

Définition 9.143.
Soit une forme bilinéaire[51] *$b \colon E \times E \to \mathbb{K}$ et une base quelconque $\{f_\alpha\}$ de E. Nous définissons les nombres*

$$B_{\alpha\beta} = b(f_\alpha, f_\beta), \tag{9.294}$$

*qui forment une matrice symétrique dans $\mathbb{M}(n,\mathbb{K})$. Cette matrice est la **matrice associée** à la forme bilinéaire b.*

La matrice d'une forme quadratique est celle associée à sa forme bilinéaire associée.

50. Définition 9.138.
51. Définition 9.119.

Lemme 9.144.
Soit une forme bilinéaire $b: E \times E \to \mathbb{K}$ et une base quelconque $\{f_\alpha\}$ de E. Nous notons B la matrice de b (definition 9.143) et q la forme quadratique associée.

Alors nous avons

$$b(x,y) = \sum_{\alpha\beta} B_{\alpha\beta} x_\alpha y_\beta. \tag{9.295}$$

et

$$b(x,y) = x \cdot By. \tag{9.296}$$

où le point est le produit scalaire usuel (composante par composante).

Démonstration. Si $x = \sum_\alpha x_\alpha f_\alpha$ et $y = \sum_\beta y_\beta f_\beta$:

En utilisant la convention (4.87) et les choses autour (voir aussi -2.1),

$$b(x,y) = \sum_\alpha x_\alpha \sum_\beta B_{\alpha\beta} y_\beta = \sum_\alpha x_\alpha (By)_\alpha = x \cdot By. \tag{9.297}$$

□

9.8.2 Changement de base : matrice d'une forme bilinéaire

Proposition 9.145 ([1]).
Soient une forme quadratique q sur $\mathbb{R}^n$ et une application linéaire $\phi: \mathbb{R}^n \to \mathbb{R}^n$. La matrice de $q \circ \phi$ est

$$\phi^t q \phi \tag{9.298}$$

où l'on a noté q la matrice de q et ϕ celle de ϕ.

Démonstration. C'est un calcul direct de $(q \circ \phi)(x)$:

$$q\big(\phi(x)\big) = \sum_{ij} q_{ij} \phi(x)_i \phi(x)_j \tag{9.299a}$$

$$= \sum_{ij} \sum_k \sum_l q_{ij} \phi_{ik} x_k \phi_{jl} x_l \qquad \text{prop. 4.70} \tag{9.299b}$$

$$= \sum_{kl} \Big(\sum_{ij} \phi_{ik} q_{ij} \phi_{jl} \Big) x_k x_l \qquad = \sum_{kl} (\phi^t q \phi)_{kl} x_l x_l. \tag{9.299c}$$

Et voila. □

Proposition 9.146 (Voir la section -2.1).
Soit une forme bilinéaire[52] $b: V \times V \to \mathbb{K}$ dont la matrice[53] dans la base $\{e_i\}$ est A et celle dans la base $\{f_\alpha\}$ est B. Nous supposons que les bases sont liées par $f_\alpha = \sum_i Q_{i\alpha} e_i$. Alors

$$B = Q^t A Q. \tag{9.300}$$

Démonstration. Soit $x, x' \in V$ de coordonnées (x_i) et (x'_i) dans la base $\{e_i\}$ et (y_α), (y'_α) dans la base $\{f_\alpha\}$. Par définition de la matrice associée à une forme bilinéaire,

$$b(x,x') = \sum_{ij} A_{ij} x_i x'_j = \sum_{\alpha\beta} B_{\alpha\beta} y_\alpha y'_\beta. \tag{9.301}$$

En remplaçant les x_i et x'_i par leurs valeurs en fonction de y_α et y'_β données par la proposition 4.113, nous trouvons

$$b(x,x') = \sum_{ij\alpha\beta} A_{ij} Q_{i\alpha} y_\alpha Q_{j\beta} y'_\beta \tag{9.302a}$$

$$= \sum_{\alpha\beta} (Q^t A Q)_{\alpha\beta} y_\alpha y'_\beta \tag{9.302b}$$

52. Définition 9.119
53. Définition 9.294.

où Q^t désigne la transposée de la matrice Q : $Q^t_{ij} = Q_{ji}$. Vu que les nombres y_α et y'_β sont arbitraires nous déduisons [54] que $B = Q^t A Q$. □

Remarque 9.147.
Notons que cette « loi de transformation » n'est pas la même que celle pour une application linéaire [55]. Ici nous avons Q^t alors que pour les applications linéaires nous avions Q^{-1}.

Pour cette raison, tant que nous travaillons avec des bases orthonormées, c'est-à-dire tant que Q est orthogonale [56], nous pouvons confondre une application linéaire avec une application bilinéaire en passant par la matrice. Mais cette identification n'est pas du tout canonique : elle repose sur le fait que les bases soient orthonormées.

Il en découle que la réduction des endomorphismes et la réduction des formes bilinéaires ne sont pas tout à fait les mêmes théories. Par exemple la pseudo-diagonalisation simultanée (corolaire 11.37) est un résultat de réduction de forme bilinéaire et non d'endomorphismes.

9.8.3 Isométrie, forme quadratique et bilinéaire

Exemple 9.148.
La forme quadratique $q(x) = x_1^2 + x_2^2$ donne la norme euclidienne. La forme bilinéaire associée est $b(x, y) = x_1y_1 + x_2y_2$, qui est le produit scalaire usuel. △

Il ne faudrait pas déduire trop vite que la formule $\|x\|^2 = q(x)$ donne une norme dès que q est non dégénérée. En effet q peut ne pas être définie positive. La forme $q(x) = x_1^2 - x_2^2$ prend des valeurs positives et négatives. A fortiori $d(x, y) = q(x - y)$ ne donne pas toujours une distance.

Définition 9.149.
*Une **isométrie** pour la forme quadratique q est une application bijective $f : V \to V$ telle que*

$$q(x - y) = q\big(f(x) - f(y)\big). \tag{9.303}$$

Dans les cas où q donne une distance, alors c'est une isométrie au sens usuel.

Définition 9.150 (Thème 77)**.**
*Soit un espace vectoriel E muni d'une forme bilinéaire b. Une **isométrie** pour b est une bijection $f : E \to E$ telle que*

$$b\big(f(x), f(y)\big) = b(x, y) \tag{9.304}$$

pour tout $x, y \in E$.

Lemme 9.151.
Soient q une forme quadratique et b la forme bilinéaire associée par le lemme 9.141. Une application $f : E \to E$ telle que $f(0) = 0$ est une isométrie pour b si et seulement si elle est une isométrie pour q.

Démonstration. Pour une application bijective $f : E \to E$ telle que $f(0) = 0$, nous devons prouver l'équivalence des propriétés suivantes :

(1) $b\big(f(x), f(y)\big) = b(x, y)$ pour tout $x, y \in E$;
(2) $q\big(f(x) - f(y)\big) = q(x - y)$ pour tout $x, y \in E$.

Dans le sens direct, en posant $x = y$ nous trouvons tout de suite $q(f(x)) = q(x)$; ensuite en utilisant la distributivité de b,

$$\begin{aligned} q\big(f(x) - f(y)\big) &= b\big(f(x) - f(y), f(x) - f(y)\big) && \text{(9.305a)}\\ &= q\big(f(x)\big) - 2b\big(f(x), f(y)\big) + q\big(f(y)\big) && \text{(9.305b)}\\ &= q(x) + q(y) - 2b(x, y) && \text{(9.305c)}\\ &= q(x - y). && \text{(9.305d)} \end{aligned}$$

54. Lemme 4.66.
55. Proposition 4.116.
56. Définition 4.98.

Dans l'autre sens, nous commençons par remarquer que l'hypothèse $f(0) = 0$ donne $q(x) = q\big(f(x)\big)$. Ensuite nous utilisons l'identité de polarisation (9.279) :

$$b\big(f(x), f(y)\big) = \frac{1}{2}\big[q\big(f(x)\big) + q\big(f(y)\big) - q\big(f(x-y)\big)\big] \tag{9.306a}$$
$$= \frac{1}{2}\big[q(x) + q(y) - q(x-y)\big] \tag{9.306b}$$
$$= b(x, y). \tag{9.306c}$$

□

9.8.4 Isométries

Voici un théorème pas toujours bien énoncé dans les cours de physique qui font de la relativité. Au moment de « prouver » les transformations de Lorentz [57], beaucoup oublient de justifier pourquoi elles devraient être linéaires.

Théorème 9.152 ([273]).
Une isométrie [58] d'une forme bilinéaire non dégénérée est linéaire.

Démonstration. Soient une forme bilinéaire non-dégénérée b sur l'espace vectoriel E ainsi qu'une isométrie f pour icelle. Soit $z \in E$; étant donné que f est bijective nous pouvons considérer l'élément $f^{-1}(z) \in E$ et calculer

$$b\big(f(x+y), z\big) = b\big(f(x+y), f(f^{-1}(z))\big) \tag{9.307a}$$
$$= b(x+y, f^{-1}(z)) \tag{9.307b}$$
$$= b(x, f^{-1}(z)) + b(y, f^{-1}(z)) \tag{9.307c}$$
$$= b(f(x), z) + b(f(y), z) \tag{9.307d}$$
$$= b\big(f(x) + f(y), z\big), \tag{9.307e}$$

donc $f(x+y) = f(x) + f(y)$ par le lemme 9.125.

De la même façon on trouve $b\big(f(\lambda x), z\big) = b\big(\lambda f(x), z\big)$ qui prouve que $f(\lambda x) = \lambda f(x)$ et donc que f est linéaire. □

Exemple 9.153.
Une isométrie peut ne pas être linéaire quand la forme bilinéaire est dégénérée. Par exemple pour la forme bilinéaire sur $\mathbb{R}^2$ donnée par

$$b\big((a,b),(x,y)\big) = ax, \tag{9.308}$$

nous pouvons faire

$$f(x,y) = \begin{pmatrix} x \\ \lambda(x,y) \end{pmatrix} \tag{9.309}$$

où λ est n'importe quoi. △

Définition 9.154.
*Soient deux espaces vectoriels E et V. Une application $f\colon E \to V$ est **affine** si il existe une application linéaire $u\colon E \to V$ et un élément $\alpha \in V$ tel que*

$$f(x) = u(x) + \alpha \tag{9.310}$$

pour tout $x \in E$.

57. Théorème 18.201.
58. Définition 9.150.

Théorème 9.155.
Soit un espace vectoriel E muni d'une forme quadratique q. Soit une isométrie $f : E \to E$ pour q. Alors

(1) si $f(0) = 0$, alors f est linéaire ;

(2) si $f(0) \neq 0$ alors f est affine[59].

Démonstration. Nous considérons la forme bilinéaire associée b. Si $f(0) = 0$, nous savons par le lemme 9.151 que $b\big(f(x), f(y)\big) = b(x, y)$. La proposition 9.152 nous dit alors que f est linéaire.

Si $f(0) \neq 0$, alors nous posons $g(x) = f(x) - f(0)$ qui vérifie $g(0) = 0$ et

$$q\big(g(x) - g(y)\big) = q\big(f(x) - f(0) - f(y) + f(0)\big) = q(x - y). \tag{9.311}$$

Nous pouvons donc appliquer le premier point à g, déduire que g est linéaire et donc que f est affine. C'est la caractérisation du lemme 8.59 des fonctions affines. □

Nous pouvons maintenant particulariser tout cela au cas de $\mathbb{R}^n$ muni du produit scalaire usuel et de la norme associée pour voir quel résultat nous avons à peine prouvé.

Lemme 9.156 ([274])**.**
Une isométrie d'un espace vectoriel normé de dimension finie est bijective.

Démonstration. Si $f : E \to E$ est une isométrie, elle est linéaire par le théorème 9.152. Elle vérifie également $\|f(x)\| = \|x\|$, et donc $f(x) = 0$ si et seulement si $x = 0$, c'est-à-dire que f est injective. Elle est alors bijective par le corolaire 4.48 du théorème du rang. □

Nous notons ici $T(n)$ le groupe des translations sur $\mathbb{R}^n$. Un élément de $T(n)$ est une translation τ_v donnée par un vecteur v et agissant sur $\mathbb{R}^n$ par

$$\begin{aligned} \tau_v : \mathbb{R}^n &\to \mathbb{R}^n \\ x &\mapsto x + v. \end{aligned} \tag{9.312}$$

Ce groupe est isomorphe au groupe abélien $(\mathbb{R}^n, +)$, et nous allons souvent identifier τ_v à v.

Vous savez par culture générale que les isométries de $\mathbb{R}^n$ pour le produit scalaire usuel sont les matrices orthogonales. En voici une petite généralisation (pensez à $\eta = \mathbb{1}$ dans le cas du produit scalaire usuel).

Proposition 9.157.
Soit une forme bilinéaire b sur $\mathbb{R}^n$ de matrice symétrique η. Si A est la matrice d'une application linéaire $\mathbb{R}^n \to \mathbb{R}^n$ telle que

$$b(Ax, Ay) = b(x, y) \tag{9.313}$$

pour tout $x, y \in \mathbb{R}^n$, alors

$$A^t \eta A = \eta. \tag{9.314}$$

Démonstration. En suivant la formule générale (9.295),

$$b(Ax, Ay) = \sum_{ij} \eta_{ij} (Ax)_i (Ay)_j = \sum_{ijkl} \eta_{ij} A_{ik} A_{jl} x_k y_l. \tag{9.315}$$

En imposant que ce soit égal à $\sum_{kl} \eta_{kl} x_k y_l$ pour tout x, y nous avons la contrainte

$$\sum_{ij} \eta_{ij} A_{ik} A_{jl} = \eta_{kl} \tag{9.316}$$

qui signifie exactement $A^t \eta A = \eta$. □

59. Définition 9.154.

9.9 Signature, théorème de Sylvester

Définition 9.158 (Signature[275]).
Soit une forme quadratique[60] *Q sur un espace vectoriel E de dimension finie n. L'**indice d'inertie** de Q est le nombre*

$$q = \max\{\dim(F) \text{ tel que } Q(v) < 0 \, \forall v \in F\backslash\{0\}\}. \tag{9.317}$$

Nous définissons aussi

$$p = \max\{\dim(G) \text{ tel que } Q(v) > 0 \, \forall v \in G\backslash\{0\}\}. \tag{9.318}$$

*Le couple (p, q) est la **signature** de Q.*

Définition 9.159 (Rang d'une forme quadratique).
Si $Q\colon E \to \mathbb{K}$ est une forme quadratique, nous considérons l'application

$$\begin{aligned} f_Q\colon E &\to E^* \\ x &\mapsto \big[y \mapsto B(x, y)\big]. \end{aligned} \tag{9.319}$$

*Le **rang** de Q est le rang de l'application linéaire f_Q.*

Proposition 9.160.
Le rang d'une forme quadratique est le rang de sa matrice dans n'importe quelle base.

Démonstration. Nous considérons une forme quadratique Q sur l'espace vectoriel E. Sa trace est, par définition, la trace de l'application linéaire f_Q de la définition 9.159. Or cette dernière trace ne dépend pas des bases choisies sur E et E^*. Nous la calculons donc maintenant.

Soit une base $\{e_i\}$ de E ainsi que sa base duale $\{e_i^*\}$ de E^*. Si $v = \sum_k v_k e_k \in E$, alors

$$f_Q(e_i)v = \sum_k v_k B(e_i, e_k) = \sum_k Q_{ik} v_k \tag{9.320}$$

où nous avons noté B la forme bilinéaire associée à Q et utilisé la définition 9.143 de la matrice associée à la forme quadratique Q. Nous avons donc $f_Q(ei) = \sum_k Q_{ik} e_k^*$ ou encore

$$f_Q(e_i)_k = Q_{ik}, \tag{9.321}$$

ce qui signifie, par (1) que la matrice associée à f_Q est la matrice Q^t.

Le rang de f_Q est donc celui de Q^t, qui est le même que celui de la matrice Q (ici, nous avons noté Q la matrice de la forme quadratique Q). Le rang de f_Q est celui de sa matrice par la proposition 4.107. □

Lemme 9.161 ([275]).
Soient une forme quadratique Q ainsi que deux bases Q-orthogonales $\{e_1, \dots, e_n\}$ et $\{e'_1, \dots, e'_n\}$. Nous posons

$$r = \text{Card}\{e_i \text{ tel que } Q(e_i) > 0\} \tag{9.322a}$$
$$r' = \text{Card}\{e_i \text{ tel que } Q(e'_i) > 0\} \tag{9.322b}$$
$$s = \text{Card}\{e_i \text{ tel que } Q(e_i) < 0\} \tag{9.322c}$$
$$s' = \text{Card}\{e_i \text{ tel que } Q(e'_i) < 0\} \tag{9.322d}$$

Alors $r = r'$ et $s = s'$.

Démonstration. Nous posons

$$I = \{i \text{ tel que } Q(e_i) \geqslant 0\} \tag{9.323a}$$
$$J = \{j \text{ tel que } Q(e'_j) \leqslant 0\} \tag{9.323b}$$

60. Définition 9.120.

Nous commençons par prouver que $\{e_i\}_{i\in I}\cup\{e'_j\}_{j\in J}$ est libre. Supposons pour cela que

$$\sum_{i\in I}x_ie_i+\sum_{j\in J}y_je'_j=0, \tag{9.324}$$

et posons $z=\sum_{i\in I}x_ie_i$. Nous avons

$$Q(z)=\sum_{i\in I}x_i^2Q(e_i)\geqslant 0. \tag{9.325}$$

Mais nous avons aussi $z=-\sum_{j\in J}y_je'_j$, donc

$$Q(z)=\sum_{j\in J}y_j^2Q(e'_j)\leqslant 0. \tag{9.326}$$

Donc $Q(z)=0$. Vu (9.325), et le fait que $Q(e_i)>0$, avoir $Q(z)=0$ impose $x_i=0$ pour tout i. La relation (9.326) nous donne aussi immédiatement que les y_j sont nuls. Donc la partie $\{e_i\}_{i\in I}\cup\{e'_j\}_{j\in J}$ est libre.

Le lemme 4.11 nous indique qu'une partie libre est toujours de cardinal plus petit ou égal à la dimension de l'espace[61]. Tout ça pour dire que

$$\underbrace{\text{Card}(I)}_{=r}+\underbrace{\text{Card}(J)}_{=n-r'}\leqslant n, \tag{9.327}$$

et donc $r\leqslant r'$.

Le même raisonnement, en partant de $I=\{i \text{ tel que } Q(e_i)\leqslant 0\}$ et de $J=\{j \text{ tel que } Q(e'_j)>0\}$, prouve que $r'\leqslant r$.

La preuve de $s=s'$ est du même tonneau. □

Pour l'équivalence de formes quadratiques, voir la définition 9.244 et la proposition 9.245.

9.10 Produit scalaire, produit hermitien

Définition 9.162.
*Un **produit scalaire** sur un espace vectoriel réel est une forme bilinéaire*[62] *symétrique strictement définie positive*[63].

La définition suivante est utile pour ceux qui veulent faire de la relativité[64].

Définition 9.163.
*Un **produit pseudo-scalaire** sur un espace vectoriel réel est une forme bilinéaire et symétrique.*

Définition 9.164.
*Nous dirons que deux vecteurs sont **orthogonaux** lorsque leur produit scalaire*[65] *est nul. Nous écrivons que $u\perp v$ lorsque $\langle u,v\rangle=0$.*

*Si $\{e_i\}_{i=1,\dots,n}$ est une base de E, nous disons qu'elle est **orthonormée** si*

$$\langle e_i,e_j\rangle=\delta_{ij}. \tag{9.328}$$

Lemme 9.165.
Un produit scalaire est toujours non dégénéré[66].

61. Ici nous utilisons l'hypothèse que V est de dimension finie.
62. Définition 9.119.
63. Définition 9.121.
64. Voir le théorème 18.201 qui établit les transformations de Lorentz.
65. Définition 9.162.
66. Définition 9.124.

Vu que nous allons voir un pâté d'espaces avec des produits scalaires, nous leur donnons un nom.

Définition 9.166.
Un espace vectoriel ***euclidien*** *est un espace vectoriel réel de dimension finie muni d'un produit scalaire (définition 9.162).*

Avouez que c'est drôle qu'un espace vectoriel est euclidien lorsqu'il possède une *multiplication* alors qu'un anneau est euclidien lorsqu'il possède une *division* (voir la définition 1.244). C'est pas très profond, mais si ça peut vous servir de moyen mnémotechnique...

Proposition-Définition 9.167 (Produit scalaire dans $\mathbb{R}^n$, thème 25)**.**
Si $x, y \in \mathbb{R}^n$, nous définissons

$$x \cdot y = \sum_{i=1}^{n} x_i y_i = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n. \tag{9.329}$$

Cela est un produit scalaire.

Ce produit scalaire est le ***produit scalaire*** *qui sera toujours considéré. C'est de lui qui découle toujours la norme, et la topologie de $\mathbb{R}^n$. Il sera aussi souvent noté $\langle x, y\rangle$.*

Démonstration. Il faut que $b(x, y) = \sum_i x_i y_i$ soit bilinéaire, symétrique, strictement définie positive. Ce sont toutes des vérifications immédiates. Par exemple pour la symétrique, nous avons $\sum_i x_i y_i = \sum_i y_i x_i$. □

Calculons par exemple le produit scalaire de deux vecteurs de la base canonique : $\langle e_i, e_j\rangle$. En utilisant la formule de définition et le fait que $(e_i)_k = \delta_{ik}$, nous avons

$$\langle e_i, e_j\rangle = \sum_{k=1}^{m} \delta_{ik}\delta_{jk}. \tag{9.330}$$

Nous pouvons effectuer la somme sur k en remarquant qu'à cause du δ_{ik}, seul le terme avec $k = i$ n'est pas nul. Effectuer la somme revient donc à remplacer tous les k par des i :

$$\langle e_i, e_j\rangle = \delta_{ii}\delta_{ji} = \delta_{ji}. \tag{9.331}$$

Une des propriétés intéressantes du produit scalaire est qu'il permet de décomposer un vecteur dans une base, comme nous le montre la proposition suivante.

Proposition 9.168.
Si nous notons v_i les composantes du vecteur v, c'est-à-dire si $v = \sum_{i=1}^{m} v_i e_i$, alors nous avons $v_j = \langle v, e_j\rangle$.

Démonstration.

$$v \cdot e_j = \sum_{i=1}^{m} \langle v_i e_i, e_j\rangle = \sum_{i=1}^{m} v_i \langle e_i, e_j\rangle = \sum_{i=1}^{m} v_i \delta_{ij} \tag{9.332}$$

En effectuant la somme sur i dans le membre de droite de l'équation (9.332), tous les termes sont nuls sauf celui où $i = j$; il reste donc

$$v \cdot e_j = v_j. \tag{9.333}$$

□

Le produit scalaire ne dépend en réalité pas de la base orthogonale choisie.

Lemme 9.169.
Si $\{e_i\}$ est la base canonique, et si $\{f_i\}$ est une autre base orthonormale[67]*, alors si u et v sont deux vecteurs de $\mathbb{R}^m$, nous avons*

$$\sum_i u_i v_j = \sum_i u'_i v'_j \tag{9.334}$$

67. Définition 9.164.

où u_i sont les composantes de u dans la base $\{e_i\}$ et u'_i sont celles dans la base $\{f_i\}$.

Démonstration. La preuve demande un peu d'algèbre linéaire. Étant donné que $\{f_i\}$ est une base orthonormale, il existe une matrice A orthogonale ($AA^t = \mathbb{1}$) telle que $u'_i = \sum_j A_{ij}u_j$ et idem pour v. Nous avons alors

$$\begin{aligned}\sum_i u'_i v'_j &= \sum_i \left(\sum_j A_{ij}u_j\right)\left(\sum_k A_{ik}v_k\right)\\ &= \sum_{ijk} A_{ij}A_{ik}u_j v_k\\ &= \sum_{jk}\underbrace{\sum_i (A^t)_{ji}A_{ik}}_{=\delta_{jk}} u_j v_k\\ &= \sum_{jk}\delta_{jk}u_j v_k\\ &= \sum_k u_k v_k.\end{aligned} \tag{9.335}$$

□

Cette proposition nous permet de réellement parler du produit scalaire entre deux vecteurs de façon intrinsèque sans nous soucier de la base dans laquelle nous exprimons les vecteurs.

9.10.1 Hermitien, unitaire, etc.

Définition 9.170 ([276])**.**
*Soit E est un espace vectoriel sur $\mathbb{C}$. Une application $\langle .,. \rangle : E \times E \to \mathbb{C}$ est **sesquilinéaire à droite** si pour tout $x, y \in E$ et pour tout $\lambda \in \mathbb{C}$,*

(1) $\langle \lambda x, y\rangle = \lambda\langle x, y\rangle = \langle x, \bar{\lambda}y\rangle$,

(2) $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$,

(3) $\langle x, y + z\rangle = \langle x, y\rangle + \langle x, z\rangle$.

Définitions supplémentaires :

— *La forme $\langle .,. \rangle$ est **hermitienne** si de plus*

$$\langle x, y\rangle = \overline{\langle y, x\rangle}. \tag{9.336}$$

— *Un **produit hermitien** est une forme hermitienne strictement définie positive, c'est-à-dire telle que $\langle x, x\rangle \geqslant 0$ pour tout $x \in E$ et $\langle x, x\rangle = 0$ si et seulement si $x = 0$.*

Proposition-Définition 9.171.
Soit un espace hermitien $(E, \langle .,. \rangle)$. Soit un opérateur linéaire $A \in \mathrm{End}(E)$. Il existe un unique opérateur $B \in \mathrm{End}(E)$ tel que

$$\langle Ax, y\rangle = \langle x, By\rangle \tag{9.337}$$

pour tout $x, y \in E$.

*L'opérateur B ainsi défini est noté $A^\dagger$ et est nommé **hermitien conjugué** de A.*

Lemme 9.172.
Au niveau des matrices, nous avons

$$A^\dagger_{ij} = A^*_{ji} \tag{9.338}$$

où z^* est le conjugué complexe.

Définition 9.173.
Quelque définitions.

*(1) Un opérateur A est **hermitien** si $A^\dagger = A$.*

*(2) Un opérateur A est **unitaire** si $A^\dagger = A^{-1}$.*

Note : le conjugué hermitien est parfois noté A^* au lieu de $A^\dagger$.

9.174.
Le mot « hermitien » est réservé aux opérateurs sur des espaces hermitiens, c'est-à-dire des espaces vectoriels sur $\mathbb{C}$. Le mot « autoadjoint » par contre est plutôt utilisé dans le cadre d'opérateurs sur les espaces réels. En conséquence de quoi, ces deux mots sont synonymes, mais il est préférable d'utiliser « hermitien » lorsque l'espace vectoriel est sur $\mathbb{C}$ et « autoadjoint » lorsqu'il est sur $\mathbb{R}$.

L'ensemble des opérateurs autoadjoints de E est noté $\mathrm{S}(E)$. Cette notation provient du fait que dans $\mathbb{R}^n$ muni du produit scalaire usuel, les opérateurs autoadjoints sont les matrices symétriques.

Remarque 9.175.
Le fait d'être hermitien n'implique en rien le fait d'être inversible.

9.176.
Les normes associées aux produits scalaires font intervenir une racine carré, et donc devront être données plus tard. Voir le thème 25.

Proposition 9.177 ([1])**.**
Nous considérons $\mathbb{C}^n$ vu comme espace vectoriel de dimension n sur $\mathbb{C}$.

(1) La formule, pour $x, y \in \mathbb{C}^n$,

$$\langle x, y\rangle = \sum_{k=1}^{n} x_k \bar{y}_k \tag{9.339}$$

définit une une forme sesquilinéaire sur $\mathbb{C}^n$.

(2) L'ensemble $\mathbb{C}^n$ devient un espace vectoriel hermitien.

9.10.2 Éléments de matrice

Proposition 9.178.
Soit une application linéaire $A\colon \mathbb{R}^n \to \mathbb{R}^n$. Nous considérons le produit scalaire usuel[68] *sur $\mathbb{R}^n$. Alors :*

(1) Les éléments de matrice de A sont donnés par $A_{ij} = e_i \cdot Ae_j$.

(2) Nous avons la formule $x \cdot Ay = \sum_{kl} A_{kl} x_k y_l$.

Démonstration. Pour Ae_j nous utilisons la formule 4.86 avec des notations plus décontractées : $Ae_j = \sum_k A_{kj} e_k$. Ensuite nous faisons un calcul avec la formule (9.329) :

$$e_i \cdot Ae_j = e_i \cdot \sum_k A_{kj} e_k = \sum_k A_{kj} \delta_{i,k} = A_{ij}. \tag{9.340}$$

La seconde formule à prouver est du même tonneau, en utilisant cette fois la formule (4.87) :

$$x \cdot Ay = \sum_k x_k (Ay)_k = \sum_{kl} x_k A_{kl} y_l = \sum_{kl} A_{kl} x_k y_l. \tag{9.341}$$

□

La proposition suivante est une version plus « pragmatique » de la proposition 4.130.

Proposition 9.179 ([135])**.**
Soient un espace euclidien[69] *de dimension finie V ainsi qu'un sous-espace M. Nous posons*

$$M^\perp = \{x \in V \text{ tel que } x \cdot y = 0 \forall y \in M\}. \tag{9.342}$$

Alors $M \oplus M^\perp = V$.

