

Erratum

Dans la section «0.4 Comment m'aider à rendre ces notes plus utiles?», il est dit d'écrire au jury pour demander de les avoir à l'oral. **Il ne faut pas leur écrire** parce que ce texte est vendu précisément pour ne pas avoir à demander l'autorisation. Il est donc inutile de les ennuyer avec ça.

La version commercialisée commence après cette page.

Le Frido, volume 1

Plusieurs versions et extensions de ce document.

La version courante Vous trouverez une version dédiée à l'agrégation régulièrement mise à jour à l'adresse suivante :

<http://laurent.claessens-donadello.eu/pdf/lefrido.pdf>

La version la plus complète Une version plus complète, comprenant le Frido, des exercices ainsi que de la mathématique de niveau recherche :

<http://laurent.claessens-donadello.eu/pdf/mazhe.pdf>

Tout ce qu'il faut savoir pour recompiler soi-même Pour savoir comment recompiler ce document à l'identique, il faut lire

<https://github.com/LaurentClaessens/mazhe>
<http://laurent.claessens-donadello.eu/pdf/readme.pdf>



Copyright 2011-2016 Laurent Claessens, Carlotta Donadello

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the chapter entitled “GNU Free Documentation License”.

Illustration de couverture : Pepper&Carrot <http://www.peppercarrot.com/fr> par David Revoy.

ISBN : 978-2-9540936-5-9

Thèmes

Ceci est une sorte d'index thématique.

Thème 1 : Fonctions Lipschitz

- (1) Définition : 11.189.
- (2) La notion de Lipschitz est utilisée pour définir la stabilité d'un problème, définition 25.23.

Thème 2 : Polynôme de Taylor

- (1) Énoncé : théorème 11.204.
- (2) Le polynôme de Taylor généralise à l'utilisation de toutes les dérivées disponibles le résultat de développement limité donné par la proposition 11.76.
- (3) Il est utilisé pour justifier la méthode de Newton autour de l'équation (25.128).

Thème 3 : Points fixes

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

Théorème de Picard 16.109 donne un point fixe comme limite d'itérés d'une fonction Lipschitz. Il aura pour conséquence le théorème de Cauchy-Lipschitz 16.123, l'équation de Fredholm, théorème 16.114 et le théorème d'inversion locale dans le cas des espaces de Banach 16.128.

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

- (a) Dans $\mathbb{R}^n$ en version C^∞ via le théorème de Stokes, proposition 16.117.
- (b) Dans $\mathbb{R}^n$ en version continue, en s'appuyant sur le cas C^∞ et en faisant un passage à la limite, théorème 16.118.
- (c) Dans $\mathbb{R}^2$ via l'homotopie, théorème 19.19. 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 ¹.

Théorème de Markov-Kakutani 16.121 qui donne un point fixe à une application continue d'un convexe fermé borné dans lui-même. Ce théorème donnera la mesure de Haar 16.122 sur les groupes compacts.

Théorème de Schauder 16.119 qui est une version valable en dimension infinie du théorème de Brouwer.

- (2) Pour les équations différentielles
 - (a) Le théorème de Schauder a pour conséquence le théorème de Cauchy-Arzela 16.125 pour les équations différentielles.
 - (b) Le théorème de Schauder 16.119 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 16.123) 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 25.55.
 - La convergence quadratique de la méthode de Newton est donnée par le théorème 25.61.
 - En calcul numérique, section 25.6
 - Méthode de Newton comme méthode de point fixe, sous-section 25.7.2.
- (4) D'autres utilisation de points fixes.
 - Processus de Galton-Watson, théorème 28.47.
 - Dans le théorème de Max-Milgram 17.44, le théorème de Picard est utilisé.

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

Thème 4 : Méthode de Newton

- (1) Nous parlons un petit peu de méthode de Newton en dimension 1 dans 25.7.
- (2) La méthode de Newton fonctionne bien avec les fonction convexes par la proposition 25.62.
- (3) La méthode de Newton en dimension n est le théorème 25.68.
- (4) Un intervalle de convergence autour de α s'obtient par majoration de $|g'|$, proposition 25.55.
- (5) Un intervalle de convergence quadratique s'obtient par majoration de $|g''|$, théorème 25.61.
- (6) En calcul numérique, section 25.7.

Thème 5 : Enveloppes

- (1) L'ellipse de John-Loewner donne un ellipsoïde de volume minimum autour d'un compact dans $\mathbb{R}^n$, théorème 13.212.
- (2) Le cercle circonscrit à une courbe donne un cercle de rayon minimal contenant une courbe fermée simple, proposition 14.81.
- (3) Enveloppe convexe du groupe orthogonal 12.36.

Thème 6 : Produit semi-direct de groupes

- (1) Définition 2.85.
- (2) Le corollaire 2.87 donne un critère pour prouver qu'un produit NH est un produit semi-direct.
- (3) L'exemple 12.80 donne le groupe des isométries du carré comme un produit semi-direct.
- (4) Le théorème 12.44 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.
- (5) La proposition 12.46 donne une décomposition du groupe orthogonal $O(n) = \text{SO}(n) \times_{\rho} C_2$ où $C_2 = \{\text{Id}, R\}$ où R est de déterminant -1 .
- (6) La proposition 8.44 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 7 : Racines de polynôme et factorisation de polynômes

- (1) Si $\mathbb{A}$ est une anneau, la proposition 3.111 factorise une racine.
- (2) Si $\mathbb{A}$ est un anneau, la proposition 3.113 factorise une racine avec sa multiplicité.
- (3) Si $\mathbb{A}$ est un anneau, le théorème 3.115 factorise plusieurs racines avec leurs multiplicités.
- (4) 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 4.55.
- (5) Le théorème 4.58 annule un polynôme de degré n ayant $n + 1$ racines distinctes.
- (6) La proposition 4.105 nous annule un polynôme à plusieurs variables lorsqu'il a trop de racines.
- (7) En analyse complexe, le principe des zéros isolés 19.20 annule en gros toute série entière possédant un zéro non isolé.
- (8) Polynômes irréductibles sur $\mathbb{F}_q$.

Thème 8 : Théorème de Bézout

- (1) Pour $\mathbb{Z}^*$ c'est le théorème 2.24.
- (2) Théorème de Bézout dans un anneau principal : corollaire 3.69.
- (3) Théorème de Bézout dans un anneau de polynômes : théorème 3.105.
- (4) En parlant des racines de l'unité et des générateurs du groupe unitaire dans le lemme 3.9. Au passage nous y parlerons de solfège.

Thème 9 : Équations diophantiennes

- (1) Équation $ax + by = c$ dans $\mathbb{N}$, équation (2.57).
- (2) Dans 2.5.5, nous résolvons $ax + by = c$ en utilisant Bézout (théorème 2.24).
- (3) L'exemple 3.79 donne une application de la pure notion de modulo pour $x^2 = 3y^2 + 8$. Pas de solutions.
- (4) L'exemple 3.80 résout l'équation $x^2 + 2 = y^3$ en parlant de l'extension $\mathbb{Z}[i\sqrt{2}]$ et de stathme.
- (5) Les propositions 3.81 et 3.84 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 décomposition de fractions en éléments simples, théorème 16.59.

Thème 10 : Application réciproque

- (1) Définition 5.172.
- (2) Dans le cas des réels, des exemples sont donnés en 11.268.

Thème 11 : Extension de corps et polynômes

- (1) Définition d'une extension de corps 4.37.
- (2) Pour l'extension du corps de base d'un espace vectoriel et les propriétés d'extension des applications linéaires, voir la section 6.30.
- (3) Extension de corps de base et similitude d'application linéaire (ou de matrices, c'est la même chose), théorème 6.345.
- (4) Extension de corps de base et cyclicité des applications linéaires, corollaire 6.344.
- (5) À propos d'extensions de $\mathbb{Q}$, le lemme 4.102.

Thème 12 : Rang

- (1) Définition 6.12.
- (2) Le théorème du rang, théorème 6.13
- (3) Prouver que des matrices sont équivalentes et les mettre sous des formes canoniques, lemme 6.15 et son corollaire 6.16.
- (4) Tout hyperplan de $\mathbb{M}(n, \mathbb{K})$ coupe $\text{GL}(n, \mathbb{K})$, corollaire 6.16. Cela utilise la forme canonique sus-mentionnée.
- (5) Le lien entre application duale et orthogonal de la proposition 6.32 utilise la notion de rang.
- (6) Prouver les équivalences à être un endomorphisme cyclique du théorème 6.343 via le lemme 6.342.

Thème 13 : Topologie produit

- (1) La définition de la topologie produit est 5.5.
- (2) Pour les espaces vectoriels normés, le produit est donné par la définition 6.197.
- (3) L'équivalence entre la topologie de la norme produit et la topologie produit est le lemme 6.199.

Thème 14 : Produit de compact

- (1) Les produits d'espaces métriques compacts sont compacts ; c'est le théorème de Tykhonov. Nous verrons ce résultat dans les cas suivants.
 - $\mathbb{R}$, lemme 5.106.
 - Produit fini d'espaces métriques compacts, théorème 5.147.
 - Produit dénombrable d'espaces métrique compacts, théorème 5.149.

Thème 15 : Connexité

- (1) Définition 5.67
- (2) Le groupe $SL(n, \mathbb{K})$ est connexe par arcs : proposition 12.18.
- (3) Le groupe $GL(n, \mathbb{C})$ est connexe par arcs : proposition 12.19.
- (4) Le groupe $GL(n, \mathbb{C})$ est connexe par arcs, proposition 12.19.
- (5) Le groupe $GL(n, \mathbb{R})$ a exactement deux composantes connexes par arcs, proposition 12.20.
- (6) Le groupe $O(n, \mathbb{R})$ n'est pas connexe, lemme 12.14.
- (7) Les groupe $U(n)$ et $SU(n)$ sont connexes par arcs, lemme 12.15.
- (8) Le groupe $SO(n)$ est connexe mais ce n'est pas encore démontré, proposition 12.16.
- (9) Connexité des formes quadratiques de signature donnée, proposition 16.155.

Thème 16 : Norme matricielle et rayon spectral

- (1) Définition du rayon spectral 6.83.
- (2) Lien entre norme matricielle et rayon spectral, le théorème 6.91 assure que $\|A\|_2 = \sqrt{\rho(A^t A)}$.
- (3) Pour toute norme algébrique nous avons $\rho(A) \leq \|A\|$, proposition 6.85.
- (4) Dans le cadre du conditionnement de matrice. Voir en particulier la proposition 25.42 qui utilise le théorème 6.91.

Thème 17 : Norme opérateur Pour la norme matricielle et le rayon spectral, voir le thème 16.

- (1) Définition 6.81.
- (2) Définition d'une norme d'algèbre 6.82.
- (3) Pour des espaces vectoriels normée, être borné est équivalent à être continu : proposition 6.217.

Thème 18 : Diagonalisation Des résultats qui parlent diagonalisation

- (1) Définition d'un endomorphisme diagonalisable : 6.278.
- (2) Conditions équivalentes au fait d'être diagonalisable en termes de polynôme minimal, y compris la décomposition en espaces propres : théorème 6.281.
- (3) Diagonalisation simultanée 6.284, pseudo-diagonalisation simultanée 6.298.
- (4) Diagonalisation d'exponentielle 6.307 utilisant Dunford.
- (5) Décomposition polaire théorème 12.31. $M = SQ$, S est symétrique, réelle, définie positive, Q est orthogonale.
- (6) Décomposition de Dunford 6.303. $u = s + n$ où s est diagonalisable et n est nilpotent, $[s, n] = 0$.
- (7) Réduction de Jordan (bloc-diagonale) 6.334.
- (8) L'algorithme des facteurs invariants 3.87 donne $U = PDQ$ avec P et Q inversibles, D diagonale, sans hypothèse sur U . De plus les éléments de D forment une chaîne d'éléments qui se divisent l'un l'autre.

Le théorème spectral et ses variantes :

- (1) Théorème spectral, matrice symétrique, théorème 6.292. Via le lemme de Schur.
- (2) Théorème spectral autoadjoint (c'est le même, mais vu sans matrices), théorème 6.380
- (3) Théorème spectral hermitien, lemme 6.286.
- (4) Théorème spectral, matrice normales, théorème 6.290.

Pour les résultats de décomposition dont une partie est diagonale, voir le thème 35 sur les décompositions.

Thème 19 : Sous-groupes

- (1) Théorème de Burnside sur les sous groupes d'exposant fini de $GL(n, \mathbb{C})$, théorème 6.357.
- (2) Sous-groupes compacts de $GL(n, \mathbb{R})$, lemme 12.38 ou proposition 12.39.

Thème 20 : Mesure et intégrale

- (1) Mesure de Lebesgue, définition 7.160
- (2) Intégrale associée à une mesure, définition 7.113

Thème 21 : Équivalence de normes

- (1) La proposition 6.138 sur l'équivalence des normes dans $\mathbb{R}^n$.
- (2) Montrer que le problème $a - b$ est stable dans l'exemple 25.24.

Thème 22 : Espace L^2 (L2)

- (1) Définition de $L^2(\Omega, \mu)$, 18.28.
- (2) L'espace L^2 est discuté en analyse fonctionnelle, en 18.3.6 parce que l'étude de L^2 utilise entre autres l'inégalité de Hölder 18.20.

Thème 23 : Espaces L^p (Lp)

- (1) Dual de $L^p([0, 1])$ pour $1 < p < 2$, proposition 18.45.

Thème 24 : Théorème de Stokes, Green et compagnie

- (1) Forme générale, théorème 13.165.
- (2) Rotationnel et circulation, théorème 15.9.

Thème 25 : Invariants de similitude

- (1) Théorème 6.331.
- (2) Pour prouver que la similitude d'applications linéaires résiste à l'extension du corps de base, théorème 6.345.
- (3) Pour prouver que la dimension du commutant d'un endomorphisme de E est de dimension au moins $\dim(E)$, lemme 6.342.
- (4) Nous verrons dans la remarque 6.332 à propos des invariants de similitude que toute matrice est semblable à la matrice bloc-diagonale constituées des matrices compagnon (définition 6.326) de la suite des polynômes minimaux.

Thème 26 : Endomorphismes cycliques

- (1) Définition 6.248.
- (2) Son lien avec le commutant donné dans la proposition 6.340 et le théorème 6.343.
- (3) Utilisation dans le théorème de Frobenius (invariants de similitude), théorème 6.331.

Thème 27 : Formes bilinéaires et quadratiques

- (1) Les formes bilinéaires ont été définies en 6.63.
- (2) Forme quadratique, définition 6.361

Thème 28 : Isométries

- (1) Les isométries de l'espace euclidien sont affines, 12.43.
- (2) Les isométries de l'espace euclidien comme produit semi-direct : $\text{Isom}(\mathbb{R}^n) \simeq T(n) \times_{\rho} O(n)$, théorème 12.44.
- (3) Isométries du cube, section 2.12.
- (4) Générateurs du groupe diédral, proposition 12.78.

Thème 29 : Déterminant

- (1) Les n -formes alternées forment un espace de dimension 1, proposition 6.42.
- (2) Déterminant d'une famille de vecteurs 6.45.
- (3) Déterminant d'un endomorphisme 6.48.
- (4) Des interprétations géométriques du déterminant sont dans la section 13.7.

Thème 30 : Polynôme d'endomorphismes

- (1) Endomorphismes cycliques et commutant dans le cas diagonalisable, proposition 6.340.
- (2) Racine carrée d'une matrice hermitienne positive, proposition 12.26.
- (3) Théorème de Burnside sur les sous groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 6.357.
- (4) Décomposition de Dunford, théorème 6.303.
- (5) Algorithme des facteurs invariants 3.87.

Thème 31 : Action de groupe

- (1) Action du groupe modulaire sur le demi-plan de Poincaré, théorème 10.33.

Thème 32 : Systèmes d'équations linéaires

- Algorithme des facteurs invariants 3.87.
- Méthode du gradient à pas optimal 16.154.

Thème 33 : Classification de groupes

- (1) Structure des groupes d'ordre pq , théorème 12.113.
- (2) Le groupe alterné est simple, théorème 2.83.
- (3) Théorème de Sylow 12.99. Tout le théorème, c'est un peu long. On peut se contenter de la partie qui dit que G contient un p -Sylow.
- (4) Théorème de Burnside sur les sous groupes d'exposant fini de $\mathrm{GL}(n, \mathbb{C})$, théorème 6.357.
- (5) $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, corollaire 4.122.

Thème 34 : Théorie des représentations

- (1) Table des caractères du groupe diédral, section 12.14.
- (2) Table des caractères du groupe symétrique S_4 , section 12.13.

Thème 35 : Décomposition de matrices

- (1) Décomposition de Bruhat, théorème 12.37.
- (2) Décomposition de Dunford, théorème 6.303.
- (3) Décomposition polaire 12.31.

Thème 36 : Méthodes de calcul

- (1) Théorème de Rothstein-Trager 13.205.
- (2) Algorithme des facteurs invariants 3.87.
- (3) Méthode de Newton, théorème 25.68
- (4) Calcul d'intégrale par suite équirépartie 20.21.

Thème 37 : 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 16.125 pour les équations différentielles.
- (2) Le théorème de Schauder 16.119 permet de démontrer une version du théorème de Cauchy-Lipschitz (théorème 16.123) sans la condition Lipschitz
- (3) Le théorème de Cauchy-Lipschitz 16.123 est utilisé à plusieurs endroits :
— Pour calculer la transformée de Fourier de $e^{-x^2/2}$ dans le lemme 21.15.
- (4) Théorème de stabilité de Lyapunov 24.15.
- (5) Le système proie prédateurs, Lotka-Volterra 24.16
- (6) Équation de Schrödinger, théorème 24.22.
- (7) L'équation $(x - x_0)^\alpha u = 0$ pour $u \in \mathcal{D}'(\mathbb{R})$, théorème 22.55.
- (8) La proposition 24.18 donne un résultat sur $y'' + qy = 0$ à partir d'une hypothèse de croissance.
- (9) Équation de Hill $y'' + qy = 0$, proposition 24.20.

Thème 38 : Dénombrements

- Coloriage de roulette (12.4.8.1) et composition de colliers (12.4.8.2).
- Nombres de Bell, théorème 16.82.
- Le dénombrement des solutions de l'équation $\alpha_1 n_1 + \dots + \alpha_p n_p = n$ utilise des séries entières et des décomposition de fractions en éléments simples, théorème 16.59.

Thème 39 : Densité

- (1) Densité des polynômes dans $C^0([0, 1])$, théorème de Bernstein 26.117.
- (2) Densité de $\mathcal{D}(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$ pour $1 \leq p < \infty$, théorème 18.40.
- (3) Densité de $\mathcal{S}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 23.17.
- (4) Densité de $\mathcal{D}(\mathbb{R}^d)$ dans l'espace de Sobolev $H^s(\mathbb{R}^d)$, proposition 23.19.

Cela est utilisé pour le théorème de trace 23.21.

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 16.166.

Thème 40 : Injections

- (1) L'espace de Sobolev $H^1(I)$ s'injecte de façon compacte dans $C^0(\bar{I})$, proposition 23.8.
- (2) L'espace de Sobolev $H^1(I)$ s'injecte de façon continue dans $L^2(I)$, proposition 23.8.
- (3) L'espace $L^2(\Omega)$ s'injecte continument dans $\mathcal{D}'(\Omega)$ (les distributions), proposition 22.13.

Thème 41 : Dualité Parmi les théorèmes de dualité nous avons

- (1) Le théorème de représentation de Riesz 17.19 pour les espaces de Hilbert.
- (2) La proposition 18.45 pour les espaces $L^p([0, 1])$ avec $1 < p < 2$.
- (3) Le théorème de représentation de Riesz 18.49 pour les espaces L^p en général.

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

Thème 42 : Opérations sur les distributions

- (1) Convolution d'une distribution par une fonction, définition par l'équation (22.73).
- (2) Dérivation d'une distribution, proposition-définition 22.15.
- (3) Produit d'une distribution par une fonction, définition 22.14.

Thème 43 : Permuter des limites

- (1) Les théorèmes sur les fonctions définies par des intégrales, section 13.19. Nous avons entre autres
 - (a) $\partial_i \int_B f = \int_B \partial_i f$, avec B compact, proposition 13.187.
 - (b) Si f est majorée par une fonction ne dépendant pas de x , nous avons le théorème 13.177.
 - (c) Si l'intégrale est uniformément convergente, nous avons le théorème 13.178.
- (2) Théorème de la convergence monotone, théorème 7.129.

Thème 44 : Convolution

- (1) Définition pour $f, g \in L^1$, théorème 18.33.
- (2) Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leq \|f\|_p \|g\|_1$, proposition 18.35.
- (3) $\varphi \in L^1(\mathbb{R})$ et $\psi \in \mathcal{S}(\mathbb{R})$, alors $\varphi * \psi \in \mathcal{S}(\mathbb{R})$, proposition 18.79.
- (4) Les suites régularisantes : $\lim_{n \rightarrow \infty} \rho_n * f = f$ dans la proposition 21.17.

Thème 45 : Séries de Fourier

- Formule sommatoire de Poisson, proposition 21.9.
- Inégalité isopérimétrique, théorème 20.19.
- Fonction continue et périodique dont la série de Fourier ne converge pas, proposition 20.16.

Thème 46 : Transformée de Fourier

- (1) Définition sur L^1 , définition 21.2.
- (2) La transformée de Fourier d'une fonction $L^1(\mathbb{R}^d)$ est continue, proposition 21.5.
- (3) L'espace de Schwartz est stable par transformée de Fourier. L'application $\mathcal{F}: \mathcal{S}(\mathbb{R}^d) \rightarrow \mathcal{S}(\mathbb{R}^d)$ est une bijection linéaire et continue. Proposition 21.12

Thème 47 : Applications continues et bornées

- (1) Une application linéaire non continue : exemple 6.215 de $e_k \mapsto ke_k$. Les dérivées partielles sont calculées en (17.121).
- (2) Une application linéaire est bornée si et seulement si elle est continue, proposition 6.217.

Thème 48 : Définie positive

- (1) Une application bilinéaire est définie positive lorsque $g(u, u) \geq 0$ et $g(u, u) = 0$ si et seulement si $u = 0$ est la définition 6.64.
- (2) Un opérateur ou une matrice est défini positif si toutes ses valeurs propres sont positives, c'est la définition 6.294.
- (3) Pour une matrice symétrique, définie positive implique $\langle Ax, x \rangle > 0$ pour tout x . C'est le lemme 6.296.
- (4) Une application linéaire est définie positive si et seulement si sa matrice associée l'est. C'est la proposition 6.366.

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

Thème 49 : Gaussienne

- (1) Le calcul de l'intégrale

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi} \quad (0.1)$$

est fait dans les exemples 13.81 et 13.82.

- (2) Le lemme 21.15 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 21.18 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 21.20

Thème 50 : Inégalités

Inégalité de Jensen (1) Une version discrète pour $f(\sum_i \lambda_i x_i)$, la proposition 11.226.

(2) Une version intégrale pour $f(\int \alpha d\mu)$, la proposition 18.18.

(3) Une version pour l'espérance conditionnelle, la proposition 26.42.

Inégalité de Minkowsky (1) Pour une forme quadratique q sur $\mathbb{R}^n$ nous avons $\sqrt{q(x+y)} \leq \sqrt{q(x)} + \sqrt{q(y)}$. Proposition 6.373.

(2) Si $1 \leq p < \infty$ et si $f, g \in L^p(\Omega, \mathcal{A}, \mu)$ alors $\|f + g\|_p \leq \|f\|_p + \|g\|_p$. Proposition 18.23.

(3) L'inégalité de Minkowsky sous forme intégrale s'écrit sous forme déballée

$$\left[\int_X \left(\int_Y |f(x, y)| d\nu(y) \right)^p d\mu(x) \right]^{1/p} \leq \int_Y \left(\int_X |f(x, y)|^p d\mu(x) \right)^{1/p} d\nu(y). \quad (0.2)$$

ou sous forme compacte

$$\left\| x \mapsto \int_Y f(x, y) d\nu(y) \right\|_p \leq \int_Y \|f_y\|_p d\nu(y) \quad (0.3)$$

Transformée de Fourier Pour tout $f \in L^1(\mathbb{R}^n)$ nous avons $\|\hat{f}\|_\infty \leq \|f\|_1$, lemme 21.6.

Inégalité de normes : si $f \in L^p$ et $g \in L^1$, alors $\|f * g\|_p \leq \|f\|_p \|g\|_1$, proposition 18.35.

Thème 51 : Théorème central limite

- (1) Pour les processus de Poisson, théorème 30.5.

Thème 52 : Lemme de transfert Il s'agit du résultat $\hat{f}' = i\xi \hat{f}$.

- (1) Lemme 21.11 sur $\mathcal{S}(\mathbb{R}^d)$
- (2) Lemme 23.12 pour L^2 .

Thème 53 : Dédurre 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 7.123 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 18.42.
- (3) Et encore un pour L^p dans la proposition 18.50.
- (4) Si $\int f\chi = 0$ pour tout χ à support compact alors $f = 0$ presque partout, proposition 18.1.
- (5) La proposition 18.44 donne $f = 0$ dans L^p lorsque $\int fg = 0$ pour tout $g \in L^q$ lorsque l'espace est σ -fini.
- (6) 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 16.94.