68. Définition 9.167.
69. Qui possède un produit scalaire, définition 9.166.

Démonstration. D'abord si $x \in M \cap M^\perp$, alors $x \cdot x = 0$ et donc $x = 0$. Donc nous avons déjà $M \cap M^\perp = \{0\}$. Nous considérons une base $\{b_1, \dots, b_k\}$ de M, et nous définissons l'application linéaire

$$\begin{aligned} f\colon V &\to \mathbb{R}^k \\ x &\mapsto (x \cdot b_1, \dots, x \cdot b_k). \end{aligned} \tag{9.343}$$

Nous avons que $M^\perp = \ker(f)$. Le théorème du rang 4.46 nous indique que

$$\dim(V) = \dim\big(\ker(f)\big) + \dim\big(\text{Image}(f)\big) \leqslant \dim(M^\perp) + k = \dim(M^\perp) + \dim(M). \tag{9.344}$$

Une justification : vu que f prend ses valeurs dans $\mathbb{R}^k$, la dimension de son image est majorée par k.

Nous en déduisons que

$$\dim(M) + \dim(M^\perp) \geqslant \dim(V), \tag{9.345}$$

et la proposition 4.138 nous permet de conclure que $M \oplus M^\perp = V$. □

9.10.3 Transposée : pas d'approche naïve

Il est légitime, si $t\colon E \to E$ est une application linéaire, de dire que sa transposée soit l'application linéaire $t^t\colon E \to E$ dont la matrice est la matrice transposée de celle de t. Lorsque nous travaillons sur $\mathbb{R}^n$ muni de la base canonique, cela ne pose pas de problème et nous pouvons écrire des égalités du type $\langle x, Ay\rangle = \langle A^t x, y\rangle$.

Proposition 9.180 (Matrice transposée et produit scalaire)**.**
Soit une matrice réelle A. En utilisant l'application linéaire associée[70] *$f_A\colon \mathbb{R}^n \to \mathbb{R}^n$, nous avons*

$$x \cdot f_A(y) = f_{A^t}(x) \cdot y. \tag{9.346}$$

Cette formule est souvent écrite $x \cdot Ay = A^t x \cdot y$ ou $\langle x, Ay\rangle = \langle A^t x, y\rangle$.

Démonstration. Il s'agit d'un calcul utilisant la formule (4.81) et le produit scalaire (9.329) :

$$x \cdot f_A(y) = \sum_i x_i \big(f_A(y)\big)_i = \sum_i x_i \sum_j A_{ij} y_j = \sum_{ij} A^t_{ji} x_i y_j = \sum_j f_{A^t}(x)_j y_j = f_{A^t}(x) \cdot y. \tag{9.347}$$

□

Hélas nous allons voir que cette façon de définir une transposée est mauvaise.

Soit une application linéaire $t\colon E \to E$ de matrice A dans la base $\{e_i\}_{i=1,\dots,n}$ et de matrice B dans la base $\{f_\alpha\}_{\alpha=1,\dots,n}$. Nous notons Q la matrice de passage d'une base à l'autre :

$$e_i = \sum_\alpha Q^{-1}_{\alpha i} f_\alpha. \tag{9.348}$$

Nous nommons t_1 l'application linéaire associée à A^t dans la base $\{e_i\}$ et t_2 l'application linéaire associée à la matrice B^t dans la base $\{f_\alpha\}$. Définir la transposée d'une application linéaire comme étant l'application linéaire associée à la transposée de sa matrice ne sera une bonne définition que si $t_1 = t_2$.

La première chose facile à voir est

$$t_1(e_i)_j = \sum_k (A^t)_{jk} (e_i)_k = A^t_{ji} = A_{ij}. \tag{9.349}$$

70. Définition 4.67. Ici nous considérons la base canonique sur $\mathbb{R}^n$

Pour calculer $t_2(e_i)_j$, c'est un peu plus laborieux :

$$t_2(e_i) = \sum_{\alpha} Q^{-1}_{\alpha i} t_2(f_\alpha) = \sum_{\beta\gamma\alpha} Q^{-1}_{\alpha i} B^t_{\gamma\beta} \underbrace{(f_\alpha)_\beta}_{\delta_{\alpha\beta}} f_\gamma = \sum_{\beta\gamma} Q^{-1}_{\beta i} B^t_{\gamma\beta} f_\gamma \tag{9.350a}$$

$$= \sum_{j\gamma} (B^t Q^{-1})_{\gamma i} Q_{j\gamma} e_j \tag{9.350b}$$

$$= \sum_{j} (QB^t Q^{-1})_{ji} e_j. \tag{9.350c}$$

Donc $t_2(e_i)_j = (QB^tQ^{-1})_{ji}$. En tenant compte du fait que $B = Q^{-1}AQ$ nous avons

$$t_2(e_i)_j = (QQ^tA^t(Q^{-1})^tQ^{-1})_{ji}. \tag{9.351}$$

Ceci est égal à l'expression (9.349) lorsque $Q^t = Q^{-1}$. Nous voyons que confondre transposée d'une application linéaire avec transposée de la matrice associée n'est valable que si nous sommes certain de ne considérer que des changements de base par des matrices orthogonales.

C'est la situation typique dans laquelle nous nous trouvons lorsque nous considérons des applications linéaires sur $\mathbb{R}^n$ muni de la base canonique, et que nous n'avons aucune intention de changer de base, et encore moins de chercher une base non orthonormale. Cette situation est clairement la situation la plus courante.

Exemple 9.181 ([91])**.**
Soit la base canonique $\{e_1, e_2\}$ de $\mathbb{R}^2$. Nous considérons l'application linéaire $t\colon \mathbb{R}^2 \to \mathbb{R}^2$ définie par

$$t(e_1) = e_1 \tag{9.352a}$$

$$t(e_2) = 0. \tag{9.352b}$$

La matrice de t dans cette base est

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{9.353}$$

Elle est symétrique : elle vérifie $A^t = A$. Si nous comptions sur la transposée de matrice pour définir la transposée de t, nous aurions $t^t = t$.

Soit maintenant la base $f_1 = e_1$, $f_2 = e_1 + e_2$. Nous avons $t(f_1) = f_1$ et

$$t(f_2) = t(e_1) + t(e_2) = e_1 = f_1. \tag{9.354}$$

Donc la matrice de t dans cette base est

$$B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}. \tag{9.355}$$

Et là, nous avons $B^t \neq B$. Donc en comptant sur cette base pour définir la transposée de t nous aurions $t^t \neq t$. △

9.182.
Autrement dit, la façon « usuelle » de voir la transposée d'une application linéaire, ne fonctionne dans les livres pour enfants uniquement parce qu'on y considère toujours $\mathbb{R}^n$ muni de la base canonique ou de bases orthonormées.

Notons que nous avons tout de même les notions d'opérateur adjoint et autoadjoint pour parler d'application orthogonale sans passer par la transposée, voir 9.37.

9.10.4 Transposée : la bonne approche

Définition 9.183.
Si $f\colon E \to F$ est une application linéaire entre deux espaces vectoriels, la ***transposée*** *est l'application $f^t\colon F^* \to E^*$ donnée par*

$$f^t(\omega)(x) = \omega\big(f(x)\big). \tag{9.356}$$

pour tout $\omega \in F^*$ et $x \in E$.

Lemme 9.184.
Soit E muni de la base $\{e_i\}$ et F muni de la base $\{g_i\}$ et une application $f\colon E \to F$. Si A est la matrice de f dans ces bases, alors A^t est la matrice de f^t dans les bases $\{e_i^*\}$ et $\{g_i^*\}$ de E^* et F^*.

Autrement dit, en utilisant l'application $\psi\colon \mathbb{M} \to \mathcal{L}(F^*, E^*)$ de la proposition 4.70,

$$\psi(A^t) = f^t. \tag{9.357}$$

Démonstration. Attention aux indices, ça va chauffer [71].

Nous allons montrer que $f^t = \psi(A^t)$ sur la base $\{g_i^*\}$, et pour cela nous appliquons $f^t(g_i^*)$ à $x \in E$:

$$\begin{aligned}
f^t(g_i^*)x &= g_i^*\big(f(x)\big) && \text{Définition 9.183} && (9.358a)\\
&= g_i^*\big(\sum_k x_k f(e_k)\big) && && (9.358b)\\
&= g_i^*\big(\sum_{kl} x_k A_{lk} g_l\big) && \text{eq. (4.86)} && (9.358c)\\
&= \sum_{kl} x_k A_{lk} \underbrace{g_i^*(g_l)}_{=\delta_{i,l}} && && (9.358d)\\
&= \sum_k x_k A_{ik} && && (9.358e)\\
&= \sum_k (A^t)_{ki} x_k && && (9.358f)\\
&= \sum_k (A^t)_{ki} e_k^*(x). && && (9.358g)
\end{aligned}$$

Voila. Donc nous avons

$$f^t(g_i^*) = \sum_k (A^t)_{ki} e_k^* = \psi(A^t) g_i^*. \tag{9.359}$$

□

9.185.
Intuitivement, les rangs de f et de f^t sont égaux parce que le rang est donné par la plus grande matrice carrée de déterminant non nul.

Nous donnons maintenant une vraie preuve de ce résultat.

Lemme 9.186 ([277]).
Si $f\colon E \to F$ est une application linéaire, alors

$$\operatorname{rk}(f) = \operatorname{rk}(f^t). \tag{9.360}$$

Démonstration. Soient $n = \dim(E)$ et $r = \dim(F)$. Nous posons $\dim\ker(f) = p$ et donc $\operatorname{rk}(f) = n - p$. Soit $\{e_1, \dots, e_p\}$ une base de $\ker(f)$ que l'on complète en une base $\{e_1, \dots, e_n\}$ de E. Nous considérons maintenant les vecteurs

$$g_i = f(e_{p+i}) \tag{9.361}$$

pour $i = 1, \dots, n-p$. C'est-à-dire que les g_i sont les images des vecteurs qui ne sont pas dans le noyau de f. Prouvons qu'ils forment une famille libre. Si

$$\sum_{k=1}^{n-p} a_k f(e_{p+k}) = 0, \tag{9.362}$$

alors $f\big(\sum_k a_k e_{p+k}\big) = 0$, c'est-à-dire $\sum_k a_k e_{p+k} \in \ker(f)$. Comme une base de $\ker(f)$ est $\{e_1, \dots, e_p\}$, il existe des b_l tels que $\sum_k a_k e_{p+k} = \sum_{l=1}^{p} b_l e_l$. Autrement dit,

$$\sum_k a_k e_{p+k} - \sum_{l=1}^{p} b_l e_l = 0, \tag{9.363}$$

71. Et merci à Alain Vigne pour m'avoir fait remarquer qu'il fallait mettre de l'ordre dans les indices.

qui est une combinaison linéaire nulle des e_i. Donc $a_k = b_l = 0$ pour tout k et l. Tout ça pour dire que les $\{g_i\}_{i=1,\dots,n-p}$ est libre.

Étant donné que les vecteurs $g_1, \dots, g_{n-p}$ sont libres, nous pouvons les compléter en une base de F :

$$\{\underbrace{g_1, \dots, g_{n-p}}_{\text{images}}, \underbrace{g_{n-p+1}, \dots, g_r}_{\text{complétion}}\}. \tag{9.364}$$

Nous prouvons maintenant que $\text{rk}(f^t) \geqslant n-p$ en montrant que les formes $\{g_i^*\}_{i=1,\dots,n-p}$ forment une partie libre (et donc l'espace image de f^t est au moins de dimension $n-p$). Pour cela nous prouvons que $f^t(g_i^*) = e_{i+p}^*$. En effet

$$f^t(g_i^*)(e_k) = g_i^*(f(e_k)), \tag{9.365}$$

Si $k = 1, \dots, p$, alors $f(e_k) = 0$ et donc $g_i^*(f(e_k)) = 0$; si $k = p + l$ alors

$$f^t(g_i^*)(e_k) = g_i^*(f(e_{k+l})) = g_i^*(g_l) = \delta_{i,l} = \delta_{i,k-p} = \delta_{k,i+p}. \tag{9.366}$$

Donc $f^t(g_i^*) = e_{i+p}^*$. Cela prouve que les formes $f^t(g_i^*)$ sont libres et donc que

$$\text{rk}(f^t) \geqslant n - p = \text{rk}(f). \tag{9.367}$$

En appliquant le même raisonnement à f^t au lieu de f, nous trouvons

$$\text{rk}\left((f^t)^t\right) \geqslant \text{rk}(f^t) \tag{9.368}$$

et donc, sachant que $(f^t)^t = f$, nous obtenons $\text{rk}(f) = \text{rk}(f^t)$.

□

Proposition 9.187 ([278]).
Si f est une application linéaire entre les espaces vectoriels E et F, alors nous avons

$$\text{Image}(f^t) = \ker(f)^\perp. \tag{9.369}$$

Démonstration. Soient donc l'application $f\colon E \to F$ et sa transposée $f^t\colon F^* \to E^*$. Nous commençons par prouver que $\text{Image}(f^t) \subset (\ker f)^\perp$. Pour cela nous prenons $\omega \in \text{Image}(f^t)$, c'est-à-dire $\omega = \alpha \circ f$ pour un certain élément $\alpha \in F^*$. Si $z \in \ker(f)$, alors $\omega(z) = (\alpha \circ f)(z) = 0$, c'est-à-dire que $\omega \in (\ker f)^\perp$.

Pour prouver qu'il y a égalité, nous n'allons pas démontrer l'inclusion inverse, mais plutôt prouver que les dimensions sont égales. Après, on sait que si $A \subset B$ et si $\dim A = \dim B$, alors $A = B$. Nous avons

$$\begin{aligned}
\dim\left(\text{Image}(f^t)\right) &= \text{rk}(f^t) && && \text{(9.370a)}\\
&= \text{rk}(f) && \text{lemme 9.186} && \text{(9.370b)}\\
&= \dim(E) - \dim\ker(f) && \text{théorème 4.46} && \text{(9.370c)}\\
&= \dim\left((\ker f)^\perp\right) && \text{proposition 4.130.} && \text{(9.370d)}
\end{aligned}$$

□

Lemme 9.188 ([127]).
Soit $\mathbb{K}$ un corps, E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie et une application linéaire $f\colon E \to F$. L'application f est injective si et seulement si sa transposée[72] *f^t est surjective.*

Démonstration. Supposons que f soit injective. Alors par le lemme 4.55, il existe $g\colon F \to E$ tel que $g \circ f = \text{Id}|_E$. Nous avons alors aussi $(g \circ f)^t = \text{Id}|_{E^*}$, mais $(g \circ f)^t = f^t \circ g^t$, donc f^t est surjective.

Inversement, nous supposons que $f^t\colon F^* \to E^*$ est surjective. Alors en nous souvenant que E et F sont de dimension finie et en faisant jouer les identifications $(f^t)^t = f$ et $(E^*)^* = E$ nous savons qu'il existe $s\colon E^* \to F^*$ tel que $f^t \circ s = \text{Id}|_{E^*}$. En passant à la transposée,

$$s^t \circ f = \text{Id}|_E, \tag{9.371}$$

qui implique que f est injective. □

72. Définition 9.183.

9.10.5 Polynômes de Lagrange

Lemme-Définition 9.189.
Soit $E = \mathcal{P}_n(\mathbb{R})$ l'ensemble des polynômes à coefficients réels de degré au plus n. Soient $n+1$ réels distincts $a_0, \dots, a_n$. Nous considérons les formes linéaires associées $f_i \in \mathcal{P}_n(\mathbb{R})^*$,

$$f_i(P) = P(a_i). \tag{9.372}$$

La partie $\{f_1, \dots, f_n\}$ est une base de $\mathcal{P}_n(\mathbb{R})^*$.

*Les **polynômes de Lagrange** aux points (a_i) sont les polynômes de la base préduale de la base $\{f_i\}$.*

Démonstration. Nous prouvons que l'orthogonal est réduit au singleton nul :

$$\text{Span}\{f_0, \dots, f_n\}^\perp = \{0\}. \tag{9.373}$$

La proposition 4.130 conclura. Si $P \in \text{Span}\{f_i\}^\perp$, alors $f_i(P) = 0$ pour tout i, ce qui fait que $P(a_i) = 0$ pour tout $i = 0, \dots, n$. Un polynôme de degré au plus n qui s'annule en $n+1$ points est automatiquement le polynôme nul. □

Proposition 9.190.
Les polynômes de Lagrange aux points $(a_i)_{i=1,\dots,n}$ sont donnés par

$$P_i = \prod_{k \neq i} \frac{X - a_k}{a_i - a_k}. \tag{9.374}$$

Démonstration. Il suffit de vérifier que $f_j(P_i) = \delta_{i,j}$. Nous avons

$$f_j(P_i) = P_i(a_j) = \prod_{k \neq i} \frac{a_j - a_k}{a_i - a_k}. \tag{9.375}$$

Si $j \neq i$ alors un des termes est nul. Si au contraire $i = j$, tous les termes valent 1. □

9.10.6 Dual de $\mathbb{M}(n, \mathbb{K})$

Proposition 9.191 ([102]).
Soit $\mathbb{K}$, un corps. Les formes linéaires sur $\mathbb{M}(n, \mathbb{K})$ sont les applications de la forme

$$\begin{aligned} f_A \colon \mathbb{M}(n, \mathbb{K}) &\to \mathbb{K} \\ M &\mapsto \text{Tr}(AM). \end{aligned} \tag{9.376}$$

Démonstration. Nous considérons l'application

$$\begin{aligned} f \colon \mathbb{M}(n, \mathbb{K}) &\to \mathbb{M}(n, \mathbb{K})^* \\ A &\mapsto f_A \end{aligned} \tag{9.377}$$

et nous voulons prouver que c'est une bijection. Étant donné que nous sommes en dimension finie, nous avons égalité des dimensions de $\mathbb{M}(n, \mathbb{K})$ et $(\mathbb{M}(n, \mathbb{K}))^*$, et il suffit de prouver que f est injective. Soit donc A telle que $f_A = 0$. Nous l'appliquons à la matrice $(E_{ij})_{kl} = \delta_{ik}\delta_{jl}$:

$$0 = f_A(E_{ij}) = \sum_k (AE_{ij})_{kk} = \sum_{kl} A_{kl}(E_{ij})_{lk} = \sum_{kl} A_{kl}\delta_{il}\delta_{jk} = A_{ji}. \tag{9.378}$$

Donc $A = 0$. □

Corolaire 9.192 ([102]).
Soient un corps $\mathbb{K}$ ainsi qu'une application $\phi \in \mathbb{M}(n, \mathbb{K})^*$ telle que pour tout $M, N \in \mathbb{M}(n, \mathbb{K})$ on ait

$$\phi(MN) = \phi(NM). \tag{9.379}$$

Alors il existe $\lambda \in \mathbb{K}$ tel que $\phi = \lambda \,\text{Tr}$.

Démonstration. La proposition 9.191 nous donne une matrice $A \in \mathbb{M}(n,\mathbb{K})$ telle que $\phi = f_A$. L'hypothèse nous dit que $f_A(MN) = f_A(NM)$, c'est-à-dire

$$\mathrm{Tr}(AMN) = \mathrm{Tr}(ANM) \tag{9.380}$$

pour toutes matrices $M, N \in \mathbb{M}(n,\mathbb{K})$. L'invariance cyclique de la trace[73] appliqué au membre de droite nous donne $\mathrm{Tr}(AMN) = \mathrm{Tr}(MAN)$, ce qui signifie que

$$\mathrm{Tr}\big((AM - MA)N\big) = 0 \tag{9.381}$$

ou encore que $f_{AM-MA} = 0$, et ce, pour toute matrice M. La fonction f étant injective nous en déduisons que la matrice A doit satisfaire

$$AM = MA \tag{9.382}$$

pour tout $M \in \mathbb{M}(n,\mathbb{K})$. En particulier, en prenant pour M les fameuses matrices E_{ij} et en calculant un peu,

$$A_{li}\delta_{j,m} = \delta_{i,l}A_{jm} \tag{9.383}$$

pour tout i, j, l, m. Cela implique que $A_{ll} = A_{mm}$ pour tout l et m et que $A_{jm} = 0$ dès que $j \neq m$. Il existe donc $\lambda \in \mathbb{K}$ tel que $A = \lambda\mathbb{1}$. En fin de compte,

$$\phi(X) = f_{\lambda\mathbb{1}}(X) = \lambda\,\mathrm{Tr}(X). \tag{9.384}$$

□

Corolaire 9.193 ([102]).
Soit $\mathbb{K}$ un corps. Tout hyperplan de $\mathbb{M}(n,\mathbb{K})$ coupe $\mathrm{GL}(n,\mathbb{K})$.

Démonstration. Soit $\mathcal{H}$ un hyperplan de $\mathbb{M}(n,\mathbb{K})$. Il existe une forme linéaire ϕ sur $\mathbb{M}(n,\mathbb{K})$ telle que $\mathcal{H} = \ker(\phi)$. Encore une fois la proposition 9.191 nous donne $A \in \mathbb{M}(n,\mathbb{K})$ telle que $\phi = f_A$; nous notons r le rang de A. Par le lemme 4.109 nous avons $A = PJ_rQ$ avec $P, Q \in \mathrm{GL}(n,\mathbb{K})$ et

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{9.385}$$

Pour tout $M \in \mathbb{M}(n,\mathbb{K})$ nous avons

$$\phi(M) = \mathrm{Tr}(AM) = \mathrm{Tr}(PJ_rQM) = \mathrm{Tr}(J_rQMP), \tag{9.386}$$

la dernière égalité découlant de l'invariance cyclique de la trace[74]. Ce que nous cherchons est $M \in \mathrm{GL}(n,\mathbb{K})$ telle que $\phi(M) = 0$. Nous commençons par trouver $N \in \mathrm{GL}(n,\mathbb{K})$ telle que $\mathrm{Tr}(J_rN) = 0$. Celle-là est facile : c'est

$$N = \begin{pmatrix} 0 & 1 \\ \mathbb{1}_{n-1} & 0 \end{pmatrix}. \tag{9.387}$$

Les éléments diagonaux de J_rN sont tous nuls. Par conséquent en posant $M = Q^{-1}NP^{-1}$ nous avons notre matrice inversible dans le noyau de ϕ. □

9.11 Diagonalisation et trigonalisation

Ici encore $\mathbb{K}$ est un corps commutatif.

73. Lemme 4.64.
74. Lemme 4.64.

9.11.1 Matrices semblables

Proposition-Définition 9.194 (matrices semblables[1])**.**
Nous définissons, sur l'ensemble $\mathbb{M}(n,\mathbb{K})$ *des matrices* $n\times n$ *à coefficients dans* $\mathbb{K}$*, la relation* $A\sim B$ *si et seulement si il existe une matrice* $P\in \mathrm{GL}(n,\mathbb{K})$ *telle que* $B=P^{-1}AP$*.*

Cette relation est une relation d'équivalence.

Deux matrices équivalentes en ce sens sont dites ***semblables****.*

Proposition-Définition 9.195 (Matrices équivalentes)**.**
Nous définissons, sur l'ensemble $\mathbb{M}(n,\mathbb{K})$ *des matrices* $n\times n$ *à coefficients dans* $\mathbb{K}$*, la relation* $A\sim B$ *si et seulement si il existe des matrice inversibles* P *et* Q *telles que* $A=PBQ^{-1}$*.*

Cette relation est une relation d'équivalence.

Deux telles matrice sont dite ***équivalentes****.*

Proposition-Définition 9.196.
Soit un espace vectoriel E*. Nous définissons sur* $\mathrm{End}(E)$ *la relation* $u\sim v$ *si et seulement si il existe une application inversible* $A\colon E\to E$ *telle que* $v=A^{-1}\circ u\circ A$*.*

Cette relation est une relation d'équivalence.

Deux endomorphismes équivalents en ce sens sont dits ***semblables****.*

Proposition 9.197.
Deux applications linéaires sont semblables si et seulement si leurs matrices sont semblables dans toute base.

Lemme 9.198.
Le polynôme caractéristique[75] *est un invariant sous les similitudes.*

Démonstration. En effet si P est une matrice inversible,

$$\begin{aligned}\chi_{P^{-1}AP} &= \det(P^{-1}AP-\lambda X\mathbb{1}) && (9.388a)\\ &= \det\left(P(P^{-1}AP-\lambda X\mathbb{1})P^{-1}\right) && (9.388b)\\ &= \det(A-\lambda X\mathbb{1}) && (9.388c)\\ &= \chi_A. && (9.388d)\end{aligned}$$

□

La permutation de lignes ou de colonnes ne sont pas des similitudes, comme le montrent les exemples suivants :

$$A=\begin{pmatrix}1&2\\3&4\end{pmatrix}\quad B=\begin{pmatrix}2&1\\4&3\end{pmatrix}. \tag{9.389}$$

Nous avons $\chi_A=X^2-5X-2$ tandis que $\chi_B=X^2-5X+2$ alors que le polynôme caractéristique est un invariant de similitude.

9.11.2 Trace de matrices semblables

Proposition 9.199 ([1])**.**
Invariance de la trace par similarité.

(1) Soit une application linéaire f*. Si la matrice de* f *dans une base est* A *et est* B *dans une autre base, alors*

$$\mathrm{Tr}(A)=\mathrm{Tr}(B). \tag{9.390}$$

(2) Deux opérateurs semblables[76] *ont même trace.*

75. Définition 9.107.
76. Opérateurs semblables, définition 9.194

Démonstration. Les matrices A et B sont liées par la proposition 4.116 : $B = Q^{-1}AQ$ où Q est la matrice qui lie les vecteurs des deux bases. L'invariance cyclique de la trace donnée en le lemme 4.64 implique que

$$\mathrm{Tr}(B) = \mathrm{Tr}(Q^{-1}AQ) = \mathrm{Tr}(QQ^{-1}A) = \mathrm{Tr}(A). \tag{9.391}$$

□

Lemme 9.200.
Soit une matrice A. Nous avons

$$\mathrm{Tr}(A^\dagger A) = \sum_{ij} |A_{ij}|^2. \tag{9.392}$$

Démonstration. Utilisant la proposition 9.172 pour les éléments de la matrice $A^\dagger$, nous avons

$$\mathrm{Tr}(A^\dagger A) = \sum_k (A^\dagger A)_{kk} = \sum_{kl} A^*_{lk}A_{lk} = \sum_{kl} |A_{lk}|^2. \tag{9.393}$$

□

Lemme 9.201 ([279]).
Si les matrice A et B sont unitairement semblables[77]*, alors*

$$\sum_{ij} |A_{ij}|^2 = \sum_{ij} |B_{ij}|^2. \tag{9.394}$$

Démonstration. Soit une matrice unitaire U telle que $B = UAU^\dagger$. Nous savons par le proposition 9.199 que des matrice semblables ont même trace. Or $B^\dagger B$ est unitairement semblable à $A^\dagger A$ parce que

$$B^\dagger B = UA^\dagger U^\dagger UAU^\dagger = UA^\dagger AU^\dagger. \tag{9.395}$$

Donc $\mathrm{Tr}(A^\dagger A) = \mathrm{Tr}(B^\dagger B)$. Le lemme 9.200 conclut. □

9.11.3 Endomorphismes nilpotents

La **trace** d'une matrice $A \in \mathbb{M}(n, \mathbb{K})$ est la somme de ses éléments diagonaux :

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} A_{ii}. \tag{9.396}$$

Une propriété importante est son invariance cyclique.

Lemme 9.202.
Quelques propriétés de la trace.

(1) Si A et B sont des matrices carrées, alors $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

(2) La trace est un invariant de similitude.

Démonstration. C'est un simple calcul :

$$\mathrm{Tr}(AB) = \sum_{ik} A_{ik}B_{ki} = \sum_{ik} A_{ki}B_{ik} = \sum_{ik} B_{ik}A_{ki} = \sum_i (BA)_{ii} = \mathrm{Tr}(BA) \tag{9.397}$$

où nous avons simplement renommé les indices $i \leftrightarrow k$.

En particulier, la trace est un invariant de similitude parce que $\mathrm{Tr}(ABA^{-1}) = \mathrm{Tr}(A^{-1}AB) = \mathrm{Tr}(B)$ par l'invariance cyclique démontrée en 4.64(2). □

La trace étant un invariant de similitude, nous pouvons donc définir la **trace** comme étant la trace de sa matrice dans une base quelconque. Si la matrice est diagonalisable, alors la trace est la somme des valeurs propres.

77. Définition 9.194.

Lemme 9.203 ([111]).
L'endomorphisme $u \in \mathrm{End}(\mathbb{C}^n)$ est nilpotent si et seulement si $\mathrm{Tr}(u^p) = 0$ pour tout p.

Démonstration. Supposons que u est nilpotent. Alors ses valeurs propres sont toutes nulles et celles de u^p le sont également. La trace étant la somme des valeurs propres, nous avons alors tout de suite $\mathrm{Tr}(u^p) = 0$.

Supposons maintenant que $\mathrm{Tr}(u^p) = 0$ pour tout p. Le polynôme caractéristique (9.227) est

$$\chi_u = (-1)^n X^\alpha (X - \lambda_1)^{\alpha_1} \dots (X - \lambda_r)^{\alpha_r}. \tag{9.398}$$

où les λ_i $(i = 1, \dots, r)$ sont les valeurs propres non nulles distinctes de u.

Il est vite vu que le coefficient de X^{n-1} dans χ_u est $-\mathrm{Tr}(u)$ parce que le coefficient de X^{n-1} se calcule en prenant tous les X sauf une fois $-\lambda_i$. D'autre part le polynôme caractéristique de u^p est le même que celui de u, en remplaçant λ_i par λ_i^p ; cela est dû au fait que si v est vecteur propre de valeur propre λ, alors $u^p v = \lambda^p v$.

Par l'équation (9.398), nous voyons que le coefficient du terme X^{n-1} dans le polynôme caractéristique est

$$0 = \mathrm{Tr}(u^p) = \alpha_1 \lambda_1^p + \dots + \alpha_r \lambda_r^p. \tag{9.399}$$

Donc les nombres $(\alpha_1, \dots, \alpha_r)$ sont une solution non triviale [78] du système

$$\begin{cases} \lambda_1 X_1 + \dots + \lambda_r X_r = 0 & \text{(9.400a)} \\ \quad \vdots & \text{(9.400b)} \\ \lambda_1^r X_1 + \dots + \lambda_r^r X_r = 0. & \text{(9.400c)} \end{cases}$$

Ce sont les équations (9.399) écrites pour $p = 1, \dots, r$. Le déterminant de ce système est

$$\lambda_1 \dots \lambda_r \det \begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_r \\ \vdots & & \vdots \\ \lambda_1^{r-1} & \dots & \lambda_r^{r-1} \end{pmatrix} \neq 0, \tag{9.401}$$

qui est un déterminant de Vandermonde (proposition 9.12) valant

$$0 = \lambda_1 \dots \lambda_r \prod_{1 \leqslant i \leqslant j \leqslant r} (\lambda_i - \lambda_j). \tag{9.402}$$

Étant donné que les λ_i sont distincts et non nuls, nous avons une contradiction et nous devons conclure que $(\alpha_1, \dots, \alpha_r)$ était une solution triviale du système (9.400). □

Proposition 9.204 ([280]).
Soit un $\mathbb{K}$-espace vectoriel E. Un endomorphisme $u \in \mathrm{End}(E)$ est nilpotent si et seulement si il existe une base de E dans laquelle la matrice de u est strictement triangulaire supérieure.

Démonstration. (i) $\Rightarrow$ Nous faisons la démonstration par récurrence sur la dimension de E. Lorsque $n = 1$ nous avons $u = (a)$ avec $a \in \mathbb{K}$. Puisque $a^k = 0$ pour un certain k nous avons $a = 0$ parce qu'un corps est toujours un anneau intègre [79].

Lorsque $\dim(E) = n$ nous savons que u a un noyau non réduit au vecteur nul (parce qu'il est nilpotent). Soit donc un vecteur non nul $x \in \ker(u)$ et une base

$$\{x, e_2, \dots, e_n\} \tag{9.403}$$

donnée par le théorème de la base incomplète 4.13. La matrice de u dans cette base s'écrit

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A & \\ 0 & & & \end{array}\right). \tag{9.404}$$

78. Si $\alpha_1 = \dots = \alpha_r = 0$, alors les valeurs propres sont toutes nulles et la matrice est en réalité nulle dès le départ.
79. Lemme 1.193.

Un tout petit peu de calcul de produit de matrice montre que la matrice de u^k est de la forme

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A^k & \\ 0 & & & \end{array}\right). \tag{9.405}$$

Étant donné que l'endomorphisme u est nilpotent, la matrice A l'est aussi. L'hypothèse de récurrence dit alors que A est strictement triangulaire supérieure (ou en tout cas peut le devenir par un changement de base adéquat).

(ii) $\Leftarrow$ Soit une base $\{e_1, \ldots, e_n\}$ dans laquelle la matrice de u est strictement triangulaire supérieure.

Alors $u(e_1) = 0$ et plus généralement, $u(e_k) \in \text{Span}\{e_1, \ldots, e_{k-1}\}$. Voyez par récurrence que $u^l(e_k) \in \text{Span}\{e_1, \ldots, e_{k-l}\}$. Donc $u^l(e_k) = 0$ dès que $l \geqslant k$.

□

Lemme 9.205 ([1]).
Si $N \in \mathbb{M}(n, \mathbb{C})$ est une matrice nilpotente d'ordre de nilpotence r, alors $\{N^k\}_{k=0,\ldots,r-1}$ est libre dans $\mathbb{M}(n, \mathbb{C})$.

Proposition 9.206 (Thème 40).
Soit E un espace de Banach (espace vectoriel normé complet[80]). Si $A \in \mathcal{L}(E, E)$ est nilpotente, alors $(\mathbb{1} - A)$ est inversible et son inverse est donné par

$$(\mathbb{1} - A)^{-1} = \sum_{k=0}^{\infty} A^k, \tag{9.406}$$

où l'infini peut évidemment être remplacé par l'ordre de nilpotence de A.

Démonstration. En ce qui concerne la convergence de la somme, elle ne fait pas de doute parce que A étant nilpotente, la somme contient seulement une quantité finie de termes non nuls.

Montrons à présent que la somme est l'inverse de $\mathbb{1} - A$ en multipliant terme à terme :

$$\sum_{k=0}^{n} A^k(\mathbb{1} - A) = \sum_{k=0}^{n} (A^k - A^{k+1}) = \mathbb{1} - A^{n+1}. \tag{9.407}$$

Par conséquent

$$\|\mathbb{1} - \sum_{k=0}^{n} A^k(\mathbb{1} - A)\| = \|A^{n+1}\| \to 0. \tag{9.408}$$

La dernière limite est en réalité une égalité pour n assez grand. □

9.11.4 Endomorphismes diagonalisables

Définition 9.207.
*Une matrice est **diagonalisable** si elle est semblable[81] à une matrice diagonale.*

Une application linéaire est diagonalisable si elle est semblable[82] à une application linéaire diagonale.

Autrement dit, A est diagonalisable si il existe un opérateur diagonal D et un opérateur inversible P tels que $PAP^{-1} = D$.

La proposition 9.197 nous assure que la notion de diagonalisabilité pour les matrices et pour les applications sont les mêmes.

80. Définition 7.241.
81. Définition 9.194.
82. Définition 9.196.

Proposition 9.208.
Si A est un opérateur diagonalisable dont les valeurs propres sont λ_i, alors il existe un opérateur inversible Q tel que

$$A = Q^{-1}DQ \tag{9.409}$$

où D est l'opérateur diagonal contenant les λ_i sur sa diagonale.

Lemme 9.209.
Une matrice triangulaire supérieure avec des 1 sur la diagonale n'est diagonalisable que si elle est diagonale (c'est-à-dire si c'est la matrice unité).

Démonstration. Si A est une matrice triangulaire supérieure de taille n telle que $A_{ii} = 1$, alors $\det(A - \lambda\mathbb{1}) = (1 - \lambda)^n$, ce qui signifie que $\text{Spec}(A) = \{1\}$. Pour la diagonaliser, il faudrait une matrice $P \in \text{GL}(n, \mathbb{K})$ telle que $\mathbb{1} = P^{-1}AP$, ce qui est uniquement possible si $A = \mathbb{1}$. □

Lemme 9.210.
Soit F un sous-espace stable par u. Soit une décomposition du polynôme minimal

$$\mu_u = P_1^{n_1} \dots P_r^{n_r} \tag{9.410}$$

où les P_i sont des polynômes irréductibles unitaires distincts. Si nous posons $E_i = \ker P_i^{n_i}$, alors

$$F = (F \cap E_1) \oplus \dots \oplus (F \cap E_r). \tag{9.411}$$

Théorème 9.211.
Soit E, un espace vectoriel de dimension n sur le corps commutatif $\mathbb{K}$ et $u \in \text{End}(E)$. Les propriétés suivantes sont équivalentes.

1. *L'endomorphisme u est diagonalisable.*
2. *Il existe un polynôme $P \in \mathbb{K}[X]$ non constant, scindé sur $\mathbb{K}$, dont toutes les racines sont simples, tel que $P(u) = 0$.*
3. *Le polynôme minimal μ_u est scindé sur $\mathbb{K}$ et toutes ses racines sont simples*[83].
4. *Tout sous-espace de E possède un supplémentaire stable par u.*
5. *Dans une base adaptée, la matrice de u est diagonale et les éléments diagonaux sont ses valeurs propres.*

Démonstration. Plein d'implications à prouver.

(i) **(2) implique (3)** Étant donné que $P(u) = 0$, il est dans l'idéal des polynômes annulateurs de u, et le polynôme minimal μ_u le divise parce que l'idéal des polynômes annulateurs est généré par μ_u par le théorème 6.43.

(ii) **(3) implique (1)** Étant donné que le polynôme minimal est scindé à racines simples, il s'écrit sous forme de produits de monômes tous distincts, c'est-à-dire

$$\mu_u(X) = (X - \lambda_1) \dots (X - \lambda_r) \tag{9.413}$$

où les λ_i sont des éléments distincts de $\mathbb{K}$. Étant donné que $\mu_u(u) = 0$, le théorème de décomposition des noyaux (théorème 9.86) nous enseigne que

$$E = \ker(u - \lambda_1) \oplus \dots \oplus \ker(u - \lambda_r). \tag{9.414}$$

Mais $\ker(u - \lambda_i)$ est l'espace propre $E_{\lambda_i}(u)$. Donc u est diagonalisable.

83. Le polynôme *caractéristique*, lui, n'a pas spécialement ses racines simples ; il peut encore être de la forme

$$\chi_u(X) = \prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i}, \tag{9.412}$$

mais alors $\dim(E_{\lambda_i}) = \alpha_i$.

(iii) **(1) implique (4)** Soit $\{e_1, \dots, e_n\}$ une base qui diagonalise u, soit F un sous-espace de E et $\{f_1, \dots, f_r\}$ une base de F. Par le théorème 4.17(2), nous pouvons compléter la base de F par des éléments de la base $\{e_i\}$. Le complément ainsi construit est stable par u.

(iv) **(4) implique (1)** En dimension un, tout endomorphisme est diagonalisable, nous supposons donc que $\dim E = n \geqslant 2$. Nous procédons par récurrence sur le nombre de vecteurs propres connus de u. Supposons avoir déjà trouvé p vecteurs propres $e_1, \dots, e_p$ de u. Considérons H, un hyperplan qui contient les vecteurs $e_1, \dots, e_p$. Soit F un supplémentaire de H stable par u ; par construction $\dim F = 1$ et si $e_{p+1} \in F$, il doit être vecteur propre de u.

(v) **(1) implique (2)** Nous supposons maintenant que u est diagonalisable. Soient $\lambda_1, \dots, \lambda_r$ les valeurs propres deux à deux distinctes, et considérons le polynôme

$$P(x) = (X - \lambda_1) \dots (X - \lambda_r). \tag{9.415}$$

Alors $P(u) = 0$. En effet si e_i est un vecteur propre pour la valeur propre λ_i,

$$P(u)e_i = \prod_{j \neq i} (u - \lambda_j) \circ (u - \lambda_i)e_i = 0 \tag{9.416}$$

par le lemme 9.85. Par conséquent $P(u)$ s'annule sur la base $\{e_i\}$.

(vi) **(5) implique (2)** Si la matrice A est diagonale alors le polynôme $P = \prod_{i=1}^{n} (X - A_{ii})$ est annulateur de A. En effet,

$$P(A)e_k = \prod_{i=1}^{n} (A - A_{ii})x = \prod_{i=1}^{n} \big(u(e_k) - A_{ii}e_k\big) = \prod_{i=1}^{n} \big(A_{kk}e_k - A_{ii}e_k\big) = 0 \tag{9.417}$$

parce que le facteur $i = k$ est nul.

(vii) **(3) implique (5)** le polynôme minimal de u s'écrit

$$\mu = (X - \lambda_1) \dots (X - \lambda_r), \tag{9.418}$$

et les espaces E_i du lemme 9.210 sont les espaces propres $E_i = \ker(u - \lambda_i)$. Nous avons donc une somme directe

$$E = E_1 \oplus \dots \oplus E_r. \tag{9.419}$$

Dans chacun des espaces propres, u a une matrice diagonale avec la valeur propre correspondante sur la diagonale. Une base de E constituée d'une base de chacun des espaces propres est donc une base comme nous en cherchons.

□

Corolaire 9.212.
Si u est diagonalisable et si F est un sous-espace stable par u, alors

$$F = \bigoplus_{\lambda} E_\lambda(u) \cap F \tag{9.420}$$

où $E_\lambda(u)$ est l'espace propre de u pour la valeur propre λ. En particulier la restriction de u à F, $u|_F$ est diagonalisable.

Démonstration. Par le théorème 9.211, le polynôme μ_u est scindé et ne possède que des racines simples. Notons le

$$\mu_u(X) = (X - \lambda_1) \dots (X - \lambda_r). \tag{9.421}$$

Les espaces E_i du lemme 9.210 sont maintenant les espaces propres.

En ce qui concerne la diagonalisabilité de $u|_F$, notons que nous avons une base de F composée de vecteurs dans les espaces $E_\lambda(u)$. Cette base de F est une base de vecteurs propres de u. □

Lemme 9.213.
Soient E un $\mathbb{K}$-espace vectoriel et $u \in \mathrm{End}(E)$. Si $\mathrm{Card}\big(\mathrm{Spec}(u)\big) = \dim(E)$ alors u est diagonalisable.

Démonstration. Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres distinctes de u. Nous savons que les espaces propres correspondants sont en somme directe (lemme 9.84). Par conséquent $\mathrm{Span}\{E_{\lambda_i}(u)\}$ est de dimension $n = \dim(E)$ et u est diagonalisable. □

Voici un résultat de diagonalisation simultanée. Nous donnerons un résultat de trigonalisation simultanée dans le lemme 12.105.

Proposition 9.214 (Diagonalisation simultanée)**.**
Soit $(u_i)_{i\in I}$ une famille d'endomorphismes qui commutent deux à deux.

(1) Si $i, j \in I$ alors tout sous-espace propre de u_i est stable par u_j. Autrement dit $u_j\big(E_\lambda(u_i)\big) \subset E_\lambda(u_i)$.
(2) Si les u_i sont diagonalisables, alors ils le sont simultanément.

Démonstration. Supposons que u_i et u_j commutent et soit x un vecteur propre de u_i : $u_i(x) = \lambda x$. Nous montrons que $u_j(x) \in E_\lambda(u_i)$. Nous avons

$$u_i\big(u_j(x)\big) = u_j\big(u_i(x)\big) = \lambda u_j(x). \tag{9.422}$$

Par conséquent $u_j(x)$ est vecteur propre de u_i de valeur propre λ.

Montrons maintenant l'affirmation à propos des endomorphismes simultanément diagonalisables. Si $\dim E = 1$, le résultat est évident. Nous supposons également qu'aucun des u_i n'est multiple de l'identité. Nous effectuons une récurrence sur la dimension.

Soit u_0 un des u_i et considérons ses valeurs propres deux à deux distinctes $\lambda_1, \dots, \lambda_r$. Pour chaque k nous avons

$$E_{\lambda_k}(u_0) \neq E, \tag{9.423}$$

sinon u_0 serait un multiple de l'identité. Par contre le fait que u_0 soit diagonalisable permet de décomposer E en espaces propres de u_0 :

$$E = \bigoplus_k E_{\lambda_k}(u_0). \tag{9.424}$$

Ce que nous allons faire est de simultanément diagonaliser les $(u_i)_{i\in I}$ sur chacun des E_{λ_k} séparément. Par le point (1), nous avons $u_i \colon E_{\lambda_k}(u_0) \to E_{\lambda_k}(u_0)$, et nous pouvons considérer la famille d'opérateurs

$$\Big(u_i|_{E_{\lambda_k}(u_0)}\Big)_{i\in I}. \tag{9.425}$$

Ce sont tous des opérateurs qui commutent et qui agissent sur un espace de dimension plus petite. Par hypothèse de récurrence nous avons une base de $E_{\lambda_k}(u_0)$ qui diagonalise tous les u_i. □

Exemple 9.215.
Soit un espace vectoriel sur un corps $\mathbb{K}$. Un opérateur **involutif** est un opérateur différent de l'identité dont le carré est l'identité. Typiquement une symétrie orthogonale dans $\mathbb{R}^3$. Le polynôme caractéristique d'une involution est $X^2 - 1 = (X + 1)(X - 1)$.

Tant que $1 \neq -1$, $X^2 - 1$ est donc scindé à racines simples et les involutions sont diagonalisables (9.211). Cependant si le corps est de caractéristique 2, alors $X^2 - 1 = (X + 1)^2$ et l'involution n'est plus diagonalisable.

Par exemple si le corps est de caractéristique 2, nous avons

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{9.426a}$$

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{9.426b}$$

Cette matrice A représente donc une involution, mais n'est pas diagonalisable. △

9.11.5 Diagonalisation : cas complexe, pas toujours

Il n'est pas vrai qu'une matrice de $\mathbb{M}(n,\mathbb{C})$ soit toujours diagonalisable. En effet le théorème 9.211(3) dit qu'une matrice est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples. Certes sur $\mathbb{C}$ le polynôme minimal sera scindé, mais il ne sera pas spécialement à racines simples.

Exemple 9.216.
La matrice

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{9.427}$$

a pour polynôme caractéristique $\chi_A(X) = X^2$. C'est également son polynôme minimal, qui n'est pas à racine simple.

Il est par ailleurs facile de voir que le seul espace propre de A est $\text{Span}\{(1,0)\}$ (ici le span est sur $\mathbb{C}$). Donc l'espace $\mathbb{C}^2$ ne possède pas de base de vecteurs propres de A. △

Ce qui est vrai, c'est que le polynôme caractéristique a des racines, et que ces racines correspondent à des vecteurs propres. Mais il n'y a pas toujours autant de vecteurs propres que la multiplicité des racines.

9.217.
Lorsque la diagonalisation n'est pas possible, il est souvent possible de trigonaliser. Les matrices triangulaires ne sont pas aussi faciles à manipuler que les matrices diagonales, mais c'est toujours ça de pris.

Nous étudierons ça plus tard, en 12.10.1 parce que ça va nécéssiter le théorème de d'Alembert.

9.11.6 Diagonalisation : cas réel

Lemme 9.218 (Lemme de Schur réel)**.**
Soit $A \in \mathbb{M}(n,\mathbb{R})$. Il existe une matrice orthogonale Q telle que $Q^{-1}AQ$ soit de la forme

$$Q^{-1}AQ = \begin{pmatrix} \lambda_1 & * & * & * & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \lambda_r & * & * \\ 0 & 0 & 0 & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & * \\ 0 & 0 & 0 & 0 & \begin{pmatrix} a_s & b_s \\ c_s & d_s \end{pmatrix} \end{pmatrix}. \tag{9.428}$$

Le déterminant de A est le produit des déterminants des blocs diagonaux et les valeurs propres de A sont les $\lambda_1,\dots,\lambda_r$ et celles de ces blocs.

Démonstration. Si la matrice A a des valeurs propres réelles, nous procédons comme dans le cas complexe. Cela nous fournit le partie véritablement triangulaire avec les valeurs propres $\lambda_1,\dots,\lambda_r$ sur la diagonale. Supposons donc que A n'a pas de valeurs propres réelles. Soit donc $\alpha+i\beta$ une valeur propre ($\beta\neq 0$) et $u+iv$ un vecteur propre correspondant où u et v sont des vecteurs réels. Nous avons

$$Au + iAv = A(u+iv) = (\alpha+i\beta)(u+iv) = \alpha u - \beta v + i(\alpha v + \beta u), \tag{9.429}$$

et en égalisant les parties réelles et imaginaires,

$$Au = \alpha u - \beta v \tag{9.430a}$$
$$Av = \alpha v + \beta u. \tag{9.430b}$$

Sur ces relations nous voyons que ni u ni v ne sont nuls. De plus u et v sont linéairement indépendants (sur $\mathbb{R}$), en effet si $v = \lambda u$ nous aurions $Au = \alpha u - \beta\lambda u = (\alpha - \beta\lambda)u$, ce qui serait une valeur propre réelle alors que nous avions supposé avoir déjà épuisé toutes les valeurs propres réelles.

Étant donné que u et v sont deux vecteurs réels non nuls et linéairement indépendants, nous pouvons trouver une base orthonormée $\{q_1, q_2\}$ de $\text{Span}\{u, v\}$. Nous pouvons étendre ces deux vecteurs en une base orthonormée $\{q_1, q_2, q_3, \ldots, q_n\}$ de $\mathbb{R}^n$. Nous considérons à présent la matrice orthogonale dont les colonnes sont formées de ces vecteurs : $Q = [q_1\, q_2\, \ldots\, q_n]$.

L'espace $\text{Span}\{e_1, e_2\}$ est stable par $Q^{-1}AQ$, en effet nous avons

$$Q^{-1}AQe_1 = Q^{-1}Aq_1 = Q^{-1}(aq_1 + bq_2) = ae_1 + be_2. \tag{9.431}$$

La matrice $Q^{-1}AQ$ est donc de la forme

$$Q^{-1}AQ = \begin{pmatrix} \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix} & C_1 \\ 0 & A_1 \end{pmatrix} \tag{9.432}$$

où C_1 est une matrice réelle $2 \times (n-1)$ quelconque et A_1 est une matrice réelle $(n-2) \times (n-2)$. Nous pouvons appliquer une récurrence sur la dimension pour poursuivre.

Notons que si A n'a pas de valeurs propres réelles, elle est automatiquement d'ordre pair parce que les valeurs propres complexes viennent par couple complexes conjugués.

En ce qui concerne les valeurs propres, il est facile de voir en regardant (9.428) que les valeurs propres sont celles des blocs diagonaux. Étant donné que $Q^{-1}AQ$ et A ont même polynôme caractéristique, ce sont les valeurs propres de A. □

Théorème 9.219 (Théorème spectral, matrice symétrique[102])**.**
Une matrice symétrique réelle,

(1) a un spectre contenu dans $\mathbb{R}$

(2) est diagonalisable par une matrice orthogonale.

Si M est une matrice symétrique réelle alors $\mathbb{R}^n$ possède une base orthonormée de vecteurs propres de M.

Démonstration. Soit A une matrice réelle symétrique. Elle agit sur l'espace $\mathbb{C}^n$ par la définition 4.67, et en particulier la formule 4.82. Nous munissons de plus $\mathbb{C}^n$ de la forme sesquilinéaire définie en la proposition 9.177.

Si λ est une valeur propre complexe pour le vecteur propre complexe v, alors d'une part $\langle Av, v\rangle = \lambda\langle v, v\rangle$ et d'autre part $\langle Av, v\rangle = \langle v, Av\rangle = \bar{\lambda}\langle v, v\rangle$. Par conséquent $\lambda = \bar{\lambda}$, et λ est réelle.

Le lemme de Schur réel 9.218 donne une matrice orthogonale Q qui trigonalise A. Les valeurs propres étant toutes réelles, la matrice $Q^{-1}AQ$ est même triangulaire (il n'y a pas de blocs dans la forme (9.428)). Prouvons que $Q^{-1}AQ$ est symétrique :

$$(Q^{-1}AQ)^t = Q^tA^t(Q^{-1})^t = Q^{-1}A^tQ = Q^{-1}AQ \tag{9.433}$$

où nous avons utilisé le fait que Q était orthogonale ($Q^{-1} = Q^t$) et que A était symétrique ($A^t = A$). Une matrice triangulaire supérieure symétrique est obligatoirement une matrice diagonale.

En ce qui concerne la base de vecteurs propres, soit $\{e_i\}_{i=1,\ldots,n}$ la base canonique de $\mathbb{R}^n$ et Q une matrice orthogonale telle que $A = Q^tDQ$ avec D diagonale. Nous posons $f_i = Q^te_i$ et en tenant compte du fait que $Q^t = Q^{-1}$ nous avons $Af_i = Q^tDQQ^te_i = Q^t\lambda_ie_i = \lambda_if_i$. Donc les f_i sont des vecteurs propres de A. De plus ils sont orthonormés parce qu'en utilisant la proposition 9.180,

$$\langle f_i, f_j\rangle = \langle Q^te_i, Q^te_j\rangle = \langle e_i, Q^tQe_j\rangle = \langle e_i, e_j\rangle = \delta_{ij}. \tag{9.434}$$

□

Le théorème spectral pour les opérateurs autoadjoints sera traité plus bas parce qu'il a besoin de notions sur les formes bilinéaires, théorème 11.6.

Remarque 9.220.
Une matrice symétrique est diagonalisable par une matrice orthogonale. Nous pouvons en réalité nous arranger pour diagonaliser par une matrice de $\mathrm{SO}(n)$. Plus généralement si A est une matrice diagonalisable par une matrice $P \in \mathrm{GL}^+(n,\mathbb{R})$ alors elle est diagonalisable par une matrice de $\mathrm{GL}^-(n,\mathbb{R})$ en changeant le signe de la première ligne de P. Et inversement.

En effet, si nous avons $P^tDP = A$, alors en notant $*$ les quantités qui ne dépendent pas de a, b ou c,

$$\begin{aligned}\begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix}\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}\begin{pmatrix} a & b & c \\ * & * & * \\ * & * & * \end{pmatrix} &= \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix}\begin{pmatrix} \lambda_1 a & \lambda_1 b & \lambda_1 c \\ * & * & * \\ * & * & * \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 a^2 + * & \lambda_1 ab + * & \lambda_1 ac + * \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{pmatrix}.\end{aligned} \tag{9.435}$$

Nous voyons donc que si nous changeons les signes de a, b et c en même temps, le résultat ne change pas.

Proposition 9.221.
Une forme bilinéaire est non-dénénérée[84] *si et seulement si sa matrice associée est inversible.*

Démonstration. Nous savons que la matrice associée est symétrique et qu'elle peut donc être diagonalisée (théorème 9.219). En nous plaçant dans une base de diagonalisation, nous devons prouver que la forme est non-dégénérée si et seulement si les éléments diagonaux de la matrice sont tous non nuls.

Écrivons $b(x,z)$ en choisissant pour z le vecteur de base e_k de composantes $(e_k)_j = \delta_{kj}$:

$$b(x,e_k) = \sum_{ij} x_i (e_k)_j = \sum_i b_{ik} x_i = b_{kk} x_k. \tag{9.436}$$

Si b est dégénérée et si x est un vecteur non nul (disons que la composante x_i est non nulle) de E tel que $b(x,z) = 0$ pour tout $z \in E$, alors $b_{ii} = 0$, ce qui montre que la matrice de b n'est pas inversible.

Réciproquement si la matrice de b est inversible, alors tous les b_{kk} sont différents de zéro, et le seul vecteur x tel que $b_{kk}x_k = 0$ pour tout k est le vecteur nul. □

9.11.7 Matrice définie positive

Définition 9.222 (Matrice définie positive, opérateur défini positif)**.**
*Un opérateur sur un espace vectoriel sur $\mathbb{C}$ ou $\mathbb{R}$ est **défini positif** si toutes ses valeurs propres sont réelles et strictement positives. Il est **semi-défini positif** si ses valeurs propres sont réelles positives ou nulles.*

Mêmes définitions pour une matrice.

Afin d'éviter l'une ou l'autre confusion, nous disons souvent *strictement* défini positif pour positif.

9.223.
Quelques ensembles de matrices symétriques.

(1) $S(n,\mathbb{R})$ est l'ensemble des matrices symétriques réelles $n \times n$.

(2) $S^+(n,\mathbb{R})$ l'ensemble des matrices réelles symétriques $n \times n$ définies positives.

(3) $S^{++}(n,\mathbb{R})$ le sous-ensemble de $S^+(n,\mathbb{R})$ des matrices strictement définies positives.

84. Définition 9.124.

Remarque 9.224.
Nous ne définissons pas la notion de matrice définie positive pour une matrice non symétrique.

Proposition 9.225.
Soit M, une matrice symétrique. Nous avons

(1) $\det(M) > 0$ *et* $\mathrm{Tr}(M) > 0$ *implique M définie positive*[85],

(2) $\det(M) > 0$ *et* $\mathrm{Tr}(M) < 0$ *implique M définie négative,*

(3) $\det(M) < 0$ *implique ni semi-définie positive, ni définie négative*

(4) $\det(M) = 0$ *implique M semi-définie positive ou semi-définie négative.*

Lorsqu'un énoncé parle d'une matrice symétrique, le premier réflexe est de la diagonaliser : considérer une matrice orthogonale Q telle que $Q^tMQ = D$ avec D diagonale. Et les valeurs propres sur la diagonale : $D_{kk} = \lambda_k$. Les matrices symétriques définies positives ont cependant des propriétés même en dehors de leur base de diagonalisation.

Pour rappel, $\langle x, y\rangle$ est le produit scalaire dans $\mathbb{R}^n$ défini par la proposition 9.167.

Lemme 9.226.
Soit une matrice symétrique M.

(1) Elle est strictement définie positive si et seulement si $\langle x, Mx\rangle > 0$ pour tout x non nul dans $\mathbb{R}^n$.

(2) Elle est semi-définie positive si et seulement si $\langle x, Mx\rangle \geqslant 0$ pour tout x non nul dans $\mathbb{R}^n$.

(3) Si elle est seulement définie positive, alors $\langle x, Mx\rangle \geqslant \lambda\|x\|^2$ dès que $\lambda \geqslant 0$ minore toutes les valeurs propres.

Démonstration. Démonstration en trois parties.

(i) **(1)** Soit $\{e_i\}_{i=1,\dots,n}$ une base orthonormée de vecteurs propres de M dont l'existence est assurée par le théorème spectral 9.219. Nous nommons x_i les coordonnées de x dans cette base. Alors,

$$\langle x, Mx\rangle = \sum_{i,j} x_i\langle e_i, x_jMe_j\rangle = \sum_{i,j} x_ix_j\langle e_i, \lambda_je_j\rangle = \sum_{ij} x_ix_j\lambda_j\delta_{ij} = \sum_i \lambda_ix_i^2 \tag{9.437}$$

où les λ_i sont les valeurs propres de M. Le produit$\langle x, Mx\rangle$ est strictement positif pour tout x si et seulement si tous les λ_i sont strictement positifs.

(ii) **(2)** Nous avons encore

$$\langle x, Mx\rangle = \sum_i \lambda_ix_i^2 \tag{9.438}$$

qui est plus grand ou égal à zéro si et seulement si tous les λ_i sont plus grands ou égaux à zéro.