Table des matières

Thématique	2
Table des matières	11
Index	35
0 Introduction	57
0.1 Préface	57
0.2 Auteurs, contributeurs, sources et remerciements	57
0.3 Les questions pour lesquelles je n'ai pas (encore) de réponse	59
0.3.1 Mes questions d'analyse.	59
0.3.2 Mes questions d'algèbre, géométrie.	61
0.3.3 Mes questions de probabilité et statistiques.	62
0.3.4 Mes questions de modélisation	63
0.3.5 Les preuves à relire par des experts	63
0.4 Comment m'aider à rendre ces notes plus utiles ?	68
1 Construction des ensembles de nombres	69
1.1 Quelques éléments sur les ensembles	69
1.1.1 Lemme de Zorn	69
1.1.2 Complémentaire	70
1.1.3 Relations d'équivalence	70
1.2 Les naturels	71
1.3 Les entiers	71
1.4 Quelques structures algébriques	71
1.5 Les rationnels	73
1.5.1 Suites de Cauchy dans les rationnels	73
1.5.2 Insuffisance des rationnels	75
1.6 Les réels	77
1.6.1 L'ensemble	78
1.6.2 Relation d'ordre	80
1.7 Les complexes	82
1.7.1 Définitions	82
2 Théorie des groupes	85
2.1 Groupes	85
2.2 Sous groupe normal	86
2.3 Groupe dérivé	87
2.4 Théorèmes d'isomorphismes	88
2.5 Le groupe et anneau des entiers	89
2.5.1 Division euclidienne	90
2.5.2 PGCD, PPCM et Bézout	90
2.5.3 Calcul effectif du PGCD et de Bézout	92
2.5.3.1 L'idée	92

2.5.3.2	Pour le PGCD	92
2.5.3.3	Bézout : calcul effectif	93
2.5.4	Écriture des fractions	94
2.5.5	Équation diophantienne linéaire à deux inconnues	95
2.5.6	Quotients	96
2.6	Indice d'un sous-groupe et ordre des éléments	96
2.7	Suite de composition	98
2.8	Groupes résolubles	101
2.9	Action de groupes	102
2.10	Le groupe symétrique	106
2.11	Produit semi-direct de groupes	111
2.12	Isométries du cube	113
2.13	Groupe de torsion	115
2.14	Famille presque nulle	115
3	Anneaux	117
3.1	Généralités	117
3.2	Binôme de Newton et morphisme de Frobenius	118
3.3	Décomposition en facteurs premiers	119
3.4	Le groupe des racines de l'unité	119
3.5	Fonction indicatrice d'Euler (première partie)	121
3.5.1	Introduction par les racines de l'unité	122
3.5.2	Générateurs	123
3.6	Idéal dans un anneau	123
3.7	Caractéristique	124
3.8	Modules	125
3.9	Anneau intègre	127
3.9.1	PGCD et PPCM	128
3.9.2	Contenu d'un polynôme	129
3.10	Anneau factoriel	130
3.11	Anneau principal	131
3.11.1	Bézout	132
3.11.2	Anneau noetherien	133
3.12	Anneau euclidien	133
3.12.1	Équations diophantiennes	135
3.12.2	Triplet pythagoriciens et équation de Fermat pour $n = 4$	136
3.12.3	Lignes et colonnes de matrices	138
3.12.4	Algorithme des facteurs invariants	139
3.13	Anneaux des polynômes	141
3.13.1	Irréductibilité	142
3.13.2	Division euclidienne	143
3.13.3	Bézout	143
3.13.4	Idéaux	144
3.13.5	Racines des polynômes	145
3.13.6	Quelque identités	147
4	Corps	149
4.1	Généralités	149
4.1.1	Corps des fractions	150
4.1.2	Corps premier	151
4.1.3	Petit théorème de Fermat	153
4.2	Théorème des deux carrés	153
4.2.1	Un peu de structure dans $\mathbb{Z}[i]$	154
4.2.2	Résultats chinois	157

4.2.3	Anneaux principaux et polynômes	159
4.3	Extension de corps	160
4.3.1	Polynôme minimal	160
4.3.2	Racines de polynômes	163
4.3.3	Corps de rupture	164
4.3.4	Corps de décomposition	166
4.3.5	Clôture algébrique	167
4.3.6	Extensions séparables	168
4.3.7	Idéal maximum	172
4.4	Espaces de polynômes	173
4.4.1	Polynômes symétriques, alternés ou semi-symétriques	175
4.4.2	Polynôme symétrique élémentaire	175
4.4.3	Relations coefficients racines	178
4.5	Polynômes cyclotomiques	179
4.5.1	Définitions et propriétés	179
4.5.2	Nombres premiers	183
4.5.3	Théorème de Wedderburn	185
4.6	Corps finis	186
4.6.1	Existence, unicité	186
4.6.2	Symboles de Legendre et carrés	189
4.6.3	Théorème de Chevalley-Waring	194
4.6.4	Théorème de l'élément primitif	196
4.6.5	Construction de $\mathbb{F}_q$	201
4.6.5.1	La version du faignant	201
4.6.5.2	La version plus élaborée	202
4.6.6	Exemple : étude de $\mathbb{F}_{16}$	204
4.6.7	Polynômes irréductibles sur $\mathbb{F}_q$	206
4.7	Constructions à la règle et au compas	208
4.7.1	Quelque constructions	208
4.7.2	Nombres constructibles	210
4.7.3	Polygones constructibles	212
4.7.4	Matrices	217
4.8	Minuscule morceau sur la théorie de Galois	217
5	Topologie générale	219
5.1	Topologie en général	219
5.1.1	Définitions basiques	219
5.1.2	Topologie produit	220
5.1.3	Séparabilité	220
5.1.4	Topologie métrique	221
5.1.5	Espace vectoriel normé	222
5.1.6	Topologie sur l'ensemble des réels	225
5.1.7	Base de topologie	227
5.2	Limite et continuité	228
5.3	Compacité	230
5.3.1	Quelque propriétés	230
5.4	Topologie induite	231
5.5	Connexité	232
5.6	Un peu de topologie réelle	234
5.6.1	Suites numériques	234
5.6.2	Maximum, supremum et compagnie	236
5.6.2.1	...et quelque exemples	237
5.6.3	Intervalles	241
5.6.3.1	Connexité	241

5.6.3.2	Compacité	243
5.6.4	Image d'un compact	245
5.6.5	Connexité par arcs	247
5.7	Espaces métriques	247
5.7.1	Espaces métrisables	247
5.7.2	Fonctions continues	247
5.7.3	Caractérisations séquentielles	248
5.7.4	Distance entre un point et un ensemble	250
5.7.5	Compacité	251
5.7.6	Ensembles enchaînés	256
5.7.7	Produit fini d'espaces métriques	257
5.8	Ensembles nulle part denses	258
5.9	Encore de la topologie réelle	259
5.9.1	Ouverts et fermés	259
5.9.2	Intérieur, adhérence et frontière	259
5.9.3	Point d'accumulation, point isolé	261
5.9.4	Limite de suite	261
5.10	Application réciproque	262
5.11	Topologie des semi-normes	263
5.11.1	Espace dual	265
5.11.2	Espace $C^k(\mathbb{R}, E')$	265
5.12	Espaces de Baire	266
6	Espaces vectoriels	269
6.1	Parties libres, génératrices, bases et dimension	269
6.2	Applications linéaires	272
6.2.1	Définition	272
6.2.2	Rang	272
6.3	Matrice d'une application linéaire	274
6.3.1	Écriture dans une base	274
6.3.2	Changement de base : vecteurs de base	276
6.3.3	Changement de base : coordonnées	277
6.3.4	Changement de base : matrice d'une application linéaire	277
6.3.5	Changement de base : matrice d'une forme bilinéaire	277
6.4	Dualité	278
6.4.1	Orthogonal	278
6.4.2	Transposée	278
6.4.3	Transposée : sans le dual	281
6.4.4	Polynômes de Lagrange	281
6.4.5	Dual de $\mathbb{M}(n, \mathbb{K})$	282
6.5	Déterminants	283
6.5.1	Formes multilinéaires alternées	283
6.5.2	Déterminant d'une famille de vecteurs	286
6.5.3	Déterminant d'un endomorphisme	287
6.5.4	Déterminant de Vandermonde	289
6.5.5	Déterminant de Gram	292
6.5.6	Déterminant de Cauchy	292
6.5.7	Matrice de Sylvester	292
6.5.8	Théorème de Kronecker	295
6.6	Directions conservées	296
6.6.1	Généralités	296
6.6.2	Matrice orthogonale	297
6.6.3	Comment trouver la matrice d'une symétrie donnée ?	298
6.6.3.1	Symétrie par rapport à un plan	298

6.6.3.2	Symétrie par rapport à une droite	299
6.6.3.3	En résumé	300
6.7	Normes et distances	300
6.7.1	Introduction : valeur absolue et norme	300
6.7.2	Norme	300
6.8	Produit scalaire	302
6.8.1	Projection et angles	304
6.8.2	Angle entre deux vecteurs	306
6.8.3	Procédé de Gram-Schmidt	306
6.9	Norme opérateur	307
6.9.1	Norme algébrique	309
6.9.2	Normes de matrices et d'applications linéaires	311
6.10	Produit vectoriel	312
6.11	Topologie	313
6.11.1	Boules et sphères	313
6.11.2	Ouverts, fermés, intérieur et adhérence	315
6.11.3	Point isolé, point d'accumulation	321
6.12	Équivalence des normes	322
6.12.1	En dimension finie	323
6.12.2	Contre-exemple en dimension infinie	324
6.13	Suites	325
6.13.1	Limites, convergence	325
6.13.2	Critère de Cauchy	325
6.14	Séries	326
6.15	Série réelle	329
6.15.1	Rappels et définitions	329
6.15.2	Critères de convergence absolue	329
6.15.3	Critères de convergence simple	331
6.15.3.1	Critère d'Abel	331
6.15.4	Quelques séries usuelles	332
6.15.5	Moyenne de Cesaro	333
6.15.6	Écriture décimale d'un nombre	333
6.16	Exponentielle de matrice	337
6.17	Sommes de familles infinies	338
6.17.1	Convergence commutative	338
6.18	Mini introduction aux nombres p-adiques	342
6.18.1	La flèche d'Achille	342
6.18.2	La tortue et Achille	342
6.18.3	Dans les nombres p-adiques, c'est vrai	343
6.19	Fonctions	344
6.20	Produit fini d'espaces vectoriels normés	344
6.20.1	Norme	344
6.20.2	Suites	347
6.21	Applications multilinéaires	348
6.22	Méthode de Gauss pour résoudre des systèmes d'équations linéaires	349
6.23	Orthogonalité	350
6.24	Calcul différentiel dans un espace vectoriel normé	350
6.24.1	Différentielle	350
6.24.2	(non ?) Différentiabilité des applications linéaires	351
6.24.3	Dérivation en chaine et formule de Leibnitz	352
6.24.4	Différentielle partielle	356
6.24.5	Formule des accroissements finis	357
6.24.6	L'inverse, sa différentielle	360

6.24.7	Projection orthogonale	362
6.25	Polynôme d'endomorphismes	363
6.25.1	Polynômes d'endomorphismes	364
6.25.2	Calcul effectif de l'exponentielle d'une matrice	366
6.25.3	Polynôme minimal et minimal ponctuel	366
6.25.4	Polynôme caractéristique	372
6.26	Valeur propre et vecteur propre	375
6.27	Espaces hermitiens	376
6.28	Diagonalisation	377
6.28.1	Matrices semblables	377
6.28.2	Endomorphismes diagonalisables	378
6.28.3	Diagonalisation : cas complexe	381
6.28.4	Diagonalisation : cas réel	383
6.28.5	Pseudo-réduction simultanée	385
6.29	Sous espaces caractéristiques	386
6.29.1	Théorèmes de décomposition	387
6.29.2	Diverses conséquences	389
6.29.3	Diagonalisabilité d'exponentielle	391
6.29.4	Valeurs singulières	392
6.30	Extension du corps de base	392
6.30.1	Extension des applications linéaires	393
6.30.2	Projections	394
6.30.3	Rang, polynôme minimal, polynôme caractéristique	397
6.31	Frobenius et Jordan	399
6.31.1	Matrice compagnon	399
6.31.2	Réduction de Frobenius	399
6.31.3	Forme normale de Jordan	402
6.32	Commutant et endomorphismes cycliques	403
6.32.1	Endomorphisme cyclique	403
6.32.2	Commutant : cas diagonalisable	404
6.32.3	Commutant : cas général	406
6.33	Endomorphismes nilpotents et trigonalisables	409
6.33.1	Endomorphismes nilpotents	409
6.33.2	Endomorphismes trigonalisables	411
6.33.3	Théorème de Burnside	413
6.33.4	Théorème de Lie-Kolchin	414
6.34	Formes bilinéaires et quadratiques	417
6.34.1	Généralités	417
6.34.2	Topologie	417
6.34.3	Matrice associée	417
6.34.4	Dégénérescence	419
6.34.5	Inégalité de Minkowski	420
6.34.6	Ellipsoïde	421
6.35	Théorème spectral auto-adjoint	422
6.36	Mini introduction au produit tensoriel	425
6.36.1	Définitions	425
6.36.2	Application d'opérateurs	425
6.37	Coordonnées cylindriques et sphériques	426
6.38	Méthode de Gauss pour résoudre des systèmes d'équations linéaires	426

7 Tribus, théorie de la mesure	429
7.1 Tribus	429
7.1.1 Généralités	429
7.1.1.1 Tribu induite	430
7.1.1.2 Tribu borélienne	431
7.1.1.3 Les boréliens de $\mathbb{R}$	431
7.1.2 Tribu de Baire	431
7.2 Théorie de la mesure	433
7.2.1 Mesure et algèbre de parties	434
7.2.2 Mesure sur un espace mesurable	436
7.2.3 Mesure extérieure	442
7.2.4 Espace mesuré complet	444
7.2.5 Prolongement	452
7.3 Applications mesurables	454
7.3.1 Propriétés	454
7.3.2 D'une tribu à l'autre	454
7.3.3 Mesure image	457
7.3.4 Régularité d'une mesure	458
7.3.5 Théorème de récurrence	462
7.4 Mesurabilité des fonctions à valeurs réelles	463
7.4.1 Quelques mots à propos de $\overline{\mathbb{R}}$	463
7.4.2 Limite supérieure et inférieure	463
7.4.3 Fonctions à valeurs réelles sur un espace mesurable	464
7.4.4 Fonction étagée	470
7.4.5 Fonctions réelle à variables réelles	473
7.5 Intégrale par rapport à une mesure	473
7.5.1 Quelques propriétés	475
7.5.2 Permuter limite et intégrale	478
7.5.2.1 Convergence uniforme	478
7.5.2.2 Convergence monotone	479
7.5.2.3 Convergence dominée de Lebesgue	481
7.5.3 Produit d'une mesure par une fonction (mesure à densité)	483
7.6 Tribu produit, mesure produit	484
7.6.1 Produit d'espaces mesurables	484
7.6.2 Le cas des boréliens	485
7.6.3 Produit de mesures	486
7.7 Mesure de Lebesgue sur $\mathbb{R}$	491
7.7.1 Mesure et tribu de Lebesgue	495
7.7.2 Propriétés de la mesure de Lebesgue	496
7.7.3 Ensemble de Cantor	501
7.7.4 Ensemble de Vitali (non mesurable)	503
7.8 Tribu et mesure de Lebesgue sur $\mathbb{R}^d$	504
7.8.1 Ensembles négligeables	505
7.8.2 Parties et fonctions mesurables	506
7.8.3 Propriétés d'unicité	506
7.8.4 Régularité	508
8 Espaces affines	509
8.1 Repères affines	509
8.2 Classification affine des conique	510
8.3 Applications affines	512
8.4 Isomorphismes	513
8.5 Sous espaces affines	513
8.6 Barycentre	515

8.6.1	Enveloppe convexe	517
8.7	Repères, coordonnées cartésiennes et barycentriques	520
8.7.1	Équation de droite	522
8.8	Structure du groupe des applications affines	522
9	Géométrie hyperbolique	525
9.1	Inversion	525
9.1.1	Cercles perpendiculaires	525
9.1.2	Inversion	526
10	Espaces projectifs	531
10.1	Sous espaces projectifs	531
10.2	Espace projectifs comme «complétés» d'espaces affines	533
10.3	Théorème de Pappus	535
10.4	Homographies	536
10.4.1	Homographies	536
10.4.2	Le groupe projectif	537
10.5	Coordonnées homogènes	538
10.5.1	Dualité	538
10.5.2	Polynômes	540
10.5.3	Repères projectifs	541
10.5.4	Birapport	542
10.6	Sphère de Riemann	544
10.6.1	Action du groupe modulaire	544
11	Analyse réelle	551
11.1	Limite et continuité	551
11.1.1	Définition	551
11.1.2	Propriétés de base	552
11.1.3	Limites de fonctions	553
11.1.4	Règles simples de calcul	558
11.2	Limites à plusieurs variables	558
11.2.1	Règle de l'étau	560
11.2.2	Méthode des chemins	561
11.2.3	Méthode des coordonnées polaires	562
11.2.4	Méthode du développement asymptotique	566
11.2.5	Continuité	566
11.2.6	La fonction la moins continue du monde	568
11.2.7	Approche topologique	569
11.2.8	Continuité de la racine carrée, invitation à la topologie induite	571
11.2.9	Limites en des nombres	573
11.2.10	Limites quand tout va bien	573
11.2.11	Discussion avec mon ordinateur	578
11.2.12	Limites et prolongement	578
11.3	Dérivée : exemples introductifs	579
11.3.1	La vitesse	579
11.3.2	La tangente à une courbe	580
11.3.3	L'aire en dessous d'une courbe	581
11.4	Définition de la dérivée	581
11.5	Continuité et dérivabilité	582
11.6	Dérivation de fonctions d'une variable réelle	583
11.6.1	Exemples	583
11.6.1.1	La fonction $f(x) = x$	583
11.6.1.2	La fonction $f(x) = x^2$	583

11.6.1.3 La fonction $f(x) = \sqrt{x}$	583
11.6.2 Calcul de la dérivée	584
11.6.3 Interprétation géométrique : tangente	584
11.6.4 Interprétation géométrique : approximation affine	585
11.7 Opérations sur les dérivées	586
11.7.1 Développement limité au premier ordre	587
11.8 Espace des fonctions continues	587
11.9 Uniforme continuité	592
11.10 Compacité	594
11.11 Dérivation et croissance	595
11.12 Dérivée directionnelle	599
11.12.1 Dérivée partielle et directionnelles	600
11.12.1.1 Quelques propriétés et notations	601
11.13 Dérivée suivant un vecteur	601
11.13.1 Gradient : direction de plus grande pente	604
11.14 Différentielle	605
11.14.1 Exemples introductifs	605
11.14.2 Définition de la différentielle	606
11.14.3 Unicité de la différentielle	609
11.14.4 Cas particuliers	610
11.14.5 Calcul de valeurs approchées	610
11.14.6 Prouver qu'une fonction n'est pas différentiable	613
11.14.6.1 Continuité	613
11.14.6.2 Linéarité	613
11.14.6.3 Cohérence des dérivées partielles et directionnelle	615
11.14.6.4 Un candidat dans la définition (marche toujours)	615
11.14.7 Règles de calcul	616
11.14.8 Linéarité	617
11.14.9 Produit	617
11.14.10 Différentielle de fonction composée	619
11.14.11 Différentielle et dérivées partielles	622
11.14.12 Plan tangent	623
11.14.13 Calcul de différentielles	623
11.14.14 Notes idéologiques quant au concept de plan tangent	624
11.14.15 Gradient et recherche du plan tangent	624
11.15 Jacobienne	626
11.15.1 Rappels et définitions	626
11.16 Fonctions à valeurs dans $\mathbb{R}^n$	626
11.17 Graphes de fonctions de plusieurs variables	627
11.18 Graphes de fonctions à plusieurs variables	630
11.19 Courbes de niveau	631
11.20 Fonctions de classe $\mathcal{C}^1$	635
11.21 Dérivée directionnelle de fonctions composées	636
11.22 Théorèmes des accroissements finis	638
11.23 Fonctions Lipschitziennes	639
11.24 Différentielles d'ordre supérieur	641
11.24.1 Identification des espaces d'applications multilinéaires	641
11.24.2 Fonctions différentiables plusieurs fois	641
11.25 Développement asymptotique, théorème de Taylor	644
11.25.1 Fonctions «petit o»	644
11.25.2 Autres formulations	645
11.25.3 Formule et reste	646
11.25.4 Reste intégral	646

11.25.5 Exemple : un calcul heuristique de limite	647
11.26 Fonctions convexes	647
11.26.1 Inégalité des pentes	647
11.26.2 Convexité et régularité	649
11.26.3 Dérivées d'une fonction convexe	649
11.26.4 Graphe d'une fonction convexe	651
11.26.5 Quelques inégalités	655
11.26.5.1 Inégalité de Jensen	655
11.26.5.2 Inégalité arithmético-géométrique	655
11.26.5.3 Inégalité de Kantorovitch	656
11.27 Suites de fonctions	657
11.27.1 Convergence de suites de fonctions	657
11.27.2 Convergence uniforme	657
11.27.3 Permuter avec les dérivées partielles	659
11.28 Recherche d'extrema	659
11.29 Fonctions réelles de deux variables réelles	660
11.29.1 Limites de fonctions à deux variables	660
11.29.2 Dérivées partielles	662
11.29.3 Différentielle et accroissement	662
11.29.4 Recherche d'extrema locaux	663
11.30 Les fonctions à valeurs vectorielles	663
11.31 Fonctions vectorielles de plusieurs variables	664
11.32 Champs de vecteurs	664
11.32.1 Matrice jacobienne	664
11.33 Divergence, rotationnel et l'opérateur nabla	665
11.34 Interprétation de la divergence	667
11.35 Quelques formules de Leibnitz	668
11.36 La différentielle revisitée	669
11.36.1 Les formes différentielles de base	669
11.36.2 Différentielle comme élément de l'espace dual	669
11.36.3 Différentielles de fonctions composées	670
11.36.4 Exemple de composée : les coordonnées polaires	671
11.37 Quelques rappels	672
11.38 Continuité et dérivabilité	672
11.38.1 Quelques formules à connaître	675
11.39 Application réciproque	675
11.39.1 Définitions	675
11.39.2 Graphe de la fonction réciproque	676
11.39.3 Théorème de la bijection	677
11.40 Rappels de trigonométrie	679
11.41 Fonctions trigonométriques réciproques	681
11.41.1 La fonction arc sinus	681
11.41.2 La fonction arc cosinus	683
11.41.3 La fonction arc tangente	684
11.42 Trigonométrie hyperbolique	685
11.43 Développement limité autour de zéro	686
11.44 Règles de calcul	689
11.44.1 Linéarité des développements limités	689
11.44.2 Développement limité d'un quotient	691
11.44.3 Développement limité d'une fonction composée	691
11.45 Développement au voisinage de $x_0 \neq 0$	692
11.46 Application au calcul de limites	693
11.47 Développement au voisinage de l'infini	694

11.48	Étude d'asymptote	694
12	Retour sur les groupes	705
12.1	Action de groupe et connexité	705
12.2	Espaces de matrices	707
12.2.1	Dilatations et transvections	707
12.2.2	Connexité de certains groupes	713
12.2.3	Densité	715
12.2.4	Racine carré d'une matrice hermitienne positive	717
12.2.5	Racine carré d'une matrice symétrique positive	718
12.2.6	Décomposition polaires : cas réel	718
12.2.7	Enveloppe convexe	721
12.2.8	Décomposition de Bruhat	723
12.3	Sous-groupes du groupe linéaire	725
12.4	Isométries de l'espace euclidien	728
12.4.1	Structure du groupe $\text{Isom}(\mathbb{R}^n)$	729
12.4.2	Classification des isométries de $\mathbb{R}$	732
12.4.3	Classification des isométries de $\mathbb{R}^2$	733
12.4.4	Isométries dans $\mathbb{R}^n$	738
12.4.5	Groupes finis d'isomorphismes	741
12.4.6	Théorème de Sylvester	744
12.4.7	Groupe diédral	744
12.4.7.1	Définition et générateurs : vue géométrique	744
12.4.7.2	Générateurs : vue abstraite	746
12.4.7.3	Classes de conjugaison	749
12.4.7.4	Le compte pour n pair	750
12.4.7.5	Le compte pour n impair	750
12.4.8	Applications : du dénombrement	750
12.4.8.1	Le jeu de la roulette	750
12.4.8.2	L'affaire du collier	751
12.5	Théorèmes de Sylow	752
12.6	Un peu de classification de groupes	757
12.6.1	Automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$	757
12.6.2	Groupes abéliens finis	758
12.6.3	Groupes d'ordre pq	761
12.6.4	Groupe monogène	763
12.6.5	Fonction indicatrice d'Euler	764
12.7	Nombres premiers	764
12.8	Chiffrement RSA	766
12.8.1	Mise en place par Bob	766
12.8.2	Chiffrement	767
12.8.3	Déchiffrement	767
12.8.4	Une imprudence à ne pas commettre	767
12.8.5	Problèmes calculatoires	768
12.8.6	La solidité de RSA	768
12.8.7	Note non mathématique pour doucher l'enthousiasme	768
12.9	Représentations et caractères	769
12.9.1	Crochet de dualité et transformée de Fourier	770
12.9.2	Groupes non abéliens	771
12.9.3	Représentations linéaires des groupes finis	772
12.9.4	Module	773
12.9.5	Structure hermitienne	775
12.9.6	Caractères	775
12.10	Équivalence de représentations et caractères	776

12.10.1 Représentation régulière	778
12.10.2 Caractères et représentations : suite et fin	779
12.11 Représentation produit tensoriel	782
12.12 Exemple sur le groupe symétrique	782
12.13 Table des caractères du groupe symétrique S_4	783
12.14 Table de caractères du groupe diédral	784
12.14.1 Représentations de dimension un	785
12.14.2 Représentations de dimension deux	785
12.14.3 Le compte pour n pair	787
12.14.4 Le compte pour n impair	787

13 Intégration 789

13.1 Théorème de la moyenne	789
13.2 Mesure à densité	789
13.2.1 Théorème de Radon-Nikodym	789
13.2.2 Mesure complexe	791
13.2.3 Théorème d'approximation	792
13.2.4 Mesure à densité	792
13.3 Constructions plus naïves de la mesure et de l'intégrale dans le cas réel	792
13.3.1 Mesure de Lebesgue, version rapide	792
13.3.2 Pavés et subdivisions	793
13.3.3 Intégrale d'une fonction en escalier	796
13.3.4 Intégrales partielles	796
13.3.5 Réduction d'une intégrale multiple	797
13.3.6 Propriétés de l'intégrale	798
13.3.7 Intégrales multiples, cas général	799
13.3.8 Réduction d'une intégrale multiple	799
13.3.9 Intégrales sur des parties de $\mathbb{R}^2$	801
13.3.10 Intégrales sur des parties de $\mathbb{R}^3$	804
13.3.11 Fonctions et ensembles non bornés	807
13.4 Propriétés	807
13.5 Primitives et intégrales	808
13.5.1 Primitives et intégrales	811
13.5.2 Intégrales impropres	812
13.6 Théorème de Fubini	815
13.6.1 Théorème de Fubini-Tonelli et de Fubini	815
13.7 Interprétation géométrique du déterminant	820
13.7.1 Par rapport à la mesure de Lebesgue	820
13.7.2 En petite dimension	821
13.7.3 Produit vectoriel	822
13.7.4 Produit mixte	823
13.7.5 Déterminant en dimension deux	825
13.7.6 Déterminant en dimension trois	825
13.8 Changement de variables dans une intégrale multiple	826
13.8.1 Des lemmes	826
13.8.2 Le théorème et sa démonstration	827
13.8.3 Exemples	831
13.8.4 Récapitulatif des changements de variables	834
13.8.4.1 Coordonnées polaires	834
13.8.4.2 Coordonnées cylindriques	834
13.8.4.3 Coordonnées sphériques	834
13.8.5 Changement de variables	835
13.8.5.1 Coordonnées polaires	835
13.8.5.2 Coordonnées sphériques	836

13.8.6	Coordonnées polaires	836
13.8.7	Coordonnées cylindriques	837
13.8.8	Coordonnées sphériques	837
13.9	Forme différentielle	838
13.9.0.1	L'isomorphisme musical	839
13.10	Intégrale sur une variété	840
13.10.1	Mesure sur une carte	840
13.10.1.1	Exemple : la mesure de la sphère	841
13.10.2	Intégrale sur une carte	841
13.10.3	Exemples	842
13.10.4	Orientation	842
13.10.5	Formes différentielles	844
13.10.6	Intégrale d'une fonction sur une variété	845
13.11	Intégrales curvilignes	846
13.11.1	Chemins de classe C^1	846
13.11.2	Intégrer une fonction	846
13.11.3	Intégrer un champ de vecteurs	848
13.11.4	Intégrer une forme différentielle sur un chemin	848
13.11.5	Intégration d'une forme différentielle sur un chemin	849
13.11.6	Interprétation physique : travail	850
13.11.7	Intégrer un champs de vecteurs sur un bord en $2D$	851
13.11.8	Intégrer une forme différentielle sur un bord en $2D$	851
13.11.9	Intégrer une forme différentielle sur un bord en $3D$	851
13.11.10	Intégrer d'un champ de vecteurs sur un bord en $3D$	852
13.11.11	Dérivées croisées et forme différentielle exacte	852
13.12	Surfaces paramétrées	853
13.12.1	Graphe d'une fonction	854
13.13	Intégrales de surface	855
13.13.1	Intégrale d'une fonction	855
13.13.2	Intégrale d'un champ de vecteurs	856
13.14	Intégrales de surface	857
13.14.1	Aire d'une surface paramétrée	857
13.14.2	Intégrale d'une fonction sur une surface	858
13.14.3	Aire d'une surface de révolution	859
13.14.4	Intégrale d'une 2	861
13.15	Flux d'un champ de vecteurs à travers une surface	861
13.16	Divergence, Green, Stokes	864
13.16.1	Théorème de la divergence	864
13.16.2	Formule de Green	865
13.16.3	Formule de Stokes	867
13.16.3.1	Quelle est la bonne orientation ?	867
13.17	Résumé des intégrales vues	868
13.17.1	L'intégrale d'une fonction sur les réels	868
13.17.2	Intégrale d'une fonction sur un chemin	868
13.17.3	Intégrale d'une fonction sur une surface	868
13.17.4	Intégrale d'une fonction sur un volume	869
13.17.5	Conclusion pour les fonctions	870
13.17.6	Circulation d'un champ de vecteurs	870
13.17.7	Flux d'un champ de vecteurs	870
13.17.8	Conclusion pour les champs de vecteurs	870
13.17.9	Attention pour les surfaces fermées !	871
13.18	Intégrales convergeant uniformément	872
13.18.1	Définition et propriété	872

13.18.2 Critères de convergence uniforme	873
13.19 Fonctions définies par une intégrale	874
13.19.1 Continuité sous l'intégrale	874
13.19.2 Le coup du compact	876
13.19.3 Dérivabilité sous l'intégrale	876
13.19.4 Absolue continuité	877
13.19.5 Différentiabilité sous l'intégrale	879
13.20 Formes différentielles exactes et fermées	882
13.21 Théorème d'Abel angulaire	884
13.21.1 Passage à la limite sous le signe intégral	888
13.21.2 Intégrale en dimension un	888
13.21.3 Intégrales convergentes	889
13.21.4 La méthode de Rothstein-Trager	889
13.22 Ellipsoïde de John-Loewer	894
13.23 Rappel sur les intégrales usuelles	897
13.24 Intégrales le long de chemins	898
13.24.1 Circulation d'un champ de vecteur	898
13.25 Circulation d'un champ conservatif	900
13.26 Intégration de fonction à deux variables	901
13.26.1 Intégration sur un domaine rectangulaire	901
13.26.2 Intégration sur un domaine non rectangulaire	902
13.26.3 Changement de variables	905
13.26.3.1 Le cas des coordonnées polaires	906
13.26.3.2 Les coordonnées cylindriques	907
13.26.3.3 Coordonnées sphériques	907
13.26.3.4 Un autre système utile	907
13.27 Les intégrales triples	908
13.27.1 Volume	910
13.28 Un petit peu plus formel	912
13.28.1 Intégration sur un domaine non rectangulaire	912
13.28.2 Changement de variables	912
13.28.2.1 Coordonnées polaires	913
13.28.2.2 Coordonnées sphériques	913
13.29 Primitives et surfaces	914
13.29.1 Longueur d'arc de courbe	914
13.29.2 Aire de révolution	915
13.30 L'aire en dessous d'une courbe	915
13.31 Propriétés des intégrales	916
13.32 Techniques d'intégration	917
13.32.1 Intégration par parties	918
13.32.2 Changement de variables – pour trouver des primitives	920
13.32.3 Changement de variables – pour calculer des intégrales	921
13.32.4 Intégrations des fractions rationnelles réduites	923
13.32.5 Quelques formules à connaître	924
13.33 Trucs et astuces de calcul d'intégrales	924
13.33.1 Quelques intégrales «usuelles»	924
13.33.2 Reformer un carré au dénominateur	927
13.33.3 Décomposer en fractions simples	927

14 Arc paramétré	929
14.1 Définitions, quelques exemples remarquables	929
14.2 Courbes paramétrés	930
14.2.1 Définitions et exemples	930
14.3 Longueur d'arc	931
14.4 Abscisse curviligne	934
14.4.1 Formule intégrale de la longueur	935
14.5 Élément de longueur	939
14.5.1 Élément de longueur : cartésiennes	939
14.5.2 Élément de longueur : polaires (1)	939
14.5.3 Élément de longueur : polaires (2)	939
14.5.4 Approximation de la longueur par des cordes	941
14.6 Arc géométrique	943
14.6.1 Abscisse curviligne et paramétrisation normale	944
14.6.2 Tangente à une courbe paramétrée	949
14.7 Repère de Frenet	951
14.7.1 Torsion	953
14.8 Hors des coordonnées normales	954
14.9 Tracer des courbes paramétriques dans $\mathbb{R}^2$	957
14.10 Courbes planes	958
14.10.1 Angle	958
14.10.2 Courbure signée	959
14.10.3 Degré, indice et homotopie	962
14.11 Courbes fermées planes	968
14.11.1 Cercle circonscrit	968
14.11.2 Description locale	970
14.11.3 Enveloppe convexe	971
14.11.4 Courbure et convexité	974
14.11.5 Théorème des quatre sommets	975
14.11.6 Le théorème de Jordan	978
15 Analyse vectorielle	979
15.1 Le théorème de Green	979
15.2 Théorème de la divergence dans le plan	983
15.2.1 La convention de sens de parcours	983
15.2.2 Théorème de la divergence	983
15.3 Théorème de Stokes	985
15.4 Théorème de Gauss	986
15.5 Coordonnées curvilignes	988
15.5.1 Base locale	988
15.5.2 Importance de l'orthogonalité	988
15.5.3 Coordonnées polaires	990
15.5.4 Coordonnées cylindriques	990
15.5.5 Coordonnées sphériques	991
15.5.6 Gradient en coordonnées curvilignes	991
15.5.6.1 Coordonnées sphériques	992
15.5.7 Divergence en coordonnées curvilignes	992
15.5.7.1 Coordonnées cylindriques	994
15.5.7.2 Coordonnées sphériques	994
15.5.8 Laplacien en coordonnées curvilignes orthogonales	994
15.5.9 Rotationnel en coordonnées curvilignes orthogonales	995
15.5.9.1 Coordonnées cylindriques	996
15.5.9.2 Coordonnées sphériques	996
15.6 Les formules	996

15.6.1	Coordonnées polaires	996
15.6.2	Coordonnées cylindriques	996
15.6.3	Coordonnées sphériques	997
16	Suite de l'analyse	999
16.0.1	Dérivabilité au sens complexe et différentielle	999
16.1	Série de fonctions	1002
16.2	Séries entières	1007
16.2.1	Disque de convergence	1007
16.2.2	Propriétés de la somme	1009
16.2.3	Dérivation, intégration	1012
16.2.4	Exponentielle et logarithme	1017
16.2.5	Forme polaire ou trigonométrique des nombres complexes	1021
16.3	Vitesses de x^α , de l'exponentielle et du logarithme	1021
16.3.1	Dénombrement des solutions d'une équation diophantienne	1022
16.4	Le cercle trigonométrique	1024
16.4.1	Les fonctions sinus et cosinus	1024
16.4.2	La fonction tangente	1025
16.4.3	Les coordonnées polaires	1026
16.4.3.1	Transformation inverse : théorie	1026
16.4.3.2	Transformation inverse : pratique	1027
16.4.4	Série génératrice d'une suite	1027
16.4.5	Développement en série et Taylor	1028
16.4.6	Resommer une série	1030
16.4.6.1	Les sommes du type $\sum_n P(n)x^n$	1030
16.4.6.2	Les sommes du type $\sum_n x^n/P(n)$	1031
16.4.6.3	Sage, primitives et logarithme complexe	1033
16.4.6.4	Nombres de Bell	1035
16.4.7	Séries entières de matrices	1035
16.4.8	Exponentielle et logarithme de matrice	1038
16.5	Nombres de Bell	1041
16.6	Lemme de Borel	1043
16.6.1	Fonctions plateaux	1043
16.6.2	Le lemme de Borel	1044
16.7	Densité des polynômes	1046
16.7.1	Théorème de Stone-Weierstrass	1046
16.7.2	Primitive de fonction continue	1049
16.7.3	Théorème taubérien de Hardy-Littlewood	1050
16.7.4	Théorème de Müntz	1054
16.8	Complétude avec la norme uniforme	1057
16.9	Théorèmes de point fixe	1058
16.9.1	Points fixes attractifs et répulsifs	1058
16.9.2	Picard	1058
16.9.3	Brouwer	1061
16.9.4	Théorème de Schauder	1063
16.9.5	Théorème de Markov-Kakutani et mesure de Haar	1065
16.10	Théorèmes de point fixes et équations différentielles	1066
16.10.1	Théorème de Cauchy-Lipschitz	1066
16.10.2	Théorème de Cauchy-Arzella	1068
16.11	Théorèmes d'inversion locale et de la fonction implicite	1068
16.11.1	Mise en situation	1068
16.11.2	Théorème d'inversion locale	1069
16.11.3	Théorème de la fonction implicite	1074
16.11.4	Exemple	1076

16.11.5 Théorème de Von Neumann	1077
16.12 Recherche d'extrema	1080
16.12.1 Extrema à une variable	1080
16.12.2 Extrema libre	1080
16.12.3 Extrema liés	1081
16.12.4 Algorithme du gradient à pas optimal	1084
16.13 Formes quadratiques, signature, et lemme de Morse	1087
16.13.1 Lemme de Morse	1091
16.14 Variétés	1093
16.14.1 Introduction	1093
16.14.2 Définition et propriétés	1093
16.14.3 Espace tangent	1094
16.15 Prolongement de fonctions et complétion d'espaces métriques	1095
16.16 Un petit extra	1101
17 Espaces de Hilbert	1103
17.1 Espaces de Hilbert	1103
17.2 Théorème de la projection	1104
17.3 Systèmes orthogonaux et bases	1107
17.3.1 Orthogonalité	1107
17.3.2 Dual	1109
17.3.3 Séparabilité	1110
17.3.4 Bases d'espaces de Hilbert	1114
17.3.5 Digression sur les normes opérateurs	1117
17.3.6 Applications linéaires et continuité	1118
17.4 Théorème de Kochen-Specker	1119
17.5 Théorème de Lax-Milgram	1120
18 Analyse fonctionnelle	1123
18.1 Théorème d'Ascoli	1123
18.2 Théorème de Banach-Steinhaus	1124
18.3 Espaces L^p	1126
18.3.1 Généralités	1126
18.3.2 L'espace L^∞	1128
18.3.3 Inégalité de Jensen, Hölder et de Minkowski	1129
18.3.4 Ni inclusions ni inégalités	1131
18.3.5 Complétude	1132
18.3.6 L'espace L^2	1136
18.3.7 Coefficients et série de Fourier	1138
18.4 Convolution	1139
18.4.1 Densité des fonctions infiniment dérivables à support compact	1140
18.4.2 Dualité et théorème de représentation de Riesz	1142
18.4.3 Approximation de l'unité	1151
18.4.4 Densité des polynôme trigonométrique	1153
18.5 Théorèmes de Hahn-Banach	1154
18.6 Théorème de Tietze	1156
18.7 Espace de Schwartz	1159
18.7.1 Topologie	1161
18.7.2 Produit de convolution	1163

19 Analyse complexe	1165
19.1 Fonctions holomorphes	1165
19.1.1 Équations de Cauchy-Riemann	1165
19.1.2 Intégrales sur des chemins fermés	1166
19.1.3 Lacets, indice et homotopie	1169
19.1.4 Théorème de Cauchy et analyticit��	1170
19.1.5 Théor��me de Brouwer en dimension 2	1172
19.1.6 Principe des z��ros isol��s	1173
19.1.7 Prolongement de fonctions holomorphes	1174
19.1.8 Th��or��me de Runge	1174
19.2 Int��grales de fonctions holomorphes	1177
19.3 Conditions ��quivalentes �� l'holomorphie	1181
19.4 Singularit��s, p��les et m��romorphe	1182
19.5 Fonctions d'Euler	1183
19.5.1 Euler et factorielle	1186
19.6 Partition d'un entier en parts fix��es	1186
19.7 Exponentielle complexe	1189
19.7.1 Int��grale de Fresnel	1191
19.8 Th��or��me de Weierstrass	1193
19.9 Th��or��me de Montel	1195
19.10Espaces de Bergman	1196
20 S��rie de Fourier	1201
20.1 Densit�� des polyn��mes trigonom��triques	1201
20.1.1 Convergence pour les fonctions continues (Weierstrass)	1201
20.1.2 Convergence pour les fonctions continues (Fej��r)	1202
20.1.3 Densit�� dans L^p	1205
20.2 Fonctions de Dirichlet	1205
20.3 Coefficients et s��rie de Fourier	1206
20.3.1 Le contre-exemple que nous attendions tous	1208
20.3.2 In��galit�� isop��rim��trique	1210
20.3.3 Suite ��quir��partie, crit��re de Weyl	1212
20.3.4 �� propos des coefficients	1214
21 Transformation de Fourier	1217
21.1 Transform��e de Fourier dans $L^1(\mathbb{R}^d)$	1217
21.1.1 Formule sommatoire de Poisson	1220
21.2 Transform��e de Fourier dans l'espace de Schwartz	1222
21.2.1 Quelques transform��es de Fourier	1225
21.3 Suite r��gularisante	1227
21.3.1 Formule d'inversion	1229
21.4 Transform��e de Fourier sur $L^2(\mathbb{R}^d)$	1231
21.4.1 Extension de $L^1 \cap L^2$ vers L^2	1231
22 Distributions	1235
22.0.0.1 D��riv��e partielle au sens faible	1235
22.1 Topologie	1235
22.2 Distributions	1238
22.2.1 Multiplication d'une distribution par une fonction	1240
22.2.2 D��riv��e de distribution	1240
22.2.3 Ordre et support d'une distribution	1241
22.3 Distributions temp��r��es	1244
22.3.1 Topologie	1245
22.3.2 Distributions associ��es �� des fonctions	1245

22.3.3	Composition avec une fonction	1245
22.3.4	Transformée de Fourier d'une distribution tempérée	1246
22.3.5	Convolution d'une distribution par une fonction	1246
22.3.6	Approximation de la distribution de Dirac	1247
22.3.7	Peigne de Dirac	1250
22.4	L'espace $C^\infty(\mathbb{R}, \mathcal{D}'(\mathbb{R}^d))$	1251
22.4.1	Dérivation	1253
22.5	L'espace $C^\infty(\mathbb{R}, \mathcal{S}'(\mathbb{R}^d))$	1253
22.5.1	Propriétés générales	1253
22.5.2	Dérivation	1256
22.6	Une équation de distribution	1258
23	Espaces de Soblev, équations elliptiques	1261
23.1	Espaces de Soblev	1261
23.1.1	Sur un intervalle de $\mathbb{R}$	1261
23.1.2	Sur un ouvert de $\mathbb{R}^n$	1267
23.1.2.1	Définition	1268
23.1.3	Espace de Soblev fractionnaire	1269
23.2	Trace	1271
23.3	Théorème de plongement	1274
24	Équations différentielles	1279
24.1	Que faire avec $f(z)dz = g(t)dt$?	1280
24.2	Équations linéaires du premier ordre	1281
24.2.1	Pourquoi la variation des constantes fonctionne toujours ?	1282
24.3	Équations à variables séparées	1283
24.3.1	La méthode rapide	1283
24.3.2	La méthode plus propre	1284
24.3.3	Les théorèmes	1284
24.4	Équations linéaires d'ordre supérieur	1286
24.4.1	Équations et systèmes linéaire à coefficients constants	1286
24.4.2	Si les coefficients ne sont pas constants ?	1286
24.5	Système d'équations linéaires	1287
24.5.1	La magie de l'exponentielle...	1287
24.5.2	... mais la difficulté	1287
24.5.3	La recette	1287
24.5.4	Système d'équations linéaires avec matrice constante	1288
24.5.5	Système d'équations linéaires avec matrice non constante	1289
24.6	Réduction de l'ordre	1289
24.7	Propriété des solutions	1290
24.7.1	Fuite des compacts et explosion en temps fini	1290
24.7.2	Stabilité de Lyapunov	1291
24.7.3	Système proie et prédateurs : Lokta-Voltera	1295
24.8	Équation du second ordre	1298
24.8.1	Wronskien	1298
24.8.2	Avec second membre	1299
24.8.3	Équation $y'' + q(t)y = 0$	1299
24.8.4	Équation de Hill	1301
24.9	Différents types d'équations différentielles	1304
24.9.1	Équation homogène	1304
24.9.2	Équation de Bernoulli	1305
24.9.3	Équation de Riccati	1305
24.9.4	Équation différentielle exacte	1305
24.9.4.1	Résolution lorsque tout va bien	1305

24.9.4.2	Facteur intégrant (quand tout ne va pas bien)	1306
24.10	Distributions pour les équations différentielles	1306
24.10.1	Équation de Schrödinger	1306
24.11	Équations différentielles du premier ordre	1310
24.12	Équations différentielles du premier ordre à variables séparables	1313
24.13	Équations différentielles linéaires du premier ordre	1315
24.13.1	Méthode de variation de la constante	1317
24.14	Équations différentielles linéaires du second ordre	1318
24.14.1	Résolution des équations différentielles linéaires du second ordre homogènes à coefficients constants	1318
24.14.2	Équations différentielles linéaires du second ordre à coefficients constants, non homogènes	1320
25	Calcul numérique	1323
25.1	Représentations numériques	1323
25.1.1	Entier relatif en complément à deux (binaire)	1323
25.1.2	Représentation en virgule flottante	1324
25.1.3	Simple précision, IEEE-754	1325
25.2	Problèmes pour écrire des nombres	1327
25.2.1	Troncature : la base	1328
25.2.2	Troncature : le drift	1328
25.2.3	Quelque bonnes règles	1329
25.3	Erreur de “cancellation”	1329
25.3.1	Erreur d’absorption	1331
25.3.2	Calcul d’une dérivée	1332
25.4	Conditionnement et stabilité	1332
25.4.1	Comment choisir et penser le K ?	1335
25.5	Conditionnement d’une matrice	1336
25.5.1	Perturbation du vecteur	1338
25.5.2	Perturbation de la matrice	1339
25.6	Un peu de points fixes	1340
25.6.1	Choix de la fonction à point fixe	1340
25.6.2	Convergence quadratique	1342
25.6.3	Convergence	1344
25.7	Méthode de Newton	1345
25.7.1	«Justification» par la formule par Taylor	1345
25.7.2	«Justification» par points fixes	1346
25.7.3	Convergence de la méthode de Newton	1346
25.7.4	Formalisation de l’algorithme	1348
25.7.5	Caractéristiques	1349
25.7.6	Exemple de la racine carré	1349
25.7.7	Si multiplicité	1350
25.7.8	Et la dérivée ?	1350
25.7.9	Méthode de Newton : le cas général	1351
25.8	Estimation de l’ordre de convergence	1353
25.9	Autres méthodes	1353
25.9.1	Méthode de Schröder	1353
25.9.2	Halley	1353
25.10	Méthode des sécantes variables	1354
25.10.1	Aitken	1354
25.11	Équations algébrique	1355
25.11.1	Résoudre un système linéaire	1355
25.11.2	Caractéristiques	1356
25.11.3	Définitions	1356

25.12	Équations non linéaire	1357
25.12.1	Méthode de bisection	1358
25.13	Efficacité	1360
25.14	Exercices	1361
25.15	Approximations de fonctions	1364
25.15.1	Critère d'interpolation	1364
25.15.2	Base de Newton	1365
25.15.3	Méthode des minima quadratiques	1367
25.15.4	Notre espace de Hilbert	1368
25.15.5	Droite de régression	1369
25.16	Système linéaires (généralités)	1370
25.16.1	Les méthodes directes	1371
25.16.2	Méthodes itératives	1371
25.17	Système linéaires (méthodes directes)	1372
25.17.1	Inversion de matrice triangulaire	1372
25.17.2	Transformation gaussienne	1372
25.17.3	Méthode de Gauss sans pivot (décomposition LU)	1373
25.17.4	Matrice de permutation élémentaires	1377
25.17.5	Méthode de Gauss avec pivot partiel	1378
25.17.6	Déterminant	1386
25.17.7	Plusieurs termes indépendants	1386
25.17.8	Cholesky	1387
25.18	Système linéaire (méthodes itératives)	1390
25.18.1	La méthode générale	1391
25.18.2	Jacobi	1391
25.18.3	Gauss-Seidel	1391
25.18.4	Autres	1391
26	Variables aléatoires et théorie des probabilités	1393
26.1	Espace de probabilité	1393
26.2	Variables aléatoires	1394
26.2.1	Indépendance	1394
26.2.2	Lois conjointes et indépendance	1397
26.2.3	Somme et produit de variables aléatoires indépendantes	1398
26.2.4	Espérance	1400
26.2.5	Variance	1401
26.2.6	Covariance	1402
26.2.7	Probabilité conditionnelle, première	1403
26.2.8	Espérance conditionnelle	1404
26.2.9	Probabilité conditionnelle, seconde	1410
26.2.10	Un petit paradoxe	1411
26.2.10.1	Le cas facile	1411
26.2.10.2	Premier raisonnement	1412
26.2.10.3	Simulation	1412
26.2.10.4	La vraie réponse	1413
26.2.10.5	Le même, tourné à peine différemment	1414
26.2.11	Résumé des choses conditionnelles	1414
26.2.12	Inégalité de Jensen	1415
26.2.13	Fonction de répartition	1415
26.2.14	Fonction caractéristique	1415
26.2.15	Fonction génératrice des moments, transformée de Laplace	1417
26.2.16	Loi d'une variable aléatoire	1418
26.2.17	Changement de variables	1419
26.3	Convergence	1419

26.4	Loi des grands nombres, théorème central limite	1424
26.4.1	Loi des grands nombres	1424
26.4.2	Théorème central limite	1426
26.4.3	Marche aléatoire	1429
26.5	Les lois usuelles	1430
26.5.1	Loi de Bernoulli	1430
26.5.2	Loi binomiale	1430
26.5.3	Loi multinomiale	1431
26.5.4	Loi géométrique	1432
26.5.5	Loi de Poisson	1432
26.5.6	Loi exponentielle	1433
26.5.7	Approximation de la binomiale par une Poisson	1436
26.5.8	Loi de Poisson et loi exponentielle	1436
26.5.9	Loi normale	1438
26.5.10	Vecteurs gaussiens	1439
26.5.11	Variable aléatoire de Rademacher	1443
26.5.12	Loi de Student	1445
26.5.13	Indépendance, covariance et variance de somme	1445
26.6	Estimation des grands écarts	1446
26.7	Simulations de réalisations de variables aléatoires	1450
26.7.1	Générateur uniforme	1450
26.7.1.1	Première méthode	1450
26.7.1.2	Seconde méthode	1450
26.7.2	Simulation par inversion	1450
26.7.2.1	Loi exponentielle	1451
26.7.3	Algorithme de Box-Muller	1451
26.7.4	Méthode du rejet	1452
26.7.5	Simuler une loi géométrique à l'ordinateur	1454
26.7.6	Simuler une loi exponentielle à l'ordinateur	1454
26.7.7	Simuler une loi de Poisson à l'ordinateur	1454
26.8	Sage	1455
26.8.1	Loi exponentielle	1455
26.8.2	Inverser des lois	1455
26.9	Monte-Carlo	1456
26.9.1	Intervalle de confiance	1457
26.9.1.1	Principe	1457
26.9.1.2	Échantillonnage préférentiel	1458
26.9.1.3	Méthode de la variable de contrôle	1458
26.9.1.4	Variables antithétiques	1458
26.10	Résultats qui se démontrent avec des variables aléatoires	1459
26.10.1	Nombres normaux	1459
26.10.2	Théorème de Bernstein	1461