(iii) **(3)** Soit une matrice orthogonale T diagonalisant M, c'est-à-dire telle que $T^tMT = D$ avec D diagonale. Nous allons vérifier que si $\lambda \leqslant \min\{\lambda_i\}$, alors

$$\langle Tx, MTx\rangle \geqslant \lambda\|Tx\|^2 \tag{9.439}$$

pour tout x. Si nous considérons la base de diagonalisation $\{e_k\}$ pour les valeurs propres λ_k,

85. Définition 9.222.

nous avons le calcul

$$\begin{aligned}\langle Tx, MTx\rangle &= \langle x, T^tMTx\rangle && (9.440a)\\ &= \langle x, Dx\rangle && (9.440b)\\ &= \sum_k \langle x, x_k De_k\rangle && (9.440c)\\ &= \sum_k \lambda_k x_k \underbrace{\langle x, e_k\rangle}_{=x_k} && (9.440d)\\ &\geqslant \sum_k \lambda |x_k|^2 \qquad \text{en posant} \lambda = \min\{\lambda_i\} && (9.440e)\end{aligned}$$

Nous avons donc

$$\langle Tx, MTx\rangle \geqslant \sum_k \lambda |x_k|^2 = \lambda \|x\|^2 = \lambda \|Tx\|^2. \tag{9.441}$$

Au dernier passage nous avons utilisé le fait que T est une isométrie (proposition 9.40). L'inéquation (9.439) est démontrée.

Comme T est une bijection[86], cela implique le résultat pour tout x.

□

Les personnes qui aiment les vecteurs lignes et colonnes écriront des inégalités comme

$$x^tMx \geqslant x^tx. \tag{9.442}$$

Tout à l'autre bout du spectre des personnes névrosées des notations, on trouvera des inégalités comme

$$M(x \otimes x) \geqslant x \cdot x. \tag{9.443}$$

Le penchant personnel de l'auteur de ces lignes est la notation avec le produit tensoriel. Si vous aimez ça, vous pouvez lire la section 11.12.12 et en particulier ce qui suit (11.612).

La notation adoptée ici avec le produit scalaire $\langle x, Mx\rangle$, qui peut aussi être écrite $x \cdot Mx$ est entre les deux. Elle a l'avantage de n'être pas technologique comme le produit tensoriel (si vous y mettez les pieds, vous devez savoir ce que vous faites), tout en évitant de se casser la tête à savoir qui est un vecteur ligne ou un vecteur colonne.

Proposition 9.227.
Une application bilinéaire est définie positive[87] *si et seulement si sa matrice symétrique associée*[88] *l'est.*

Démonstration. La définition 9.121 dit que b est strictement définie positive lorsque $b(x,x) \geqslant 0$ et $b(x,x) = 0$ si et seulement si $x = 0$.

D'autre part, le lemme 9.226 dit que la matrice B est strictement définie positive lorsque $x \cdot Bx \geqslant 0$ et $x \cdot Bx = 0$ si et seulement si $x = 0$.

Le lien entre les deux est que le lemme 9.144 nous enseigne que pour tout x et y,

$$b(x,y) = x \cdot By \tag{9.444}$$

où B est la matrice de b. □

Proposition 9.228.
Soit une forme quadratique $q\colon E \to \mathbb{K}$ et sa matrice[89] *$(q_{ij}) \in \mathbb{M}(n,\mathbb{K})$. Nous avons*

$$q(x) = \sum_{i=1}^n \sum_{j=1}^n q_{ij}x_ix_j = \sum_{i=1}^n q_{ii}x_i^2 + 2\sum_{1\leqslant i<j\leqslant n} q_{ij}x_ix_j. \tag{9.445}$$

86. Une matrice orthogonale a un déterminant qui vaut ± 1.
87. Définition 9.121.
88. Par la proposition 9.137.
89. Matrice associée à une forme quadratique, définition 9.143.

Démonstration. La première égalité est seulement l'expression de la matrice de q. Pour la seconde, on découpe la somme sur j en trois parties : $j<i$, $j=i$ et $j>i$:

$$q(x)=\sum_i\sum_{j<i}q_{ij}x_ix_j+\sum_i q_{ii}x_i^2+\sum_i\sum_{j>i}q_{ij}x_ix_j. \tag{9.446}$$

Nous pouvons utiliser le lemme 1.304 en posant $A=\{(i,j)\text{ tel que }j<i\}$, $B=\{(i,j)\text{ tel que }j>i\}$, et en considérant la bijection

$$\begin{aligned}\varphi\colon A&\to b\\(i,j)&\mapsto(j,i).\end{aligned} \tag{9.447}$$

Nous avons alors

$$\sum_{(i,j)\in A}q_{ij}x_ix_j=\sum_{(i,j)\in B}q_{ji}x_jx_i=\sum_{(i,j)\in B}q_{ij}x_ix_j. \tag{9.448}$$

La première égalité est le lemme et la seconde est la symétrie de q. Bref, dans (9.446), le premier et le dernier termes sont égaux. □

9.229.
De nombreux auteurs préfèrent écrire des choses comme x^tBy ou xB^ty ou xBy^t et se poser de longues questions sur qui est un « vecteur colonne » et qui est un « vecteur ligne », et si la matrice B soit être transposée ou non. Toutes ces notations servent(?) à cacher un bête produit scalaire.

9.230.
Notons que la matrice associée à une forme bilinéaire (ou quadratique associée) est uniquement valable pour une base donnée. Si nous changeons de base, la matrice change. Cependant lorsque nous travaillons sur $\mathbb{R}^n$, la base canonique est tellement canonique que nous allons nous permettre de parler de « la » matrice associée à une forme bilinéaire.

Corolaire 9.231.
Une matrice symétrique strictement définie positive est inversible.

Démonstration. Si $Ax=0$ alors $\langle Ax,x\rangle=0$. Mais dans le cas d'une matrice strictement définie positive, cela implique $x=0$ par le lemme 9.226. □

Lemme 9.232.
Pour une base quelconque, les éléments diagonaux d'une matrice symétrique semi-définie positive sont positifs. Si la matrice est strictement définie positive, alors les éléments diagonaux sont strictement positifs.

Démonstration. Il s'agit d'une application du lemme 9.226. Si A est définie positive et que $\{e_i\}$ est une base, alors

$$A_{ii}=\langle Ae_i,e_i\rangle\geqslant\lambda\|e_i\|^2=\lambda\geqslant 0. \tag{9.449}$$

Si A est strictement définie positive, alors λ peut être choisi strictement positif. □

9.11.8 Réduction de Gauss

Théorème 9.233 (Réduction de Gauss[281, 282])**.**
Soit une forme quadratique non nulle q sur l'espace vectoriel E sur le corps $\mathbb{K}$. Il existe une base $\{l_i\}_{i=1,\dots,n}$ de E^* et des coefficients $\alpha_i\in\mathbb{K}$ tels que

$$q(x)=\sum_{i=1}^n\alpha_il_i(x)^2. \tag{9.450}$$

Démonstration. Notre point de départ sont les formules (9.445) pour la forme quadratique. Nous allons faire la preuve par récurrence sur la dimension de l'espace. Si $n=1$, alors nous avons seulement

$$q(x)=\alpha x^2 \tag{9.451}$$

et donc le théorème est fait avec $l(x) = x$.

Nous supposons que le théorème est prouvé pour tout espace de dimension n. Une forme quadratique pour un espace de dimension $n+1$ s'écrit

$$q(x) = \sum_{i=1}^{n+1} m_{ii}x_i^2 + 2 \sum_{1\leqslant i<j\leqslant n+1} m_{ij}x_ix_j. \tag{9.452}$$

Vu que q est non nulle, un des m_{ij} est non nul. Nous allons diviser en plusieurs cas.

— $m_{11} \neq 0$

— $m_{kk} \neq 0$ avec $k \neq 1$

— $m_{12} \neq 0$ et $m_{ii} = 0$ pour tout i.

— $m_{kl} \neq 0$ avec $(k,l) \neq (1,2)$ et $m_{ii} = 0$ pour tout i.

Ces cas ne sont pas exclusifs, mais ils couvrent toutes les possibilités.

(i) **Si $m_{11} \neq 0$** Nous écrivons q sous la forme

$$q(x) = m_{11}x_1^2 + \sum_{i=2}^{n+1} m_{ii}x_i^2 + 2\sum_{i=1}^{n}\Big(\sum_{j=i+1}^{n+1} m_{ij}x_ix_j\Big) \tag{9.453a}$$

$$= m_{11}x_1^2 + \sum_{i=2}^{n+1} m_{ii}x_i^2 + 2\sum_{j=2}^{n+1} m_{1j}x_1x_j + 2\sum_{i=2}^{n}\sum_{j=i+1}^{n+1}(m_{ij}x_ix_j) \tag{9.453b}$$

$$= m_{11}x_1^2 + 2x_1\sum_{j=2}^{n+1} m_{1j}x_k + R(x_2,\dots,x_{n+1}) \tag{9.453c}$$

$$= m_{11}\left(x_1^2 + 2x_1\sum_{j=2}^{n+1}\frac{m_{1j}}{m_{11}}x_j\right) + R(x_2,\dots,x_{n+1}) \tag{9.453d}$$

$$= m_{11}\big(x_1^2 + 2x_1 f(x_2,\dots,x_{n+1})\big) + R(x_2,\dots,x_{n+1}) \tag{9.453e}$$

$$= m_{11}\big(x_1 + f(x_2,\dots,x_{n+1})\big)^2 - m_{11}f(x_2,\dots,x_{n+1})^2 + R(x_2,\dots,x_{n+1}) \tag{9.453f}$$

où

— R est une forme quadratique de $n-1$ variables ;

— nous avons noté $f(x_2,\dots,x_{n+1}) = \sum_{j=2}^{n+1}\frac{m_{1j}}{m_{11}}x_j$.

Maintenant, toute la partie $-f(x_2,\dots,x_{n+1})^2 + R(x_2,\dots,x_{n+1})$ est une forme quadratique de n variables. Par hypothèse de récurrence, il existe des coefficients α_i et des formes linéairement indépendantes sur $\mathbb{K}^n$ $l'_i(x_2,\dots,x_{n+1})$ telles que

$$-f(x_2,\dots,x_{n+1})^2 + R(x_2,\dots,x_{n+1}) = \sum_{i=2}^{n+1}\alpha_i l'_i(x_2,\dots,x_{n+1})^2. \tag{9.454}$$

En posant ensuite $l_j(x_1,\dots,x_{n+1}) = l'_j(x_2,\dots,x_{n+1})$, ainsi que $l_1(x_1,\dots,x_{n+1}) = x_1 + f(x_2,\dots,x_{n+1})$, nous avons

$$q(x) = m_{11}l_1(x)^2 + \sum_{j=2}^{n+1}\alpha_j l_j(x)^2. \tag{9.455}$$

(ii) **Si $m_{kk} \neq 0$ avec $k \neq 1$** Nous nommons k le plus petit entier pour lequel $m_{kk} \neq 0$, et nous supposons que $k \neq 1$, parce que nous avons déjà couvert ce cas. Dans ce cas, nous avons

$$q(x) = m_{kk}x_k^2 + \sum_{j=k+1}^{n+1} m_{jj}x_j^2 + 2\sum_{i=1}^{n}\Big(\sum_{j=i+1}^{n+1} m_{ij}x_ix_j\Big), \tag{9.456}$$

et tout tourne comme dans le premier cas.

(iii) $\underline{m_{ii} = 0 \textbf{ pour tout } i \textbf{ et } m_{12} \neq 0}$ Nous écrivons q en séparant les termes m_{1k} :

$$q(x) = 2 \sum_{1\leqslant i<j\leqslant n+1} m_{ij}x_ix_j \tag{9.457a}$$

$$= 2m_{12}x_1x_2 + 2 \sum_{2\leqslant j\leqslant n+1} m_{1j}x_1x_j + 2 \sum_{2\leqslant i<j\leqslant n+1} m_{ij}x_ix_j \tag{9.457b}$$

$$= 2m_{12}x_1x_2 + 2x_1 \sum_{2\leqslant j\leqslant n+1} m_{1j}x_j + 2 \sum_{3\leqslant j\leqslant n+1} m_{2j}x_2x_j + 2 \sum_{3\leqslant i<j\leqslant n+1} m_{ij}x_ix_j \tag{9.457c}$$

$$= 2m_{12}x_1x_2 + x_1f(x_2,\dots,x_{n+1}) + x_2g(x_3,\dots,x_{n+1}) + T(x_3,\dots,x_{n+1}) \tag{9.457d}$$

où f et g sont linéaires et T est multilinéaire.

À ce moment, nous tentons de factoriser toute la partie concernant x_1 et x_2. L'idée est d'utiliser ceci :

$$(x_1 + g)(x_2 + f) = x_1x_2 + x_1f + x_2g + fg, \tag{9.458}$$

mais en mettant les bons coefficients pour reproduire ce que nous avons dans (9.457d) :

$$(2m_{12} + 2g)(x_2 + \frac{f}{m_{12}}) - \frac{2fg}{m_{12}} = 2m_{12}x_1x_2 + 2x_1f + 2x_2g. \tag{9.459}$$

Cela pour dire que

$$q(x) = 2(m_{12}x_1 + g)(x_2 + \frac{f}{m_{12}}) - \frac{2fg}{m_{12}} + T \tag{9.460}$$

où $-2fg/m_{12} + T$ est une forme quadratique de $x_3,\dots,x_{n+1}$, c'est-à-dire de $n-1$ variables. L'hypothèse de récurrence nous donne des formes linéaires $(l_i)_{i=3,\dots,n+1}$ telles que

$$\frac{2fg}{m_{12}} + T = \sum_{i=3}^{n+1} \alpha_i l_i(x)^2. \tag{9.461}$$

Nous pouvons donc déjà écrire

$$q(x) = 2l_1'(x)l_2'(x) + \sum_{i=3}^{n+1} \alpha_i l_i(x)^2 \tag{9.462}$$

où

- Les forme l_i avec $i \geqslant 3$ ne dépendent pas de x_1 et x_2, et sont donc indépendantes de l_1 et l_2.
- La forme l_1' ne dépend pas de x_2,
- La forme l_2' ne dépend pas de x_1.

Ce sont donc $n+1$ formes linéaires indépendantes. Le seul problème résiduel est que les formes l_1' et l_2' arrivent en produit l'une de l'autre. Nous en définissons donc deux de plus :

$$\begin{aligned} l_1(x) &= \frac{1}{2}(l_1' + l_2') \\ l_2(x) &= \frac{1}{2}(l_1' - l_2'), \end{aligned} \tag{9.463}$$

qui sont linéairement indépendantes l'une de l'autre et indépendantes des l_i ($i \geqslant 3$). Au final,

$$q(x) = l_1(x)^2 + l_2(x)^2 + \sum_{i=3}^{n+1} \alpha_i l_i(x)^2. \tag{9.464}$$

(iv) **Si $m_{ii} = 0$ et $m_{12} = 0$ et $m_{kl} \neq 0$ avec $k < l$** Nous considérons la permutation

$$\begin{aligned}\sigma\colon \{1,\dots,n+1\} &\to \{1,\dots,n+1\}\\ i &\mapsto \begin{cases} 1 & \text{si } i = k\\ 2 & \text{si } i = l\\ k & \text{si } i = 1\\ l & \text{si } i = 2\\ i & \text{sinon,}\end{cases}\end{aligned} \tag{9.465}$$

c'est-à-dire que σ permute 1 et k ainsi que 2 et l. Ensuite nous posons

$$\begin{aligned}s\colon \mathbb{R}^{n+1} &\to \mathbb{R}^{n+1}\\ e_i &\mapsto e_{\sigma(i)}.\end{aligned} \tag{9.466}$$

Nous allons un peu considérer $q \circ s$, pour changer :

$$(q \circ s)(x) = \sum_{i,j} m_{ij} s(x)_i s(x)_j = \sum_{ij} x_{\sigma(i)} x_{\sigma(j)}. \tag{9.467}$$

parce que $s(x)_i = x_{\sigma(i)}$.
Utilisons un petit abus de notation pour considérer

$$\begin{aligned}\sigma\colon \{1,\dots,n+1\} \times \{1,\dots,n+1\} &\to \{1,\dots,n+1\} \times \{1,\dots,n+1\}\\ (i,j) &\mapsto \big(\sigma(i),\sigma(j)\big).\end{aligned} \tag{9.468}$$

Cela est une bijection ; nous pouvons utiliser le lemme 1.302 pour permuter les termes dans (9.467) :

$$(q \circ s)(x) = \sum_{ij} m_{\sigma(i)\sigma(j)} x_{\sigma\sigma(i)} x_{\sigma\sigma(j)} \tag{9.469a}$$

$$= \sum_{ij} a_{ij} x_i x_j \tag{9.469b}$$

où nous avons posé $a_{ij} = m_{\sigma(i)\sigma(j)}$ et utilisé le fait que $\sigma = \sigma^{-1}$. Le point intéressant de l'histoire est que dans (9.469b), $a_{12} = m_{kl} \neq 0$. La forme $q \circ s$ est donc dans le cas déjà traité et il existe des formes linéaires l'_i telles que

$$(q \circ s)(x) = \sum_{i=1}^{n+1} \alpha_i l'_i(x)^2. \tag{9.470}$$

En évaluant cela en $s(x)$, et en tenant compte de $s = s^{-1}$, nous trouvons

$$q(x) = \sum_i \alpha_i (l_i \circ s)(x)^2, \tag{9.471}$$

de telle sorte que $l_i = l'_i \circ s$ soit la réponse à notre théorème.

□

9.11.9 Orthogonalité pour une forme bilinéaire

Proposition 9.234 ([282]).
Soient un espace vectoriel $(E, \mathbb{K})$ et une forme quadratique[90] *q. Une base de E est q-orthogonale*[91] *si et seulement si la matrice de q dans cette base est diagonale.*

90. Définition 9.120.
91. Définition 9.142.

Démonstration. La matrice de q est donnée par $Q_{ij} = b(e_i, e_j)$. Donc oui, cette matrice est diagonale si et seulement si les e_i sont orthogonaux. □

Proposition 9.235 ([1])**.**
Si b est une forme bilinéaire symétrique non dégénérée, et si q est la forme quadratique associée, alors il existe une base q-orthogonale.

Les vecteurs de cette base ne sont pas isotropes[92]

Démonstration. Nous considérons une base $\{e_i\}$ de E. Vu que b est symétrique, elle est donnée par une matrice symétrique selon la formule $b(x, y) = \sum_{kl} S_{kl}x_k y_l$. Le théorème 9.219 permet de diagonaliser S par une matrice orthogonale : il existe une matrice diagonale D et une matrice orthogonale A telles que $S = A^t DA$.

Nous posons alors $s_i = Ae_i$, et nous vérifions que c'est bon. Nous avons :

$$\begin{aligned} b(s_i, s_j) &= \sum_{kl} S_{kl}(s_i)_k(s_j)_l && \text{(9.472a)}\\ &= \sum_{kl} S_{kl}(Ae_i)_k(Ae_j)_l && \text{(9.472b)}\\ &= \sum_{kl} S_{kl}A_{ki}A_{lj} && \text{(9.472c)}\\ &= \sum_{kl} (A^t)_{ik}S_{kl}A_{lj} && \text{(9.472d)}\\ &= D_{ij}. && \text{(9.472e)} \end{aligned}$$

Vu que b n'est pas dégénérée, les éléments diagonaux de D ne sont pas nuls. Donc les vecteurs s_i vérifient $b(s_i, s_i) \neq 0$. □

Proposition 9.236.
Soit une forme quadratique q. Si une base (e_i) de E est q-orthogonale, alors $\mathcal{B} = \{e_i \text{ tel que } q(e_i) = 0\}$ est une base de $\ker(q)$.

Démonstration. Nous considérons un vecteur de base e_j, et nous montrons que $q(e_j) = 0$ si et seulement si $e_j \in \ker(q)$. Nous savons par la proposition 9.234 que la matrice de q dans la base (e_i) est diagonale et que les éléments diagonaux sont les $q(e_i)$. Soit $K = \{i \text{ tel que } q(e_i) = 0\}$.

(i) $\underline{\text{Span}\{e_i\}_{i\in K} \subset \ker(q)}$ Si $x = \sum_{i\in K} x_i e_i$, alors

$$q(x) = b(x, x) = \sum_{i,j\in K} |x_i|^2 b(e_i, e_j) = \sum_{i,j\in K} |x_i|^2 \delta_{ij} q(e_i) = 0 \tag{9.473}$$

parce que $q(e_i) = 0$ dès que $i \in K$.

(ii) $\underline{\ker(q) \subset \text{Span}\{e_i\}_{i\in K}}$ Soit $x \in \ker(q)$ et écrivons-le sous la forme $x = \sum_{i=1}^{n} x_i e_i$. Nous avons

$$0 = q(x) = \sum_i |x_i|^2 q(e_i). \tag{9.474}$$

Mais $|x_i|^2 \geqslant 0$ et $q(e_i) \geqslant 0$, donc si $q(e_i) \neq 0$, alors $x_i = 0$. Donc les seules composantes non nulles de x sont celles sur lesquelles q s'annule. En d'autres termes $x = \sum_i x_i e_i \in \text{Span}\{e_i\}_{i\in K}$.

□

Théorème 9.237 ([282, 1])**.**
Toute forme quadratique sur un espace vectoriel de dimension finie admet une base formée de vecteurs 2 à 2 orthogonaux (pour la forme considérée).

92. Définition 9.138.

Démonstration. Nous considérons la base $\{l_i\}$ de E^* donnée par la réduction de Gauss (théorème 9.233). La forme quadratique q s'écrit

$$q(x) = \sum_{i=1}^{n} \alpha_i l_i(x)^2. \tag{9.475}$$

La base préduale[93] $\{e_i\}$ de $\{l_i\}$ répond aux conditions. Pour le vérifier, nous considérons la forme bilinéaire associée à q par l'identité de polarisation 9.136 :

$$b(e_i, e_j) = \frac{1}{2}\big(q(e_i) + q(e_j) - q(e_i - e_j)\big). \tag{9.476}$$

Vu que $l_k(e_i) = \delta_{ki}$, nous avons

$$q(e_i) = \sum_{k=1}^{n} \alpha_k l_k(e_i)^2 = \alpha_i. \tag{9.477}$$

En utilisant la linéarité,

$$\begin{aligned} q(e_i - e_j) &= \sum_k \alpha_k l_k(e_i - e_j)^2 && (9.478a)\\ &= \sum_k \alpha_k (\delta_{ki} - \delta_{kj})^2 && (9.478b)\\ &= \sum_k \alpha_k (\delta_{ki} + \delta_{kj} - 2\delta_{ki}\delta_{kj}) && (9.478c)\\ &= \alpha_i + \alpha_j - 2\delta_{ij}\alpha_i. && (9.478d) \end{aligned}$$

Donc

$$b(e_i, e_j) = \delta_{ij}\alpha_i. \tag{9.479}$$

Les vecteurs $\{e_i\}$ sont donc bien deux à deux q-orthogonaux. □

Notons qu'en l'absence de notion de racine carrée sur $\mathbb{K}$, il n'est pas possible de considérer $\sqrt{\alpha_i}$ et donc de base q-orthonormée.

Proposition 9.238 ([1]).
Si $A \in \mathbb{M}(n, \mathbb{K})$ est telle que $\det(A) = 0$, alors il existe des matrices de manipulation de lignes et de colonnes[94] *$G_1, \dots, G_p$ et $H_1, \dots, H_q$ telles que $G_1 \dots G_N A H_1 \dots H_q$ ait une colonne de zéros.*

Démonstration. Si la matrice A n'a pas de colonnes de zéros, il existe un i tel que $A_{i1} \neq 0$. Nous utilisons une matrice de permutation de ligne 1 et i :

$$\big(S(n, i, 1)A\big)_{11} \neq 0. \tag{9.480}$$

Nous notons s ce nombre. Alors en multipliant la première ligne par $1/s$ nous avons un 1 dans la première case :

$$\big(T(n, 1, 1/s)S(n, i, 1)A\big)_{11} = 1. \tag{9.481}$$

Pour la suite nous n'allons plus être aussi explicite.

Maintenant, en faisant des combinaisons entre la première colonne et les autres, nous pouvons annuler toutes les autre entrées 1_{1i}. Tout ça pour dire qu'il existe des matrices $G_1, \dots, G_{p'}$ et $H_1, \dots, H_{q'}$ telles que

$$G_1 \dots G_{p'} A H_1 \dots H_{q'} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A^{(1)} & \\ 0 & & & \end{pmatrix}. \tag{9.482}$$

93. Définition, existence, unicité dans la proposition 4.128.
94. Les opérations élémentaires sur les lignes sont résumées en 4.85.

Si $A^{(1)}$ ne possède pas de colonnes de zéros, nous pouvons continuer.

Si nous parvenons à faire n pas de la sorte, alors nous aurions

$$G_1 \dots G_p A H_1 \dots H_q = \delta, \tag{9.483}$$

et donc, par le lemme 4.86, nous aurions $\det(G_1 \dots G_p)\det(A)\det(H_1 \dots H_q) = 1$, ce qui est impossible lorsque $\det(A) = 0$. Nous en concluons que le processus doit s'arrêter et qu'une des matrices $A^{(k)}$ doit avoir une colonne de zéros [95]. □

Proposition 9.239.
Une matrice dont le déterminant est nul n'est pas inversible.

Démonstration. Par la proposition 9.238, il existe des matrices de manipulation de lignes et de colonnes $G_1, \dots, G_p$ telles que la matrice $G_1 \dots G_p\, A\, H_1 \dots H_q$ ait une colonne de zéros. De là, la proposition 4.96 implique que la matrice

$$G_1 \dots G_p A H_1 \dots H_q \tag{9.484}$$

n'est pas inversible. Vu les déterminants des matrices G_i, la proposition 4.95 implique que $G_1 \dots G_p$ et $H_1 \dots H_q$ sont inversibles. Si A était inversible, tout le produit serait inversible, ce qui est faux. □

Théorème 9.240.
Une matrice sur un corps commutatif est inversible si et seulement si son déterminant est non nul.

Démonstration. Dans un sens c'est la proposition 4.95 et dans l'autre sens c'est la proposition 9.239. □

Proposition 9.241.
Soient des matrices A et B sur un corps commutatif. Alors

$$\det(AB) = \det(A)\det(B). \tag{9.485}$$

Démonstration. Les propositions 4.99 et 4.100 ont déjà fait une grosse partie du travail. Il ne reste que le cas où $\det(A) = \det(B) = 0$.

Dans ce cas, les matrices A et B ne sont pas inversibles (proposition 9.240). Le produit AB n'est alors pas inversible non plus [96]. La proposition 9.240, utilisée dans le sens inverse, nous dit alors que $\det(AB) = 0$.

Au final dans le cas $\det(A) = \det(B) = 0$ nous avons $0 = \det(AB) = \det(A)\det(B) = 0$. □

Faisons maintenant le cas général des manipulations de lignes et colonnes.

Proposition 9.242.
Soit une matrice carrée $A \in \mathbb{M}(n, \mathbb{K})$. La matrice B obtenue par la substitution simultanée

$$C_j \to \sum_k a_{kj} C_k \tag{9.486}$$

a pour déterminant

$$\det(B) = \det(a)\det(A). \tag{9.487}$$

Démonstration. L'élément B_{ij} de la matrice B est une combinaison linéaire de tous les éléments de sa ligne :

$$B_{ij} = \sum_k a_{kj} A_{ik} = (Aa)_{ij}. \tag{9.488}$$

Donc $B = Aa$. La proposition 9.241 nous dit alors que $\det(B) = \det(a)\det(A)$. □

95. En réalité, le processus tel que nous l'avons décrit ne s'arrête que lorsque la première colonne est remplie de zéros.

96. Citez le lemme 4.92 si vous voulez justifier ça.

Théorème 9.243 (de Sylvester[275]).
Soit Q une forme quadratique réelle de signature[97] *(p,q). Alors pour toute base Q-orthogonale $\{e_i\}$ de $\mathbb{R}^{p+q}$ nous avons les propriétés suivantes.*

(1) Les nombres p et q sont donnée par

$$p = \text{Card}\{i \text{ tel que } Q(e_i) > 0\} \tag{9.489a}$$
$$q = \text{Card}\{i \text{ tel que } Q(e_i) < 0\}. \tag{9.489b}$$

(2) Si A est la matrice de Q dans une base, alors il existe une matrice inversible P telle que

$$P^tAP = \begin{pmatrix} -\mathbb{1}_q & & \\ & \mathbb{1}_p & \\ & & 0 \end{pmatrix}. \tag{9.490}$$

(3) Le rang de Q est $p+q$.

Démonstration. Soit F un sous-espace de dimension maximale q sur lequel Q est définie négative. Le fait que la dimension de F soit q est la définition 9.158 de la signature. Nous notons $F^\perp$ sont Q-orthogonal, c'est-à-dire que

$$F^\perp = \{v \in E \text{ tel que } B(v,x) = 0 \, \forall x \in F\}. \tag{9.491}$$

Le lemme 9.134 nous assure que $E = F \oplus F^\perp$.

Le théorème 9.237 sur l'existence de bases Q-orthogonales nous permet de considérer une base Q-orthogonale de F et une de $F^\perp$. En réunissant les deux, nous avons une base de E. Nous la notons $\{f_1, \dots, f_n\}$ avec

— La partie $\{f_1, \dots, f_q\}$ est une base de F,
— La partie $\{f_{q+1}, \dots, f_n\}$ est une base de $F^\perp$,
— Remarquez cependant qu'il n'est pas dit que $n = q + p$.