27 Statistiques 1465

27.1	Notations et hypothèses	1465
27.2	Modèle statistique	1465
27.3	Modèles d'échantillonnages	1468
27.4	Estimation ponctuelle	1471
27.5	Statistiques et estimateurs	1473
27.5.1	Qualité des estimateurs	1473
27.5.2	Méthode des moments	1474
27.5.3	Méthode de substitution	1476
27.5.4	Méthode du maximum de vraisemblance	1476
27.5.5	Estimation d'une fonction de répartition	1478

27.5.6	Espérance et variance d'un estimateur	1481
27.6	Estimation par intervalle de confiance	1481
27.6.1	Région de confiance	1484
27.6.2	Fonction pivotale	1484
27.6.3	Sondage de proportion	1487
27.7	Estimer une densité lorsqu'on ne sait rien	1488
27.7.1	Distance entre des mesures	1489
27.7.2	Estimateur par fenêtres glissantes	1489
27.8	Test d'hypothèses, prise de décision	1492
27.8.1	Exemple : qualité des pièces d'usine	1492
27.8.2	Exemple : la résistance d'un fil	1492
27.8.3	Vocabulaire et théorie	1493
27.8.4	Risque de première et seconde espèce	1494
27.8.5	Modèle paramétrique de loi gaussienne	1495
27.9	Tests paramétriques	1496
27.10	Tests d'adéquation	1497
28	Chaînes de Markov à temps discret	1503
28.1	Généralités	1503
28.2	Chaînes de Markov sur un ensemble fini	1504
28.3	Marche aléatoire sur $\mathbb{Z}$	1506
28.3.1	Chaînes de Markov homogènes	1508
28.3.2	Graphe de transition	1509
28.3.3	Chaîne de Markov définie par récurrence	1509
28.3.3.1	Le cas général	1509
28.3.3.2	Exemple : la file de réparation de machines à laver	1511
28.4	Classification des états	1511
28.4.1	Chaînes irréductibles	1514
28.4.2	Nombre de visites	1515
28.5	Mesure invariante	1520
28.6	Convergence vers l'équilibre	1522
28.7	Processus de Galton-Watson	1524
29	Martingales	1529
29.1	Convergence de martingales	1529
29.2	Temps d'arrêt et martingale terminée	1532
29.3	Décomposition de martingales	1534
29.4	Problème de la ruine du joueur	1536
29.4.1	Le cas où la pièce est truquée	1537
29.4.1.1	Introduction d'une martingale	1537
29.4.1.2	Finitude du temps d'arrêt	1538
29.4.1.3	Temps moyen de jeu	1538
29.4.1.4	Probabilité de victoire du joueur	1539
29.4.2	Le cas où la pièce est non truquée	1540
29.4.2.1	Probabilité de gagner	1540
29.4.2.2	Temps moyen de jeu	1542
29.4.3	Un petit complément	1542
30	Processus de Poisson	1543
30.1	Processus de Poisson	1543
30.2	Quelques trucs sur la simulation	1546
30.2.1	Le théorème central limite pour Markov	1547
30.2.2	Feuille 5	1547
30.2.3	Feuille 6	1547

30.2.4	Feuille 7	1548
30.2.5	Simuler des lois conditionnelles	1548
31	Utilisation dans les autres sciences	1549
31.1	Démystification du MRUA	1549
31.1.1	Preuve de la formule	1549
31.1.2	Interprétation graphique	1550
31.2	Relativité en mécanique newtonienne	1550
31.2.1	Relativité du mouvement	1550
31.2.2	Bob et Alice	1550
31.3	Invariance de la vitesse de la lumière	1551
31.3.1	Champ de gravitation et électrique	1551
31.3.1.1	Finitude de la vitesse de propagation de la force électrique	1551
31.3.1.2	Pourquoi pas la gravitation ?	1551
31.3.2	Support du champ : pas d'éther	1552
31.3.3	Le problème	1552
31.4	Conséquences	1552
31.4.1	Ligne d'univers	1552
31.4.2	Transformations de Lorentz	1553
31.4.3	Conditions d'existence	1556
31.4.4	La notion d'intervalle	1557
31.4.4.1	En mécanique newtonienne	1557
31.4.4.2	En mécanique relativiste	1557
31.4.5	Le cône de lumière d'un point	1557
31.4.6	Contraction des longueurs	1558
31.4.7	Dilatation des intervalles de temps	1558
31.4.8	Invariance de l'intervalle	1559
31.4.8.1	Rappel de trigonométrie hyperbolique	1560
31.4.8.2	Les transformations de Lorentz (bis)	1562
31.4.9	Vitesse limite	1564
31.5	Applications	1564
31.5.1	Le GPS	1564
31.5.2	Les ondes électromagnétiques	1564
31.6	Mécanique relativiste	1564
31.6.1	Des problèmes, toujours des problèmes	1565
31.6.2	Loi d'addition des vitesses	1565
31.6.3	L'action d'une force	1566
31.6.4	Équivalence entre la masse et l'énergie	1567
31.7	Principe de correspondance	1567
32	Exemples avec Sage	1569
A	GNU Free Documentation License	1589
	Bibliographie	1597
	Liste des notations	1615

Index

- λ -système, 439
- p -Sylow, 752
- p -groupe, 752
- Éther, 1552
- Événement, 1557
- élément
 - primitif, 161
- élémentaire
 - polynôme symétrique, 175
- éléments
 - associés dans un anneau, 130
- équation
 - de Riccati, 1305
 - des classes, 105
 - des orbites, 104
 - différentielle
 - étude qualitative, 1302
 - Hill, 1301
 - homogène, 1304
 - système, 1302
 - diophantienne, 95, 135, 137
 - Fredholm, 1061
 - orbite-stabilisateur, 104
- équation différentielle
 - linéaire du premier ordre, 1315
 - linéaire du premier ordre, homogène, 1315
 - linéaire du second ordre, 1318
 - linéaire du second ordre, homogène, 1318
 - premier ordre, 1310
 - second ordre, 1311
 - variables séparables, 1313
- équation homogène associée, 1315
- équilibre
 - point point une équation différentielle, 1291
- équivalence
 - de norme, 323
- étagée
 - fonction, 470
- état
 - apériodique, 1523
 - récurrent, 1512
 - récurrent positif, 1512
 - transitoire, 1512
- étranger
 - dans leur ensemble, 143
- abélianisé, 87
- Abel
 - angulaire, 885
 - convergence radiale, 1011
- abscisse
 - curviligne, 944
- absolument continue, 877
- absorbant, 1511
- accélération d'un chemin, 930
- accroissement, 662
- accumulation
 - dans $\mathbb{R}$, 261
 - dans espace vectoriel normé, 321
- action
 - adjointe, 103
 - de groupe
 - Wedderburn, 185
 - domaine fondamental, 105
 - fidèle, 103
 - libre, 106
 - transitive, 106
- action de groupe, 290
 - sur des matrices, 1091
- adhérence, 259, 318
- affine
 - application, 512
 - espace, 509
 - sous-espace, 513
- affine (application), 275
- aire, 803
- algébrique
 - extension, 160
 - nombre, 166
 - par rapport à une extension de corps, 172
- algébriquement
 - indépendant, 217
- algèbre, 149
 - de parties, 434
 - engendrée, 149
 - polynômes, 141
- algorithme, 1356
 - consistant, 1356

- convergent, 1356
- facteurs invariants, 139
- fortement consistant, 1356
- stable, 1356
- alterné
 - groupe, 109
 - polynôme, 175
- alternée
 - forme linéaire, 283
- analytique
 - au sens complexe, 1170
- angle
 - d'une courbe, 961
 - entre deux droites, 734
 - entre vecteurs, 306
- Anneau
 - $\mathbb{Z}/n\mathbb{Z}$
 - polynôme cyclotomique, 181
- anneau, 71
 - $\mathbb{Z}/n\mathbb{Z}$, 184, 188, 761, 766
 - à division, 149
 - de séries formelles, 1041
 - euclidien
 - facteurs invariants, 139
 - factoriel, 130
 - intègre, 127
 - noetherien, 133
 - principal, 132, 154, 370
 - utilisation, 156
 - quotient par un idéal, 123
- anneaux
 - de séries formelles
 - utilisation, 1186
- apériodique
 - état d'une chaîne de Markov, 1523
 - chaîne de Markov, 1523
- application
 - affine, 522
 - définie positive, 302
 - de classe C^k , 642
 - différentiable, 606, 608, 639, 642, 1070, 1091
 - extrema lié, 1082
 - en escalier, 795
 - linéaire
 - bornée, 351
 - théorème de Banach-Steinhaus, 1124
 - mesurable, 438
 - multilinéaire, 348
 - ouverte, 346
 - semi-définie positive, 302
 - tangente, 612
- application réciproque, 262
- approximation
 - de fonctions
 - par des polynômes, 1461
 - de l'unité, 1151
 - par polynômes, 1052
 - polynômiale, 1174
- arc
 - géométriques, 943
 - paramétré, 929
- arc cosinus, 683
- arc sinus, 681
- arc tangente, 684
- archimédien, 72
- associé, 130
- associée
 - subdivision, 795
- asymptotiquement pivotale, 1484
- attractif
 - point fixe, 1058
- automorphisme, 272
- axiome
 - du choix, 69
- Bézout
 - anneau principal, 132
 - calcul effectif, 93
 - nombres entiers, 90
 - polynômes, 144
- Baire
 - espace, 266
 - théorème, 258, 267
 - tribu, 432
- Banach
 - espace, 1103
- barycentre
 - cas affine, 515
 - cas vectoriel, 741
 - enveloppe convexe, 519
- base, 269
 - canonique de $\mathbb{R}^m$, 269
 - d'un module, 126
 - de Newton, 1365
 - de topologie, 221
 - dénombrable, 227
 - espace métrique, 227
 - duale, 669, 838
 - espace préhilbertien, 1114
 - hilbertienne
 - utilisation, 1211
 - locale, 988
- Bergman (espace), 1196
- Bernoulli, 1430
 - somme, 1447
- Berry-Esséen (borne), 1429
- Bessel

- inégalité, 1111
- biais
 - d'estimateur, 1474
- bien
 - conditionné, 1333
 - enchaîné, 256
- bijection, 262
- bilinéaire, 348
- binormale, 952
- birégulier
 - point sur une courbe, 941
- birapport, 542
- Bolzano-Weierstrass
 - espaces métriques, 251
- borélienne
 - fonction, 454
 - tribu, 431
- boréliens, 431
- bord, 260
- borné, 221
 - partie de V , 314
 - temps d'arrêt, 1532
- bornée, 241
 - différentielle, 635
 - partie de $\mathbb{R}^m$, 592
 - suite, 235
- boule
 - avec semi-normes, 263
 - fermée, 259, 313
 - ouverte, 221, 259, 313
- Bruhat (décomposition), 723
- Burnside
 - formule, 105
- Cône de lumière, 1557
- canonique
 - base, 269
 - décomposition, 71
 - espace affine, 509
- Cantor
 - ensemble, 501
- caractéristique
 - d'un anneau, 124
 - polynôme, 372
 - sous-groupe, 85
- caractère, 775
 - abélien, 769
 - de S_4 , 783
 - groupe diédral, 784
 - irréductible, 776
- cardioïde, 941
- carré
 - dans un corps fini, 189
- catégorie
 - ensemble de première, 258
- Cauchy
 - critère
 - uniforme, 658
 - déterminant, 292
 - formule, 1170
 - produit, 1009
 - théorème, 752
- Cauchy-Riemann, 1165
- Cauchy-Schwarz, 302, 1104
- Cayley
 - théorème, 752
- cellule d'un pavage, 794
- centrale (application), 776
- centralisateur, 85, 117
- centre
 - d'un anneau, 117
 - d'un groupe, 85
- cercle
 - circonsrit à une courbe, 64, 968
- cercles
 - perpendiculaires, 525
- Cesaro
 - moyenn, 333
- chaîne, 256
 - de Markov, 1503
 - apériodique, 1523
 - convergence, 1524
 - finie, 1504
 - homogène, 1503
 - irréductible, 1509
 - récurrente positive, 1518
 - régulière, 1505
- champ
 - conservatif, 900
 - de vecteurs, 848
- champ dérivant d'un potentiel, 900
- changement de variable, 943
- Chasles, 509
- Chemin
 - classe C^2 , 846
- chemin, 846, 930
 - dans $\mathbb{R}^p$, 929
- circulation, 898
- clôture algébrique, 166
- classe
 - conjugaison
 - dans S_4 , 108
- classe C^1 , 351, 627
- codimension, 272
- coefficient
 - de Fourier, 1201
- coefficients

- de Fourier, 1138
- coefficients binomiaux, 118
- coercion, 1120
- coercive, 1084
- colinéarité, 531
- combinaison
 - convexe, 515
- combinatoire, 750
- commutant, 403
- commutateur
 - dans un groupe, 87
- compacité, 251, 253, 257, 1178, 1193
 - sous-groupes du groupe linéaire, 725
 - théorème de Dini, 658
 - utilisation, 895
 - théorème de Montel, 1195
- compact, 220, 316, 594
 - arc paramétré, 929
 - Bolzano-Weierstrass dans $\mathbb{R}^n$, 245
 - boule unité, 244
 - et fonction continue, 245, 252
 - fermé et borné, 244
 - implique fermé, 230
 - intervalle $[a, b]$, 243
 - le coup du, 876
 - localement, 220
 - opérateur, 1123
 - produit dénombrable, 258
 - produit fini, 257
 - quasi, 220
 - relatif, 1123
 - relativement, 220
 - séquentiellement, 221
 - suite exhaustive, 255
- complément
 - à deux, 1323
- complémentaire, 70
- complété
 - d'un espace métrique, 1099
- complétion
 - projective, 533
- complétude, 1097, 1099, 1132
 - de $\mathbb{R}$, 326
 - espaces L^p , 1134
- complète
 - famille de projecteurs, 126
- complet
 - $\mathbb{R}$, 226
 - corps, 72
 - espace mesuré, 444
 - espace topologique, 223
- composante, 663
- composition
 - suite de, 99
- concave, 647
 - log-concave, 654
- condition initiale, 1312
- conditionnement
 - absolu, 1333
 - d'une matrice inversible, 1336
 - relatif asymptotique, 1356
- conjugués
 - éléments d'une extension, 160
- connexe
 - par arc, 247
- connexité, 257
 - définition, 233
 - et intervalles, 242
 - fonction holomorphe, 1173
 - indice d'une courbe, 1169
 - le groupe $GL^+(n, \mathbb{R})$, 714
 - par arc
 - fonction différentiable, 639
 - points d'accumulation, 253
 - prolongement analytique, 1101
 - signature d'une forme quadratique, 1088
 - théorème de Runge, 1174
 - théorème des valeurs intermédiaires, 570
 - utilisation
 - Brouwer, 1172
- Conservative, 850
- consistance
 - estimateur, 1473
- constructible
 - angle, 212
 - point, 208
 - réel, 208
- construction
 - des réels, 78
- contenu, 129
- continue, 567
 - fonction
 - en un point, 229, 672
 - sur un intervalle, 673
 - fonction entre espaces métriques, 247
 - fonction entre espaces topologiques, 229
 - fonction réelle, 567
 - forme différentielle, 838
 - sur espace métrique, 572
 - uniformément, 592
- continuité, 553
 - fonction définie par une intégrale, 874
 - séquentielle, 248
 - sur un intervalle, 567
- contraction, 1058
- convergence

- absolue, 327
- commutative, 338
- dans un espace vectoriel normé, 325
- de martingales, 1533
- de suite, 220
- en loi, 1420
- en norme, 657
- en probabilité, 1420
- normale, 327
- ordre, 1353
- presque sûrement, 1419
- quadratique, 1342
- rapidité, 765, 1220, 1221, 1351, 1447
- série, 326
- suite
 - dans un corps, 72
 - suite dans $\mathbb{R}^m$, 261
 - suite numérique, 234, 1052, 1212
 - Abel angulaire, 885
 - uniforme, 657
 - intégrale, 872
 - série de fonctions, 327
 - suite de fonctions, 657
 - théorème de Dini, 658
- convergent
 - estimateur, 1473
- convexité
 - barycentre, 517
 - enveloppe de $O(n)$, 722
 - fonction, 647
 - inégalité de Jensen, 655
 - locale, 1156
 - méthode de Newton, 1348
 - stricte, 647
 - utilisation, 895
- convolution, 1399, 1526
- coordonnées
 - barycentriques, 521
 - cartésiennes
 - dans un espace affine, 521
 - curvilignes, 988
 - cylindrique, 426
 - dans un espace affine, 510
 - homogène, 538
 - sphériques, 426
- corps, 71
 - archimédien, 72
 - complet, 72
 - de décomposition, 166
 - de rupture, 164
 - polynôme cyclotomique, 181
 - des fractions, 151
 - des fractions rationnelles
 - utilisation, 1186
 - extension, 169, 176
 - fini, 188, 192, 195
 - Wedderburn, 185
 - ordonné, 72
 - premier, 151
- cosinus
 - angle entre deux vecteurs, 306
 - hyperbolique, 685
- courbe, 930
 - étude métrique, 1211
 - de Jordan, 978, 1210
 - efficacité, 1494
 - fermée, 958
 - simple, 958
- courbe de niveau, 628, 631
- courbure, 952
 - signée, 959
 - totale, 960
- covariance, 1402
- critère
 - Abel, 1007
 - Abel pour intégrales, 873
 - Cauchy
 - uniforme, 658
 - de Cauchy, 326
 - série alternée, 331
 - Weierstrass, 873
 - série de fonctions, 1004
- critique
 - Galton-Watson, 1526
 - point, 1080
 - point d'un arc, 941
 - région, 1493
 - valeur, 1494
- cyclique
 - endomorphisme, 368
 - groupe, 85
 - matrice, 368
- cycloïde
 - coordonnées normales, 946
 - longueur, 940
- décalage, 1325
- décimale
 - décomposition, 336
- décomposition
 - Bruhat, 723
 - canonique, 71
 - corps, 166
 - Dunford, 388
 - application, 391
 - exponentielle de matrice, 389
 - Jordan

- et exponentielle de matrice, 389
 - polaire, 719
 - primaire, 387
 - sous-espaces caractéristiques, 387
 - spectrale, 387
- dénombrable, 71
 - à l'infini, 221
- dénombrement, 750
 - partitions de $\{1, \dots, n\}$, 1041
- dérivé
 - groupe, 87
- dérivée, 581
 - au sens de distributions, 1261
 - dans Sobolev $H^1(I)$, 1261
 - directionnelle, 601, 604
 - distributionnelle, 1240
 - faible, 1235
 - fonction à valeurs dans E' , 266
 - partielle, 600, 602, 662
 - seconde, 581, 675
- dérivabilité
 - fonction définie par une intégrale, 876
 - lemme de Borel, 1044
- dérivable, 582, 675
 - au sens complexe, 999
 - fonction, 581, 1279
- dérivation
 - au sens des distribution
 - Sobolev, 1265
- déterminant, 283
 - Cauchy, 1055
 - d'un endomorphisme, 288
 - d'une famille de vecteurs, 286
 - de Cauchy, 292
 - et inversibilité, 288
 - forme linéaire alternée, 283
 - Gram, 292, 1055
 - interprétation géométrique, 820
 - résultant, 293, 889
 - utilisation, 895
 - Vandermonde, 289
- développable
 - en série entière, 1028
- développement
 - asymptotique, 694
 - limité
 - en zéro, 686
 - fonction holomorphe, 1165
 - premier ordre, 587
 - Taylor, 1091
- degré
 - application $S^1 \rightarrow S^1$, 962
 - d'une représentation, 769
 - extension de corps, 161
- dense
 - nulle part, 258
- densité, 1099
 - conjointe, 1398
 - d'une variables aléatoire, 1394
 - dans un espace de fonction
 - critère de Weyl, 1212
 - de $\mathbb{Q}$ dans $\mathbb{R}$, 226
 - utilisation, 653
 - de $GL(n, \mathbb{R})$ dans $M(n, \mathbb{R})$, 715
 - de $\mathcal{D}(\mathbb{R}^n)$ dans $L^1(\mathbb{R}^n)$, 1162
 - de $C_c^\infty(\mathbb{R}^d)$ dans $L^p(\mathbb{R}^d)$, 1140
 - de $L^2([0, 1])$ dans $L^p([0, 1])$, 1142
 - de $S^+(n, \mathbb{R})$ dans $S^{++}(n, \mathbb{R})$, 719
 - des fonctions étagées dans L^p , 1140
 - des polynômes
 - dans $C_c^0[0, 1]$, 1461
 - des polynômes trigonométriques dans $L^p(S^1)$, 1154
 - matrices diagonalisables dans $M(n, \mathbb{C})$, 715
 - mesure, 63, 483
 - points extrémaux dans $\mathcal{L}$, 721
 - prolongement, 1097
- densité d'une mesure, 792
- diédral, 751
- diagonalisable, 378
 - et polynôme minimum scindé, 378
 - exponentielle, 391
- diagonalisation
 - cas complexe, 382
 - cas réel, 384
 - endomorphisme auto-adjoint, 422
 - simultanée, 380
- diamètre, 592
- difféomorphisme, 355, 835, 913
 - de classe C^k , 642
- différence
 - divisée, 1366
- différentiabilité, 639
- différentiable, 611
 - dans un Banach, 350
 - deux fois, 641
 - sur un ouvert, 616
- différentielle, 351, 606
 - de $u \mapsto u^{-1}$, 360
 - partielle, 356
 - totale, 662
- dilatation, 708
- dilatation (matrice), 138
- dimension, 271
 - n -formes multilinéaires alternées, 283
 - définition, 271

- sous espace affine, 513
- utilisation, 519
- direction, 601, 949
 - sous-espace affine, 513
- Dirichlet
 - noyau, 1202
 - théorème, 1202
 - théorème (sur les nombres premiers), 184
- disque de convergence, 1007, 1008
- distance, 221
 - associée à une norme, 224
 - entre deux mesures de probabilités, 1489
 - point et ensemble, 250
- distingué, 85
- distribution, 1238
 - équation de Schrödinger, 1307
 - de Dirac, 1244
 - produit par une fonction, 1240
 - tempérée, 1244
- divergence, 665
- diviseur
 - de zéro, 127
 - de zéro à droite, 127
 - polynôme, 143
- division
 - euclidienne, 90, 143
- domaine, 672
 - fondamental d'une action, 105
- dominé
 - modèle statistique, 1472
- dominée
 - convergence (Lebesgue), 482
 - mesure, 790
- droite
 - projective, 531
- dual, 278
 - d'un espace de Hilbert, 1109
 - de $M(n, \mathbb{K})$, 282
 - de $L^p(\Omega)$, 1150
 - de L^p , 1145
 - de $L^p([0, 1])$ avec $1 < p < 2$, 1143
 - espaces L^p , 1142
 - topologique, 278
- Dunford
 - décomposition, 388
- dyadique, 504
- écart-type, 1401
- échantillon, 1466, 1468
- effectif
 - empirique, 1497
- efficacité
 - courbe, 1494
 - d'une méthode itérative, 1360
- élément
 - de surface, 858
 - de torsion, 115
- élément de surface, 840
- ellipsoïde, 421
- endomorphisme, 272
 - auto-adjoint, 422
 - cyclique, 368
- décomposition
 - polaire, 719
- diagonalisable, 413, 717, 1302
 - Dunford, 388
- diagonalisation, 384
- nilpotent
 - Dunford, 388
- préservant une forme quadratique, 728
- sous-espace stable, 388, 1302
- engendré, 131
 - λ -système, 439
 - corps et anneau, 161
 - idéal dans un anneau, 131
 - sous-espace affine, 514
 - sous-groupe, 85
 - tribu, 430
 - par une variable aléatoire, 1395
- ensemble
 - de Cantor, 501
 - différence symétrique, 70
 - infini, 69
- entrelacement, 776
- enveloppe
 - convexe, 517
- équation
 - différentielle
 - linéaire, 1281
 - ordinaire d'ordre 1, 1279
 - variables séparées, 1283
 - générale de degré n , 218
- équicontinuité, 1123
- équi-intégrable, 1533
- équivalence
 - arcs paramétrés, 943
 - chemin, 937
 - classe de fonctions, 1126
 - de représentations, 776
 - de suites, 326
 - homotopie, 1169
 - norme, 323
 - relation, 70
 - suite de composition, 100
- erreur, 1367, 1390
 - assignation, 1328
 - quadratique, 1370

- troncature, 1328
- erreur relative, 1327
- escalier, 470
- espérance, 1400
 - conditionnelle, 1404, 1409
 - événement, 1410
 - événements, 1410
 - variable aléatoire, 1409
- Espace
 - de Sobolev, 1268
- espace
 - L^2
 - Sobolev, 1265
 - L^p , 1127
 - affine, 509
 - canonique, 509
 - Banach, 1103
 - complet, 1099
 - $C_b^0(X, Y)$, norme uniforme, 1057
 - $\mathcal{D}(K)$, 1237
 - $\mathcal{S}(\Omega)$, 1254
 - de Baire, 266
 - de Bergman, 1196
 - de fonctions
 - L^p , 1134
 - Sobolev H^1 , 1265
 - de Hilbert
 - espace de Sobolev H^1 , 1265
 - de probabilité, 1393
 - de Schwartz, 1160, 1244
 - de Sobolev, 1261, 1269
 - euclidien, 306
 - métrique, 221
 - base de topologie, 227
 - mesuré, 436
 - complété, 447
 - mesurable, 429
 - projectif, 531
 - propre, 375
 - tangent, 1095
 - topologique, 232
 - métrisable, 247
 - vectériel
 - dimension, 283
- espace vectoriel
 - topologique, 222
- estimateur, 1473
 - biais, 1474
 - consistant, 1473
 - convergent, 1473
 - de fonction de répartition, 1479
 - maximum de vraisemblance, 1476
- estimation
 - des grands écarts, 1447
- étrangers
 - polynômes, 143
- Euclide
 - algorithme étendu, 92
 - lemme, 94
- euclidien
 - anneau, 133
 - espace, 303
- Euler
 - indicatrice, 122
- événement, 1393
- exact
 - intervalle de confiance, 1482
- excès
 - intervalle de confiance, 1482
- exhaustive (suite de compacts), 255
- exponentielle, 1019
 - complexe, 1189
 - convergence, 333
 - de matrice, 337, 389, 391, 1038
 - utilisation, 1078
 - existence, 1017
 - rapide, 768
 - unicité, 1018
- exposant, 413, 758
 - d'un groupe, 86
- extension
 - corps de base, 393
 - de corps, 160, 176
 - algébrique, 160, 165
 - finie, 196
 - monogène, 161
 - simple, 161
 - utilisation, 213
 - isométrie, 1098
- extrémal
 - point dans un convexe, 721
- extrémité
 - d'un intervalle, 241
- extrapolation, 1365
- extrema, 1081
 - lié, 1082
 - local
 - relatif, 1081
 - volume d'un ellipsoïde, 895
- extremum, 1091
- facteur
 - intégrant, 1306
- factoriel
 - anneau, 130
- factorisation
 - de polynôme, 146, 163

- faisceau de droites, 539
- famille
 - sommable, 340
- Fatou, 481
- Fejér
 - noyau, 1202
- fermé, 219, 260, 316
 - dans un compact, 230
- fermeture, 318
 - séquentielle, 249
- fidèle (action), 103
- filtration, 1529
- fine
 - subdivision, 932
- fixateur, 102
- flux
 - d'un champ de vecteur, 865
- flux d'un champ de vecteurs, 862
- fonction, 672
 - Γ d'Euler, 1183
 - étagée, 1140
 - à décroissance rapide, 1160
 - borélienne, 454
 - caractéristique, 797
 - d'une variable aléatoire, 1415
 - continue
 - égales, 250
 - par morceaux, 473
 - convexe, 647, 653
 - croissante, 672
 - décroissante, 672
 - définie par une intégrale, 874, 879, 1044, 1193
 - Γ d'Euler, 1183
 - utilisation, 1435
 - de classe $\mathcal{C}^1$, 635
 - de Dirichlet, 1205
 - de Möbius, 206
 - de répartition, 1415
 - différentiable, 1081
 - en escalier intégrable, 796
 - génératrice, 1417
 - holomorphe, 999, 1193
 - théorème de Montel, 1195
 - image, 672
 - méromorphe
 - Γ d'Euler, 1183
 - monotone, 672
 - par morceaux, 473
 - valeurs vectorielles, 663
- fondamental
 - domaine d'une action, 105
- forme
 - bilinéaire, 302
 - non dégénérée, 419
- différentielle, 838
 - exacte, 882
 - fermée, 882
- linéaire
 - différentielle, 1082
- quadratique, 417, 744, 1088, 1090, 1091
 - groupe orthogonal, 728
 - matrice associée, 417
- forme canonique
 - fonction simple, 470
- forme linéaire
 - alternée, 283
- formule
 - Bayes, 1403
 - Burnside, 105
 - d'expulsion (produit vectoriel), 313
 - de Cauchy, 1170
 - Hadamard, 1008
 - inversion Möbius, 206
 - probabilité totales, 1403
 - sommatoire de Poisson, 1220
 - Stirling, 326
 - Taylor
 - reste intégral, 646
 - utilisation, 1351
- Fourier, 1220
 - série
 - utilisation, 1211
 - transformée
 - groupe abélien fini, 771
- fréquence
 - empirique, 1497, 1515
- fraction
 - rationnelle
 - intégration, 889
- fraction rationnelle, 923
- fractions (corps), 151
- Fredholm
 - équation, 1061
- Frenet
 - formules, 953
- Fresnel
 - intégrale, 1191
- Frobénius
 - réduction, 400
- Frobenius
 - morphisme, 125
- frontière, 260, 320
- Fubini
 - théorème
 - dans $\mathbb{R}^n$, 820
- générateur, 85, 269

- génératrice
 - partir d'un module, 126
- géométrie
 - avec des groupes, 545, 745
 - avec nombres complexes, 545, 745
- géométrique
 - avec des nombres complexes, 1211
- Galton-Watson
 - sous-critique, 1526
 - sur-critique, 1526
- Gauss
 - lemme
 - polynômes, 152
 - somme de, 190
- Grönwall (lemme), 1279
- gradient, 607, 617, 626
- Gram (déterminant), 292
- Gram-Schmidt, 306
- graphe, 584, 672
 - de transition (chaîne de Markov), 1509
 - fonction, 628
 - fonction de deux variables, 630
- groupe
 - p -groupe, 752
 - $GL(n, \mathbb{R})$, 1090
 - action, 545
 - utilisation, 728
 - agissant sur un ensemble
 - diédral, 744
 - alterné, 109
 - dérivé, 87
 - de $GL(n, \mathbb{K})$, 713
 - de $SL(n, \mathbb{K})$, 713
 - du groupe alterné, 111
 - du groupe symétrique, 109
 - de Galois, 217
 - de permutation, 784
 - caractères de S_4 , 783
 - de permutations, 750
 - de torsion, 115
 - des isométries
 - espace métrique, 222
 - des symétries, 742
 - diédral, 744, 751
 - générateurs (preuve), 745
 - générateurs (utilisation), 784
 - en géométrie, 744
 - et géométrie, 283, 545, 750
 - isométries du cube, 113
 - fini, 185, 188, 750, 754, 761, 766
 - alterné, 110
 - diédral, 744
 - Wedderburn, 185
 - linéaire, 723
 - décomposition polaire, 719
 - enveloppe convexe de $\Omega(n)$, 722
 - hyperplan, 283
 - sous-groupes compacts, 725
 - modulaire, 544
 - orthogonal, 297
 - d'une forme quadratique, 728
 - partie génératrice, 110, 545, 766
 - permutation, 283, 290, 723, 766
 - diédral, 744
 - projectif, 537
 - quotient, 98
 - résoluble, 101
 - spécial orthogonal, 298
 - symétrique, 106
 - action sur un triangle, 773
- groupe dérivé
 - de $GL(n, \mathbb{C})$, 707
- Hadamard
 - formule, 1008
- Hardy-Littlewood (théorème), 1052
- Hausdorff, 220
- Heine (théorème), 593
- hermitien
 - produit scalaire, 376
- hessienne, 644
- Hilbert, 1103
- holomorphe, 999
- homéomorphisme, 228
- homogène
 - chaîne de Markov, 1503
- homographie, 536, 545
- homotopie, 964
- hyperplan, 738
 - de $M(n, \mathbb{K})$, 283
- sépare
 - au sens strict, 1156
- séparer
 - au sens large, 1156
- hypothèse
 - alternative, 1493
 - composite, 1493
 - multiple, 1493
 - nulle, 1493
 - simple, 1493
- idéal
 - bilatère, 123
 - dans un anneau, 71
 - maximal, 131
 - maximum, 172
 - principal

- à droite, 131
- à gauche, 131
- identifiable, 1472
- identité
 - polarisation, 417
- image, 672
- inégalité
 - arithmético-géométrique, 656
 - Bessel, 1111
 - Cauchy-Schwarz, 302, 1104
 - de Khintchine, 1444
 - de la moyenne, 639
 - des pentes, 648
 - Hölder, 1129
 - utilisation, 1401, 1462
 - isopérimétrique, 1211
 - Jensen, 655
 - espérance conditionnelle, 1415
 - pour une somme, 655
 - version intégrale, 1129
 - Kantorovitch, 656
 - Markov, 1424
 - Minkowski, 1131
 - triangulaire, 221, 223
 - produit scalaire, 303
- incompressible
 - champ de vecteur, 667
- indécomposable
 - module, 126
- indépendance, 1397
 - événements, 1394
 - utilisation, 1459, 1536
 - affine, 520
 - algébrique, 217
 - sous tribus, 1394
 - variables aléatoires, 1395
- indicatrice d'Euler, 122
- indice, 96
 - d'une courbe dans $\mathbb{C}$, 1169
 - de rotation, 963
- inductif, 69
- induite
 - topologie, 317
 - tribu, 430
- inférence statistique, 1465
- infimum, 238
- injection, 262
- intégrable, 474
 - fonction non en escalier, 802
 - fonction positive, 807
- intégrale
 - calcul, 1212
 - convergente, 813, 889
 - d'une fonction sur une carte, 841
 - d'une fonction sur une variété, 846
 - d'une forme différentielle, 849
 - fonction en escalier, 796
 - fonction sur un intervalle, 811
 - Fresnel, 1191
 - impropre, 812, 813
 - sur un chemin, 846
- intégration
 - fraction rationnelle, 889
- intérieur, 259
 - d'un ensemble, 315
 - point, 315
- intègre
 - anneau, 127
- interpolation, 1365
- Intervalle, 1557
- intervalle, 241, 672
 - fermé, 672
 - longueur, 492
 - ouvert, 672
- intervalle de confiance
 - asymptotique, 1486
- invariant
 - de similitude, 400
- invariante
 - mesure
 - pour une chaîne de Markov, 1520
- inverse généralisé, 1451
- inversion, 526
 - dans le groupe symétrique, 107
- involution, 380
- irréductible
 - chaîne de Markov, 1509
 - dans un anneau, 130
 - module, 126
 - polynôme, 142
 - représentation, 773
- irrationalité
 - $\sqrt{2}$, 75
- isobarycentre, 515
- isolé
 - élément de $\mathbb{R}$, 261
 - point dans un espace vectoriel normé, 321
- isométrie
 - d'espaces métriques, 222
 - de forme quadratique, 729
 - de l'espace euclidien $\mathbb{R}^2$, 745
 - espace euclidien
 - isométries du cube, 113
 - groupe, 222
- isomorphisme
 - $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, 188

- d'espaces topologiques, 228
- espace affine, 513
- isotrope
 - cône, 420
 - totalement, 420
- isotrope (vecteur), 420
- jacobien, 626, 664
- Jordan
 - chemin, 865
 - courbe, 1210
 - réduction, 402
- Jordan-Hölder, 99
- Kronecker, 269
- lacet, 1169
- Lagrange
 - multiplicateur, 1082
 - polynôme, 281
- lagrangien, 1082
- Laplace
 - transformée, 1417
- Laplacien, 994
- Legendre
 - symbole, 189
- Leibnitz, 584, 586
 - applications entre espaces vectoriels normés, 356
- lemme
 - Borel, 1044
 - d'Euclide, 94
 - de Borel-Cantelli, 1423
 - de Gauss
 - contenu de polynôme, 129
 - pour des entiers, 94
 - de Morse, 1091
 - de Schreider, 100
 - de Slutsky, 1421
 - de transfert, 455
 - de Zorn, 69
 - des noyaux, 364
 - Fatou, 481
 - Gauss
 - dans un anneau principal, 133
 - polynômes, 152
 - Grönwall, 1279
 - Hadamard, 881
 - regroupement, 1397
 - Schur complexe, 381
 - Schur réel, 383
- Levi-Civita, 989
- libre, 269
 - action, 106
 - partie, 269
 - partie d'un module, 126
- Ligne d'univers, 1553
- limite, 344
 - d'ensembles, 438
 - d'une fonction, 228
 - de fonctions holomorphes, 1193
 - de suite
 - espace topologique, 220
 - fonction, 228, 551
 - fonction de plusieurs variables, 553
 - inférieure, 463, 464
 - inversion, 1041, 1052, 1127, 1193
 - permutation
 - utilisation, 1417
 - suite, 325
 - suite dans $\mathbb{R}^m$, 261
 - suite numérique, 234
 - supérieure, 463, 464
 - unicité, 229
- linéaire (application), 272
- Lipschitz, 1058
 - localement, 640
- Lipschitzienne, 639
- localement
 - intégrable, 812
- log-concave, 654
- logarithme, 679, 1020
 - de matrice, 1038
- loi
 - χ^2 , 1445
 - binomiale
 - comportement asymptotique, 1447
 - conjointe, 1397
 - d'une variable aléatoire, 1418
 - de Poisson, 1432
 - des grands nombres
 - forte, 1425
 - pour les chaînes de Markov, 1522
 - processus de Poisson, 1544
 - utilisation, 1447, 1459
 - marginale, 1397
 - normale
 - vecteur gaussien, 1439
 - parente, 1465, 1466
 - parente d'un échantillon, 1468
 - réciprocité quadratique, 192
 - sans mémoire, 1434
 - Student, 1445
- Lokta-Volterra, 1295
- longueur
 - élément de, 939
 - arc géométrique, 944

- d'un arc paramétré compact, 932
- d'un intervalle, 492
- d'une arrête, 794
- longueur d'arc, 934
- méromorphe, 1182
- Méthode
 - de Newton, 1346
- méthode
 - des chemins, 561
 - Newton, 1351
 - cas convexe, 1348
- métrique
 - discrète, 222
- maigre, 431
- maigre (ensemble), 258
- majorant, 236, 237
 - essentiel, 1128
- Markov
 - inégalité, 1424, 1471
- martingale, 1529
 - bornée dans $L^2(\Omega)$, 1530
- matrice, 545, 723
 - équivalence, 273
 - dans le groupe linéaire, 728
 - associée à une forme quadratique, 417
 - compagnon, 399
 - creuse, 1371
 - cyclique, 368
 - de dilatation, 138
 - de permutation, 138
 - de similitude, 999
 - de Sylvester, 292
 - de transition, 1503
 - de transvection, 138
 - dense, 1371
 - hermitienne
 - racine carré, 717
 - jacobienne, 617, 626
 - normale, 707
 - orthogonale, 297
 - permutation
 - élémentaire, 1377
 - racine carré, 717
 - semblable, 717
 - semblables, 744, 1090
 - stochastique, 1503
 - symétrique, 1090
 - réelle, 1088
 - trigonalisable, 411
- matrices
 - similitude, 273
- maximal
 - idéal, 131
- maximum, 237, 239
 - global, 1080
 - local, 1080
- mesurable
 - application, 438
 - au sens de m^* , 443
 - ensemble, 436
 - fonction, 454
 - Lebesgue, 792
- mesure
 - σ -finie, 436
 - absolument continue, 790
 - complexe, 791
 - dans une carte, 840
 - de Borel, 460
 - de comptage, 437, 819
 - de Haar, 1065
 - de Lebesgue, 495
 - de Radon, 460, 1179
 - extérieure, 433
 - externe, 792
 - finie, 436
 - sur algèbre de partie, 434
 - image, 457
 - positive, 436
 - probabilité, 1393
 - produit, 489
 - régulière, 460
 - extérieure, 460
 - intérieure, 460
 - sur algèbre de partie, 434
- minimum, 239
- minorant, 237
- modèle
 - échantillonnage, 1466, 1468
 - paramétrique, 1466
 - statistique, 1465
- modulaire (groupe), 544
- module
 - de continuité, 1096
 - indécomposable, 126
 - irréductible, 126
 - simple, 126
 - sur un anneau, 125
- moment, 1400
 - fonction génératrice, 1417
- monôme, 141
- monogène, 85
 - extension de corps, 161
- monotonie, 1300
- morceau
 - fonction continue ou monotone, 473
- morphisme

- d'algèbres, 149
- d'anneaux, 117
- Frobenius, 125
- moyenne
 - de Cesaro, 333
 - empirique, 1402
 - empirique d'un échantillon, 1469
 - quadratique, 1401
- multiplicateur
 - de Lagrange, 1082
- multiplicité
 - racine d'un polynôme, 145
 - racine de $f(x) = 0$, 1345
 - valeur propre
 - algébrique, 373
 - géométrique, 373
- négatif, 81
- négligeable
 - partie d'un espace mesuré, 444
- nabla, 625
- Newton
 - méthode, 1351
- nilpotent, 125
- niveau de confiance, 1482
- nombre
 - complexe
 - norme 1, 185
 - dénormalisé, 1326
 - de Fermat, 213
 - de Néper, 1019
 - normal, 1459
 - normalisée, 1326
 - premier, 154, 184, 188, 757, 761, 765, 766
 - dans leur ensemble, 90
 - deux nombres entre eux, 90
 - théorème des deux carrés, 156
 - tours d'une courbe plane, 962
- nombre premier
 - polynôme cyclotomique, 181
- non dénombrable, 71
- normé
 - espace vectoriel, 223
- normal
 - arc paramétré, 944
 - endomorphisme, 707
 - nombre, 1459
 - sous-groupe, 85
- normal extérieur
 - vecteur, 864
- normale
 - loi réduite, 1438
 - principale, 952
- normalisateur, 85
- norme, 307
 - équivalence, 323
 - d'algèbre, 309
 - d'application linéaire, 308
 - d'une application linéaire, 308
 - définition, 223
 - euclidienne, 301
 - dans $\mathbb{R}^m$, 425
 - opérateur, 309
 - subordonnée, 309
 - supremum, 301
 - vecteur, 304
- noyau
 - d'une forme bilinéaire, 420
 - Dirichlet, 1202
 - Fejér, 1202
- nulle part dense, 258
- observation, 1393
- opérateur
 - adjoint, 377
 - autoadjoint, 377
 - définit positif, 384
 - hermitien, 377
 - linéaire
 - borné, 351
- opérateurs
 - compatibles, 1119
- opposés
 - chemins, 937
- ordre, 69
 - élément, 86
 - d'un groupe, 86
 - d'un polynôme, 197
 - dans un corps, 72
 - distribution, 1241
 - sur un anneau factoriel, 130
 - total, 69
- orientable
 - variété, 843
- orientation, 842
- origine
 - abscisse curviligne, 944
 - repère affine, 521
- orthogonal, 424, 1107
 - coordonnées curviligne, 988
 - famille de projecteurs, 126
 - matrice, 297
 - sous-espace, 278
 - vecteur, 304
- orthonormé, 425
 - système, 1110
- oscillation
 - d'une fonction, 587

- d'une fonction en un point, 587
- osculateur (cercle), 957
- ouvert, 219, 241, 260, 316
 - dans $\mathbb{R}^n$, 259
- parallèle
 - sous-espaces affines, 513
- paramétrages
 - admissible, 943
- paramétrisation, 938
 - normale, 944
- Parseval, 1114
- partie
 - régulière, 686
 - totale, 1110
- partie génératrice, 85
- partition
 - d'un entier en parts fixées, 1186
 - dénombrable mesurable, 466
 - de l'unité, 845
- pavé, 792, 793
- pavable, 793
- Pearson
 - theoreme, 1498
- peigne de Dirac, 1250
- permutation
 - matrice, 138
- permuter
 - dérivée et intégrale
 - $\mathbb{R}^n$, 879
 - dans $\mathbb{R}$, 876
 - dans $\mathbb{R}$ avec les bornes, 878
 - dérivée et limite, 659
 - différentielle et intégrale
 - $\mathbb{R}^n$, 880
 - intégrale
 - et série, 819
 - limite et intégrale, 874
 - convergence dominée, 482
 - convergence monotone, 479
 - espace mesuré, 874, 875
 - série entière et dérivation, 1013
 - série entière et intégration, 1013
 - somme et intégrale, 480, 1004
- petit théorème de Fermat, 153
- PGCD
 - dans un anneau intègre, 128
 - polynômes, 144
- pgcd, 117
 - calcul effectif, 92
- pivotale, 1484
- plan
 - projectif, 531
 - tangent, 626, 662
- Plancherel, 1114
- plongement, 1097
- Poincaré (demi-plan), 544
- point
 - d'équilibre
 - stable, 1291
 - pondéré, 515
- point critique
 - définition, 1093
- point fixe, 1526
 - attractif, 1058
 - Brouwer, 1061
 - Picard, 1059
 - Schauder, 1063
- Poisson
 - formule sommatoire, 1220
 - processus, 1543
- polarisation (identité), 417
- polynôme
 - à plusieurs indéterminées, 195, 295
 - alterné, 175
 - annulateur, 364, 367
 - caractéristique, 372, 382
 - contenu, 129
 - cyclotomique, 179
 - irréductibilité, 181
 - propriétés, 180
 - d'endomorphisme, 717
 - décomposition de Dunford, 388
 - de Bernstein, 1461
 - irréductible, 142
 - séparable, 168
 - sur $\mathbb{F}_q$, 207
 - Lagrange, 281
 - minimal, 163, 366
 - d'un élément d'une extension, 160
 - ponctuel, 367
 - primitif, 197
 - primitif (au sens du contenu), 129
 - racines, 176
 - séparable, 168
 - scindé, 143
 - semi-symétrique, 175
 - symétrique, 175, 176, 195, 290, 295
 - élémentaire, 175, 178
 - trigonométrique, 1153
- portée
 - mesure, 790
- positif, 80
- potentiel, 853, 900
- PPCM
 - dans un anneau intègre, 128
- précision

- simple, 1325, 1326
- préhilbertien, 1103
- premier
 - corps, 151
 - deux éléments d'un anneau principal, 132
 - deux polynômes entre eux, 143
 - idéal, 131
 - sous corps, 151
- premier temps d'atteinte, 1511
- premier type
 - région solide, 805
- presque
 - nulle, 115
 - partout, 438
 - surjective, 1156
- primitif
 - élément d'un corps, 188
 - élément d'une extension de corps, 161
 - polynôme, 143, 197
 - racine, 200
- primitive, 581, 811, 897
 - de fonction continue, 1049
 - et intégrale, 809, 814
 - fonction, 599
- principal
 - anneau, 131
 - idéal, 131
- principe
 - prolongement analytique, 1101
 - zéros isolés, 1173
- Principe de correspondance, 1568
- probabilité
 - conditionnelle, 1403
- problème de Cauchy, 1312
- processus
 - adapté à une filtration, 1529
 - arrêté, 1534
 - croissant prévisible, 1534
 - Galton-Watson, 1524
 - Poisson, 1543
 - sans mémoire, 1434
- produit
 - d'espaces vectoriels normés, 344
 - d'une mesure par une fonction, 63, 483
 - de Cauchy, 1009
 - de convolution, 1139
 - et Fourier, 1217
 - distribution et fonction, 1240
 - espaces mesurés, 491
 - espaces topologiques, 220
 - mixte, 313, 823
 - scalaire
 - en général, 302
 - hermitien, 376
 - sur $M(n, \mathbb{R})$, 311
 - sur $\mathbb{R}^n$, 423
- semi-direct, 112
- tensoriel
 - de représentations, 782
- vectorel, 312, 822
- produit remarquable, 1176
- projecteur
 - dans un module, 126
- projectif
 - complétion, 533
 - droite, 531, 533
 - espace, 531
 - groupe, 537
 - hyperplan, 532
 - plan, 531
 - repère, 541
 - sous-espace, 531
- projection
 - orthogonale, 1106
- prolongement
 - analytique, 1101
 - utilisation, 1195
 - de fonctions, 1097
 - lemme de Borel, 1044
 - méromorphe de la fonction Γ , 1183
 - par continuité, 579, 673
 - dans $H^1(I)$, 1264
 - par densité, 1097
 - théorème de Hahn, 452
- propriété d'intersection non vide, 230
- puissance
 - d'un point, 525
 - d'un test, 1494
- quasi-compact, 220
- quaternion, 171
- quotient, 90, 143
 - dans une suite de composition, 99
 - de groupe, 98
 - de groupes, 761
- réciroque
 - continuité, 262
 - dérivabilité, 585
- récurrent
 - état, 1512
 - nul, 1512
 - point d'un système dynamique, 462
 - positif, 1512
- réduction
 - d'endomorphisme, 388
 - Frobénius, 400

- Jordan, 402
- réel, 78
- réflexif, 1149
- réflexion, 732
 - glissée, 736
 - par rapport à un hyperplan, 738
- région
 - critique, 1493
 - de confiance exact, 1484
 - de rejet, 1493
- régularité
 - d'une mesure, 460
 - extérieure de la mesure de Lebesgue, 498
 - intérieure de la mesure de Lebesgue, 500
- régulière
 - surface, 854
- régulier
 - arc, 941
 - chemin, 865
 - point d'un arc, 941
- régulier à droite, 117
- répulsif
 - point fixe, 1058
- résidu
 - méthode itérative, 1390
- résolvante, 1288
- résultant, 293
 - utilisation, 295, 889
- règle
 - du produit nul, 127
- Règle de Leibnitz, 586
- racine
 - carré
 - de matrice hermitienne, 717
 - carré de matrice
 - hermitienne positive, 717
 - de l'unité, 119, 181, 184, 413, 545, 745
 - primitive, 121
 - utilisation, 180
 - de polynôme, 163
 - multiple, 1345
 - primitive, 200
 - simple, 1345
- racine carré, 570
- raffinement, 932
 - subdivision d'un pavé, 794
- rang, 272, 283, 744
 - classe d'équivalence, 273
 - diagonalisation, 384
 - différentielle, 1082
 - utilisation, 1109
- rare, 431
- rayon
 - de convergence, 1007
 - de courbure, 952
 - de torsion, 953
 - spectral, 309, 389
- recouvrement, 594
- rectangle
 - produit de tribus, 484
- rectifiable, 932
 - arc géométrique, 944
- rejet
 - région dans une prise de décision, 1493
- relèvement, 962
- relations
 - coefficient-racines, 178
 - de Chasles, 509, 916
- relativement
 - compact, 220, 1123
- repère
 - affine, 520
 - cartésien
 - espace affine, 509
 - de Frenet, 952
 - projectif, 541
- Représentation
 - virgule flottante normalisée, 1324
- représentation, 772
 - de groupe fini
 - caractères de S_4 , 783
 - fidèle, 769
 - groupe diédral, 784
 - irréductible, 773, 774
 - produit tensoriel, 782
 - régulière gauche, 778
 - virgule fixe, 1324
- reste, 90, 143
 - d'un développement limité, 686
- risque
 - première espèce, 1494
 - quadratique, 1473
 - seconde espèce, 1494
- rupture
 - corps, 164
- séparé, 220
 - espace topologique, 220
- séparable, 1110
 - élément d'une extension, 170
 - espace topologique, 220
 - extension de corps, 170
 - polynôme irréductible, 168
 - polynôme non constant, 168
- sépare
 - les points, 1047
- série