Notons que pour $i > q$, nous avons $Q(f_i) \geqslant 0$, sinon la maximalité de F serait contredite par $\text{Span}\{f_1, \dots, f_q, f_i\}$.

Cela prouve que

$$\text{Card}\{i \text{ tel que } Q(f_i) > 0\} = p. \tag{9.492}$$

Le lemme 9.161 nous dit alors que

$$\text{Card}\{i \text{ tel que } Q(e_i) > 0\} = \text{Card}\{i \text{ tel que } Q(f_i) > 0\} = p. \tag{9.493}$$

C'est l'égalité (9.489b). L'égalité (9.489a) se prouve de la même façon, en prenant F maximal pour la propriété que Q y est strictement définie positive.

Le point (1) est prouvé.

Dans une base Q-orthogonale, la matrice de Q est diagonale, et contient sur la diagonale les valeurs de $Q(e_i)$. Parmi celles-ci, on en a p strictement positives et q strictement négatives. Les $n-p-q$ autres sont nulles. Vu que Q est à valeur réelle, nous avons une notion de racine carré, et nous pouvons considérer $e_i/\sqrt{|Q(e_i)|}$ au lieu de e_i. De cette façon, $Q(e_i)$ est normalisé. Avec ça, la matrice de Q est

$$D = \begin{pmatrix} \mathbb{1}_p & & \\ & -\mathbb{1}_q & \\ & & 0 \end{pmatrix}. \tag{9.494}$$

Nous venons de prouver qu'il existe une base $\{e_i\}$ dans laquelle la matrice de Q est (9.494). Si A est la matrice de Q dans une base quelconque $\{f_i\}$ et si P est la matrice de changement de base $f_j = \sum_i P_{ij} e_i$, la proposition 9.146 donne $D = P^tAP$.

Le point (2) est prouvé.

Pour (3), la proposition 9.160 nous permet de calculer le rang de Q par le rang de sa matrice dans n'importe quelle base. Nous choisissons la base qui donne la matrice (9.494). Le rang est alors bien $p+q$. □

97. Définition 9.158.

9.11.10 Équivalence de formes quadratiques

Définition 9.244 (Équivalence de forme quadratique[267])**.**
*Deux formes quadratiques q et q' sont **équivalentes** si il existe une application linéaire inversible ϕ telle que $q' = q \circ \phi$.*

Proposition 9.245 ([275])**.**
Deux formes quadratiques sont équivalentes[98] *si et seulement si elles ont même signature.*

Démonstration. En deux parties, et en utilisant tout le temps le théorème de Sylvester 9.243. Dans la suite nous allons toujours noter de la même façon les formes quadratiques, les applications linéaires et leurs matrices correspondantes.

(i) $\Rightarrow$ Soient deux formes quadratiques équivalentes q et q'. Nous avons une application linéaire ϕ telle que $q' = q \circ \phi$. Soit une matrice inversible P telle que

$$P^t A P = \begin{pmatrix} -\mathbb{1}_{q'} & & \\ & \mathbb{1}_{p'} & \\ & & 0 \end{pmatrix}. \tag{9.495}$$

où (p', q') est la signature de q'. Par équivalence et par le changement de base de la proposition 9.145, nous avons $q' = \phi^t q \phi$, et donc

$$P^t q' P = (\phi P)^t q (\phi P). \tag{9.496}$$

Dans la base des $(\phi \circ P)e_i$, la matrice de q est (9.495). Donc le point 9.243(1) du théorème de Sylvester montre que la signature de q est également (p', q').

(ii) $\Rightarrow$ Nous supposons que q et q' ont la même signature. Il existe donc des matrices inversibles P et Q telles que $P^t q' P$ et $Q^t q Q$ aient la même forme (celle de la matrice (9.495)). Autrement dit,

$$q' \circ P = q \circ Q, \tag{9.497}$$

d'où nous déduisons que $q' = q \circ Q \circ P^{-1}$ parce que P est inversible. Comme l'application $Q \circ P^{-1}$ est inversible, les formes quadratiques q et q' sont équivalentes.

□

9.11.11 Diagonalisation

Lemme-Définition 9.246.
Soit une forme quadratique[99] *q sur l'espace vectoriel V sur $\mathbb{K}$. Soit A la matrice de q dans la base $\{e_i\}$ et B sa matrice dans la base $\{f_\alpha\}$. Nous supposons que le changement de base est orthogonal.*
Alors les valeurs propres de A et B sont les mêmes.
*Ces valeurs sont les **valeurs propres** de q.*

Démonstration. Nous nous rappelons de la définition 9.143 de la matrice associée à q, et à la proposition 9.146 qui parle de changement de base : $B = Q^t A Q$ où Q est orthogonale.

Soit un vecteur propre v de A, de valeur propre λ. Alors nous prouvons que $Q^t v$ est un vecteur propre pour B, de même valeur propre λ. En effet,

$$B Q^t v = Q^t A Q Q^t v = Q^t A v = \lambda Q^t v \tag{9.498}$$

où nous avons utilisé $Q Q^t = \mathbb{1}$ et $Av = \lambda v$. □

98. Définition 9.244.
99. Définition 9.120.

Proposition 9.247.
Dans la base de diagonalisation de sa matrice associée, une forme quadratique a la forme

$$q(x) = \sum_i \lambda_i x_i^2 \tag{9.499}$$

où les λ_i sont les valeurs propres de la matrice associée à q.

Démonstration. Soit q une forme quadratique et b la forme bilinéaire associée. Si $\{f_i\}$ est une base de diagonalisation [100] de la matrice de b alors dans cette base nous avons

$$q(x) = b(x,x) = \sum_{ij} x_i x_j b(f_i, f_j) = \sum_i \lambda_i x_i^2 \tag{9.500}$$

où les λ_i sont les valeurs propres de la matrice de b. □

Notons que si nous choisissons une autre base de diagonalisation, les λ_i ne changement pas (à part l'ordre éventuellement).

Cela justifie la définition pour dire que nous nous permettrons de parler des **valeurs propres** d'une forme quadratique comme étant les valeurs propres de la matrice associée.

Le théorème 9.237 a déjà donné une base orthogonale pour toute forme quadratique sur un espace vectoriel $(E, \mathbb{K})$ de dimension finie. Dans le cas de $\mathbb{R}^n$, nous pouvons en donner une preuve basée sur le théorème spectral, c'est la proposition 9.248.

Proposition 9.248.
Soit une forme bilinéaire symétrique b sur un $\mathbb{R}^n$. Il existe une matrice orthogonale Q telle que

(1) $D = Q^t b Q$ est diagonale

(2) $D(x,y) = b(Qx, Qy)$ pour tout $x, y \in \mathbb{R}^n$.

Il existe une base $(f_i)_{i=1,\dots,n}$ qui est b-orthogonale.

Dans cet énoncé, nous mélangeons sans vergogne les formes et les matrices, en supposant qu'une base soit fixée [101]*. Par exemple*

$$D(x,y) = \sum_{ij} D_{ij} x_i y_j. \tag{9.501}$$

Démonstration. Pour la matrice diagonale, c'est le théorème spectral 9.219(2) qui joue parce que la matrice d'une forme bilinéaire symétrique est symétrique (c'est vu de la définition (9.294)).

Pour le reste c'est un calcul :

$$\begin{aligned} D(x,y) &= \sum_{ijkl} Q^t_{ik} b_{kl} Q_{lj} x_i y_j && \text{(9.502a)}\\ &= \sum_{ijkl} b_{kl} (Q_{ki} x_i)(Q_{lj} y_j) && \text{(9.502b)}\\ &= \sum_{kl} b_{kl} (Qx)_k (Qy)_l && \text{(9.502c)}\\ &= b(Qx, Qy). && \text{(9.502d)} \end{aligned}$$

Nous avons utilisé le produit matrice fois vecteur donné par (4.82).

En ce qui concerne l'existence d'une base b-orthogonale, vu que D est diagonale, nous avons, pour $i \neq j$ que $D(e_i, e_j) = 0$. Donc en posant $f_i = Qe_i$, nous trouvons

$$0 = D(e_i, e_j) = b(Qe_i, Qe_j) = b(f_i, f_j). \tag{9.503}$$

La base $(Qe_i)_{i=1,\dots,n}$ est donc b-orthogonale. □

100. Qui existe parce que la matrice est symétrique, théorème 9.219.

101. Autrement dit, si vous avez en tête d'utiliser cette proposition pour $\mathbb{R}^n$ c'est bon ; mais sinon vous devez choisir une base et considérer toutes les matrices dans cette base.

9.12 Fonctions

Soient $(E, \|.\|_E)$ et $(F, \|.\|_F)$ deux espaces vectoriels normés, et une fonction f de E dans F. Il est maintenant facile de définir les notions de limites et de continuité pour de telles fonctions en copiant les définitions données pour les fonctions de $\mathbb{R}$ dans $\mathbb{R}$ et en changeant simplement les valeurs absolues par les normes sur E et F.

La proposition suivante explicite la définition 7.101 dans le cas où la topologie est donnée par des boules.

Proposition 9.249 (Caractérisation de la limite)**.**
Soient des espaces vectoriels normés. Soit $f\colon E \to F$ une fonction de domaine $\mathrm{Dom}(f) \subset E$ et soit a un point d'accumulation de $\mathrm{Dom}(f)$.

(1) Si F est séparé[102] *et si f admet une limite en a, alors cette limite est unique.*

(2) La fonction f admet une limite en $a \in E$ si et seulement si il existe un élément $\ell \in F$ tel que pour tout $\varepsilon > 0$, il existe un $\delta > 0$ tel que pour tout $x \in D = \mathrm{Dom}(f)$,

$$0 < \|x - a\|_E < \delta \Rightarrow \|f(x) - \ell\|_F < \varepsilon. \tag{9.504}$$

*Si la limite existe et est unique, nous écrivons $\lim_{x\to a} f(x) = \ell$ et nous disons que ℓ est la **limite** de f lorsque x tend vers a.*

Démonstration. L'unicité est la proposition 7.104.

(i) $\Rightarrow$ La définition 7.101 nous assure de l'existence d'un élément ℓ tel que pour tout voisinage S de ℓ, il existe un ouvert U autour de a tel que $f\big(U \cap D\backslash\{a\}\big) \subset S$.

Soit $\epsilon > 0$. Nous posons $S = B(\ell, \epsilon)$. Il existe un voisinage U de a tel que $f\big(U \cap D\backslash\{a\}\big) \subset B(\ell, \epsilon)$. Puisque U est un voisinage de a, il contient une boule centrée en a (c'est dans la définition 7.108 de la topologie métrique). Soit donc $\delta > 0$ tel que $B(a, \delta) \subset U$.

Un élément de D qui est dans $B(0, \delta)\backslash\{a\}$ est un élément de D qui vérifie $0 < \|x - a\| < \delta$. Nous avons donc, pour $x \in D$ que

$$0 < \|x - a\| < \delta \Rightarrow \|f(x) - \ell\| < \epsilon. \tag{9.505}$$

(ii) $\Leftarrow$ C'est le même raisonnement.

□

Remarque 9.250.
Le fait que nous limitions la formule (9.504) aux x dans le domaine de f n'est pas anodin. Considérons la fonction $f(x) = \sqrt{x^2 - 4}$, de domaine $|x| \geqslant 2$. Nous avons

$$\lim_{x\to 2} \sqrt{x^2 - 4} = 0. \tag{9.506}$$

Nous ne pouvons pas dire que cette limite n'existe pas en justifiant que la limite à gauche n'existe pas. Les points $x < 2$ sont hors du domaine de f et ne comptent dons pas dans l'appréciation de l'existence de la limite.

Vous verrez plus tard que ceci provient de la topologie induite de $\mathbb{R}$ sur l'ensemble $[2, \infty[$.

9.13 Sous espaces caractéristiques

Lorsqu'un opérateur n'est pas diagonalisable, les valeurs propres jouent quand même un rôle important.

102. C'est le cas en dimension finie et en particulier pour $\mathbb{R}^n$. En dimension infinie, il faut être très prudent.

Définition 9.251.
Soient E un $\mathbb{K}$-espace vectoriel et $f \in \mathrm{End}(E)$. Pour $\lambda \in \mathbb{K}$ nous définissons

$$F_\lambda(f) = \{v \in E \text{ tel que } (f - \lambda\mathbb{1})^n v = 0, n \in \mathbb{N}\} \tag{9.507}$$

*et nous appelons cet ensemble un **sous-espace caractéristique** de f.*

L'espace $F_\lambda(f)$ est l'ensemble de nilpotence de l'opérateur $f - \lambda\mathbb{1}$ et

Lemme 9.252.
L'ensemble $F_\lambda(f)$ est non vide si et seulement si λ est une valeur propre de f. L'espace $F_\lambda(f)$ est invariant sous f.

Démonstration. Si $F_\lambda(f)$ est non vide, nous considérons $v \in F_\lambda(f)$ et n le plus petit entier non nul tel que $(f - \lambda)^n v = 0$. Alors $(f - \lambda)^{n-1} v$ est un vecteur propre de f pour la valeur propre λ. Réciproquement, si v est un vecteur propre de f pour la valeur propre λ, alors $v \in F_\lambda(f)$.

En ce qui concerne l'invariance, remarquons que f commute avec $f - \lambda\mathbb{1}$. Si $x \in F_\lambda(f)$ il existe n tel que $(f - \lambda\mathbb{1})^n x = 0$. Nous avons aussi

$$(f - \lambda\mathbb{1})^n f(x) = f\big((f - \lambda\mathbb{1})^n x\big) = 0, \tag{9.508}$$

par conséquent $f(x) \in F_\lambda(f)$. □

Contrairement à ce que l'on pourrait croire, il n'est pas vrai que toute matrice à coefficient réel est diagonalisable, même pas sur $\mathbb{C}$. La raison est qu'une telle matrice peut très bien avoir des valeurs propres multiples.

Exemple 9.253.
Le théorème 9.211 nous donne une façon simple de trouver des matrices non diagonalisables sur $\mathbb{C}$: il suffit que le polynôme minimal ne soit pas scindé à racines simples. Par exemple

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \tag{9.509}$$

dont le polynôme caractéristique est $\chi_A = (1 - X)^2$. Ce polynôme n'a manifestement pas des racines simples. Nous pouvons faire le calcul explicite pour montrer que A n'est pas diagonalisable. D'abord l'unique valeur propre de A est 1 et nous pouvons sans peine résoudre

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{9.510}$$

qui revient au système

$$\begin{cases} x + y = x & \text{(9.511a)} \\ y = y. & \text{(9.511b)} \end{cases}$$

La première équation donne directement $y = 0$. Le seul espace propre est de dimension 1 et est engendré par $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. △

Nous donnons maintenant un exemple un peu plus avancé de matrice réelle non diagonalisable, qui montre la multiplicité algébrique et géométrique d'une racine d'un polynôme caractéristique.

Remarque 9.254.
Considérons l'endomorphisme $f \in \mathrm{End}(\mathbb{C}^3)$ donné par la matrice

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \tag{9.512}$$

avec $a \neq b$, $a \neq 0$, $b \neq 0$, $\alpha \neq 0$, β et γ sont des nombres complexes quelconques. Son polynôme caractéristique est

$$\chi_f(X) = (a - X)^2(b - X), \tag{9.513}$$

et les valeurs propres sont donc a et b. Nous trouvons les vecteurs propres pour la valeur a en résolvant

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax \\ ay \\ az \end{pmatrix}. \tag{9.514}$$

La troisième équation est $bz = az$ qui oblige $z = 0$ parce que $a \neq b$ et $0 \neq a$. La première est $ax + \alpha y = ax$ qui implique $y = 0$ parce que $\alpha \neq 0$. Enfin la première équation se réduit à $ax = ax$ qui ne donne pas de contraintes sur x. En résumé : l'espace propre $E_a(f)$ est réduit à une seule dimension générée par $(1, 0, 0)$.

De la même façon l'espace propre correspondant à la valeur propre b est donné par le système

$$\begin{pmatrix} a & \alpha & \beta \\ & a & \gamma \\ & & b \end{pmatrix} \begin{pmatrix} w \\ y \\ z \end{pmatrix} = \begin{pmatrix} bx \\ by \\ bz \end{pmatrix} \tag{9.515}$$

La seconde équation donne $ay + \gamma z = by$, et donc

$$y = \frac{\gamma}{b - a} z. \tag{9.516}$$

La première équation est $ax + \alpha y + \beta z = bx$ qui donne

$$x = \frac{1}{b - a}(\alpha y + \beta z). \tag{9.517}$$

En y remettant la valeur déjà trouvée de y, nous trouvons que l'espace propre pour la valeur propre b est engendré par le vecteur

$$\begin{pmatrix} \frac{1}{b-a}\left(\beta + \frac{\alpha\gamma}{b-a}\right) \\ \frac{\gamma}{b-a} \\ 1 \end{pmatrix}. \tag{9.518}$$

Vu que nous savons que a et b sont les seules valeurs propres et que nous venons de voir que leurs espaces propres sont de dimension 1, il n'y a donc pas trois vecteurs propres linéairement indépendants, et l'opérateur f n'est pas diagonalisable.

Par contre nous pouvons voir que $(f - a\mathbb{1})^2 e_2 = 0$. En effet :

$$(f - a\mathbb{1})^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha & \beta \\ 0 & 0 & \gamma \\ 0 & 0 & b - a \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \tag{9.519}$$

de telle sorte que le vecteur $(0, 1, 0)$ est également dans l'espace caractéristique $F_a(f)$.

Dans cet exemple, la multiplicité algébrique de la racine a du polynôme caractéristique vaut 2 tandis que sa multiplicité géométrique vaut seulement 1.

9.13.1 Théorèmes de décomposition

Théorème 9.255 (Théorème spectral, décomposition primaire)**.**
Soit E un espace vectoriel de dimension finie sur le corps algébriquement clos $\mathbb{K}$ et $f \in \mathrm{End}(E)$. Alors

$$E = F_{\lambda_1}(f) \oplus \ldots \oplus F_{\lambda_k}(f) \tag{9.520}$$

où la somme est sur les espaces caractéristiques engendrés par les valeurs propres distinctes de f.

Les projecteurs sur les espaces caractéristiques forment un système complet et orthogonal.

Démonstration. Soit P le polynôme caractéristique de f et une décomposition

$$P = (f-\lambda_1)^{\alpha_1}\dots(f-\lambda_r)^{\alpha_r} \tag{9.521}$$

en facteurs irréductibles. Par le théorème des noyaux (9.86) nous avons

$$E = \ker(f-\lambda_1)^{\alpha_1} \oplus \dots \oplus \ker(f-\lambda_r)^{\alpha_r}. \tag{9.522}$$

Les projecteurs sont des polynômes en f et forment un système orthogonal. Il nous reste à prouver que $\ker(f-\lambda_i)^{\alpha_i} = F_{\lambda_i}(f)$. L'inclusion

$$\ker(f-\lambda_i)^{\alpha_i} \subset F_{\lambda_i}(f) \tag{9.523}$$

est évidente. Nous devons montrer l'inclusion inverse.

(i) $F_{\lambda_i}(f) \cap F_{\lambda_j}(f) = 0$ Soit $v \in F_{\lambda_i}(f) \cap F_{\lambda_j}(f)$. Le fait que $v \in F_{\lambda_i}(f)$ implique qu'il existe $n \in \mathbb{N}$ tel que $(f-\lambda_i)^n v \neq 0$ et $(f-\lambda_i)^{n+1}v = 0$ (éventuellement $n = 0$ si v est un vecteur propre). Posons $v_1 = (f-\lambda_i)^n v$.
Étant donné que $(f-\lambda_i)$ commute avec $(f-\lambda_j)$, ce v_1 est encore dans $F_{\lambda_j}(f)$. En effet, si k est tel que $(f-\lambda_j)^k v = 0$, alors

$$(f-\lambda_j)^k v_1 = (f-\lambda_j)^k (f-\lambda_i)^n v = (f-\lambda_i)^n (f-\lambda_j)^k v = 0. \tag{9.524}$$

Il existe donc $m \in \mathbb{N}$ tel que $(f-\lambda_j)^m v_1 \neq 0$ et $(f-\lambda_j)^{m+1}v_1 = 0$. En posant $w = (f-\lambda_j)^m v_1$, nous avons

$$\begin{cases} (f-\lambda_i)w = (f-\lambda_j)^m (f-\lambda_i)^{n+1} v = 0 & \text{(9.525a)} \\ (f-\lambda_j)w = (f-\lambda_j)^{m+1} v_1 = 0. & \text{(9.525b)} \end{cases}$$

Ce w serait donc un vecteur propre simultané pour les valeurs propres λ_i et λ_j. Vu que les espaces propres sont linéairement indépendants, les seules possibilités sont $i = j$ ou $w = 0$.

(ii) **Questions de dimension** Étant donné que espaces F_{λ_i} sont en somme directe, la somme de leurs dimensions est au maximum la dimension de E :

$$\sum_i \dim F_{\lambda_i}(f) \leqslant \dim E. \tag{9.526}$$

En tenant compte de l'inclusion (9.523) nous avons même

$$\dim E = \sum_i \dim \ker(f-\lambda_i)^{\alpha_i} \leqslant \sum_i \dim F_{\lambda_i}(f) \leqslant \dim E. \tag{9.527}$$

Vu qu'il y a $\dim(E)$ des deux côtés des inégalités, toutes les inégalités sont des égalités et nous avons

$$\sum_i \dim \ker(f-\lambda_i)^{\alpha_i} = \sum_i \dim F_{\lambda_i}(f). \tag{9.528}$$

L'inclusion (9.523) nous dit qu'il y a une inégalité terme à terme dans les sommes de (9.528). Vu qu'il y a égalité des sommes, il y a en réalité égalité de chacun des termes : $\dim\ker(f-\lambda_i)^{\alpha_i} = \dim F_{\lambda_i}(f)$ et l'égalité des deux espaces de (9.523) :

$$\ker(f-\lambda_i)^{\alpha_i} = F_{\lambda_i}(f). \tag{9.529}$$

□

¡¡ Avertissement/question à la lectrice !! 9.256
Dans le cas où le corps n'est pas algébriquement clos, il paraît qu'il faut remplacer « diagonalisable » par « semi-simple ».

Si vous connaissez un énoncé précis et une démonstration, écrivez-moi.

Il y a peut-être une réponse dans [283].

Si l'espace vectoriel est sur un corps algébriquement clos, alors les endomorphismes semi-simples [103] sont les endomorphismes diagonaux.

Théorème 9.257 (Décomposition de Dunford)**.**
Soit E un espace vectoriel sur le corps algébriquement clos [104] $\mathbb{K}$ *et $u \in \mathrm{End}(E)$ un endomorphisme de E.*

(1) L'endomorphisme u se décompose de façon unique sous la forme

$$u = s + n \tag{9.530}$$

où s est diagonalisable, n est nilpotent et $[s, n] = 0$ [105].

(2) Les endomorphismes s et n sont des polynômes en u et commutent avec u.

(3) Si notons $\{\lambda_i\}$ les valeurs propres distinctes de u, et $F_{\lambda_i}(u)$ les espaces caractéristiques correspondants, alors les parties s et n sont données par

$$s = \sum_i \lambda_i p_i \tag{9.531a}$$

$$n = \sum_i (s - \lambda_i \mathbb{1}) p_i \tag{9.531b}$$

$p_i \colon E \to F_{\lambda_i}(u)$ est la projection de E sur $F_{\lambda_i}(u)$.

Démonstration. Le théorème spectral 9.255 nous indique que

$$E = \bigoplus_i F_{\lambda_i}(f). \tag{9.532}$$

Nous considérons l'endomorphisme s de E qui consiste à dilater d'un facteur λ_i l'espace caractéristique $F_{\lambda_i}(f)$:

$$s = \sum_i \lambda_i p_i \tag{9.533}$$

où $p_i \colon E \to F_{\lambda_i}(u)$ est la projection de E sur $F_{\lambda_i}(u)$.

Nous allons prouver que $[s, f] = 0$ et $n = f - s$ est nilpotent. Cela impliquera que $[s, n] = 0$.

Si $x \in F_\lambda(f)$, alors nous avons $sf(x) = \lambda f(x)$ parce que $f(x) \in F_\lambda(f)$ tandis que $fs(x) = f(\lambda x) = \lambda f(x)$. Par conséquent f commute avec s.

Pour montrer que $f - s$ est nilpotent, nous en considérons la restriction

$$f - s \colon F_\lambda(f) \to F_\lambda(f). \tag{9.534}$$

Cet opérateur est égal à $f - \lambda\mathbb{1}$ et est par conséquent nilpotent.

Prouvons à présent l'unicité. Soit $u = s' + n'$ une autre décomposition qui satisfait aux conditions : s' est diagonalisable, n' est nilpotent et $[n', s'] = 0$. Commençons par prouver que s' et n' commutent avec u. En multipliant $u = s' + n'$ par s' nous avons

$$s'u = s'^2 + s'n' = s'^2 + n's' = (s' + n')s' = us', \tag{9.535}$$

par conséquent $[u, s'] = 0$. Nous faisons la même chose avec n' pour trouver $[u, n'] = 0$. Notons que pour obtenir ce résultat nous avons utilisé le fait que n' et s' commutent, mais pas leur propriétés de nilpotence et de diagonalisibilité.

Si $s' + n' = s + n$ est une autre décomposition, s' et n' commutent avec u, et par conséquent avec tous les polynômes en u. Ils commutent en particulier avec n et s. Les endomorphismes s

103. Définition 9.102.

104. Je crois quo'n peut remplacer l'ypothèse de corps alébriquement clos par une hypothèse de polynôme caractéristique scindé. Écrivez-moi si vous avez une idée à ce propos.

105. Lorsque a et b sont des opérateurs, la notation $[a, b]$ signifie le commutateur entre a et b, c'est-à-dire $a \circ b - b \circ a$. Dire que $[a, b] = 0$ signifie que $ab = ba$.

et s' sont alors deux endomorphismes diagonalisables qui commutent. Par la proposition 9.214, ils sont simultanément diagonalisables. Dans la base de diagonalisation simultanée, la matrice de l'opérateur $s' - s = n - n'$ est donc diagonale. Mais $n - n'$ est également nilpotent, en effet si A et B sont deux opérateurs nilpotents,

$$(A + B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k}. \tag{9.536}$$

Si n est assez grand, au moins un parmi A^k ou B^{n-k} est nul.

Nous savons que $n - n'$ est diagonal et nilpotent. Le seul opérateur diagonal à être nilpotent est l'opérateur nul[106]. Nous en déduisons que $n = n'$. Nous avons alors immédiatement aussi $s = s'$. □

9.258.
Le théorème 12.420 montrera que $A^n x \to 0$ pour tout x si et seulement si $\rho(A) < 1$, mais ça demande un résultat de vitesse comparée entre l'exponentielle et la puissance.

Une application de la décomposition de Jordan est l'existence d'un logarithme pour les matrices. La proposition suivante va d'une certaine manière donner un logarithme pour les matrices inversibles complexes. Dans le cas des matrices réelles m telles que $\|m - \mathbb{1}\| < 1$, nous donnerons au lemme 15.150 une formule pour le logarithme sous forme d'une série ; ce logarithme sera réel.

9.13.2 Valeurs singulières

Définition 9.259.
*Soit M une matrice $m \times n$ sur $\mathbb{K}$ ($\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$). Un nombre réel σ est une **valeur singulière** de M si il existe des vecteurs unitaires $u \in \mathbb{K}^m$, $v \in \mathbb{K}^n$ tels que*

$$Mv = \sigma u \tag{9.537a}$$
$$M^* u = \sigma v. \tag{9.537b}$$

Théorème 9.260 (Décomposition en valeurs singulières)**.**
Soit $M \in \mathbb{M}(m \times n, \mathbb{K})$ où $\mathbb{K} = \mathbb{R}, \mathbb{C}$. Alors M se décompose en

$$M = ADB \tag{9.538}$$

où il existe deux matrices unitaires $A \in \mathrm{U}(m \times m)$, $B \in \mathrm{U}(n \times n)$ et une matrice (pseudo)diagonale $D \in \mathbb{M}(m \times n)$ tels que

(1) $A \in \mathrm{U}(m \times m)$, $B \in \mathrm{U}(n \times n)$ sont deux matrices unitaires,

(2) D est (pseudo)diagonale,

(3) les éléments diagonaux de D sont les valeurs singulières de M,

(4) le nombre d'éléments non nuls sur la diagonale de D est le rang[107] de M.

Corolaire 9.261.
Soit $M \in \mathbb{M}(n, \mathbb{C})$. Il existe un isomorphisme $f : \mathbb{C}^n \to \mathbb{C}^n$ tel que fM soit autoadjoint.

Démonstration. Si $M = ADB$ est la décomposition de M en valeurs singulières, alors nous pouvons prendre $f = \overline{B}^t A^{-1}$ qui est une matrice inversible. Pour la vérification que ce f répond bien à la question, ne pas oublier que D est réelle, même si M ne l'est pas. □

106. Parce qu'une puissance d'un opérateur diagonal est diagonal.
107. Définition 4.45.

9.14 Extension du corps de base

Nous avons discuté dans la section 6.4 de ce qui arrive au corps lorsqu'on l'étend. Dans cette section nous allons étudier ce qui arrive aux applications linéaires entre deux $\mathbb{K}$-espaces vectoriels lorsque nous étendons le corps $\mathbb{K}$ en un corps $\mathbb{L}$.

Soient $\mathbb{K}$ un corps (commutatif) et une extension $\mathbb{L}$ de $\mathbb{K}$. Soient E et F, des $\mathbb{K}$-espaces vectoriels de dimension finie, et entrons dans le vif du sujet [108].