- dans un espace vectoriel normé, 326
 - de Fourier, 1206, 1220
 - utilisation, 1211
 - de Laurent, 1182
 - de puissance, 1007
 - divergence, 326
 - donnant $(1 - A)^{-1}$, 328
 - entière, 1007, 1041, 1220
 - Abel angulaire, 885
 - fonctions holomorphes, 1170
 - processus de Markov, 1526
 - utilisation, 1186, 1417
 - fonctions, 1052, 1220
 - génératrice d'une suite, 1028
 - utilisation, 1186
 - géométrique, 332
 - harmonique, 332
 - nombres, 1052
 - numérique, 765, 1041
 - Riemann, 332
 - Taylor, 1029
- Schrödinger, 1307
- Schur (théorème), 776
- section, 602
 - de graphe, 628
 - propriété des, 486
- segment
 - dans $\mathbb{R}^p$, 241
 - dans un espace affine, 515
- semblables
 - matrices, 377
- semi-définie positive, 384
- semi-norme, 263
- semi-simple
 - endomorphisme, 369
- semi-symétrique
 - polynôme, 175
- signature
 - d'une permutation, 107
- similitude, 999
- simple
 - extension de corps, 161
 - fonction, 470
 - module, 126
- singularité, 1182
 - effaçable, 1182
 - pôle, 1182
- sinus
 - hyperbolique, 685
- sinus cardinal, 926
- solfège, 120
- solution
 - générale, 1310
 - particulière, 1310
- somme
 - inférieure, 799
 - partielle, 326
 - supérieure, 799
- somme directe (de représentations), 773
- somme partielles
 - Abel angulaire, 885
- sommet, 976
- sous anneau, 123
- sous arc, 929
- sous-additivité
 - sur algèbre de parties, 434
- sous-espace
 - affine engendré par une partie, 514
 - caractéristique, 386
- sous-groupe
 - caractéristique, 85
 - distingué, 761
 - dans le groupe alterné, 110
 - engendré, 85
 - normal, 98, 761
- sous-martingale, 1529
- sous-module, 126
- sous-suite, 592
- spectre
 - d'un endomorphisme, 375
 - matrice hermitienne, 381
 - matrice symétrique réelle, 384
- sphère, 313
 - de Riemann, 544
- stabilité
 - d'un point d'équilibre, 1291
 - Lyapunov, 1292
- stable, 1332
- stathme
 - sur $\mathbb{Z}[i]$, 154
- stathme euclidien, 133
- stationnaire
 - chaîne de Markov, 1520
- statistique, 1473
- statistiques
 - descriptives, 1465
- structure
 - complexe, 959
- structure d'anneau canonique, 117
- Student, 1445, 1486
- subdivision, 794
 - associée à une fonction, 795
 - d'un intervalle, 932
- suite, 115
 - équirépartie, 1212
 - critère de Weyl, 1212

- arithméticogéométrique, 333
- définie par itération, 1351
- de Cauchy, 223, 325
 - dans un corps, 72
- de composition, 99
- de fonctions, 1127
 - théorème de Montel, 1195
- de fonctions intégrables, 874, 1193
- de Jordan-Hölder, 99
- exacte, 111
- régularisante, 1227
- support, 796
 - distribution, 1241
 - famille d'éléments, 115
- supremum, 237, 238
 - d'une suite d'ensembles, 429
- sur-martingale, 1529
- surface paramétrée, 853
- surjection, 262
- Sylow
 - p -Sylow, 752
- Sylvester (matrice), 292
- symétrique
 - polynôme, 175
- symbole
 - de Legendre, 189
- système
 - fondamental, 1286
 - orthonormé, 1110
 - trigonométrique, 1111, 1153
- tangent
 - vecteur unitaire, 952
- tangente, 679, 949, 1025
- tangente à un chemin, 1094
- Tangente hyperbolique, 1562
- tangente hyperbolique, 686
- taubérien, 1050
- taux d'accroissement, 647
- Taylor, 644
 - série entière, 1028
- temps d'arrêt, 1532
- temps de retour, 1511
- terminée
 - martingale, 1533
- test, 1493
 - bilatéral, 1494
 - unilatéral, 1494
- théorème
 - élément primitif, 170, 197, 198
 - accroissements finis, 358
 - dérivée directionnelle, 603
 - dans $\mathbb{R}$, 598
 - forme générale, 639
- Ascoli, 1123
- Bézout
 - polynômes, 144
 - utilisation, 293
- Baire, 258
- Banach-Steinhaus, 1124
 - avec semi-normes, 1125
- base incomplète, 271
- Beppo-Levi, 479
- Bolzano-Weierstrass, 251
- Bolzano-Weierstrass dans $\mathbb{R}^n$, 245
- Borel-Cantelli, 1393
- Borel-Lebesgue, 244
- Brouwer, 1062
 - dimension 2, 1172
- Carathéodory, 519
- Cauchy, 752
- Cauchy-Arzela, 1068
- Cauchy-Lipschitz, 1066
- Cayley-Hamilton, 374, 716
- central limite, 1427
 - processus de Poisson, 1545
- Chevalley-Warning, 195
- chinois, 158
 - anneau des polynômes, 142
 - anneau principal, 132
- Cochran, 1470
- Cochrane, 1471
- convergence
 - dominée de Lebesgue, 482
 - monotone, 479
- d'Alembert-Gauss, 142
- décomposition des noyaux
 - et exponentielle de matrice, 366
- de Baire, 267
- de Jordan, 978
- de représentation de Riesz, 1109
- des deux carrés, 156
 - version faible, 154
- Dini, 658
- Dirichlet, 1202
 - forme faible, 184
- Doob, 1533
- du rang, 273
- extension d'isométrie, 1098
- extrema
 - lié, 1082
- Fejér, 1203
- fonction implicite dans $\mathbb{R}^n$, 1075
- fonction implicite dans Banach, 1074
- fondamental du calcul intégral, 810
- Fubini
 - dans $\mathbb{R}^n$, 820

- espace mesuré, 816
- version compacte dans $\mathbb{R}^2$, 902
- Fubini-Tonelli, 815
- fuite des compacts, 1290
- Gauss
 - polynômes, 152
- Gauss-Wantzel, 213
- Glivenko-Cantelli, 1479
- Hahn-Banach, 1154
- Hardy-Littlewood, 1052
- Heine, 593
- incidence, 532
- inversion locale, 1070
 - utilisation, 1082, 1091
- isomorphisme
 - premier, 88
 - second, 88
 - troisième, 89
- isomorphisme de Banach, 1123
- Jordan, 1210
- Kronecker, 295
- Lagrange, 96
- Lie-Kolchin, 415
- Lokta-Volterra, 1296
- Markov-Takutani, 1065
- Montel, 1195
- Pappus
 - affine, 535
 - projectif, 536
- Pearson, 1498
- petit de Fermat, 153
- Picard, 1059
- point fixe
 - Brouwer, 1172
- projection
 - cas vectoriel, 1106
 - partie fermée convexe, 1104
- prolongement de Hahn, 452
- prolongement de Riemann, 1182
- Radon-Nikodym, 790
 - complexe, 791
- représentation de Riesz, 1150
- Rolle, 597
- Rothstein-Trager, 889
- Runge, 1174
- Schauder, 1063
- Schur, 776
- spectral, 387
 - autoadjoint, 422
 - matrice symétrique, 384
 - matrices normales, 382
- stabilité de Lyapunov, 1292
- Stone-Weierstrass, 1047, 1049
- Sylvester, 744
- taubérien, 1050
- taubérien faible, 887
- transfert, 1418
- Tykhonov, 256
 - dénombrable, 258
 - fini, 257
- valeurs intermédiaires, 570
- Von Neumann, 1078
- Wedderburn, 185
- Weierstrass, 252
- topologie, 219, 317
 - *-faible, 265, 1239
 - p -adique, 343
 - et semi-normes, 263
 - faible, 309
 - forte, 309
 - induite, 231
 - métrique, 221, 241
 - produit, 220
 - sur $\mathcal{D}(\Omega)$, 1236
 - sur $\mathcal{D}(K)$, 1236
 - sur $C^\infty(\Omega)$, 1236
 - sur dual topologique, 265
 - usuelle sur $\mathbb{R}^n$, 317
- topologique
 - somme directe, 1107
- torsion, 953
 - d'un groupe, 115
- totale, 1110
- trace, 1271
 - dual de $M(n, \mathbb{K})$, 282
 - endomorphisme, 409
 - matrice, 409
 - produit scalaire sur $M(n, \mathbb{R})$, 311
 - unicité pour la propriété de trace, 282
- transcendant, 172
 - par rapport à une extension de corps, 172
- transformée
 - de Cauchy, 1179
 - de Fourier, 1217, 1416
 - continuité, 1218
 - groupe abélien fini, 771
 - Fourier
 - distribution tempérée, 1246
 - Laplace, 1417
- transformation
 - Fourier, 1220
 - gaussienne, 1372
- transient
 - état, 1512
- transition
 - probabilité, 1503

- transitive, 106
- transitoire
 - état, 1512
- transposée, 278
- transvection, 708
- transvection (matrice), 138
- transversale, 105
- tribu, 429
 - borélienne, 431
 - de Baire, 432
 - de Lebesgue, 495
 - engendrée, 430
 - par un événement, 1395
 - par une application, 455
 - par une variable aléatoire, 1395
 - induite, 430
 - produit, 484
- trigonalisation
 - et polynôme caractéristique, 412
 - simultanée, 415
- triplet
 - pythagoricien, 137
- type
 - fini
 - en algèbre, 172
 - espace vectoriel, 270
- unicité
 - des mesures, 441
- unipotent, 125
- unitaire
 - normale principale, 952
- valeur
 - principale (distribution), 1244
 - propre, 375
 - singulière, 392
- valeur absolue
 - p -adique, 343
- valeur propre
 - d'une forme quadratique, 419
- valuation, 142
 - p -adique, 343
- Vandermonde (déterminant), 289
- variété, 1082
- variété
 - orientée, 843
- variable
 - de décision, 1494
- variable aléatoire, 1394
 - absolument continue, 1394
 - Bernoulli
 - marche aléatoire, 1506
 - utilisation, 1461
 - binomiale
 - utilisation, 1536
 - centrée, 1400
 - de Bernoulli
 - utilisation, 1536
 - de Rademacher, 1443
 - intégrable, 1400
 - suite de variables aléatoire de Bernoulli, 1524
- variance, 1401
 - empirique, 1401, 1469
 - empirique corrigée, 1469
 - vecteur gaussien, 1439
- variation des constantes, 1282, 1286
- vecteur
 - cyclique, 368
 - gaussien, 1439
 - propre, 375
 - unitaire normal, 952
 - unitaire tangent, 950
- Vitali (ensemble), 503
- vitesse d'un chemin, 930
- voisinage, 240, 317
- volume
 - d'une région solide, 806
 - région bornée dans $\mathbb{R}^3$, 803
- vraisemblance, 1476
- Wronskien, 1299

Chapitre 0

Introduction

0.1 Préface

Ce livre s'adresse principalement au candidat à l'agrégation qui y trouvera de quoi dire pour presque toutes les leçons. La matière de ce livre (sous-entendu : les trois volumes ensemble) recouvre l'épreuve d'analyse, d'algèbre et de l'option de modélisation.

Petit avertissement : ce livre ne contient pas beaucoup d'exemples, alors que le titre de presque toutes les leçons contient le mot «exemple». Ce livre peut vous aider à

- apprendre la mathématique,
- trouver des développements
- remplir votre plan de théorèmes.

Pour les exemples, il faudra souvent aller chercher ailleurs.

Mon modèle économique

Mon modèle économique est le don. Chaque achat sur thebookedition.com me génère exactement zéro euros. Si vous aimez ce livre, vous pouvez faire un don, surtout si vous avez réussi l'agrégation et que vous pensez que ce livre en est pour quelque chose.

Dons en espèces :

RIB 30004 00406 00003524977 84

IBAN FR76 3000 4004 0600 0035 2497 784

BIC BNPAFRPPBSC

Dons en nature acceptés : rédaction d'un chapitre, un développement, relecture d'une partie, réponse à l'une ou l'autre des questions qui restent en suspend ...

0.2 Auteurs, contributeurs, sources et remerciements

Les remerciements sont mis dans l'ordre chronologique approximatif.

Les personnes qui ont mis du code $\text{\LaTeX}$ Des personnes qui m'ont donné du code $\text{\LaTeX}$ à inclure dans cet ouvrage.

- (1) 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.
- (2) Carlotta Donadello pour la partie géométrie analytique : topologie dans $\mathbb{R}^n$, courbes, intégrales, limites. (Université de Franche-Comté 2010-2012)
- (3) Lilian Besson pour m'avoir signalé un paquet de fautes, et quelques points pas clairs en statistiques.

Ceux à qui je dois beaucoup plus que un ou deux développements Certaines personnes ont tapé des recueils de développements dans lesquels j'ai abondamment puisé.

- (1) Arnaud Girand[1] 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[2] pour son document en ligne tout plein de développements.

Autres contributions et aides Beaucoup de monde m'a fourni de l'aide, en me donnant des cours, en rédigeant des textes bien faits, en me donnant des exemples ou en me signalant des fautes.

- (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) 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).
- (3) 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.
- (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. Il n'y a à peu près pas un résultat important de ces notes dont je n'aie pas lu la page Wikipédia, et souvent plusieurs pages connexes.
- (5) Des centaines de profs qui ont mis leurs polys sur internet. Des dizaines d'entre eux ont des sites dédiés à l'agrégation. Ils sont cités en bibliographie aux endroits où ils sont utilisés. Merci à toutes et à tous d'avoir codé et publié. Encore plus merci à celles et ceux qui ont pris la peine de préciser une licence et merci spécial pour les licences libres (quant à ceux dont la licence libre couvre également le code L^AT_EX publié ...).
- (6) Le forum usenet de math, en particulier pour la construction des corps fini dans la fil « Vérifier qu'un polynôme est primitif » initié le 20 décembre 2011.
- (7) Les intervenants du fil « Antisymétrisation, alterné, déterminant et caractéristique » sur [les-mathematiques.net](http://www.les-mathematiques.net) m'ont bien aidé pour la section sur les déterminants 6.5 (bien qu'ils ne le savent pas).
- (8) Plouf qui m'a signalé une coquille dans le fil la-selection-scientifique-de-la-semaine-numero-106.
- (9) Xavier Mauquoy pour l'énoncé et la preuve du théorème 11.53.
- (10) Benjamin de block pour des coquilles et une mise au point sur les conventions à propos de $\mathbb{R}^+$ et $(\mathbb{R}^+)^*$.

J'ai souvent donné entre parenthèse 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 hypertexte vers des sites, des blogs, etc. Tous ces gens ont fait du bon boulot. Sans toute cette « communauté », l'internet serait mort ¹.

1. 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.

0.3 Les questions pour lesquelles je n'ai pas (encore) de réponse

Ces notes ne sont pas relues de façon systématique. Aucune garantie. Merci de me signaler toute faute ou remarque : le relecteur c'est toi.

Voici une petite liste de questions que je me pose ou de choses écrites dont je ne suis pas certain. Si vous avez un avis ou une réponse à un des points, merci de vous faire connaître.

0.3.1 Mes questions d'analyse.

- (1) Soit $f \in L^p(\mathbb{R})$ et l'application $\tau_s(f)(x) = f(x - s)$ avec $s \in \mathbb{R}$. Est-ce que l'application

$$\begin{aligned} k: \mathbb{R} &\rightarrow \mathbb{R} \\ s &\mapsto \|f - \tau_s(f)\|_p \end{aligned} \quad (0.1)$$

est continue en $s = 0$? Il me semble que [3] l'utilise dans sa démonstration des suites régularisantes.

- (2) Est-ce que l'énoncé du théorème de Müntz 16.99 est correct? Voir en particulier la remarque 16.100 à propos de la présence du monôme 1 dans la liste.
- (3) Que penser de la remarque 17.27 qui dit qu'on doit avoir un théorème de complétion de partie orthonormale en une base orthonormale pour un espace de Hilbert? C'est vrai?
- (4) À propos de formule sommatoire de Poisson, est-ce que l'exemple 21.10 est bien fait? En particulier la formule (21.44) est-elle correcte et bien justifiée?
- (5) L'exemple 13.185 parle d'inverser une intégrale et une dérivée au sens des distributions pour prouver que la dérivée de $\int_0^x g(t)dt$ par rapport à x est g . Rendre cela rigoureux.
- (6) À propos du théorème de récurrence de Poincaré 7.81, l'application ϕ doit être mesurable? Répondre à la question posée sur la page de discussion de l'article sur wikipédia.
- (7) Toujours à propos du théorème de récurrence de Poincaré, il me semble qu'il y a un énoncé qui insiste sur la compacité de l'espace des phase et une démonstration utilisant la propriété de sous-recouvrement fini. Je serais content de retrouver cela. (ce serait sans doute mettable dans la leçon sur l'utilisation de la compacité)
- (8) Pour l'équation différentielle de Hill : $y'' + qy = 0$ avec q de classe C^1 , moi j'argumente dans la sous-section 24.8.4 que les solutions sont C^3 . Dans le document [1], il ne dit que C^2 . Il n'y a pas contradiction, mais...
- (9) Est-ce qu'on peut permuter la limite et l'intégrale dans $L^2(I)$ avec $I =]0, 1[$? Si (u_n) est une suite convergente dans L^2 vers u , est-ce qu'on a $\lim_{n \rightarrow \infty} \int_I u_n = \int_I u$? Voir le problème 12.
- (10) Est-ce que $L^p(S^1) = L^p([0, 2\pi]) = L^p(]0, 2\pi[)$? J'imagine que oui parce qu'un point de plus ou de moins ne change rien dans L^p . En tout cas je vois bien une bijection :

$$\begin{aligned} \psi: L^p([0, 2\pi]) &\rightarrow L^p(]0, 2\pi[) \\ [f] &\mapsto \text{la classe de } f(x) = \begin{cases} f(x) & \text{si } x \in]0, 2\pi[\\ 0 & \text{si } x = 0 \text{ ou } x = 2\pi. \end{cases} \end{aligned} \quad (0.2)$$

Si ces espaces ne sont pas égaux, alors il faut un peu faire attention aux notations que j'utilise dans toute la partie sur les approximations de l'unité, et dans le théorème 18.58 qui donne la densité des polynômes trigonométriques dans $L^p(S^1)$ – qui est le point de départ de la théorie de Fourier sur L^2 .

- (11) Dans [4], on parle de la proposition 22.33 à sa page 10. Comment est-ce qu'on justifie le passage

$$\int_{\mathbb{R}^d} T(y \mapsto \varphi(x)\psi(x-y))dx = T\left(y \mapsto \int_{\mathbb{R}^d} \varphi(x)\psi(x-y)dx\right). \quad (0.3)$$

Sylvie Benzoni précise que «ceci demanderait quelque justification». Où trouver lesdites justifications? Il s'agit de permuter une distribution et une intégrale.

- (12) En ce qui concerne les questions « fines » de topologie concernant l'espace $\mathcal{D}(K)$ des fonctions C^∞ à support dans le compact K , il faut voir les énoncés, les preuves et l'enchaînement des théorèmes et propositions
- (a) Proposition 22.7 pour dire que $\mathcal{D}(K)$ est métrique et complet (et donc de Baire).
 - (b) La proposition 16.103 qui donne la complétude de $(C(X, Y), \|\cdot\|_\infty)$ lorsque X est compact et Y métrique complet.
 - (c) Le théorème 18.10 de Banach-Steinhaus avec les semi-normes. Le fait qu'il s'applique bien à $\mathcal{D}(K)$.
 - (d) L'utilisation de cette version du théorème de Banach-Steinhaus dans la proposition 22.44. En particulier l'utilisation de la famille de fonctionnelles (22.118) et la preuve qu'elles sont continues.
 - (e) L'équivalence entre les deux topologies de la proposition 5.180 et le fait que cela s'applique bien à $\mathcal{D}(K)$.
 - (f) Et enfin l'utilisation de tout ça pour donner l'unique solution de l'équation de Schrödinger du théorème 24.22. Est-ce que l'énoncé de ce théorème est déjà correct ?
 - (g) En particulier la fonction (24.227) me semble être un petit bricolage.
- (13) Dans la démonstration du théorème de Baire (5.151), il manque peut-être quelques fermetures sur les boules.
- (14) Préciser l'énoncé et donner une démonstration de la proposition 6.193 qui traite de sommes dénombrables.
- (15) La justification que f_n est borélienne dans la proposition 21.4 mérite plus de détails.
- (16) Où trouver une preuve de la proposition 17.12 sur le supplémentaire topologique ?
- (17) La partie « unicité » du théorème de Cauchy-Lipschitz 16.123.
- (18) L'inversion entre la somme et l'intégrale de l'équation (19.117).
- (19) À propos de différentiabilité pour une application entre deux espaces de Banach. Le théorème 6.233 dit que si

$$\frac{d}{dt} \left[f(x + tu) \right]_{t=0} \quad (0.4)$$

existe pour tout $x \in B(a, r)$ et est continue (par rapport à x) en $x = a$, et que de plus $\frac{\partial f}{\partial u}(a) = 0$ pour tout u , alors f est différentiable en a .

Est-ce que cet énoncé est encore vrai lorsque $\frac{\partial f}{\partial u}(a) \neq 0$? Est-ce qu'il existe un théorème comparable à la proposition 11.157 pour la dimension infinie ? Il me semble que non, mais je n'ai pas de contre-exemples en tête. Par contre, je vois bien où la preuve bloque : c'est le lien entre la linéarité et la différentiabilité.

- (20) À propos du théorème de la fonction implicite 16.133. Est-ce que la partie unicité est correctement énoncée et démontrée ? En particulier il me semble qu'il manque la mention d'un voisinage de y_0 dans [5].
- (21) Il me faudrait un exemple de partie de $\mathbb{R}$ qui soit non borélienne mais mesurable au sens de Lebesgue. Comme je suis exigeant, je le veux le plus constructif possible : pas d'axiome du choix. Pour l'instant le mieux que j'aie trouvé est une feuille de TD[6] qui utilise des ordinaux.
- (22) À propos de l'écriture décimale des nombres, la proposition 6.173 et le théorème 6.174 sont à relire attentivement parce que les démonstrations sont presque complètement des inventions personnelles.
- (23) À propos de l'ensemble de Cantor, le lemme 7.174 et la proposition 7.176 sont à relire attentivement : les démonstrations sont des inventions personnelles.
- (24) La démonstration du théorème de Lyapunov 24.15 est en grande partie de l'invention personnelle extrapolée de divers morceaux pris par-ci par-là. En particulier tout ce qu'il y a autour de (24.115) et l'utilisation par le théorème d'explosion en temps fini pour déduire l'existence sur $\mathbb{R}$ de la solution mérite d'être relu, et plutôt deux fois qu'une.

- (25) Dans la preuve de la dualité de L^p , théorème 18.47, il y a une partie dans laquelle on diffère le cas $p = 1$ des autres. À quelle endroit la partie $p = 1$ ne fonctionne pas ? Est-ce seulement le fait que

$$\|\mathbb{1}_E\|_p = \mu(E)^{1/p} \quad (0.5)$$

et non $\mu(E)$?

- (26) Pour démontrer qu'une série entière est de classe C^∞ dans son disque de convergence, on s'appuie sur la proposition 16.42 qui donne la différentiabilité et ensuite sur le corollaire 16.43 qui effectue une parieuse récurrence. Toutes ces preuves sont de moi. À relire.
- (27) Est-ce que la proposition 5.35 qui donne le critère $d(x_p, x_q) \leq \epsilon$ pour être une suite de Cauchy est valide dans un espace topologique métrique au lieu de normé ? Dans quels cas a-t-on

$$d(a, b) = d(a + u) + d(b + u) \quad (0.6)$$

lorsque d est une distance qui n'est pas spécialement induite d'une norme ?

- (28) En ce qui concerne la limite de fonction étagées pour les fonctions mesurables, le lemme 7.104 démontre ça beaucoup plus simplement que le théorème 7.107. Pourquoi ?

0.3.2 Mes questions d'algèbre, géométrie.

- (1) La «décomposition en facteurs premiers» dans $\mathbb{Z}[i\sqrt{2}]$ que je donne dans l'exemple 3.77 est-elle correcte ? En particulier le lemme 3.78 ?
- (2) Est-ce que la fin de la démonstration 4.115 avec cette histoire d'ensemble $\{\xi_k^q \text{ tel que } q \in \mathbb{N}\}$ fini est compréhensible ?
- (3) Les représentations *irréductibles* sont les modules *indécomposables*. Quid des modules irréductibles ? C'est pas un peu dingue de ne pas utiliser le mot «irréductible» pour désigner les mêmes choses dans le cas des modules et celui des représentations ?
- (4) Rendre rigoureuse la remarque (6.329) qui dit que les matrices ont le polynôme minimal est égal au polynôme caractéristique sont denses dans les matrices.
- (5) Soit $\mathbb{L}$ une extension algébrique de corps de $\mathbb{K}$ et $a \in \mathbb{L}$. Est-ce que le polynôme minimal de a dans $\mathbb{K}[X]$ est l'unique polynôme irréductible unitaire $P \in \mathbb{K}[X]$ tel que $P(a) = 0$? D'ailleurs, est-ce qu'un tel polynôme existe ? est unique ? J'utilise cela dans la proposition 4.82.
- (6) La partie initiation de récurrence ($r = 2$) de la preuve de la proposition 8.30 à propos de convexe et de barycentre est-elle correcte ? Ce passage de l'espace affine à l'espace vectoriel sous-jacent me paraît un peu facile.
- (7) Le lemme 3.108 à propos de PGCD de polynômes est-il correct ? J'imagine que le polynôme $\text{pgcd}(P, PU + R)$ ne dépend pas de U . Est-ce exact ?
- (8) Est-ce que parler de sous-groupe «normal» au lieu de «distingué» est un anglicisme ?
- (9) Est-ce que l'énoncé et la démonstration de la proposition 4.53 sont corrects ? Si a et b sont des racines de P , alors $\mu_a \mu_b$ divise P (si $\mu_a \neq \mu_b$). Cette proposition est utilisée dans la démonstration de l'irréductibilité des polynômes cyclotomiques (proposition 4.113).
- (10) À quoi sert l'hypothèse «autre que $\mathbb{F}_2$ » dans le lemme 6.43 ? Peut-être dans la notion de déterminant parce qu'en caractéristique 2, l'antisymétrie d'une forme linéaire n'implique le fait qu'elle soit alternée.
- (11) L'inversibilité de la somme de Gauss (proposition 4.129) est-elle bien démontrée ?
- (12) Des commentaires sur l'exemple 4.70 qui montre que $X^p - X + 1$ est irréductible sur $\mathbb{F}_p$.
- (13) Les idéaux de A/I sont en bijection avec les idéaux de A contenant I . Justification de l'équation (3.34).
- (14) L'énoncé et la démonstration d'une des multiples version du théorème de l'élément primitif, proposition 4.155.