9.14.1 Extension des applications linéaires

Définition 9.262 ([284]).
L'espace vectoriel obtenu par ***extension du corps de base*** *de E est l'espace vectoriel*

$$E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E. \tag{9.539}$$

Ce dernier est le quotient $\mathbb{L} \otimes_{\mathbb{K}} E = (\mathbb{L} \times E)/\sim$ par la relation d'équivalence

$$(\lambda, v) \sim \big(a\lambda, \frac{1}{a}v\big) \tag{9.540}$$

pour tout $a \in \mathbb{K}\backslash\{0\}$. Nous noterons $[\lambda, v]$ ou $\lambda \otimes v$ ou encore $\lambda \otimes_{\mathbb{K}} v$ la classe de (λ, v) pour la relation d'équivalence $\sim$:

$$[\lambda, v] = \{(\mu, w) \in \mathbb{L} \times E \text{ tel que } (\mu, w) \sim (\lambda, v)\}. \tag{9.541}$$

Un élément de $E_{\mathbb{L}}$ est de la forme $\sum_k [\lambda_k, v_k]$ avec $\lambda_k \in \mathbb{L}$ et $v_k \in E$. Si $f\colon E \to F$ est une applications linéaire, nous définissons

$$\begin{aligned} f_{\mathbb{L}}\colon E_{\mathbb{L}} &\to F_{\mathbb{L}} \\ [\lambda, v] &\mapsto [\lambda, f(v)]. \end{aligned} \tag{9.542}$$

Remarque 9.263.
Si deux vecteurs de $E_{\mathbb{L}}$ sont linéairement indépendants pour $\mathbb{K}$, ils ne le sont pas spécialement pour $\mathbb{L}$. Par exemple si $\mathbb{C}$ est vu comme $\mathbb{R}$-espace vectoriel, alors $\{1, i\}$ est une partie libre. Mais dans $\mathbb{C}$, vu comme $\mathbb{C}$-espace vectoriel, la partie $\{1, i\}$ n'est pas libre.

Lemme 9.264.
Soient trois $\mathbb{K}$-espaces vectoriels E, F et G ainsi que deux applications linéaires $f\colon E \to F$ et $g\colon G \to E$. Si $\mathbb{L}$ est une extension de $\mathbb{K}$, alors

$$f_{\mathbb{L}} \circ g_{\mathbb{L}} = (f \circ g)_{\mathbb{L}}. \tag{9.543}$$

Démonstration. Il suffit de composer la définition (9.542) :

$$\begin{aligned} (f_{\mathbb{L}} \circ g_{\mathbb{L}})\big([\lambda, v]\big) &= f_{\mathbb{L}}\big([\lambda, g(v)]\big) && \text{(9.544a)} \\ &= [\lambda, (f \circ g)(v)] && \text{(9.544b)} \\ &= (f \circ g)_{\mathbb{L}}\big([\lambda, v]\big). && \text{(9.544c)} \end{aligned}$$

□

Nous définissons aussi l'injection canonique

$$\begin{aligned} \tau\colon E &\to E_{\mathbb{L}} \\ v &\mapsto [1, v]. \end{aligned} \tag{9.545}$$

Proposition 9.265 ([127]).
Injectivité et surjectivité respectées.

108. Le sujet étant le corps étendu.

(1) L'application $f_{\mathbb{L}}$ est injective si et seulement si f est injective.

(2) L'application $f_{\mathbb{L}}$ est surjective si et seulement si f est surjective.

Démonstration. En plusieurs parties.

(i) **Si $f_{\mathbb{L}}$ est injective** Supposons pour commencer que $f_{\mathbb{L}}$ soit injective. Le diagramme

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ E_{\mathbb{L}} & \xrightarrow[f_{\mathbb{L}}]{} & F_{\mathbb{L}} \end{array} \tag{9.546}$$

est un diagramme commutatif. En effet

$$(\tau \circ f)(v) = [1, f(v)] \tag{9.547}$$

tandis que

$$(f_{\mathbb{L}} \circ \tau)(v) = f_{\mathbb{L}}[1, v] = [1, f(v)]. \tag{9.548}$$

Donc si $f(v) = 0$ avec $v \neq 0$ nous aurions $(\tau \circ f)(v) = 0$ et donc aussi $(f_{\mathbb{L}} \circ \tau)(v) = 0$, alors que $\tau(v) \neq 0$ dans $E_{\mathbb{L}}$.

(ii) **Si f est injecive** Nous supposons que f est injective et que $f_{\mathbb{L}}(\lambda \otimes v) = f_{\mathbb{L}}(\mu \otimes w)$. Cela signifie que $\lambda \otimes f(v) = \mu \otimes f(w)$, ou encore qu'il existe $a \neq 0$ dans $\mathbb{K}$ tel que

$$\begin{cases} \mu = a\lambda & \text{(9.549a)} \\ f(w) = \dfrac{1}{a} f(v). & \text{(9.549b)} \end{cases}$$

Par linéarité de f, $f(v) = f(aw)$ et par injectivité de f, nous déduisons que $v = aw$. Enfin nous avons l'injectivité de $f_{\mathbb{L}}$ parce que

$$\mu \otimes w = a\lambda \otimes \frac{v}{a} = \lambda \otimes v. \tag{9.550}$$

□

Proposition 9.266 ([1, 285])**.**
Soit $\{e_i\}_{i=1,\dots,p}$ une base de E. Alors $\{1 \otimes e_i\}_i$ est une base de $E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E$.

Démonstration. L'espace vectoriel E peut être écrit comme somme directe $E = \bigoplus_i \mathbb{K}e_i$. Si $\lambda \in \mathbb{L}$ et $k \in \mathbb{K}$ nous avons

$$\lambda \otimes ke_i = \frac{\lambda}{k} \otimes e_i = \frac{\lambda}{k}(1 \otimes e_i). \tag{9.551}$$

Cela pour introduire l'application

$$\begin{aligned} \psi \colon \mathbb{L} \otimes_{\mathbb{K}} E &\to \bigoplus_i \mathbb{L}(1 \otimes e_i) \\ \sum_k \lambda_k \otimes v_k &\mapsto \oplus_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) \end{aligned} \tag{9.552}$$

où $v_k = \sum_i v_{ik} e_i$ avec $v_{ik} \in \mathbb{K}$, qui représente un isomorphisme de $\mathbb{L}$-espaces vectoriels. La surjectivité est facile. En ce qui concerne l'injectivité, si

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = 0 \tag{9.553}$$

alors les quantités suivantes sont nulles également :

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = \sum_{ik} (\lambda_k \otimes v_{ik} e_i) = \sum_k (\lambda_k \otimes \sum_i v_{ik} e_i) = \sum_k (\lambda_k \otimes v_k). \tag{9.554}$$

La dernière est l'argument de ψ. Le fait qu'il soit nul implique que ψ est injective. □

Remarque 9.267.
Nous n'avons pas dû prouver que chacun des $\lambda_k \otimes v_k$ était nul. Et encore heureux, parce que cela pouvait très bien être faux, puisqu'il y a plusieurs façons de noter un élément de $E_{\mathbb{L}}$ sous la forme de tels termes.

Corolaire 9.268.
La $\mathbb{L}$-dimension de $E_{\mathbb{L}}$ est égale à la $\mathbb{K}$-dimension de E.

9.14.2 Projections

¡¡ Avertissement/question à la lectrice !! 9.269
Nous allons définir `proj`$\colon \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \to \mathcal{L}(E, F)$ *en faisant appel à des bases et en prouvant que les quantités définies ne dépendent pas des bases choisies. Il y a surement une façon plus « intrinsèque » de faire.*

Nous savons que $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel dans lequel nous pouvons voir $\mathbb{K}$ comme un sous-espace (lemme 6.60). Dans cette optique nous choisissons dans $\mathbb{L}$ un supplémentaire de $\mathbb{K}$, c'est-à-dire un sous-espace vectoriel de $\mathbb{L}$ tel que

$$\mathbb{L} = \mathbb{K} \oplus V. \tag{9.555}$$

Nous avons alors naturellement une projection $\texttt{proj}\colon \mathbb{L} \to \mathbb{K}$.

Soit $\{e_i\}$ une base de E et $\{e_a\}$ une de F. Nous noterons également e_i et e_a les éléments $\tau(e_i)$ et $\tau(e_a)$ correspondants. Grâce à la proposition 9.266, ce sont des bases de $E_{\mathbb{L}}$ et $F_{\mathbb{L}}$. Si la fonction $f\colon E_{\mathbb{L}} \to F_{\mathbb{L}}$ s'écrit dans ces bases comme

$$f(e_i) = \sum_a f_{ai} e_a \tag{9.556}$$

alors nous définissons $\texttt{proj}(f)$ par

$$(\texttt{proj}\, f)e_i = \sum_a \texttt{proj}(f_{ai}) e_a. \tag{9.557}$$

Proposition 9.270 ([1]).
L'application `proj` *définie en* (9.557) *est indépendante du choix des bases.*

Démonstration. Notons que dans ce qui suit, les sommes sur a ou b et celles sur i ou j ne vont pas jusqu'au même indice (dimensions de E et F). De plus nous manipulons deux quantités qui se notent `proj`. La première est la projection $\texttt{proj}\colon \mathbb{L} \to \mathbb{K}$ qui ne dépend que d'un choix de supplémentaire et que nous supposons fixée ici. D'autre part il y a $\texttt{proj}\colon E_{\mathbb{L}} \to E$ qui dépend à priori des bases choisies.

Nous choisissons de nouvelles bases qui sont liées aux anciennes bases par

$$\begin{cases} e'_b = \sum_a B_{ab} e_a & \text{(9.558a)} \\ e'_j = \sum_i A_{ji} e_i. & \text{(9.558b)} \end{cases}$$

Les matrices A et B sont dans $\mathrm{GL}(\mathbb{K})$. Nous allons écrire l'opérateur $\texttt{proj}'$ qui correspond à ces bases et montrer que pour toute application linéaire $f\colon E_{\mathbb{L}} \to F_{\mathbb{L}}$ nous avons $\texttt{proj}(f) = \texttt{proj}'(f)$. Nous avons :

$$\begin{aligned} f(e'_j) &= \sum_i A_{ji} f(e_i) && \text{(9.559a)} \\ &= \sum_a \sum_b \sum_i A_{ji} f_{ai} (B^{-1})_{ba} e'b && \text{(9.559b)} \\ &= \sum_b \Big(\sum_{ai} A_{ji} f_{ai} (B^{-1})_{ba} \Big) e'b, && \text{(9.559c)} \end{aligned}$$

ce qui donne

$$(\mathtt{proj}'\, f)e'_j = \sum_b \Big(\mathtt{proj}\left(A_{ji} f_{ai} (B^{-1})_{ba}\right)\Big) e'_b. \tag{9.560}$$

Nous calculons maintenant $(\mathtt{proj}'\, f)e_j$ en substituant $e_j = \sum_l (A^{-1})_{lj} e'_l$ et en utilisant (9.560), la linéarité de $\mathtt{proj}'$ et la $\mathbb{K}$-linéarité de $\mathtt{proj}\colon \mathbb{L} \to \mathbb{K}$:

$$\begin{aligned}(\mathtt{proj}'\, f)\Big(\sum_l (A^{-1})_{lj} e'_l\Big) &= \sum_l (A^{-1})_{lj} \sum_b \sum_{ai} \mathtt{proj}\left(A_{li} f_{ai} (B^{-1})_{ba}\right) e_b && (9.561a)\\ &= \sum_a \mathtt{proj}(f_{aj}) e_a && (9.561b)\\ &= (\mathtt{proj}\, f) e_j. && (9.561c)\end{aligned}$$

Donc $\mathtt{proj} = \mathtt{proj}'$. □

Note au passage : il y a un abus systématique de notation entre $e_i \in E$ et $\tau(e_i) = 1 \otimes e_i \in E_{\mathbb{L}}$.

Remarque 9.271 ([1]).
L'opération $\mathtt{proj}\colon \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \to \mathcal{L}(E, F)$ ne dépend pas des bases choisies un peu partout. Mais elle dépend de l'application $\mathtt{proj}\colon \mathbb{L} \to \mathbb{K}$ déjà construite. Et celle-là dépend du choix d'un supplémentaire V qui fournit $\mathbb{L} = \mathbb{K} \oplus V$.

Si $\mathtt{proj}(\lambda) = 0$ pour un de ces choix, cela n'implique nullement que $\lambda = 0$. Penser à $i \in \mathbb{C}$ si la projection $\mathtt{proj}\colon \mathbb{C} \to \mathbb{R}$ est l'application $(x + iy) \mapsto x$ parallèle à l'axe des imaginaires.

Par contre si $\mathtt{proj}(\lambda) = 0$ pour tout choix de V, alors nous avons bien $\lambda = 0$. Dans la suite nous « fixons » un choix de V générique, et lorsque nous rencontrerons l'égalité $\mathtt{proj}(\lambda) = 0$ nous en déduirons $\lambda = 0$.

Proposition 9.272.
Si $f\colon E \to F$ et si $f_{\mathbb{L}}(e_j) = \sum_a (f_{\mathbb{L}})_{aj} e_a$ et si $f(e_j) = \sum_a f_{aj} e_a$ alors

(1) $\mathtt{proj}\, f_{\mathbb{L}} = f$,

(2) $(f_{\mathbb{L}})_{aj} = f_{aj} \in \mathbb{K}$.

Démonstration. Nous avons

$$f_{\mathbb{L}}(e_i) = \sum_a f_{ai}(1 \otimes e_a) = \sum_a f_{ai} \tau(e_a), \tag{9.562}$$

donc

$$(\mathtt{proj}\, f_{\mathbb{L}}) e_i = \sum_a \mathtt{proj}(f_{ai}) e_a = \sum_a f_{ai} e_a = f(e_i). \tag{9.563}$$

Cela prouve que $\mathtt{proj}\, f_{\mathbb{L}} = f$.

Par ailleurs,

$$f_{\mathbb{L}}(\tau(e_i)) = f_{\mathbb{L}}(1 \otimes e_i) = 1 \otimes f(e_i) = \tau\big(f(e_i)\big) = \sum_a f_{ai} \tau(e_a) \tag{9.564}$$

alors que par définition,

$$f_{\mathbb{L}}(\tau(e_i)) = \sum_a (f_{\mathbb{L}})_{ai} \tau(e_a). \tag{9.565}$$

Les éléments $\tau(e_a)$ formant une base[109], la comparaison de (9.564) avec (9.565) donne $(f_{\mathbb{L}})_{ai} = f_{ai} \in \mathbb{K}$. □

Lemme 9.273.
Soient des espaces vectoriels E, F et G ainsi que des applications linéaires

(1) $f\colon E \to F$,

(2) $\tilde{h}\colon G_{\mathbb{L}} \to E_{\mathbb{L}}$.

109. Encore la proposition 9.266.

Alors nous avons

$$\texttt{proj}(f_{\mathbb{L}} \circ \tilde{h}) = \texttt{proj}(f_{\mathbb{L}}) \circ \texttt{proj}(\tilde{h}). \tag{9.566}$$

De même[110] *si* $f\colon E \to F$ *et* $\tilde{h}\colon F_{\mathbb{L}} \to G_{\mathbb{L}}$, *alors*

$$\texttt{proj}(\tilde{h} \circ f_{\mathbb{L}}) = \texttt{proj}(\tilde{h}) \circ \texttt{proj}(f_{\mathbb{L}}). \tag{9.567}$$

Démonstration. Nous considérons une base $\{e_i\}$ de E, une base $\{e_a\}$ de F, et une base $\{e_\alpha\}$ de G. Pour écrire $\texttt{proj}(f_{\mathbb{L}} \circ \tilde{h})$ à partir de la définition (9.557) nous commençons par écrire

$$(f_{\mathbb{L}} \circ \tilde{h})e_\alpha = \sum_a (f_{\mathbb{L}} \circ \tilde{h})_{a\alpha} e_a = \sum_{ai} (f_{\mathbb{L}})_{ai} (\tilde{h})_{i\alpha} e_a = \sum_a \Big(\sum_i f_{ai} (\tilde{h})_{i\alpha} \Big) e_a \tag{9.568}$$

où nous avons utilisé le fait que $(f_{\mathbb{L}})_{ai} = f_{ai}$. Donc, en utilisant la $\mathbb{K}$-linéarité de $\texttt{proj}$,

$$\texttt{proj}(f_{\mathbb{L}} \circ \tilde{h})e_\alpha = \sum_a \sum_i \texttt{proj}\Big(f_{ai} (\tilde{h})_{i\alpha} \Big) e_a = \sum_a \sum_i f_{ai}\, \texttt{proj}\Big((\tilde{h})_{i\alpha} \Big) e_a. \tag{9.569}$$

D'autre part,

$$\begin{aligned} \texttt{proj}(f_{\mathbb{L}}) \circ \texttt{proj}(\tilde{h})e_\alpha &= \texttt{proj}(f_{\mathbb{L}}) \sum_i \texttt{proj}\Big((\tilde{h})_{i\alpha} \Big) e_i \\ &= \sum_i \texttt{proj}\Big((\tilde{h})_{i\alpha} \Big) \sum_a f_{ai} e_a \\ &= \sum_{ai} \texttt{proj}\Big((\tilde{h})_{i\alpha} \Big) f_{ai} e_a, \end{aligned} \tag{9.570}$$

et c'est égal à (9.569). □

Remarque 9.274.
Nous n'avons en général pas $\texttt{proj}(xy) = \texttt{proj}(x)\,\texttt{proj}(y)$ pour tout $x, y \in \mathbb{L}$. Par exemple si $\mathbb{K} = \mathbb{R}$ et $\mathbb{L} = \mathbb{C}$ avec la projection canonique,

$$\texttt{proj}(i \cdot i) = \texttt{proj}(-1) = -1 \tag{9.571}$$

alors que $\texttt{proj}(i) = 0$.

Proposition 9.275.
Soient trois $\mathbb{K}$*-espaces vectoriels* E, F *et* G. *Nous considérons deux applications linéaires* $f\colon E \to F$ *et* $g\colon E \to G$.

Il existe une application linéaire $h\colon F \to G$ *telle que* $g = h \circ f$ *si et seulement si il existe une application linéaire* $\tilde{h}\colon F_{\mathbb{L}} \to G_{\mathbb{L}}$ *telle que* $g_{\mathbb{L}} = \tilde{h} \circ f_{\mathbb{L}}$.

Démonstration. Dans le sens direct, il suffit de poser $\tilde{h} = h_{\mathbb{L}}$ et d'invoquer le lemme 9.264.

Dans le sens inverse, si nous avons $\tilde{h}\colon F_{\mathbb{L}} \to G_{\mathbb{L}}$ tel que $g_{\mathbb{L}} = \tilde{h} \circ f_{\mathbb{L}}$ alors en appliquant $\texttt{proj}$ des deux côtés et en utilisant le lemme 9.273,

$$\texttt{proj}(g_{\mathbb{L}}) = \texttt{proj}(\tilde{h}) \circ \texttt{proj}(f_{\mathbb{L}}) \tag{9.572}$$

c'est-à-dire

$$g = \texttt{proj}(\tilde{h}) \circ f, \tag{9.573}$$

c'est-à-dire que l'application $\texttt{proj}(\tilde{h})\colon F \to G$ est la réponse à la proposition. □

110. Je n'ai pas vérifié cette deuxième partie. Soyez prudent.

9.14.3 Rang, polynôme minimal, polynôme caractéristique

Proposition 9.276 (Stabilité du rang par extension des scalaires[127]).
Si $f\colon E\to F$ est linéaire alors nous avons

$$\operatorname{rk}(f)=\operatorname{rk}(f_{\mathbb{L}}). \tag{9.574}$$

où à droite nous considérons le rang de l'application $\mathbb{L}$-linéaire $f_{\mathbb{L}}\colon E_{\mathbb{L}}\to F_{\mathbb{L}}$.

Démonstration. Il existe un supplémentaire V tel que $E=\ker(f)\oplus V$ avec $\dim(V)=\operatorname{rk}(f)$. Nous pouvons factoriser f en

$$f=f_2\circ f_1 \tag{9.575}$$

avec $f_1\colon E\to V$ est la projection parallèle à $\ker(f)$ et est surjective (vers V) parce que $\dim(V)=\operatorname{rk}(f)=\dim\big(\text{Image}(f)\big)$. De plus $f_2\colon V\to F$ est injective parce que si $v\in V$ est tel que $f_2(v)=0$ alors on aurait

$$f(v)=(f_2\circ f_1)(v)=f_2(v)=0. \tag{9.576}$$

Cela donne $v\in\ker(f)\cap V=\{0\}$. Par la proposition 9.265, les applications $(f_1)_{\mathbb{L}}$ et $(f_2)_{\mathbb{L}}$ sont respectivement surjective et injective.

L'application $(f_2)_{\mathbb{L}}\colon V_{\mathbb{L}}\to F_{\mathbb{L}}$ est forcément surjective sur son image, donc

$$(f_2)_{\mathbb{L}}\colon V_{\mathbb{L}}\to\text{Image}(f_{\mathbb{L}}) \tag{9.577}$$

est un isomorphisme de $\mathbb{L}$-espaces vectoriels. Nous avons alors les égalités

$$\dim_{\mathbb{L}}(V_{\mathbb{L}})=\dim_{\mathbb{L}}\big(\text{Image}(f_{\mathbb{L}})\big)=\operatorname{rk}(f_{\mathbb{L}}). \tag{9.578}$$

Mais aussi, par les définitions posées plus haut,

$$\dim(V)=\operatorname{rk}(f)=\dim\big(\text{Image}(f)\big). \tag{9.579}$$

Mais le corolaire 9.268 nous dit que $\dim_{\mathbb{L}}(V_{\mathbb{L}})=\dim_{\mathbb{K}}(V)$. Donc il y a égalité des deux lignes (9.578) et (9.579), ce qui donne $\operatorname{rk}(f)=\operatorname{rk}(f_{\mathbb{L}})$. □

Proposition 9.277.
Nous avons

(1) $\det(f)=\det(f_{\mathbb{L}})$

(2) $\chi_f=\chi_{f_{\mathbb{L}}}$.

Démonstration. Dès que l'on a des bases nous avons $(f_{\mathbb{L}})_{ai}=f_{ai}$ par la proposition 9.272(2). Le nombre $\det(f)\in\mathbb{K}$ est un polynôme en les f_{ai}. Entendons nous : il existe un polynôme indépendant de f et de $\mathbb{K}$ et de $\mathbb{L}$ donnant le déterminant de n'importe quelle matrice. Donc $\det(f)=\det(f_{\mathbb{L}})$.

Même chose pour le polynôme caractéristique (définition 9.107) : les coefficients de ce polynôme sont des polynômes en les f_{ai} qui sont indépendants de $\mathbb{L}$, de $\mathbb{K}$ et de f.

Notons que $\chi_{f_{\mathbb{L}}}$ est un polynôme à coefficients dans $\mathbb{K}$. □

La situation est très différente avec le polynôme minimal [111]. Autant il existe une « recette » pour créer le polynôme caractéristique, il n'en n'existe pas pour le polynôme minimal (ou en tout cas, il ne suffit pas d'appliquer des polynômes en les coefficients de la matrice). La proposition suivante montre que le polynôme minimal est conservé par extension de corps, mais que pour le savoir, il faut travailler plus.

Proposition 9.278 ([127, 1]).
Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$ et une application linéaire $f\colon E\to F$ entre deux $\mathbb{K}$-espaces vectoriels. Alors $\mu_f=\mu_{f_{\mathbb{L}}}$.

111. Définition 6.64.

Démonstration. Nous allons montrer que l'application

$$\begin{aligned}\tilde{g}\colon \frac{\mathbb{L}[X]}{(\mu)} &\to \mathrm{End}(E_{\mathbb{L}})\\ [P] &\mapsto P(f_{\mathbb{L}})\end{aligned} \tag{9.580}$$

est bien définie et injective. La proposition 9.97 nous dira alors que μ est le polynôme minimal de $f_{\mathbb{L}}$.

Pour prouver que l'application $\tilde{g}$ est bien définie, nous commençons par prouver que $P(f_{\mathbb{L}}) = P(f)_{\mathbb{L}}$:

$$P(f_{\mathbb{L}})\lambda\otimes v = \sum_k a_k f_{\mathbb{L}}^k\lambda\otimes v \tag{9.581a}$$
$$= \lambda\otimes\sum_k a_k f^k(v) \tag{9.581b}$$
$$= \lambda\otimes P(f)v \tag{9.581c}$$
$$= P(f)_{\mathbb{L}}\lambda\otimes v. \tag{9.581d}$$

Par conséquent $\mu(f_{\mathbb{L}}) = 0$ et l'application est bien définie.

Sur $\mathbb{L}[X]/(\mu)$ nous considérons la base $\{1, [X], \dots, [X^{\deg(\mu)-1}]\}$, et sur $\mathrm{End}(E_{\mathbb{L}})$ nous considérons une base qui commence [112] par $\{f_{\mathbb{L}}^k\}_{k=0,\dots,\deg(\mu)-1}$. Montrons tout de même que cette partie est libre (sinon le théorème de la base incomplète ne s'applique pas) : si $\sum_k \lambda_k f_{\mathbb{L}}^k = 0$ alors

$$\sum_k \mathtt{proj}\left(\lambda_k f_{\mathbb{L}}^k\right) = 0. \tag{9.582}$$

Pour détailler ce que cela implique, nous calculons ceci :

$$(\lambda f_{\mathbb{L}})(\tau(e_i)) = \lambda f_{\mathbb{L}}(\tau(e_i)) = \sum_a \lambda f_{ai} e_a, \tag{9.583}$$

par conséquent $\mathtt{proj}(\lambda f_{\mathbb{L}})e_i = \sum_a \mathtt{proj}(\lambda f_{ai})e_a$, et comme $\mathtt{proj}$ est $\mathbb{K}$-linéaire et que $f_{ai}\in\mathbb{K}$,

$$\mathtt{proj}(\lambda f_{\mathbb{L}})e_i = \mathtt{proj}(\lambda)\sum_a f_{ai}e_a = \mathtt{proj}(\lambda)\,\mathtt{proj}(f_{\mathbb{L}})e_i = \mathtt{proj}(\lambda)f(e_i). \tag{9.584}$$

Appliquer la projection $\mathtt{proj}$ à l'équation (9.582) donne alors $\sum_k \mathtt{proj}(\lambda)_k f^k = 0$. Mais comme les f^k sont linéairement indépendants sur $\mathbb{K}$ nous avons pour tout k : $\mathtt{proj}(\lambda_k) = 0$ (égalité dans $\mathbb{K}$). En nous souvenant de la remarque 9.271 nous en déduisons $\lambda_k = 0$ dans $\mathbb{L}$.

Dans les choix de bases effectués, l'application $\tilde{g}$ a la forme

$$\tilde{g} = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \\ * & * & * \\ * & * & * \\ * & * & * \end{pmatrix}, \tag{9.585}$$

qui est injective.

Puisque $\tilde{g}$ est injective, μ est le polynôme minimal de $f_{\mathbb{L}}$ et donc $\mu = \mu_{\mathbb{L}}$. □

9.15 Frobenius et Jordan

9.15.1 Matrice compagnon

Définition 9.279.
*Soit le polynôme $P = X^n - a_{n-1}X^{n-1} - \dots - a_1X - a_0$ dans $\mathbb{K}[X]$. La **matrice compagnon** de*

112. Théorème de la base incomplète 4.13(2).

P est la matrice donnée par

$$C(P) = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix} \tag{9.586}$$

si $n \geqslant 2$ et par (a_0) si $n = 1$.

Une matrice est dite compagnon si elle a cette forme.

Proposition 9.280.
Si f est l'endomorphisme associé à la matrice $C(P)$ nous avons

$$f(e_i) = \begin{cases} e_{i+1} & si\ 1 \leqslant i < n \\ (a_0, \dots, a_{n-1}) & si\ i = n. \end{cases} \tag{9.587}$$

De plus l'endomorphisme f vérifie $P(f)e_1 = 0$.

Lemme 9.281 ([286])**.**
Un polynôme sur un corps commutatif est le polynôme caractéristique de sa matrice compagnon. En d'autres termes nous avons $\chi_{C(P)} = P$.

Démonstration. Nous notons f l'endomorphisme associé à $C(P)$. La propriété $P(f)e_1 = 0$ nous indique que le polynôme minimal ponctuel de f en e_1 divise P. L'ensemble des puissances de f appliquées à e_1, $\big(f^k(e_1)\big)_{k=1,\dots,n-1}$ est libre, donc le polynôme minimal ponctuel en e_1 est de degré n au minimum. En reprenant les notations du théorème 6.43, nous avons $I_{e_1} = (P)$ parce que P est de degré minimum dans I_{e_1} et $\chi_f \in I_{e_1}$.

Donc P divise χ_f et est de degré égal à celui de χ_f. Étant donné qu'ils sont tous deux unitaires, ils sont égaux. □

Remarque 9.282.
Les matrices compagnons ne sont pas les seules dont le polynôme caractéristique est égal au polynôme minimal. En fait les matrices dont le polynôme caractéristique est égal au polynôme minimal sont denses dans l'ensemble des matrices. En effet une matrice dont le polynôme minimal n'est pas égal au polynôme caractéristique a un polynôme caractéristique avec une racine double. Il est possible, en modifiant arbitrairement peu la matrice, de séparer la racine double en deux racines distinctes.

9.15.2 Réduction de Frobenius

Lemme 9.283.
Soit un endomorphisme $f : E \to E$ sur l'espace vectoriel de dimension finie n. Nous notons μ et χ les polynômes minimal et caractéristique. Si f est cyclique, alors $\mu = \chi$.

Le théorème 9.296 donnera une version plus complète de ce lemme.

Démonstration. Soit v un vecteur cyclique de f, c'est-à-dire que $\{f^k(v)\}_{k=0,\dots,n-1}$ est libre. Donc si P est un polynôme de degré jusqu'à $n-1$ nous ne pouvons pas avoir $P(f) = 0$ parce que, appliqué à v, ce serait une combinaisons nulle non triviale des $f^k(v)$. Donc le polynôme minimal est au minimum de degré n. Mais le polynôme caractéristique est annulateur de degré n (Cayley-Hamilton 9.115), donc il est le polynôme minimal. □

Théorème 9.284 (Réduction de Frobenius [287, 288, 289])**.**
Soit E, un $\mathbb{K}$-espace vectoriel, et $f \in \mathrm{End}(E)$. Alors il existe une suite de sous-espaces $E_1, \dots, E_r$ stables par f tels que

(1) $E = \bigoplus_{i=1}^{r} E_i$;

(2) pour chaque E_i, *l'endomorphisme restreint* $f_i = f|_{E_i}$ *est cyclique ;*

(3) si μ_i *est le polynôme minimal de* f_i *alors* μ_{i+1} *divise* μ_i ;

Une telle décomposition vérifie automatiquement $\mu_1 = \mu_f$ *et* $\mu_1 \cdots \mu_r = \chi_f$, *et la suite* $(\mu_i)_{i=1,\dots,r}$ *ne dépend que de* f, *et non du choix de la décomposition du point (1).*

Les polynômes μ_i sont les **invariants de similitude** de l'endomorphisme f.

Démonstration. Nous commençons par montrer que si une telle décomposition existe, alors

$$\chi_f = \prod_{i=1}^{r} \mu_i \tag{9.588a}$$

$$\mu_f = \mu_1 \tag{9.588b}$$

où χ_f est le polynôme caractéristique de f et μ_f est le polynôme minimal. D'abord le polynôme caractéristique de f devra être égal au produit des polynômes caractéristiques des $f|_{E_i}$, mais ces derniers endomorphismes étant cycliques [113], leurs polynômes caractéristiques sont égaux à leurs polynômes minimaux (lemme 9.283). Cela prouve l'égalité (9.588a). Ensuite tous les μ_i doivent diviser le polynôme minimal, donc $\operatorname{ppcm}(\mu_1, \dots, \mu_r)$ divise μ_f. Cependant le polynôme minimal doit contenir une et une seule fois chacun des facteurs irréductibles du polynôme caractéristique, et chacun de ces facteurs sont dans les polynômes μ_i. Par conséquent $\operatorname{ppcm}(\mu_1, \dots, \mu_r) = \mu_f$. Mais par ailleurs $\mu_1 = \operatorname{ppcm}(\mu_1, \dots, \mu_r)$ parce qu'on a supposé $\mu_{i+1} \mid \mu_i$, donc $\mu_1 = \mu_f$.

Soit d, le degré du polynôme minimal de f et $y \in E$ tel que $\mu_f = \mu_{f,y}$ (voir lemme 9.98). Le plus petit espace stable sous f contenant y est

$$E_y = \operatorname{Span}\{y, f(y), \dots, f^{d-1}(y)\}. \tag{9.589}$$

Nous notons $e_i = f^{i-1}(y)$. Notons que les vecteurs donnés forment bien une base de E_y parce que si les e_i n'était pas linéairement indépendants, alors nous aurions des a_k tels que $\sum_k a_k e_k = 0$ et avec lesquels

$$\big(\sum_k a_k X^k\big)(f)y = 0, \tag{9.590}$$

ce qui contredirait la minimalité de $\mu_{f,y}$.

La difficulté du théorème est de trouver un complément de E_y qui soit également stable sous f. Nous commençons par étendre [114] $\{e_1, \dots, e_d\}$ en une base $\{e_1, \dots, e_n\}$ de E. Ensuite nous allons montrer que

$$E = E_y \oplus F \tag{9.591}$$

avec

$$F = \{x \in E \text{ tel que } e_d^*\big(f^k(x)\big) = 0, \forall k \in \mathbb{N}\}. \tag{9.592}$$

qui fait appel aux définitions d'espace dual (définition 4.123) et de base duale (définition 4.124).

Par construction, F est invariant sous f. Montrons pour commencer que $E_y \cap F = \{0\}$. Un élément de E_y s'écrit

$$z = a_1 e_1 + \cdots + a_k e_k \tag{9.593}$$

avec $k \leqslant d$. Étant donné que f décale les vecteurs de base, nous avons $e_d^*\big(f^{d-k}(z)\big) = a_k$. Du coup $z \in F$ si et seulement si $a_1 = \ldots = a_d = 0$, c'est-à-dire que $E_y \cap F = \{0\}$.

Nous montrons maintenant que $\dim F = n - d$. Pour cela nous considérons l'application

$$\begin{aligned} T\colon \mathbb{K}[f] &\to E^* \\ g &\mapsto e_d^* \circ g. \end{aligned} \tag{9.594}$$

113. Définition 9.99.

114. Pour autant que j'aie compris, cette extension manque dans [287]. Corrigez-moi si je me trompe.

Cette application est injective. En effet un élément général de $\mathbb{K}[f]$ est

$$g = a_1 \operatorname{Id} + a_2 f + \cdots + a_p f^{p-1} \tag{9.595}$$

avec $p \leqslant d$. Si $T(g) = 0$, alors nous avons en particulier

$$0 = T(g)e_{d-p+1} = e_d^*(a_1 e_{d-p+1} + a_2 e_{d-p+2} + \cdots + a_p e_d) = a_p. \tag{9.596}$$

Donc $a_p = 0$ et en appliquant maintenant $T(g)$ à e_{d-p} nous obtenons $a_{p-1} = 0$. Au final nous trouvons que $g = 0$ et donc que T est injective.

Étant donné que $\dim \mathbb{K}[f] = d$ et que T est injective, $\dim \operatorname{Image}(T) = d$. Étudions l'orthogonal [115] de l'image de T :

$$(\operatorname{Image}(T))^\perp = \{x \in E \text{ tel que } T(g)x = 0, \forall g \in \mathbb{K}[f]\} \tag{9.597a}$$
$$= \{x \in E \text{ tel que } e_d^*\big(g(x)\big) = 0, \forall g \in \mathbb{K}[f]\} \tag{9.597b}$$
$$= F. \tag{9.597c}$$

Par conséquent $F^\perp = \operatorname{Image}(T)$. Puisque $\dim \operatorname{Image}(T) = d$, nous avons donc $\dim F = n - d$ et il est établi que $E = E_y \oplus F$.

Nous avons donc trouvé F, stable par f et tel que $E = E_y \oplus F$. Nous devons maintenant nous assurer que cette décomposition tombe bien pour les polynômes minimaux. Si P_1 est le polynôme minimal de $f|_{E_y}$, alors par le lemme 9.100 nous avons $P_1 = \mu_{f,y} = \mu_f$ parce que $f|_{E_y}$ est cyclique sur E_y. Mettons P_2, le polynôme minimal de $f|_F$. Étant attendu que F est stable par f, le polynôme P_2 divise P_1. En recommençant la construction sur F, nous construisons un nouvel espace F' stable sous F et vérifiant $\mu_{f|_{F'}} = P_2$, etc.

Nous passons maintenant à la partie unicité du théorème. Soient deux suites $F_1, \ldots, F_r$ et $G_1, \ldots, G_s$ de sous-espaces stables par f et vérifiant

(1) $E = \bigoplus_{i=1}^r F_i$,
(2) $f|_{F_i}$ est cyclique,
(3) $\mu_{f|_{F_{i+1}}}$ divise $\mu_{f|_{F_i}}$,

et, *mutatis mutandis*, les mêmes conditions pour la famille $\{G_i\}$. Nous posons $P_i = \mu_{f|_{F_i}}$ et $Q_i = \mu_{f|_{G_i}}$. Nous allons montrer par récurrence que $P_i = Q_i$ et $\dim F_i = \dim G_i$. Il ne sera cependant pas garanti que $F_i = G_i$. D'abord, $P_1 = Q_1$ parce qu'ils sont tous deux égaux à μ_f par les relations (9.588). Nous supposons que $P_i = Q_i$ pour $1 \leqslant i \leqslant j-1$ et nous tentons de montrer que $P_j = Q_j$.

Nous avons

$$P_j(f) = P_j(f)|_{F_1} \oplus \ldots \oplus P_j(f)|_{F_{j-1}}. \tag{9.598}$$

En effet étant donné que P_{j+k} divise P_j, il existe un polynôme A tel que $P_j = AP_{j+k}$, et donc tel que [116] $P_j(f) = A(f) \circ P_{j+k}(f)$, mais $P_{j+k}(f)F_{j+k} = 0$, donc $P_j(f)F_{j+k} = 0$. Les espaces G_i n'ayant à priori aucun rapport avec les polynômes P_i, nous écrivons

$$P_j(f) = P_j(f)|_{G_1} \oplus \ldots \oplus P_j(f)|_{G_{j-1}} \oplus P_j(f)|_{G_j} \oplus \ldots \oplus P_j(f)|_{G_s}. \tag{9.599}$$

Pour $1 \leqslant i \leqslant j-1$, nous avons supposé $P_i = Q_i$. Étant donné que la matrice de $f|_{F_i}$ est semblable à C_{P_i} et celle de $f|_{G_i}$ est semblable à C_{Q_i}, la matrice de $f|_{F_i}$ est semblable à la matrice de $f|_{G_i}$. En particulier,

$$\dim P_j(f)F_i = \dim P_j(f)G_i. \tag{9.600}$$

En prenant les dimensions des images dans les égalités (9.598) et (9.599), nous trouvons que

$$P_j(f)|_{G_j} = \ldots = P_j(f)|_{G_s} = 0. \tag{9.601}$$

Par conséquent P_j est annulateur de $f|G_j$, et il divise donc Q_j, qui est générateur de l'idéal des polynômes annulateurs de $f|_{G_j}$. La situation étant symétrique entre P et Q, nous montrons de même que Q_j divise P_j et donc que $P_j = Q_j$.

Ceci achève la démonstration du théorème de réduction de Frobenius.

□

115. Définition 4.129.
116. En vertu du lemme 9.85.

Remarque 9.285.
Sous forme matricielle, ce théorème dit que toute matrice est semblable à une matrice de la forme bloc-diagonale

$$f = \begin{pmatrix} C_{\mu_1} & & \\ & \ddots & \\ & & C_{\mu_r} \end{pmatrix} \tag{9.602}$$

où les C_{μ_i} sont des matrices compagnons (définition 9.279).

En particulier, et ceci est très important, deux applications sont semblables si et seulement si elles ont même suite d'invariants de similitude.

Remarque 9.286.
Si nous travaillons sur $\mathbb{R}$, la réduite de Frobenius restera une matrice réelle, même si les valeurs propres sont complexes. En effet le procédé de Frobenius ne regarde absolument pas les valeurs propres, mais seulement les facteurs irréductibles du polynôme caractéristique. La réduite de Frobenius ne tente pas de résoudre ces polynômes, mais se contente d'en utiliser les matrices compagnon.

La situation sera différente dans le cas de la forme normale de Jordan.

9.15.3 Forme normale de Jordan

Il existe une preuve directe de la réduction de Jordan ne nécessitant pas la réduction de Frobenius[290]. Cette dernière passe par les espaces caractéristiques [117] et est à mon avis plus compliquée que la démonstration de Frobenius elle-même. Nous allons donc nous contenter de donner la réduction de Jordan comme un cas particulier de réduction de Frobenius.

Théorème 9.287 (Réduction de Jordan)**.**
Soit E un espace vectoriel sur $\mathbb{K}$, et $f \in \mathrm{End}(E)$ un endomorphisme dont le polynôme caractéristique χ_f est scindé[118]*. Il existe une base de E dans laquelle la matrice de f s'écrit sous la forme*

$$M = \begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \\ 0 & \ddots & \\ & & J_{n_k}(\lambda_k) \end{pmatrix} \tag{9.603}$$

où les λ_i sont les valeurs propres de f (avec éventuelles répétitions) et $J_{n_i}(\lambda)$ représente le bloc $n_i \times n_i$

$$J_{n_i}(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & & \\ & \lambda & 1 & 0 & \\ 0 & & \lambda & & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}. \tag{9.604}$$

En d'autres termes, $J_{n_i}(\lambda)_{ii} = \lambda$ et $J_n(\lambda)_{i-1,i} = 1$.

Démonstration. Nous commençons par le cas où f est nilpotente ; nous notons M sa matrice. Dans ce cas la seule valeur propre est zéro et le polynôme caractéristique est X^m pour un certain m. Nous savons par le lemme 9.281 que (la matrice de) f est semblable à sa matrice compagnon. En l'occurrence pour f nous avons

$$C_{X^m} = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix}. \tag{9.605}$$

117. Aussi appelés « espaces propres généralisés ».
118. C'est à cause de cette hypothèse que $\mathbb{K} = \mathbb{R}$ n'est pas le bon exemple de contexte de travail.

Ensuite le changement de base (qui est une similitude) $(e_1, e_2, \dots, e_n) \mapsto (e_n, \dots, e_2, e_1)$ montre que C_{X^m} est semblable à un bloc de Jordan $J_m(0)$.

Supposons à présent que f ne soit pas nilpotente. Par l'hypothèse de polynôme caractéristique scindé, nous supposons que f a m valeurs propres distinctes et que son polynôme caractéristique est

$$\chi_f = (X - \lambda_1)^{l_1} \dots (X - \lambda_m)^{l_m}. \tag{9.606}$$

Le lemme des noyaux (théorème 9.86) nous enseigne que

$$E = \bigoplus_{i=1}^{m} \underbrace{\ker(f - \lambda_i \mathbb{1})^{l_i}}_{F_i}. \tag{9.607}$$

La restriction de $f - \lambda_i \mathbb{1}$ à F_i est par construction un endomorphisme nilpotent, et donc peut s'écrire comme un bloc de Jordan avec des zéros sur la diagonale. En utilisant la décomposition

$$f|_{F_i} = (f - \lambda_i \mathbb{1})|_{F_i} + \lambda_i \mathbb{1}_{F_i}, \tag{9.608}$$

nous voyons que $f|_{F_i}$ s'écrit comme un bloc de Jordan avec λ_i sur la diagonale. □

Remarque 9.288.
Nous pouvons calculer la forme normale de Jordan pour une matrice complexe ou réelle, mais dans les deux cas nous devons nous attendre à obtenir une matrice complexe parce que les valeurs propres d'une matrice réelle peuvent être complexes. Cependant nous demandons que le polynôme caractéristique de f soit scindé sur $\mathbb{K}$. En pratique, la décomposition de Jordan n'est garantie que sur les corps algébriquement clos, c'est-à-dire sur $\mathbb{C}$.

La suite des invariants de similitude sur laquelle repose la réduction de Frobenius, elle, est disponible sur tout corps, y compris $\mathbb{R}$.

9.16 Commutant et endomorphismes cycliques

9.16.1 Endomorphisme cyclique

Lemme 9.289.
Si A est la matrice de l'endomorphisme f alors nous avons équivalence des propriétés suivantes :

(1) La matrice A est cyclique.

(2) L'endomorphisme f est cyclique.

Si f est un endomorphisme de l'espace vectoriel E et si $x \in E$, nous notons

$$E_{f,x} = \text{Span}\{f^k(x) \text{ tel que } k \in \mathbb{N}\}. \tag{9.609}$$

Définition 9.290 (Commutant $\mathcal{C}(f)$ de f)**.**
*Soit E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et un endomorphisme $f : E \to E$. Le **commutant** de f est l'ensemble des endomorphismes de E qui commutent avec f :*

$$\mathcal{C}(f) = \{g \in \mathcal{L}(E, E) \text{ tel que } g \circ f = f \circ g\}. \tag{9.610}$$

Il n'est pas très compliqué de vérifier que $\mathcal{C}(f)$ est un sous-espace vectoriel de $\mathcal{L}(E, E)$.

Notons l'inclusion évidente $\mathbb{K}[f] \subset \mathcal{C}(f)$. L'inclusion inverse va un peu nous occuper durant les prochaines pages.

9.16.2 Commutant : cas diagonalisable

Proposition 9.291 ([291]).
Si f est diagonalisable, alors

$$\dim\big(\mathcal{C}(f)\big) = \sum_{\lambda\in\mathrm{Spec}(f)} \dim(E_\lambda)^2. \tag{9.611}$$

où les E_λ sont les espaces propres de f.

Démonstration. D'abord, soit $g \in \mathcal{C}(f)$ alors E_λ est stable par g. En effet si $v \in E_\lambda$ alors $f\big(g(v)\big) = g\big(f(v)\big) = g(\lambda v) = \lambda g(v)$, ce qui montre que $g(v)$ est un vecteur propre de f pour la valeur propre λ, et donc que $g(v) \in E_\lambda$.

Nous considérons ensuite l'application

$$\begin{aligned}\psi\colon \mathcal{C}(f) &\to \mathrm{End}(E_1)\times\ldots\times\mathrm{End}(E_r)\\ g &\mapsto g|_{E_1}\times\ldots\times g|_{E_r}\end{aligned} \tag{9.612}$$

qui est bien définie parce que g se restreint aux espaces propres de f. Nous allons noter $\psi(g)_\lambda$ la restriction de g à E_λ.

(i) ψ **est injective** Supposons que $g, h \in \mathcal{C}(f)$ tels que $\psi(g) = \psi(h)$. Puisque f est diagonalisable nous pouvons décomposer $x \in E$ en ses composantes sur les espaces propres [119] :

$$x = \sum_{\lambda\in\mathrm{Spec}(f)} x_\lambda \tag{9.613}$$

avec $x_\lambda \in E_\lambda$. Nous avons alors

$$g(x) = \sum_\lambda g(x_\lambda) = \sum_\lambda \psi(g)_\lambda(x_\lambda). \tag{9.614}$$

Par hypothèse nous avons $\psi(g)_\lambda = \psi(h)_\lambda$, et donc aussi

$$g(x) = \sum_\lambda \psi(g)_\lambda(x_\lambda) = \sum_\lambda \psi(h)_\lambda(x_\lambda) = \sum_\lambda h(x_\lambda) = h(x). \tag{9.615}$$

Cela prouve $g = h$ et donc que ψ est injective.

(ii) ψ **est surjective** Si nous avons pour chaque $\lambda \in \mathrm{Spec}(f)$ un endomorphisme g_λ de E_λ alors en posant

$$g(x) = \sum_{\lambda\in\mathrm{Spec}(f)} g_\lambda(x_\lambda) \tag{9.616}$$

nous avons bien

$$\psi(g) = \big(g_{\lambda_1},\ldots,g_{\lambda_r}\big). \tag{9.617}$$

Nous pouvons donc conclure en écrivant

$$\dim\big(\mathcal{C}(f)\big) = \sum_{\lambda\in\mathrm{Spec}(f)} \dim\big(\mathrm{End}(E_\lambda)\big) = \sum_{\lambda\in\mathrm{Spec}(f)} \dim(E_\lambda)^2. \tag{9.618}$$

□

Remarque 9.292.
Nous avons alors immédiatement

$$\dim\big(\mathcal{C}(f)\big) \geqslant \dim(E) \tag{9.619}$$

lorsque f est diagonalisable.

119. Théorème 9.211(5).

En suivant la notation (9.194), un endomorphisme est cyclique lorsqu'il existe $x \in E$ tel que $E_x = E$.

Proposition 9.293 ([291]).
Si f est un endomorphisme diagonalisable d'un espace vectoriel E de dimension n. Nous avons équivalence des points suivants.

(1) *Le polynôme minimal est égal au polynôme caractéristique : $\mu_f = \chi_f$*
(2) *L'endomorphisme f est cyclique.*
(3) $\mathcal{C}(f) = \mathbb{K}[f]$ [120].
(4) $\dim\big(\mathcal{C}(f)\big) = n$
(5) *L'endomorphisme f possède n valeurs propres distinctes.*
(6) $\dim\big(\mathbb{K}[f]\big) = n$

Démonstration. Le point important de cette proposition réside dans les équivalences (1)-(3). Les autres sont des résultats intermédiaires. En particulier, dans le cas diagonalisable, nous allons voir que le point (5) est essentiellement une reformulation de (1).

(i) **(4) implique (5)** Par la formule (9.611), les espaces propres de f ont tous une dimension de 1. Par conséquent f possède n valeurs propres distinctes.

(ii) **(5) implique (6)** Le théorème 9.211 nous dit que le polynôme minimal est scindé à racines simples. Puisque f possède n valeurs propres distinctes, μ est de degré n. Par l'isomorphisme $\mathbb{K}[f] = \mathbb{K}[X]/(\mu)$ de la proposition 9.106 nous avons $\dim\big(\mathbb{K}[f]\big) = \deg(\mu) = n$ par la proposition 6.44.

(iii) **(6) implique (1)** Par l'isomorphisme $\mathbb{K}[f] = \mathbb{K}[X]/(\mu)$ de la proposition 9.106 et la proposition 6.44 nous avons $n = \dim\big(\mathbb{K}[f]\big) = \deg(\mu)$. Comme χ est un polynôme annulateur (Caley-Hamilton 9.115), il est divisé par μ. Maintenant μ et χ sont des polynômes unitaires de degré n et μ divise χ. Ils sont donc égaux.

(iv) **(1) implique (2)** Le fait que f soit diagonalisable permet d'utiliser le théorème 9.211 pour dire que μ est scindé à racines simples. L'égalisation avec χ nous permet de dire que f possède n valeurs propres distinctes. Soient $\{e_1, \dots, e_n\}$ une base de diagonalisation, et prouvons que le vecteur $v = e_1 + \cdots + e_n$ est cyclique. Nous avons

$$f^k(v) = \sum_{i=1}^{n} \lambda_i^k e_i. \tag{9.620}$$

Pour prouver que cette famille (avec $k = 0, \dots, n-1$) est libre [121] nous en prenons une combinaison linéaire nulle et nous prouvons que les coefficients sont tous nuls. Soit donc

$$0 = \sum_{l=0}^{n-1} a_l f^l(v) = \sum_{l=0}^{n-1} a_l \sum_{i=1}^{n} \lambda_i^l e_i = \sum_{i=1}^{n} \Big(\sum_{l=0}^{n-1} a_l \lambda_i^l \Big) e_i. \tag{9.621}$$

Par hypothèse, la double somme est nulle, et nous avons pour tout i :

$$\sum_{l=0}^{n-1} a_l \lambda_i^l = 0. \tag{9.622}$$

En posant la matrice $A_{ij} = \lambda_i^j$, cela revient à étudier le système $\sum_j A_{ij} a_j = 0$. Ce système n'a des solutions non nulles que si $\det(A) = 0$; sinon il possède une unique solution qui est $a_j = 0$ pour tout j. Nous devons donc calculer le déterminant

$$\det \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \cdots & \lambda_n^{n-1} \end{pmatrix}. \tag{9.623}$$

120. Rappel : $\mathcal{C}(f)$ est le commutant de f, définition 9.290.
121. Ce sera alors une base parce que n vecteurs libres dans un espace de dimension n est toujours une base, proposition 4.18.

Il s'agit du déterminant de Vandermonde déjà étudié par la proposition 9.12. Nous avons $\det(A) = \prod_{1\leqslant i<j\leqslant n}(\lambda_j - \lambda_i)$. Ce déterminant est bien non nul parce que toutes les valeurs propres sont distinctes.

(v) **(2) implique (3)** Soit v un vecteur cyclique[122] de f. Si g est un endomorphisme, nous définissons des coefficients $(a_k(g))_{k=0,\dots,n-1}$ par

$$g(v) = \sum_{k=0}^{n-1} a_k(g) f^k(v). \tag{9.624}$$

C'est une bonne définition parce que $\{f^k(v)\}$ est une base.

Nous définissons alors l'application

$$\begin{aligned}\psi\colon \mathcal{C}(f) &\to \mathbb{K}[f]\\ g &\mapsto \sum_{k=0}^{n-1} a_k(g) f^k.\end{aligned} \tag{9.625}$$

C'est une application injective parce que si $\psi(g) = 0$ alors $g(v) = 0$ et pour tout k nous avons $g\big(f^k(v)\big) = f^k\big(g(v)\big) = 0$. L'endomorphisme g s'annulant sur une base, il est nul.

L'application ψ est surjective. En effet si un polynôme $P = \sum_{k=0}^{n-1} a_k f^k$ est donné, il suffit de poser

$$g(x) = \sum_k a_k f^k(x) \tag{9.626}$$

pour avoir $\psi(g) = P$.

(vi) **(3) implique (4)** Si $n_1, \dots, n_r$ sont les dimensions des différents espaces propres de f, nous avons les inégalités

$$\dim\big(\mathbb{K}[f]\big) = \deg(\mu) \leqslant n = n_1 + \cdots + n_r \leqslant n_1^2 + \cdots + n_r^2 = \dim\big(\mathcal{C}(f)\big). \tag{9.627}$$

Par hypothèse d'égalité entre le premier et le dernier terme de cette suite d'inégalités, toutes les inégalités sont des égalités et en particulier $\dim\big(\mathcal{C}(f)\big) = n$.

Nous avons fini de prouver toutes les équivalences demandées. □

Exemple 9.294.
Pour mieux comprendre pourquoi le fait d'avoir n valeurs propres distinctes est équivalent à être cyclique, notons que si deux valeurs propres sont identiques, alors un morceau de la matrice de f serait par exemple $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, et dans ce cas n'importe quelle combinaison $ae_i + be_j$ reste proportionnelle à elle-même après application de f. Si nous avons des valeurs propres différentes par contre, nous avons par exemple dans $\mathbb{R}^2$ la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ qui donne $f(e_1 + e_2) = e_1 + 2e_2$. La partie $\{e_1 + e_2, e_1 + 2e_2\}$ est une base. △

9.16.3 Commutant : cas général

Nous considérons encore un espace vectoriel E de dimension finie n et un endomorphisme $f\colon E \to E$. Nous notons μ son polynôme minimal et μ_x le polynôme minimal ponctuel en x.

Lemme 9.295 ([292, 287, 127])**.**
Nous avons

$$\dim\big(\mathcal{C}(f)\big) \geqslant \dim(E) \tag{9.628}$$

Démonstration. Si f est donnée, l'espace $\mathcal{C}(f)$ est l'espace des solutions de $fg = gf$. Supposons avoir choisi une base de E et notons A la matrice de f et X celle de g. L'équation est $AX - XA = 0$.

122. Définition 9.290.

(i) **Si A est trigonalisable** Nous supposons avoir choisi la base de telle sorte que A soit triangulaire supérieure, et nous allons nous contenter de chercher les solutions X qui sont également triangulaires supérieure. Si il y en a déjà plus que n, a fortiori le résultat sera vrai.
Le produit de deux matrices triangulaires supérieures étant une matrice triangulaire supérieure, l'équation $AX - XA$ contient, pour les coefficients de X, $n(n+1)/2$ équations. Mais il se fait que les termes diagonaux ne sont pas de vraies équations parce que

$$(AX - XA)_{kk} = \sum_i \big(A_{ki}X_{ik} - X_{ki}A_{ik}\big) = \sum_{k\leqslant i\leqslant k} (A_{ki}X_{ik} - X_{ki}A_{ik}) = 0. \tag{9.629}$$

Nous avons donc au maximum

$$\frac{n(n+1)}{2} - n \tag{9.630}$$

équations linéairement indépendantes pour un minimum de $n(n+1)/2$ inconnues. L'espace des solutions est donc de dimension au minimum n.
Cela a l'air d'être une majoration assez large, mais il existe des cas d'égalité.

(ii) **Si A n'est pas trigonalisable** La preuve que nous donnons ici est valable même pour les endomorphismes trigonalisables.
Nous considérons le résultat de Frobenius 9.284. Nous avons donc la structure suivante :

— une décomposition en somme directe $E = E_1 \oplus \dots \oplus E_r$,
— les espaces E_i sont fixés par f,
— les endomorphismes $f_i = f|_{E_i}$ sont cycliques
— le polynôme minimal de f_i est μ_i et $\prod_{i=1}^r \mu_i = \chi_f$.

Les endomorphismes f_i^k commutent évidemment avec f_j, et la partie $\{f_i^k\}_{k=0,\dots,\deg(\mu_i)-1}$ est libre. Libre en tout cas en tant que partie de $\mathrm{End}(E_i)$. Mais en prolongeant par 0 sur E, ça reste libre en tant que partie de $\mathrm{End}(E)$.
Bien entendu les f_j^k et les f_i^k $(i \neq j)$ sont linéairement indépendants dans $\mathrm{End}(E)$ parce qu'ils n'agissent pas sur les mêmes vecteurs. Donc les endomorphismes $f_i^{k_i}$ avec $k_i = 0, \dots, \deg(\mu_i) - 1$ forment une partie libre de $\mathrm{End}(E)$ composée d'endomorphismes qui commutent avec f. Il y en a en tout

$$\sum_{i=1}^r \deg(\mu_i) = \deg(\chi_f) = n. \tag{9.631}$$

Par conséquent $\dim\big(\mathcal{C}(f)\big) \geqslant \dim(E)$.

□

Théorème 9.296 ([262])**.**
Soit un endomorphisme $f\colon E \to E$ sur l'espace vectoriel de dimension finie n. Nous notons μ et χ les polynômes minimal et caractéristique. Nous avons équivalence entre les points suivants :

(1) $\mu = \chi$,
(2) f *est cyclique,*
(3) $\mathcal{C}(f) = \mathbb{K}[f]$.