- (15) Pourquoi la pseudo-réduction simultanée (corollaire 6.298) est-elle *pseudo*? Pourtant les matrices sont bel et bien simultanément diagonalisées.
- (16) À propos d'extensions algébriques, est-ce que la proposition 4.65 est correcte? Est-ce qu'implicitement, il n'y a pas un sur-corps de $\mathbb{K}$ dans lequel il faut travailler?
- (17) Est-ce que la proposition 4.40 disant qu'un polynôme minimal est irréductible et premier avec tout polynôme non annulateur est correcte?
- (18) À propos de construction à la règle et au compas. Pour l'addition d'angles, l'exemple 4.168 explique comment on construit la somme de deux angles. Le problème est que cette construction se fait par intersection de deux cercles. Une des deux intersections donne $\alpha + \beta$ et l'autre donne $\alpha - \beta$. Comment par construction peut-on choisir le bon point?
- (19) À propos de chiffrement RSA, quelle est la probabilité que le message M ne soit pas premier avec p ? Est-ce que Alice (qui est celle qui chiffre avec la clef de Bob) peut le vérifier? Que penser des points que j'énumère à la page 767 au dessus du problème 8?
- (20) Extension des scalaires. Si $\{e_i\}_i$ est une base du $\mathbb{K}$ -espace vectoriel E , alors $\{1 \otimes e_i\}$ est une base de $E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E$ où $\mathbb{L}$ est une extension de $\mathbb{K}$. C'est vrai? Que penser de la preuve donnée au lemme 6.314?
- (21) Si $f: V \rightarrow V$ est une application linéaire, on ne peut pas définir la transposée $f^t: V \rightarrow V$ comme étant l'application linéaire dont la matrice est la transposée de la matrice de f parce que cette définition n'est pas invariante par changement de base. C'est vrai? Voir le problème 4.

0.3.3 Mes questions de probabilité et statistiques.

- (1) Le paradoxe des familles de 26.2.10 est-il correctement énoncé et résolu?
- (2) Si X est une variable aléatoire et A un événement, est-ce qu'il est vrai que $E(P(A|X)) = P(A)$? Démonstration?
- (3) À propos de convergence en loi et en probabilité vers une constante, dans [7], l'équation (26.223b) arrive avec une inégalité. Pourquoi?
- (4) Est-ce qu'une partie compacte d'un espace mesuré est toujours mesurable et de mesure finie? Est-ce que la question a un sens? Quelle est la topologie associée à une mesure? Les ouverts seraient une base des mesurables en un certain sens? (par analogie aux ouverts qui sont la base des boréliens dans $\mathbb{R}^n$)
 Dans cette optique, on pourrait sans doute affaiblir l'hypothèse «de mesure finie» de l'énoncé du corollaire 16.90 du théorème de Stone-Weierstrass.
- (5) Est-ce que le théorème d'arrêt de Doob 29.14 est correctement énoncé? En particulier la seconde condition.
- (6) À propos du problème de la ruine du joueur. Dans [1], l'équation (29.66) vient avec une $\limsup$ et non une limite normale. Je ne comprends pas pourquoi.
- (7) Est-ce que si X et Y sont des variables aléatoires indépendantes on a

$$E(XY|\mathcal{A}) = E(X|\mathcal{A})E(Y|\mathcal{A}). \quad (0.7)$$

Cela permettrait de ne pas utiliser la proposition 26.36 pour prouver l'équation (29.76).

- (8) À propos du théorème central limite 26.74, est-ce que la remarque 26.75 est correcte? Si pour une certaine variable aléatoire X on a $E(X) = m$, alors $P(X = m + a) = P(X = m - a)$. Cela me semble un peu facile, et même faux.

Par contre si n est assez grand on a

$$P(\bar{X}_n = m + a) = P(\bar{X}_n = m - a). \quad (0.8)$$

Cela est correct?

0.3.4 Mes questions de modélisation

- (1) Pour un état d'une chaîne de Markov, est-ce que le mot «transient» est un anglicisme pour «transitoire» ?

0.3.5 Les preuves à relire par des experts

Ici lorsque je parle d'«expert», j'entends quelqu'un qui est sûr de son coup dans un domaine particulier. Soit quelqu'un qui donne un cours dans le domaine, soit un étudiant qui a eu une bonne note dans un cours du domaine. Je m'adresse donc à des personnes qui ont déjà lu et compris une preuve des résultats *avant* de les lire ici.

Les preuves des résultats suivants sont en tout ou en partie des inventions personnelles, et doivent donc être lues avec beaucoup de prudence. Si vous les lisez, que vous ne voyez pas de fautes et que vous êtes sûr de votre coup, écrivez moi. Si au contraire, vous y trouvez des fautes ou des raccourcis, écrivez moi même si vous n'êtes pas sûr de votre coup.

- (1) La proposition 13.187.

Proposition 0.1 (Dérivation sous l'intégrale).

Supposons $A \subset \mathbb{R}^m$ ouvert et $B \subset \mathbb{R}^n$ compact. Nous considérons une fonction $f: A \times B \rightarrow \mathbb{R}$. Si pour un $i \in \{1, \dots, n\}$, la dérivée partielle $\frac{\partial f}{\partial x_i}$ existe dans $A \times B$ et est continue, alors la fonction

$$F(x) = \int_B f(x, t) dt \quad (0.9)$$

admet une dérivée partielle dans la direction x_i sur A . Cette dérivée partielle y est continue et

$$\frac{\partial F}{\partial x_i}(a) = \int_B \frac{\partial f}{\partial x_i}(a, t) dt, \quad (0.10)$$

pour tout a dans l'ouvert A .

- (2) La proposition 7.137

Proposition 0.2.

Soit un espace mesuré $(S, \mathcal{F}, \mu)$ et une fonction mesurable positive $w: S \rightarrow \bar{\mathbb{R}}^+$. Alors la formule

$$(w \cdot \mu)(A) = \int_A w d\mu \quad (0.11)$$

pour tout $A \in \mathcal{F}$ définit une mesure positive sur $(S, \mathcal{F})$ appelée **produit** de la mesure μ par la fonction w . La fonction w est la **densité** de la mesure $w \cdot \mu$ par rapport à la mesure μ .

- (3) La proposition 6.317 et la remarque 6.318.

Soit $\{e_i\}$ une base de E et $\{e_a\}$ une de F . Nous noterons également e_i et e_a les éléments τe_i et τe_a correspondants. Si la fonction $f: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ s'écrit dans ces bases comme

$$f(e_i) = \sum_a f_{ai} e_a \quad (0.12)$$

alors nous définissons $\text{proj}(f)$ par

$$(\text{proj } f)e_i = \sum_a \text{proj}(f_{ai}) e_a. \quad (0.13)$$

Proposition 0.3.

L'application **proj** définie en (0.13) est indépendante du choix des bases.

- (4) La proposition 6.325

Proposition 0.4.

Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$ et une application linéaire $f: E \rightarrow F$ entre deux $\mathbb{K}$ -espaces vectoriels. Alors $\mu_f = \mu_{f_{\mathbb{L}}}$.

(5) Le lemme 7.27

Lemme 0.5.

Résultats sur les unions croissantes d'ensembles mesurables dans $(S, \mathcal{A}, \mu)$.

(a) Si (A_k) est une suite croissante d'ensembles μ -mesurables dont l'union est mesurable, alors

$$\lim_{n \rightarrow \infty} \mu(A_k) = \mu\left(\bigcup_k A_k\right). \quad (0.14)$$

(b) Soit K_n , une suite emboîtée d'éléments de $\mathcal{A}$ tels que $K_n \rightarrow S$. Si $A \in \mathcal{A}$ alors

$$\lim_{n \rightarrow \infty} \mu(A \cap K_n) = \mu(A). \quad (0.15)$$

(6) Le lemme 7.104

Lemme 0.6.

Soit $f: (S, \mathcal{F}) \rightarrow \bar{\mathbb{R}}$ une fonction positive mesurable. Il existe une suite $f_n: S \rightarrow \mathbb{R}$ de fonctions étagées positives telles que $f_n \rightarrow f$ ponctuellement et $f_n \leq f$.

(7) La proposition 1.23

Proposition 0.7.

Soit la suite de rationnels (x_n) définie par $x_0 \in \mathbb{Q}^+$ et

$$x_{n+1} = x_n + \frac{x_n^2 - 2}{2x_n}. \quad (0.16)$$

Alors :

- (a) En posant $y_n = x_n^2$ nous avons $y_n \rightarrow 2$.
- (b) La suite (x_n) est de Cauchy.
- (c) La suite (x_n) ne converge pas dans $\mathbb{Q}$.

(8) La proposition 14.81

Proposition-définition 0.8 (Cercle circonscrit).

Soit une courbe fermée simple et continue $\gamma: [0, 1] \rightarrow \mathbb{R}^2$. Soit Γ son image. Il existe un unique cercle de rayon minimum contenant Γ . Ce cercle est le **cercle circonscrit** à γ .

Il a les propriétés suivantes :

- (a) Le cercle circonscrit à γ coupe Γ en au moins deux points distincts.
- (b) Tout arc du cercle circonscrit plus grand que le demi-cercle intersection Γ .

(9) La proposition 3.12

Proposition 0.9.

Soient des entiers positifs $\alpha_1, \dots, \alpha_p$. Nous avons

$$\bigcup_{i=1}^p U_{\alpha_i} = \{1\} \quad (0.17)$$

si et seulement si $\text{pgcd}(\alpha_1, \dots, \alpha_p) = 1$ (c'est à dire que les α_i sont premiers dans leur ensemble).

(10) La proposition 4.40

Proposition 0.10.

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

- (a) le polynôme μ_a est irréductible sur $\mathbb{K}$;
- (b) si $Q \in \mathbb{K}[X]$ est un polynôme non annulateur de a alors Q et μ_a sont premiers entre eux.

(11) La proposition 4.65

Proposition 0.11 (Propriétés d'extensions algébriques[8]).

Soit $\mathbb{K}$ un corps commutatif et a un élément algébrique sur $\mathbb{K}$, de polynôme minimal μ_a de degré n . Alors

- (a) En considérant l'application d'évaluation

$$\begin{aligned} \varphi_a: \mathbb{K}[X] &\rightarrow \mathbb{L} \\ Q &\mapsto Q(a), \end{aligned} \tag{0.18}$$

nous avons $\mathbb{K}[a] = \text{Image}(\varphi_a)$.

- (b) Une base de $\mathbb{K}[a]$ comme espace vectoriel sur $\mathbb{K}$ est donnée par $\{1, a, a^2, \dots, a^{n-1}\}$.
- (c) Le degré de l'extension $\mathbb{K}[a]$ est égal au degré du polynôme minimal :

$$[\mathbb{K}[a] : \mathbb{K}] = n. \tag{0.19}$$

- (d) L'anneau $\mathbb{K}[a]$ est l'ensemble des polynômes en a de degré $n - 1$ à coefficient dans $\mathbb{K}$.
- (e) $\mathbb{K}(a) = \mathbb{K}[a]$.
- (f) $\mathbb{K}[a] \simeq \mathbb{K}[X]/(\mu_a)$ (isomorphisme d'anneau).

(12) La proposition 5.42

Proposition 0.12 ([8]).

Quel que soit le réel r , il existe une suite croissante de rationnels convergente vers r .

(13) Le lemme 5.66

Lemme 0.13.

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) .

(14) Le lemme 5.106

Lemme 0.14.

Si K_1 et K_2 sont des compacts dans $\mathbb{R}$ alors $K_1 \times K_2$ est compact dans $\mathbb{R}^2$.

(15) La proposition 5.122

Proposition 0.15 (Caractérisation séquentielle de la continuité).

Le lien entre continuité et continuité séquentielle.

- (a) Une application continue est séquentiellement continue (quels que soient les espaces de départ et d'arrivée).
- (b) Si X et Y sont des espaces métriques, alors une fonction $f: X \rightarrow Y$ est continue en un point si et seulement si elle est y séquentiellement continue.

(16) Le théorème 5.147

Théorème 0.16.

Un produit fini d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

(17) Le lemme 12.85

Lemme 0.17.

Tout élément de G s'écrit de façon unique sous la forme $a^\epsilon b^k$ ou $b^k a^\epsilon$ avec $\epsilon = 0, 1$ et $k = 0, \dots, n-1$.

(18) La proposition 11.21

Proposition 0.18.

Si la fonction réelle $f: I = [a, b[\rightarrow \mathbb{R}$ est croissante et bornée, alors la limite

$$\lim_{x \rightarrow b} f(x) \quad (0.20)$$

existe et est finie.

(19) La proposition 11.216

Proposition 0.19.

Une fonction dérivable sur un intervalle I de $\mathbb{R}$

(a) est convexe si et seulement si sa dérivée est croissante sur I .

(b) est strictement convexe si et seulement si sa dérivée est strictement croissante sur I

(20) La proposition 11.223

Proposition 0.20.

Soit $f: \mathbb{R} \rightarrow \mathbb{R}$ une fonction convexe et $a \in \mathbb{R}$. Il existe une constante $c_a \in \mathbb{R}$ telle que pour tout x nous ayons

$$f(x) - f(a) \geq c_a(x - a). \quad (0.21)$$

Autrement dit, le graphe de la fonction f est toujours au dessus de la droite d'équation

$$y = f(a) + c_a(x - a). \quad (0.22)$$

Je me demande si ce ne serait pas un «si et seulement si».

(21) La proposition 11.224

Proposition 0.21.

Si g est une fonction convexe, il existe deux suites réelles (a_n) et (b_n) telles que

$$g(x) = \sup_{n \in \mathbb{N}} (a_n x + b_n). \quad (0.23)$$

(22) Le théorème 13.1

Théorème 0.22.

Soit Q un compact connexe par arcs et une fonction continue $f: Q \rightarrow \mathbb{R}$. Si λ est la mesure de Lebesgue, alors il existe $a \in Q$ tel que

$$f(a) = \frac{1}{\lambda(Q)} \int_Q f d\lambda \quad (0.24)$$

(23) Le lemme 14.82

Lemme 0.23.

Soit une courbe simple, convexe $\gamma: [0, 1] \rightarrow \mathbb{R}^2$ que nous supposons être de classe C^2 . Nous notons Γ l'image de γ . Alors Γ est localement le graphe d'une fonction convexe.

(24) La proposition 14.83.

Proposition 0.24.

Soit une courbe simple, fermée et convexe $\gamma: [0, 1] \rightarrow \mathbb{R}^2$ que nous supposons être de classe C^2 . Nous notons Γ l'image de γ . Alors il existe un convexe D tel que $\partial D = \Gamma$.

(25) La proposition 16.42

Proposition 0.25.

Si la série entière $\sum_{n \geq 0} a_n z^n$ a un rayon de convergence R alors

(a) La somme est une fonction holomorphe dans le disque de convergence.

(b) La somme est différentiable et

$$du_{z_0}(z) = \sum_{n=1}^{\infty} n a_n z_0^{n-1} z. \quad (0.25)$$

(c) De plus pour tout $z_0 \in B(0, R)$, on pose²

$$S(z) = \sum_{n \geq 0} a_n z^n \quad (0.26a)$$

$$T(z) = \sum_{n \geq 1} n a_n z^{n-1} = \sum_{n=0}^{\infty} (n+1) a_{n+1} z^n. \quad (0.26b)$$

Alors nous avons

$$\lim_{z \rightarrow z_0} \frac{S(z) - S(z_0)}{z - z_0} = T(z_0). \quad (0.27)$$

(26) Le corollaire 16.43

Corollaire 0.26.

La somme d'une série entière est de classe C^∞ sur le disque ouvert de convergence.

(27) La proposition 11.66

Proposition 0.27.

Soit $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ une application continue dont la variable y varie dans un compact I de $\mathbb{R}$. Alors la fonction

$$\begin{aligned} d: \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto \sup_{y \in I} f(x, y) \end{aligned} \quad (0.28)$$

est continue.

À ce propos, est-il vrai que l'opération $\sup$ vue comme application $C(\mathbb{R}^n) \rightarrow C(\mathbb{R}^{n-1})$ est continue? Pour quelle topologie sur les espaces de fonctions continues?

(28) La proposition 14.90

Proposition 0.28.

Soit $\gamma: [0, L] \rightarrow \mathbb{R}^2$ une courbe fermée simple et convexe de classe C^1 . Si la tangente en $p = \gamma(s_p)$ et la tangente en $q = \gamma(s_q)$ sont identiques (pas seulement parallèles), alors soit

$$\gamma([s_p, s_q]) = [p, q] \quad (0.29)$$

soit

$$\gamma([s_q, L]) = [p, q] \quad (0.30)$$

(29) Le corollaire 18.72

2. Pour rappel, dans tout ce texte, $B(a, r)$ est une boule ouverte.

Corollaire 0.29.

Soit φ une fonction Schwartz sur $\mathbb{R}^m \times \mathbb{R}^n$. Alors la fonction

$$y \mapsto \sup_{x \in \mathbb{R}^n} |\varphi(x, y)| \quad (0.31)$$

est intégrable.

(30) La proposition 21.13

Proposition 0.30.

Soit $\varphi \in \mathcal{S}(\mathbb{R}^n \times \mathbb{R}^m)$ et la transformée de Fourier partielle

$$\tilde{\varphi}(x, k) = \int_{\mathbb{R}^m} e^{-iky} \varphi(x, y) dy. \quad (0.32)$$

Alors $\tilde{\varphi} \in \mathcal{S}(\mathbb{R}^n \times \mathbb{R}^m)$.

Cette proposition utilise le corollaire 0.29.

0.4 Comment m'aider à rendre ces notes plus utiles ?

Voici quelques pistes.

- (1) M'écrire pour me signaler toutes les fautes.
- (2) M'envoyer une liste de théorèmes et de résultats que tout candidat à l'agrégation devrait connaître.
- (3) Répondre aux questions ci-dessus.
- (4) Si vous êtes «expert» dans un domaine, relire les preuves listées ci-dessus.
- (5) Si vous n'êtes pas expert, me signaler tous les endroits qui vous semblent obscurs. Vu que ces notes sont destinées à *apprendre*, les avis des non experts sont très importants.
- (6) Mettre vos propres notes sous licence FDL pour me permettre de les copier ou de les inclure.
- (7) Mettre une copie de (ou un lien vers) ces notes sur votre site.
- (8) Écrire au jury d'agrégation pour dire que ces notes vous plaisent et que vous voudriez les avoir pour l'oral.

Chapitre 1

Construction des ensembles de nombres

1.1 Quelques éléments sur les ensembles

Définition 1.1.

Un ensemble est **infini** si il peut être mis en bijection avec un de ses sous-ensembles propres.

1.1.1 Lemme de Zorn

1.2.

L'**axiome du choix** que nous acceptons peut s'énoncer comme ceci[9] : 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 1.3.

Une **relation d'ordre** sur un ensemble E est une relation binaire (notée $\leq$) sur E telle que pour tout $x, y, z \in E$,

- (1) *Réflexivité* : $x \leq x$
- (2) *antisymétrie* : $x \leq y$ et $y \leq x$ implique $x = y$
- (3) *transitivité* : $x \leq y$ et $y \leq z$ implique $x \leq z$.

Un ensemble est **totalelement ordonné** si deux éléments sont toujours comparables : si $x, y \in E$ alors nous avons soit $x \leq y$ soit $y \leq x$.

Notons que l'inégalité stricte (nous définissons $x < y$ si et seulement si $x \leq y$ et $x \neq y$) n'est pas une relation d'ordre parce qu'elle n'est pas réflexive.

Définition 1.4 (Ensemble inductif).

Un ensemble est **inductif** si tout sous-ensemble ordonné admet un majorant.

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 $X \subset Y$ ou $Y \subset X$.

Lemme 1.5 (Lemme de Zorn).

Tout ensemble ordonné inductif non vide admet un maximum.

Le point intéressant de ce lemme est que le majorant soit un maximum, c'est à dire qu'il appartienne à l'ensemble.

Proposition 1.6 ([10], lemme 8.1).

Si S est un ensemble infini alors il existe une bijection $\varphi: \{1, 2\} \times S \rightarrow S$.

1.1.2 Complémentaire

Soit E , un ensemble et A , une partie de E (c'est à dire un sous-ensemble de E). Nous désignons par $\complement A$ désigne le **complémentaire** de l'ensemble A dans E . Il s'agit de l'ensemble des points de E qui ne font pas partie de A :

$$\complement A = E \setminus A = \{x \in E \text{ tel que } x \notin A\}. \quad (1.1)$$

Nous allons aussi régulièrement noter le complémentaire de A par A^c .

Lemme 1.7.

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, $E \setminus (E \setminus A) = A$,
- (2) $\complement(A \cap B) = \complement A \cup \complement B$,
- (3) $\complement(A \cup B) = \complement A \cap \complement B$,
- (4) $A \setminus B = A \cap \complement B$.

Définition 1.8 (différence symétrique).

Si A et B sont des ensembles, l'ensemble $A \Delta B$ est la **différence symétrique** d'ensembles :

$$A \Delta B = (A \cup B) \setminus (A \cap B). \quad (1.2)$$

C'est l'ensemble des éléments étant soit dans A soit dans B mais pas dans les deux.

Lemme 1.9.

Si A et B sont des ensembles nous avons

- (1) $A^c \Delta B^c = A \Delta B$.
- (2) $(A \Delta B) \Delta B = A$.

Démonstration. La première assertion provient de l'égalité $X^c \setminus Y^c = Y \setminus X$ (qu'on montre de façon classique, éventuellement en séparant les cas suivant que B est inclus à A ou non) :

$$A^c \Delta B^c = (A^c \cup B^c) \setminus (A^c \cap B^c) = (A \cap B)^c \setminus (A \cup B)^c = (A \cup B) \setminus (A \cap B) = A \Delta B. \quad (1.3)$$

Pour la seconde assertion, il faut remarquer que $(A \Delta B) \cup B = A \cup B$ et que $(A \Delta B) \cap B = B \setminus A$, donc

$$(A \Delta B) \Delta B = (A \cup B) \setminus (B \setminus A) = A. \quad (1.4)$$

□

1.1.3 Relations d'équivalence

Définition 1.10.

Si E est un ensemble, une **relation d'équivalence** sur E est une relation $\sim$ telle 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 $x \sim z$.

Par exemple, sur l'ensemble de tous les polygones du plan, la relation «a le même nombre de côté» 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 côté. Cela 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 ($P \sim R$).

Soit f une application entre deux ensembles E et F . Nous définissons une relation d'équivalence sur E par

$$x \sim y \Leftrightarrow f(x) = f(y). \quad (1.5)$$

Nous notons par $\pi: E \rightarrow E/\sim$ la projection canonique. L'application

$$\begin{aligned} g: E/\sim &\rightarrow F \\ [x] &\mapsto f(x) \end{aligned} \quad (1.6)$$

est bien définie et injective. Elle n'est pas surjective tant que f ne l'est pas. La **décomposition canonique** de f est

$$f = g \circ \pi. \quad (1.7)$$

1.2 Les naturels

Définition 1.11.

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 1.1, c'est qu'un ensemble fini n'est ni dénombrable ni non dénombrable.

Proposition 1.12.

Toute partie d'un ensemble fini est finie, et toute partie d'un ensemble dénombrable est finie ou dénombrable.

1.3 Les entiers

Toutes les constructions sont faites dans [11].

1.4 Quelques structures algébriques

Définition 1.13 (Anneau[12]).

Un **anneau** est un triple $(A, +, \cdot)$ avec les conditions

- (1) $(A, +)$ est un groupe abélien. 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.

Remarque 1.14.

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.

Définition 1.15.

Un sous ensemble $I \subset A$ est un **idéal** à gauche si

- (1) I est un sous-groupe pour l'addition,
- (2) pour tout $a \in A$, $aI \subset I$.

Définition 1.16.

Un **corps** est un anneau non nul dans lequel tout élément non nul est inversible.

Définition 1.17.

Ordre et choses reliées dans un corps.

- (1) Un corps $\mathbb{K}$ est **totalelement ordonné** si il existe une relation d'ordre total¹ tel que
- (a) $x \leq y$ implique $x + z \leq y + z$ pour tout $x, y, z \in \mathbb{K}$
 - (b) $x \geq 0$ et $y \geq 0$ implique $xy \geq 0$.
- (2) Si $\mathbb{K}$ est un corps totalelement ordonné, nous y définissons la valeur absolue par

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0. \end{cases} \quad (1.8)$$

- (3) La suite (x_n) dans le corps totalelement ordonné $\mathbb{K}$ est **de Cauchy** si pour tout $\epsilon \in \mathbb{K}^+$, il existe $N \in \mathbb{N}$ tel que si $p, q \geq N$ alors $|x_p - x_q| \leq \epsilon$.
- (4) La suite (x_n) dans le corps totalelement 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 $k \geq N$ alors $|x_k - q| \leq \epsilon$.
- (5) Un corps $\mathbb{K}$ est **archimédien** si il est totalelement ordonné et si pour tout $x, y \in \mathbb{K}$ avec $x > 0$, il existe $n \in \mathbb{N}$ tel que $nx \geq y$.
- (6) Un corps totalelement ordonné est **complet** si toute suite de Cauchy dans $\mathbb{K}$ y est convergente.

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 1.18 (Propriétés de la valeur absolue).