Démonstration. Plusieurs implications. Notons que (2) implique (1) a déjà été démontré par le lemme 9.283.

(i) **(1) implique (2)** Conformément à ce que nous permet le lemme 9.98 nous choisissons[123] $a \in E$ de telle sorte à avoir $\mu_a = \mu$. De plus pour $x \in E$ nous considérons l'application

$$\begin{aligned} \varphi_x\colon \mathbb{K}[X] &\to E \\ P &\mapsto P(f)x. \end{aligned} \tag{9.632}$$

123. Dans toute la suite, nous devrions écrire μ_f et $\mu_{f,a}$ mais nous omettons d'indiquer explicitement la dépendance en f.

Nous avons $\varphi_a(P) = P(f)a$. Étant donné que E_a est engendré par les $f^k(a)$ nous avons $\varphi_a\big(\mathbb{K}[X]\big) = E_a$. De plus l'application φ_a passe aux classes pour (μ_a). Pour rappel, un élément de $\mathbb{K}[X]/(\mu_a)$ est de la forme

$$[P] = \{P + Q\mu_a\}_{Q\in\mathbb{K}[X]}. \tag{9.633}$$

Nous considérons donc l'application quotient

$$\begin{aligned}\psi\colon \frac{\mathbb{K}[X]}{(\mu_a)} &\to E_a\\ [P] &\mapsto \varphi_a(P),\end{aligned} \tag{9.634}$$

et nous prouvons que c'est un isomorphisme d'espace vectoriel.

(i) **Linéaire** Parce que $(\lambda P + Q)(f) = (\lambda P)(f) + Q(f)$.

(ii) **Injectif** Si $\psi([P]) = 0$, alors $\varphi_a(P) = 0$, c'est-à-dire que $P \in \ker(\varphi_a)$. Mais, par définition 9.94 du polynôme minimal ponctuel, μ_a est générateur de $\ker(\varphi_a)$; donc il existe $Q \in \mathbb{K}[X]$ tel que $P = Q\mu_a$. Par conséquent $[P] = 0$, ce que nous voulions.

(iii) **Surjectif** Si $x \in E_a$ alors il existe des coefficients $x_k \in \mathbb{K}$ tels que $x = \sum_{k=0}^{\deg(\mu_a)-1} x_k f^k(a)$, c'est-à-dire $x = P(f)a = \varphi_a(P) = \psi([P])$.

Mais par hypothèse et par choix de a nous avons $\mu_a = \mu = \chi$, donc en fait $E_a = \mathbb{K}[X]/(\chi)$. Nous savons aussi que $\deg(\chi) = \dim(E)$ et que $\dim\big(\mathbb{K}[X]/P\big) = \deg(P)$ par la proposition 9.106. Au final nous avons $\dim(E_a) = \deg(\chi) = \dim(E)$. Et par conséquent $E_a = E$. Cela prouve que a est un vecteur cyclique pour f.

(ii) **(2) implique (3)** Soit $g \in \mathcal{C}(f)$; nous devons prouver que g est un polynôme de f. Par hypothèse nous avons un vecteur cyclique que nous notons v. Nous avons un polynôme P (dépendant de g) tel que $g(v) = P(f)v$. Nous allons voir que $g = P(f)$. Soient $y \in E$ et Q un polynôme tels que $y = Q(f)v$; en notant que g commute avec $P(f)$ nous avons

$$g(y) = g\big(Q(f)v\big) = Q(f)\big(g(v)\big) = Q(f)\big(P(f)v\big) = P(f)Q(f)v = P(f)y. \tag{9.635}$$

Donc $g = P(f)$.

(iii) **(3) implique (1)** Nous avons les inégalités :

$$n \leqslant \dim\big(\mathcal{C}(f)\big) = \dim\big(\mathbb{K}[f]\big) = \deg(\mu) \leqslant \deg(\chi) = n. \tag{9.636}$$

La première inégalité est le lemme 9.295. Ensuite, toutes les inégalités se trouvent être des égalités. En particulier $\deg(\mu) = n$, ce qui signifie que $\mu = \chi$ parce que μ est un polynôme diviseur de χ, de même degré que χ et unitaire tout comme χ.

□

Corolaire 9.297 ([127]).
En suivant les notations sur les extensions de corps de base de la section 9.14, l'endomorphisme $f\colon E \to F$ est cyclique si et seulement si l'endomorphisme $f_{\mathbb{L}}\colon E_{\mathbb{L}} \to F_{\mathbb{L}}$ est cyclique.

Démonstration. Nous savons par le théorème 9.296 qu'un endomorphisme est cyclique si et seulement si son polynôme minimal est égal à son polynôme caractéristique. Or par les propositions 9.277 et 9.278, nous savons que ces polynômes sont identiques pour f et pour $f_{\mathbb{L}}$. □

Théorème 9.298 (Similitude et extension de corps[127]).
Les applications linéaires $f, g\colon E \to E$ sont semblables si et seulement si $f_{\mathbb{L}}$ et $g_{\mathbb{L}}$ le sont.

Démonstration. En ce qui concerne le sens direct, si il existe $m \in \mathrm{GL}(E)$ tel que $f = mgm^{-1}$ alors il suffit d'appliquer le lemme 9.273 pour avoir $f_{\mathbb{L}} = m_{\mathbb{L}} g_{\mathbb{L}} m_{\mathbb{L}}^{-1}$.

Nous considérons les invariants de similitude de f du théorème 9.284. Il existe une unique suite de polynômes unitaires μ_i $(i = 1, \dots, s)$ tels que $\mu_{i+1} \mid \mu_i$ et pour laquelle nous avons une

décomposition $E = E_1 \oplus \ldots \oplus E_s$ pour laquelle $f|_{E_i} : E \to E_i$ est cyclique et de polynôme minimal μ_i.

Nous avons aussi $E_{\mathbb{L}} = (E_1)_{\mathbb{L}} \oplus \ldots \oplus (E_s)_{\mathbb{L}}$ et les $(E_i)_{\mathbb{L}}$ sont stables sous $f_{\mathbb{L}}$ qui y sera également cyclique (corolaire 9.297). De plus le polynôme minimal de $f_{\mathbb{L}}|_{(E_i)_{\mathbb{L}}}$ est également μ_i.

Autrement dit, la suite μ_i est également la suite des invariants de similitude de $f_{\mathbb{L}}$. La remarque 9.285 nous permet de conclure que f et g sont semblables si et seulement si $f_{\mathbb{L}}$ et $g_{\mathbb{L}}$ le sont. □

9.17 Hyperplans et formes linéaires

Définition 9.299.
*Si E est un espace vectoriel de dimension n, un **hyperplan** de E est un sous-espace vectoriel de dimension $n-1$.*

Proposition 9.300 ([293]).
À propos d'hyperplans et de formes linéaires sur un espace vectoriel E sur le corps $\mathbb{K}$.

(1) Si φ est une forme linéaire non nulle, alors $\ker(\varphi)$ est un hyperplan.

(2) Si H est un hyperplan de E, il existe une forme linéaire dont H est le noyau :

$$H = \ker(\varphi). \tag{9.637}$$

Démonstration. En deux parties.

(1) Soit un supplémentaire A de H. Nous considérons la restriction $\varphi_A : A \to \mathbb{K}$. Vu que les éléments non nuls de A sont hors de H, nous avons $\varphi(x) \neq 0$ dès que x est non nul dans A. Cela implique que φ_A est surjective.

D'autre part, φ_A est également injective : si $\varphi_A(x) = \varphi_A(y)$, alors $\varphi_A(x-y) = 0$, ce qui signifie que $x - y = 0$ ou encore que $x = y$.

Donc φ_A est un isomorphisme de $\mathbb{K}$-espaces vectoriels ; nous en déduisons par le corolaire 4.44 que A est de dimension 1 sur $\mathbb{K}$, parce que $\mathbb{K}$ est de dimension 1.

(2) Nous utilisons le théorème de la base incomplète 4.13(4) pour considérer une base $\{e_i\}_{i=1,\ldots,n}$ de E telle que $\text{Span}\{e_1, \ldots, e_{n-1}\} = H$. Nous pouvons alors considérer la forme linéaire définie par

$$\varphi(e_i) = \begin{cases} 0 & \text{si } i = 1, \ldots, n-1 \\ 1 & \text{si } i = n. \end{cases} \tag{9.638}$$

Cette forme vérifie $\ker(\varphi) = H$.

□

Proposition 9.301 ([126]).
Soit un espace vectoriel E de dimension finie $n \geqslant 2$. Soit un sous-espace vectoriel V de E de dimension s. Alors V est une intersection de $n-s$ hyperplans de E.

Démonstration. Nous considérons une base de V que nous complétons[124] en une base de E : si $x = \sum_{i=1}^{n} x_i e_i$, nous avons $x \in V$ si et seulement si $x_{s+1} = \ldots = x_n = 0$. Nous considérons les formes linéaires

$$\begin{aligned} \varphi_i : E &\to \mathbb{R} \\ x &\mapsto x_i, \end{aligned} \tag{9.639}$$

et nous considérons les parties $H_i = \ker(\varphi_i)$ qui sont de hyperplans par la proposition 9.300. Les H_i avec $s+1 \leqslant i \leqslant n$ sont une famille de $n-s$ hyperplans qui vérifient

$$V = \bigcap_{i=s+1}^{n} \ker(\varphi_i) \tag{9.640}$$

124. Théorème de la base incomplète, 4.13(4).

parce que $x \in \ker(\varphi_i)$ si et seulement si $x_i = 0$.

Donc V peut être écrit comme intersection de $n - s$ hyperplans de E. □

Proposition 9.302 ([126]).
Soit un $\mathbb{K}$-espace vectoriel E de dimension finie $n \geqslant 2$. Si H_i sont des hyperplans de E, alors

$$\dim\left(\bigcap_{i=1}^{m} H_i\right) \geqslant n - m. \tag{9.641}$$

Démonstration. N'oubliez pas de prouver que $\bigcap_{i=1}^{m} H_i$ est un espace vectoriel. À part ça, nous faisons une petite récurrence.

(i) **Pour $m = 2$** Nous savons déjà par la proposition 4.47 que

$$\dim(H_1 + H_2) = \dim(H_1) + \dim(H_2) - \dim(H_1 \cap H_2). \tag{9.642}$$

De plus $\dim(H_1 + H_2) \leqslant n$. En remplaçant, par les valeurs,

$$\begin{aligned}
\dim(H_1 \cap H_2) &= \dim(H_1) + \dim(H_2) - \dim(H_1 + H_2) && \text{(9.643a)}\\
&= n - 1 + n - 1 - \dim(H_1 + H_2) && \text{(9.643b)}\\
&\geqslant 2n - 2 - n && \text{(9.643c)}\\
&= n - 2. && \text{(9.643d)}
\end{aligned}$$

Donc $\dim(H_1 \cap H_2) \geqslant n - 2$.

(ii) **La récurrence** Nous calculons $\dim(H_1 \cap \ldots \cap H_m \cap H_{m+1})$ en commençant encore par la proposition 4.47 :

$$\begin{aligned}
\dim(H_1 \cap \ldots \cap H_m \cap H_{m+1}) &= \underbrace{\dim(H_1 \cap \ldots \cap H_m)}_{\leqslant n-m} + \dim(H_{m+1}) && \text{(9.644a)}\\
&\quad - \underbrace{\dim\big((H_1 \cap \ldots H_m) + H_{m+1}\big)}_{\leqslant n} && \text{(9.644b)}\\
&\geqslant n - m + (n-1) - n && \text{(9.644c)}\\
&= n - m - 1. && \text{(9.644d)}
\end{aligned}$$

C'est bon pour la récurrence.

□

9.17.1 Trouver la matrice d'une symétrie donnée

Les notions de déterminants, produit scalaire et vectoriels[125] donnent une bonne intuition géométrique des matrices. Nous pouvons alors chercher les matrices de quelques symétries dans $\mathbb{R}^2$ ou $\mathbb{R}^3$.

9.17.1.1 Symétrie par rapport à un plan

Comment trouver par exemple la matrice A qui donne la symétrie autour du plan $z = 0$? La définition d'une telle symétrie est que les vecteurs du plan $z = 0$ ne bougent pas, tandis que les vecteurs perpendiculaires changent de signe. Ces informations vont permettre de trouver comment A agit sur une base de $\mathbb{R}^3$. En effet :

(1) Le vecteur $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ est dans le plan $z = 0$, donc il ne bouge pas,

125. Définitions 9.9, 9.162 et 11.25.

(2) le vecteur $\begin{pmatrix}0\\1\\0\end{pmatrix}$ est également dans le plan, donc il ne bouge pas non plus,

(3) et le vecteur $\begin{pmatrix}0\\0\\1\end{pmatrix}$ est perpendiculaire au plan $z=0$, donc il va changer de signe.

Cela nous donne directement les valeurs de A sur la base canonique et nous permet d'écrire

$$A=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}. \tag{9.645}$$

Pour écrire cela, nous avons juste mis en colonne les images des vecteurs de base. Les deux premiers n'ont pas changé et le troisième a changé.

Et si maintenant on donne un plan moins facile que $z=0$? Le principe reste le même : il faudra trouver deux vecteurs qui sont dans le plan (et dire qu'ils ne bougent pas), et puis un vecteur qui est perpendiculaire au plan [126], et dire qu'il change de signe.

Voyons ce qu'il en est pour le plan $x=-z$. Il faut trouver deux vecteurs linéairement indépendants dans ce plan. Prenons par exemple

$$f_1=\begin{pmatrix}0\\1\\0\end{pmatrix},\quad f_2=\begin{pmatrix}1\\0\\-1\end{pmatrix}. \tag{9.646}$$

Nous avons

$$\begin{aligned}Af_1&=f_1\\Af_2&=f_2.\end{aligned} \tag{9.647}$$

Afin de trouver un vecteur perpendiculaire au plan, calculons le produit vectoriel :

$$f_3=f_1\times f_2=\begin{vmatrix}e_1&e_2&e_3\\0&1&0\\1&0&-1\end{vmatrix}=-e_1-e_3=\begin{pmatrix}-1\\0\\-1\end{pmatrix}. \tag{9.648}$$

Nous avons

$$Af_3=-f_3. \tag{9.649}$$

Afin de trouver la matrice A, il faut trouver Ae_1, Ae_2 et Ae_3. Pour ce faire, il faut d'abord écrire $\{e_1,e_2,e_3\}$ en fonction de $\{f_1,f_2,f_3\}$. La première des équations (9.646) dit que

$$f_1=e_2. \tag{9.650}$$

Ensuite, nous avons

$$\begin{aligned}f_2&=e_1-e_3\\f_3&=-e_1-e_3.\end{aligned} \tag{9.651}$$

La somme de ces deux équations donne $-2e_3=f_2+f_3$, c'est-à-dire

$$e_3=-\frac{f_2+f_3}{2} \tag{9.652}$$

Et enfin, nous avons

$$e_1=\frac{f_2-f_3}{2}. \tag{9.653}$$

126. Pour le trouver, penser au produit vectoriel.

Maintenant nous pouvons calculer les images de e_1, e_2 et e_3 en faisant

$$\begin{aligned} Ae_1 &= \frac{Af_2 - Af_3}{2} = \frac{1}{2}\begin{pmatrix} 0 \\ 0 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}, \\ Ae_2 &= Af_1 = f_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \\ Ae_3 &= -\frac{f_2 - f_3}{2} = -\frac{1}{2}\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}. \end{aligned} \tag{9.654}$$

La matrice A s'écrit maintenant en mettant les trois images trouvées en colonnes :

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}. \tag{9.655}$$

9.17.1.2 Symétrie par rapport à une droite

Le principe est exactement le même : il faut trouver trois vecteurs f_1, f_2 et f_3 sur lesquels on connaît l'action de la symétrie. Ensuite il faudra exprimer e_1, e_2 et e_3 en termes de f_1, f_2 et f_3.

Le seul problème est de trouver les trois vecteurs f_i. Le premier est tout trouvé : c'est n'importe quel vecteur sur la droite. Pour les deux autres, il faut un peu ruser parce qu'il faut impérativement qu'ils soient perpendiculaire à la droite. Pour trouver f_2, on peut écrire

$$f_2 = \begin{pmatrix} 1 \\ 0 \\ x \end{pmatrix}, \tag{9.656}$$

et puis fixer le x pour que le produit scalaire de f_2 avec f_1 soit nul. Si il n'y a pas moyen (genre si f_1 a sa troisième composante nulle), essayer avec $\begin{pmatrix} x \\ 1 \\ 0 \end{pmatrix}$. Une fois que f_2 est trouvé (il y a des milliards de choix possibles), trouver f_3 est super facile : prendre le produit vectoriel entre f_1 et f_2.

9.17.1.3 En résumé

La marche à suivre est

(1) Trouver trois vecteurs f_1, f_2 et f_3 sur lesquels on connaît l'action de la symétrie. Typiquement : des vecteurs qui sont sur l'axe ou le plan de symétrie, et puis des perpendiculaires. Pour la perpendiculaire, penser au produit scalaire et au produit vectoriel.

(2) Exprimer la base canonique e_1, e_2 et e_3 en termes de f_1, f_2, f_3.

(3) Trouver Ae_1, Ae_2 et Ae_3 en utilisant leur expression en termes des f_i, et le fait que l'on connaisse l'action de A sur les f_i.

(4) La matrice s'obtient en mettant les images des e_i en colonnes.

9.18 Théorème de Burnside

Lemme 9.303.
Soit P, un polynôme sur $\mathbb{K}$. Une racine de P est une racine simple si et seulement si elle n'est pas racine de P'.

Théorème 9.304.
Toute représentation[127] *d'un groupe abélien d'exposant fini sur* $\mathbb{C}^n$ *a une image finie.*

Démonstration. Étant donné que G est d'exposant fini, il existe $\alpha \in \mathbb{N}^*$ tel que $g^\alpha = e$ pour tout $g \in G$. Le polynôme $P(X) = X^\alpha - 1$ est scindé à racines simples. En effet tout polynôme sur $\mathbb{C}$ est scindé. Le fait qu'il soit à racines simples provient du lemme 9.303 parce que si $a^\alpha = 1$, alors il n'est pas possible d'avoir $\alpha a^{\alpha-1} = 0$.

Par ailleurs $P(g) = 0$. Le fait que nous ayons un polynôme annulateur de g scindé à racines simples implique que g est diagonalisable (théorème 9.211). Le fait que G soit abélien montre qu'il existe une base de $\mathbb{C}^n$ dans laquelle tous les éléments de G sont diagonaux. Nous devons par conséquent montrer qu'il existe un nombre fini de matrices de la forme

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}. \tag{9.657}$$

Nous savons que $\lambda_i^\alpha = 1$ parce que $g^\alpha = \mathbb{1}$, par conséquent chacun des λ_i est une racine de l'unité dont il n'existe qu'un nombre fini. □

Théorème 9.305 (Burnside[111, 294])**.**
Un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$ *est fini si et seulement si il est d'exposant*[128] *fini.*

Démonstration. Soit G un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$. Si G est fini, l'ordre de ses éléments divise $|G|$ (corolaire 2.14 au théorème de Lagrange) et l'exposant est le PPCM qui est donc fini également. Le théorème est déjà démontré dans un sens.

Dans l'autre sens, nous notons $e < \infty$ l'exposant de G, et nous allons prouver que l'ensemble G est fini. Nous commençons par remarquer que tous les éléments de G sont des racines du polynôme $X^e - 1$, et ensuite nous nous lançons dans le travail.

(i) **Générateurs** Le groupe G est une partie de $\mathbb{M}(n, \mathbb{C})$ dont nous considérons l'algèbre engendrée[129] $\mathcal{G}$. Soit $C_1, \dots, C_r$ une famille génératrice de $\mathcal{G}$ constituée d'éléments de G et la fonction

$$\begin{aligned} \tau\colon G &\to \mathbb{C}^r \\ A &\mapsto \big(\mathrm{Tr}(AC_1), \dots, \mathrm{Tr}(AC_r)\big). \end{aligned} \tag{9.658}$$

(ii) **τ est injective** Soient $A, B \in G$ tels que $\tau(A) = \tau(B)$. Si C_i est un générateur de G, nous avons $\mathrm{Tr}(AC_i) = \mathrm{Tr}(BC_i)$ et par la linéarité de la trace, nous avons

$$\mathrm{Tr}(AM) = \mathrm{Tr}(BM) \tag{9.659}$$

pour tout $M \in G$. Notons par ailleurs

$$N = AB^{-1} - \mathbb{1}, \tag{9.660}$$

qui est diagonalisable parce que $AB^{-1} \in G$ et donc est annulé par le polynôme $X^e - 1$ qui est scindé à racines simples. Du coup AB^{-1} est diagonalisable ; posons $PAB^{-1}P^{-1} = D$, alors $P\big(AB^{-1} - \mathbb{1}\big)P^{-1} = D - \mathbb{1}$ qui est encore diagonale. Donc N est diagonalisable.

Par ailleurs nous avons

$$\begin{aligned} \mathrm{Tr}\big((AB^{-1})^p\big) &= \mathrm{Tr}\big(AB^{-1}(AB^{-1})^{p-1}\big) && \text{(9.661a)} \\ &= \mathrm{Tr}\big(BB^{-1}(AB^{-1})^{p-1}\big) \qquad (9.659) && \text{(9.661b)} \\ &= \mathrm{Tr}\big((AB^{-1})^{p-1}\big). && \text{(9.661c)} \end{aligned}$$

127. Définition 4.131.
128. Définition 1.264.
129. Définition 1.342.

En continuant nous obtenons

$$\mathrm{Tr}\left((AB^{-1})^p\right) = \mathrm{Tr}(\mathbb{1}) = n. \tag{9.662}$$

D'autre part,

$$N^k = (AB^{-1} - \mathbb{1})^k = \sum_{p=0}^{k} \binom{p}{k} (-1)^{k-p} (AB^{-1})^p \tag{9.663}$$

En prenant la trace, et en tenant compte du fait que $\mathrm{Tr}\left((AB^{-1})^p\right) = n$,

$$\mathrm{Tr}(N^k) = \sum_{p=0}^{k} \binom{p}{k} (-1)^{k-p} n = n(1-1)^k = 0. \tag{9.664}$$

Donc la trace de N^k est nulle et le lemme 9.203 nous enseigne que N est alors nilpotente. Étant donné qu'elle est aussi diagonalisable, elle est nulle. Nous en concluons que $AB^{-1} = \mathbb{1}$ et donc que $A = B$. La fonction τ est donc injective.

(iii) **Nombre fini de valeurs** Les éléments de G sont annulés par $X^e - 1$ qui est un polynôme scindé à racines simples. Dons le polynôme minimal d'un élément de G est (a fortiori) scindé à racines simples et le théorème 9.211 nous assure alors que ces éléments sont diagonalisables. Du coup les valeurs propres des matrices de G sont des racines $e$ièmes de l'unité. Par conséquent les traces des éléments de G ne peuvent prendre qu'un nombre fini de valeurs : toutes les sommes de n racines $e$ièmes de l'unité. Mais vu que les C_i sont dans G, nous avons

$$\mathrm{Image}(\tau) = \{\mathrm{Tr}(A) \text{ tel que } A \in G\}^r, \tag{9.665}$$

qui est un ensemble fini. Par conséquent G est fini parce que τ est injective.

□

9.19 Ellipsoïde

Lemme 9.306.
Toute matrice peut être décomposée de façon unique en une partie symétrique et une partie antisymétrique. Cette décomposition est donnée par

$$S = \frac{M + M^t}{2}, \quad A = \frac{M - M^t}{2} \tag{9.666}$$

Démonstration. L'existence est une vérification immédiate de $S + A = M$ en utilisant (9.666). Pour l'unicité, si $S + A = S' + A'$ alors $S - S' = A - A'$. Mais $S - S'$ est symétrique et $A - A'$ est antisymétrique ; l'égalité implique l'annulation des deux membres, c'est-à-dire $S = S'$ et $A = A'$. □

Définition 9.307.
Un ***ellipsoïde*** *dans $\mathbb{R}^n$ centré en v est le lieu des points x vérifiant l'équation*

$$\langle x - v, M(x - v)\rangle = 1 \tag{9.667}$$

où M est une matrice symétrique strictement définie positive[130].

Lorsque nous parlons d'ellipsoïde plein, *il suffit de changer l'égalité en une inégalité.*

Remarque 9.308.
Le fait que M soit symétrique n'est pas tout à fait obligatoire ; la chose important est que toutes les valeurs propres soient strictement positives. En effet si M a toutes ses valeurs propres strictement

130. Définition 9.222.

positives, nous nommons S la partie symétrique de M et A la partie antisymétrique (lemme 9.306). Alors pour tout $x \in \mathbb{R}^n$ nous avons

$$x^tAx = \langle x, Ax\rangle = \langle A^tx, x\rangle = -\langle Ax, x\rangle = -\langle x, Ax\rangle, \tag{9.668}$$

donc $x^tAx = 0$. L'équation $x^tMx = 1$ est donc équivalente à $x^tSx = 1$ (elles ont les mêmes solutions).

De plus S reste strictement définie positive parce que pour tout $x \in \mathbb{R}^n$ nous avons

$$0 < x^tMx = x^tSx. \tag{9.669}$$

Proposition 9.309.
Si $\mathcal{E}$ est un ellipsoïde centrée à l'origine, il existe une base de $\mathbb{R}^n$ dans laquelle son équation est :

$$\sum_{i=1}^{n} \frac{x_i^2}{a_i^2} = 1. \tag{9.670}$$

Démonstration. Nous avons une matrice symétrique strictement définie positive S telle que l'équation soit $\langle x, Sx\rangle = 1$. Le théorème spectral 9.219 nous fournit une base orthonormale $\{e_i\}$ dans laquelle $Se_i = \lambda_i e_i$ avec $\lambda_i > 0$. En substituant dans l'équation $\langle x, Sx\rangle = 1$ nous trouvons l'équation

$$\sum_i \lambda_i x_i^2 = 1. \tag{9.671}$$

En posant $a_i = \frac{1}{\sqrt{\lambda_i}}$, nous trouvons le résultat. Cette définition des a_i est toujours possible parce que $\lambda_i > 0$. □

Corolaire 9.310.
Un ellipsoïde plein centré en l'origine admet une équation de la forme $q(x) \leqslant 1$ où q est une forme quadratique strictement définie positive.

Pour rappel de notation, l'ensemble des formes quadratiques strictement définies positives sur l'espace vectoriel E est noté $Q^{++}(E)$.

Démonstration. Soit $\{e_i\}$ une base de $\mathbb{R}^n$ telle que l'ellipsoïde $\mathcal{E}$ ait pour équation

$$\sum_{i=1}^{n} \frac{x_i^2}{a_i^2} \leqslant 1. \tag{9.672}$$

Nous considérons la forme quadratique

$$\begin{aligned} q\colon \mathbb{R}^n &\to \mathbb{R} \\ x &\mapsto \sum_{i=1}^{n} \frac{\langle x, e_i\rangle^2}{a_i^2}. \end{aligned} \tag{9.673}$$

Nous avons évidemment $\mathcal{E} = \{x \in \mathbb{R}^n \text{ tel que } q(x) \leqslant 1\}$. De plus la forme q est strictement définie positive parce que dès que $x \neq 0$, au moins un des produits scalaires $\langle x, e_i\rangle$ est non nul et $q(x) > 0$. □

9.20 Système d'équations linéaires : méthode de Gauss

Pour résoudre un système d'équations linéaires, on procède comme suit :

(1) Écrire le système sous forme matricielle.

$$\text{p.ex. } \begin{cases} 2x + 3y &= 5 \\ x + 2y &= 4 \end{cases} \Leftrightarrow \left(\begin{array}{cc|c} 2 & 3 & 5 \\ 1 & 2 & 4 \end{array}\right)$$

(2) Se ramener à une matrice avec un maximum de 0 dans la partie de gauche en utilisant les transformations admissibles :

(2a) Remplacer une ligne par elle-même + un multiple d'une autre ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 2 & 3 & 5 \\ 1 & 2 & 4 \end{array}\right) \overset{L_1-2.L_2\mapsto L_1'}{\Longrightarrow} \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array}\right)$$

(2b) Remplacer une ligne par un multiple d'elle-même ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array}\right) \overset{-L_1\mapsto L_1'}{\Longrightarrow} \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 2 & 4 \end{array}\right)$$

(2c) Permuter des lignes.

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 0 & -2 \end{array}\right) \overset{L_1\mapsto L_2' \text{ et } L_2\mapsto L_1'}{\Longrightarrow} \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array}\right)$$

(3) Retransformer la matrice obtenue en système d'équations.

$$\text{p.ex. } \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array}\right) \Leftrightarrow \begin{cases} x &= -2 \\ y &= 3 \end{cases}$$

Remarque 9.311. — Si on obtient une ligne de zéros, on peut l'enlever :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \Leftrightarrow \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \end{array}\right)$$

— Si on obtient une ligne de zéros suivie d'un nombre non-nul, le système d'équations n'a pas de solution :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \\ 0 & 0 & 0 & 7 \end{array}\right) \Leftrightarrow \begin{cases} \cdots \\ \cdots \\ 0x + 0y + 0z = 7 \end{cases} \Rightarrow \textbf{Impossible}$$

— Si on a moins d'équations que d'inconnues, alors il y a une infinité de solutions qui dépendent d'un ou plusieurs paramètres :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 1 & 0 & -2 & 2 \\ 0 & 1 & 3 & 0 \end{array}\right) \Leftrightarrow \begin{cases} x - 2z = 2 \\ y + 3z = 0 \end{cases} \Leftrightarrow \begin{cases} x = 2 + 2\lambda \\ y = -3\lambda \\ z = \lambda \end{cases}$$