Soit $\mathbb{K}$ un corps totalelement ordonné. Si $x, y \in \mathbb{K}$ alors

- (1) Si $x \geq 0$ alors $-x \leq 0$.
- (2) $|x| \geq 0$
- (3) $|x| = 0$ si et seulement si $x = 0$
- (4) $|x + y| \leq |x| + |y|$.

Démonstration. Point par point

- (1) Nous partons de $x \geq 0$ et nous ajoutons $-x$ des deux côtés en profitant de la définition d'un corps totalelement ordonné : $x - x \geq -x$ et donc $0 \geq -x$, c'est à dire $-x \leq 0$.
- (2) Si $x \geq 0$ alors c'est vrai. Sinon, $x \leq 0$ et $|x| = -x \geq 0$ par le point (1).
- (3) 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 $\pm x \neq 0$.
- (4) Nous supposons que $x \leq y$ et nous subdivisons suivant la positivité de x et y .
 - (a) Si $x, y \geq 0$. Dans ce cas, $x + y \geq y \geq 0$, donc $|x + y| = x + y = |x| + |y|$.
 - (b) Si $x, y \leq 0$. Dans ce cas, $x + y \leq 0$ et nous avons $|x + y| = -x - y = |x| + |y|$.
 - (c) Si $x \leq 0$ et $y \geq 0$. Nous subdivisons encore en deux cas suivant que $x + y$ est positif ou négatif. Si $x + y \geq 0$, alors nous écrivons successivement

$$x \leq 0 \quad (1.9a)$$

$$x + y \leq y \leq y + |x| = |x| + |y| \quad (1.9b)$$

et donc $|x + y| = x + y \leq |x| + |y|$.

Nous supposons à présent que $x \leq 0$, $y \geq 0$ et $x + y \leq 0$. Dans ce cas il suffit d'écrire $|x + y| = |(-x) + (-y)|$ pour retomber dans le cas précédent à inversion près de x et y .

□

1. Définition 1.3.

Remarque 1.19.

La partie (4) 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

$$|x - y| = |(x - z) + (z - y)| \leq |x - z| + |z - y|. \quad (1.10)$$

1.5 Les rationnels**1.5.1 Suites de Cauchy dans les rationnels****Proposition 1.20** ([11]).

Principales propriétés des suites de Cauchy dans $\mathbb{Q}$.

- (1) *Toute suite convergente est de Cauchy*².
- (2) *Toute suite de Cauchy est bornée.*
- (3) *Si $x_n \rightarrow 0$ et si (y_n) est bornée, alors $x_n y_n \rightarrow 0$*
- (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 $x_n \rightarrow a$ et $y_n \rightarrow b$ alors $x_n + y_n \rightarrow a + b$, $x_n - y_n \rightarrow a - b$ et $x_n y_n \rightarrow ab$.*
- (6) *Soit (x_n) une suite de Cauchy qui ne converge pas vers zéro. Alors il existe n_0 tel que la suite $\left(\frac{1}{x_n}\right)_{n \geq n_0}$ soit de Cauchy.*

Démonstration. Point par point.

- (1) Soit (x_n) une suite dans $\mathbb{Q}$ qui converge vers $x \in \mathbb{Q}$. Soit aussi³ $\epsilon > 0$. Il existe $N_\epsilon \in \mathbb{N}$ tel que $n > N_\epsilon$ implique $|x_n - x| \leq \epsilon$. Si $p, q \geq N_{\epsilon/2}$ alors

$$|x_p - x_q| \leq |x_p - x| + |x - x_q| \leq \epsilon. \quad (1.11)$$

Donc la suite (x_n) est de Cauchy.

- (2) Soit (x_n) une suite de Cauchy dans $\mathbb{Q}$. Avec $\epsilon = 1$ dans la définition, si $q > N_1$, nous avons

$$|x_q - x_{N_1}| \leq 1. \quad (1.12)$$

Et donc pour tout q plus grand que N_1 , $x_N - 1 \leq x_q \leq x_N + 1$, ou encore, pour tout n :

$$|x_n| \leq \max\{|x_1|, |x_2|, \dots, |x_N|, |x_N + 1|\}. \quad (1.13)$$

La suite est donc bornée.

- (3) Soit $\epsilon > 0$. Les hypothèses disent qu'il existe un N tel que $|x_n| \leq \epsilon$ dès que $n \geq N$. Et il existe aussi $M \geq 0$ tel que $|y_n| \leq M$ pour tout n . Du coup, lorsque $n \geq N$ nous avons $|x_n y_n| \leq M\epsilon$.
- (4) En ce qui concerne la somme,

$$|x_p + y_p - x_q - y_q| \leq |x_p - x_q| + |y_p - y_q|. \quad (1.14)$$

Soit N_1 tel que si $p, q \geq N_1$ alors $|x_p - x_q| \leq \epsilon$ et N_2 de même pour la suite (y_n) . En prenant $N = \max\{N_1, N_2\}$, la somme (1.14) est plus petite que 2ϵ dès que $p, q \geq N$.

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

2. Et non la réciproque, qui sera justement la grande innovation des nombres réels.

3. Le ϵ que nous prenons maintenant est dans $\mathbb{Q}$, et ce sera toujours ainsi dans les prochaines pages ; nous ne le répéterons pas à chaque fois.

sont toutes les deux bornées par le nombre M : pour tout n nous avons $|x_n| \leq M$ et $|y_n| \leq M$. Nous avons :

$$|x_p y_p - x_q y_q| \leq |x_p y_p - x_q y_p| + |x_q y_p - x_q y_q| \leq |y_p| |x_p - x_q| + |x_q| |y_p - y_q|. \quad (1.15)$$

Vu que (x_n) et (y_n) sont de Cauchy, si p et q sont assez grand, les deux différences sont majorées par ϵ et nous avons

$$|x_p y_p - x_q y_q| \leq M\epsilon + M\epsilon = 2M\epsilon, \quad (1.16)$$

ce qui prouve que $(x_n y_n)$ est de Cauchy.

(5) En ce qui concerne la somme, nous pouvons tout de suite calculer

$$|x_n + y_n - (a + b)| \leq |x_n - a| + |y_n - b|. \quad (1.17)$$

Il existe une valeur de n à partir de laquelle le premier terme est plus petit que ϵ et une à partir de laquelle le second terme est plus petit que ϵ . En prenant le maximum des deux, la somme est plus petite que 2ϵ .

En ce qui concerne le produit,

$$|x_n y_n - ab| \leq |x_n y_n - a y_n| + |a y_n - ab| \leq |y_n| |x_n - a| + |a| |y_n - b|. \quad (1.18)$$

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

$$y_n |x_n - a| + a |y_n - b| \rightarrow 0. \quad (1.19)$$

Au passage nous avons également utilisé la propriété de la somme que nous venons de démontrer.

(6) La négation de «converge vers zéro» est : il existe $\alpha > 0$ tel que pour tout $N \in \mathbb{N}$, il existe $n \geq N$ tel que $|x_n| > \alpha$. Mais notre suite est de Cauchy, donc il existe $n_0 \in \mathbb{N}$ tel que si $p, q \geq n_0$ alors

$$|x_p - x_q| \leq \frac{\alpha}{2}. \quad (1.20)$$

Soit aussi $n \geq n_0$ tel que $|x_n| \geq \alpha$. Si $p > n$ nous avons aussi $|x_n - x_p| \leq \frac{\alpha}{2}$. Cela implique $|x_p| \geq \frac{\alpha}{2}$ et en particulier $x_p \neq 0$.

En prenant $p, q \geq n$ nous avons donc $|x_p| > \frac{\alpha}{2}$ et $|x_q| > \frac{\alpha}{2}$. Avec cela,

$$\left| \frac{1}{x_p} - \frac{1}{x_q} \right| \leq \frac{|x_q - x_p|}{|x_p x_q|} \leq \frac{4}{\alpha^2} |x_q - x_p|. \quad (1.21)$$

Mais comme (x_n) est de Cauchy, il suffit de choisir p et q à la fois plus grand que n et plus grand que le N qui fait $|x_p - x_q| \leq \epsilon$ pour $p, q \geq N$ pour obtenir

$$\left| \frac{1}{x_p} - \frac{1}{x_q} \right| \leq \frac{4}{\alpha^2} \epsilon. \quad (1.22)$$

Donc $\left(\frac{1}{x_n} \right)$ est de Cauchy.

□

1.5.2 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 $x_n^2 \rightarrow 2$.

Lemme 1.21.

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. $\square$

Proposition 1.22 (Irrationalité de $\sqrt{2}$).

Il n'existe pas de fractions d'entiers dont le carré soit égal à 2.

Le théorème 11.53 nous dira que tous les $\sqrt{n}$ sont irrationnels dès que n n'est pas un carré parfait.

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 1.21 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 en 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 comme à nouveau, 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 positifs. Impossible, me diriez vous ??? Et vous auriez bien raison : il n'y a pas de fractions d'entiers dont le carré vaut 2. $\square$

Proposition 1.23 ([8]).

Soit la suite de rationnels (x_n) définie par $x_0 \in \mathbb{Q}^+$ et

$$x_{n+1} = x_n + \frac{x_n^2 - 2}{2x_n}. \quad (1.23)$$

Alors :

- (1) *En posant $y_n = x_n^2$ nous avons $y_n \rightarrow 2$.*
- (2) *La suite (x_n) est de Cauchy.*
- (3) *La suite (x_n) ne converge pas dans $\mathbb{Q}$.*

Démonstration. Tout d'abord un petit calcul montre que

$$x_{n+1}^2 = 2 + \frac{(y_n - 2)^2}{4y_n}, \quad (1.24)$$

c'est à dire que quelle que soit la valeur de x_0 , dès le x_1 , les valeurs de y_n sont plus grandes que 2. Notons qu'il n'est pas possible d'avoir $y_n = 2$. Nous pouvons donc supposer $y_n > 2$ pour tout n . Alors en posant $y_n = 2 + s$ nous avons

$$y_{n+1} = 2 + \frac{s^2}{8 + 4s}. \quad (1.25)$$

Si $s < 1$ alors $\frac{s^2}{8+4s} < s^2$ et en réalité le processus $s \mapsto s^2/(8+4s)$ tend très vite vers zéro. Nous devons donc montrer qu'il existe un n tel que $y_n = 2 + s$ avec $s < 1$.

Montrons pour cela que si $n < s < 2n$ alors⁴

$$\frac{s^2}{8+4s} < n \quad (1.26)$$

En effet si $n < s < 2n$ nous pouvons majorer le numérateur par $4n^2$ et minorer le dénominateur par $4n$.

Prouvons à présent le résultat. Pour un $n > 1$ nous avons

$$y_{n+1} = 2 + \frac{s}{8+4s} \quad (1.27)$$

avec $s > 0$. Nous considérons $n_0 \in \mathbb{N}$ tel que $n_0 < s < 2n_0$. Alors

$$y_{n+2} = 2 + s_1 \quad (1.28)$$

avec $s_1 < n$. Il existe donc n_1 tel que $n_1 < s_1 < 2n_1$ et $n_1 < n_0$. Nous avons alors $y_{n+3} = 2 + s_2$ avec $s_2 < n_1 < n_0$.

Nous construisons ainsi des suites (s_i) et (n_i) telles que

$$y_{n+k} = 2 + s_k \quad (1.29)$$

avec $s_k < n_{k-1} < n_{k-2} < \dots < n_0$. En procédant ainsi au maximum $n-1$ fois nous avons $s_k < 1$. À partir du moment où $y_{n+k} = 2 + s_k$ avec $s_k < 1$, nous avons déjà vu qu'il est certain que $y_n \rightarrow 2$.

Prouvons que la suite (x_n) est de Cauchy. Vu que $x_n^2 \rightarrow 2$ nous avons $x_n \geq 1$ à partir d'une certaine valeur de n . Si de plus elle n'est pas de Cauchy, alors pour tout ϵ , et tout N donnés, il existe $p, q \geq N$ tels que $|x_p - x_q| \geq \epsilon$. Cela donne

$$|x_p^2 - x_q^2| = |x_p + x_q||x_p - x_q| \geq 2\epsilon. \quad (1.30)$$

Par conséquent la suite (x_n^2) n'est pas de Cauchy, alors qu'elle l'est parce qu'elle est convergente (par la proposition 1.20(1)).

Enfin supposons que $x_n \rightarrow a \in \mathbb{Q}$. Dans ce cas nous aurions $x_n^2 \rightarrow a^2 = 2$. Mais nous savons que $a^2 = 2$ est impossible dans $\mathbb{Q}$. $\square$

Bref, la suite (x_n) est de Cauchy, ne converge pas et a son carré qui converge vers 2.

Remarque 1.24.

Vu que nous n'avons pas encore défini les réels, ce qui suit n'est que informel. Ce qui a motivé la majoration (1.26) est la résolution de l'inéquation

$$\frac{s^2}{8+4s} < n \quad (1.31)$$

qui donne les bornes $2n \pm \sqrt{n^2 + 2n}$ dont une est toujours négative, et l'autre plus grande que $2n$.

Vous en voulez encore une ?

Proposition 1.25.

La suite donnée par

$$x_n = 1 + \frac{1}{1!} + \dots + \frac{1}{n!} \quad (1.32)$$

est de Cauchy et ne converge pas dans $\mathbb{Q}$.

4. Voir la remarque 1.24 pour comprendre d'où vient l'idée de cette majoration.

Démonstration. Si $p > q$ nous avons

$$x_p - x_q = \sum_{k=q+1}^p \frac{1}{k!} \quad (1.33a)$$

$$= \sum_{k=q+1}^p \frac{1}{(q+1)!} \frac{1}{(q+1)^{k-q-1}} \quad (1.33b)$$

$$\leq \frac{1}{(q+1)!} \sum_{k=0}^{\infty} \frac{1}{(q+1)^k} \quad (1.33c)$$

$$= \frac{1}{(q+1)!} \frac{1}{1 - \frac{1}{q+1}} \quad (1.33d)$$

$$= \frac{1}{q!q}. \quad (1.33e)$$

Soit $\epsilon \in \mathbb{Q}$ s'écrivant $\epsilon = \frac{a}{b}$ avec $a, b \in \mathbb{N}$. En prenant $p, q > b$, nous avons

$$x_p - x_q \leq \frac{1}{b!b} < \frac{1}{b} < \frac{a}{b} = \epsilon. \quad (1.34)$$

Donc oui, cette suite est de Cauchy.

Montrons que cette suite ne converge pas dans $\mathbb{Q}$ en supposant qu'elle y converge : $\lim_{n \rightarrow \infty} x_n = \frac{a}{b} \in \mathbb{Q}$. Pour tout $p > q$ nous avons déjà vu avoir

$$0 < x_p - x_q < \frac{1}{qq!}. \quad (1.35)$$

Prenons la limite $p \rightarrow \infty$; par stricte croissance de la suite, les inégalités restent strictes :

$$0 < \frac{a}{b} - x_q < \frac{1}{qq!}. \quad (1.36)$$

Si $n > b$ alors nous pouvons écrire

$$\frac{a}{b} - x_n = \frac{\alpha}{n!} \quad (1.37)$$

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 (1.36) nous pouvons écrire

$$0 < \frac{\alpha}{q!} < \frac{1}{qq!}, \quad (1.38)$$

c'est à dire $0 < \alpha < \frac{1}{q}$, ce qui est impossible pour $\alpha \in \mathbb{Z}$. □

1.6 Les réels

Une construction des réels via les coupures de Dedekind est donnée dans [13].

1.26.

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 5.29) alors que la topologie métrique (celle entre autres de $\mathbb{Q}$) ne sera définie que par le théorème 5.20. Nous avons donc dû définir en la définition 1.17 *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 topologie métrique que nous allons voir

que sur $\mathbb{R}$, ces trois notions coïncident avec celles topologiques⁵. Et par conséquent que $\mathbb{R}$ sera un espace topologique complet⁶.

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.

1.6.1 L'ensemble

Soit $\mathcal{E}$ l'ensemble des suites de Cauchy⁷ dans $\mathbb{Q}$. Soit aussi l'ensemble $\mathcal{E}_0$ constituée des suites qui convergent vers zéro⁸.

En posant

$$x + y = (x_n + y_n) \quad (1.39)$$

et

$$xy = (x_n y_n), \quad (1.40)$$

l'ensemble $\mathcal{E}$ devient un anneau⁹ 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 1.27.

La partie $\mathcal{E}_0$ est un idéal¹⁰ de l'anneau $\mathcal{E}$.

Démonstration. Nous savons par la proposition 1.20(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 1.20 (il s'agit du fait que la somme de deux suites convergent vers zéro est une suite convergente vers zéro).

En ce qui concerne la propriété fondamentale des idéaux, si $x \in \mathcal{E}_0$ et $y \in \mathcal{E}$ nous devons prouver que $xy \in \mathcal{E}_0$. Vu que $(\mathcal{E}_0, \cdot)$ est commutatif, cela suffira pour être un idéal bilatère. Vu que y est une suite de Cauchy, elle est bornée ; et étant donné que $x \rightarrow 0$ nous avons alors $xy \rightarrow 0$ (par la proposition 1.20(3)). $\square$

Théorème-définition 1.28 (L'anneau des réels[11]).

Sur l'ensemble quotient $\mathcal{E}/\mathcal{E}_0$, les opérations

$$(1) \quad \bar{u} + \bar{v} = \overline{u + v}$$

$$(2) \quad \bar{u} \cdot \bar{v} = \overline{uv}$$

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.

Les opérations sont bien définies Si $u, v \in \mathcal{E}$ et $h, k \in \mathcal{E}_0$ alors $h + k \in \mathcal{E}_0$ et nous avons

$$\overline{u + h} + \overline{v + k} = \overline{u + v + h + k} = \overline{u + v}. \quad (1.41)$$

ainsi que

$$\overline{u + h} \cdot \overline{v + k} = \overline{(u + h)(v + k)} = \overline{uv + uk + hv + hk} = \overline{uv} \quad (1.42)$$

parce que les suites des Cauchy u et v sont bornées, ce qui donne que uk , hv et hk sont des éléments de $\mathcal{E}_0$ par la proposition 1.20(3). Cela prouver que les définitions proposées sont bonnes.

5. Proposition 5.35.

6. Théorème 5.40.

7. Définition 1.17(3)

8. Nous rappelons qu'à ce niveau nous n'avons pas encore prouvé que toutes les suites de Cauchy convergent.

9. Définition 1.13.

10. Définition 1.15.

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

$$\bar{x} = \{\text{suites qui convergent vers } q\}. \quad (1.43)$$

Si $y \in \bar{x}$ alors $y = x + h$ avec $h \in \mathcal{E}_0$ alors $y_n \rightarrow q$ parce que $h_n \rightarrow 0$. Réciproquement si $y_n \rightarrow q$ alors pour chaque n nous avons

$$y_n = x_n + (y_n - x_n), \quad (1.44)$$

mais $y - x \rightarrow 0$. Donc $y - x \in \mathcal{E}_0$ ce qui signifie que $y \in \bar{x}$.

Neutre et unité Il est vite vérifié que $\bar{0}$ et $\bar{1}$, les classes des suites constantes sont neutre pour l'addition et unité pour la multiplication.

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 zéro¹¹ alors il existe $y \in \mathcal{E}$ tel que $xy \in \bar{1}$.

Nous savons par la proposition 1.20(6) que x étant une suite de Cauchy dans $\mathbb{Q}$, il existe $n_0 \in \mathbb{N}$ tel que $\left(\frac{1}{x_n}\right)_{n \geq n_0}$ est une suite de Cauchy. Nous posons alors

$$y_n = \begin{cases} 0 & \text{si } n \leq n_0 \\ \frac{1}{x_n} & \text{si } n > n_0. \end{cases} \quad (1.45)$$

Nous avons alors

$$(xy)_n = \begin{cases} 0 & \text{si } n \leq n_0 \\ 1 & \text{si } n > n_0 \end{cases} \quad (1.46)$$

et donc $xy \in \bar{1}$.

□

Proposition 1.29.

Soit l'application

$$\begin{aligned} \varphi: \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \bar{q}. \end{aligned} \quad (1.47)$$

où par $\bar{q}$ nous entendons la classe de la suite constante égale à q (qui est de Cauchy).

- (1) C'est un homomorphisme injectif.
- (2) Image(φ) est un sous-corps de $\mathbb{R}$
- (3) $\varphi: \mathbb{Q} \rightarrow \text{Image}(\varphi)$ est un isomorphisme de corps.

Démonstration. Le fait que ce soit un homomorphisme est simplement

- $\varphi(q + q') = \overline{q + q'} = \bar{q} + \bar{q}'$
- $\varphi(qq') = \overline{qq'} = \bar{q}\bar{q}'$.

En ce qui concerne l'injectivité, si q est tel que $\varphi(q) = \bar{0} = \mathcal{E}_0$, c'est que

$$\varphi(q) = \{\text{suites de Cauchy qui convergent vers zéro}\} \quad (1.48)$$

Mais nous savons aussi que¹²

$$\varphi(q) = \bar{q} = \{\text{suites de Cauchy qui convergent vers } q\} \quad (1.49)$$

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 .

11. $x \in \mathcal{E}$ peut soit ne pas converger du tout, soit converger vers autre chose que zéro.

12. Voir dans la démonstration du théorème 1.28.

1.6.2 Relation d'ordre

Nous définissons les parties $\mathcal{E}^+$ et $\mathcal{E}^-$ de $\mathcal{E}$ par

- (1) $x \in \mathcal{E}^+$ si et seulement si pour tout $\epsilon > 0$, il existe N_ϵ tel que $n > N_\epsilon$ implique $x_n > -\epsilon$.
- (2) $x \in \mathcal{E}^-$ si et seulement si pour tout $\epsilon > 0$, il existe N_ϵ tel que $n > N_\epsilon$ implique $x_n < \epsilon$.

Nous notons aussi $\mathcal{E}^{++} = \mathcal{E}^+ \setminus \mathcal{E}_0$.

Lemme 1.30.

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. 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 $n \geq N$. Par conséquent, $|x_n| \leq \epsilon$ pour tout $n \geq N$ et la suite x converge vers zéro, c'est à dire $x \in \mathcal{E}_0$. Cela prouve que $\mathcal{E}^+ \cap \mathcal{E}^- \subset \mathcal{E}_0$. L'inclusion inverse est évidente.

Soit $x \in \mathcal{E} \setminus \mathcal{E}^-$ et prouvons que $x \in \mathcal{E}^+$. La condition $x \notin \mathcal{E}^-$ donne qu'il existe un $\alpha > 0$ (dans $\mathbb{Q}$) tel que pour tout n , il existe $p > n$ avec $x_p > \alpha$. Mais x est une suite de Cauchy, donc nous avons un n_0 tel que si $n, p \geq n_0$ alors $|x_n - x_p| \leq \frac{\alpha}{2}$. Écrivons cette dernière inégalité avec $p > n_0$ tel que $x_p > \alpha$ et $n > n_0$:

$$x_n > \frac{\alpha}{2} > 0 \quad (1.50)$$

Par conséquent $x \in \mathcal{E}^+$ parce que $x \in \mathcal{E}$ et est positif à partir d'un certain rang. $\square$

Lemme 1.31 ([11]).

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 $n \geq N_{\epsilon/2}$ 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 $xy \in \mathcal{E}_0$ alors c'est bon. Si par contre $x, t \in \mathcal{E}^{++}$ alors 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 $n \geq n_1$. Mais $x - y \in \mathcal{E}_0$, donc il existe n_2 tel que $|x_n - y_n| < \frac{\epsilon}{2}$ dès que $n \geq n_2$. En prenant n plus grand que n_1 et n_2 , nous avons en même temps

$$\begin{cases} x_n > -\frac{\epsilon}{2} \\ |x_n - y_n| < \frac{\epsilon}{2} \end{cases} \quad (1.51a)$$

$$\quad (1.51b)$$

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 $y \in \mathcal{E}^-$. $\square$

Définition 1.32 (Positivité dans $\mathbb{R}$).

Vocabulaire et notations.

- (1) Nous notons $\mathbb{R}^+ = \mathcal{E}^+$.
- (2) Nous notons $\mathbb{R}^- = \mathcal{E}^-$.
- (3) Un élément de $\mathbb{R}$ est **positif** si il est la classe d'une suite de Cauchy appartenant à $\mathcal{E}^+$.

(4) Un élément de $\mathbb{R}$ est **négatif** si il est la classe d'une suite de Cauchy appartenant à $\mathcal{E}^-$.

Remarque 1.33.

Avec les conventions de la définition 1.32, et en anticipant sur nos connaissances à propos des réels,

- (1) zéro est positif et négatif.
- (2) L'intersection entre $\mathbb{R}^+$ et $\mathbb{R}^-$ est le singleton $\{0\}$.
- (3) L'ensemble des nombres *strictement* positifs est noté $(\mathbb{R}^+)^*$ ou $\mathbb{R}^+ \setminus \{0\}$.
- (4) Le mot «positif» signifie «positif ou nul»; le mot «négatif» signifie «négatif ou nul».

Problèmes et choses à faire

Une inconsistance dans les notations et le vocabulaire en ce qui concerne $\mathbb{R}^+$, $\mathbb{R}^-$ et le fait que zéro soit dedans ou non m'a été signalée. Nous avons tranché pour les conventions données dans la remarque 1.33 qui sont aussi celles de Wikipédia, mais il n'est pas exclu qu'il y ait des incohérences par-ci par-là dans le texte. Merci de me les signaler.

Définition 1.34 (Ordre dans $\mathbb{R}$).

Si $a, b \in \mathbb{R}$ nous notons $a \leq b$ si et seulement si $b - a$ est positif. Nous notons aussi $a > b$ si et seulement si $b - a \in \mathbb{R}^+ \setminus \{0\}$, etc.

Lemme 1.35.

Les premières propriétés de l'ordre.

- (1) L'ensemble $(\mathbb{R}, \leq)$ est un corps totalement ordonné (définitions 1.3 et 1.17).
- (2) L'application

$$\begin{aligned} \varphi: \mathbb{Q} &\rightarrow \mathbb{R} \\ q &\mapsto \bar{q} \end{aligned} \tag{1.52}$$

dont nous avons déjà parlé dans la proposition 1.29 est strictement croissante.

Démonstration. Nous prouvons la stricte croissance de φ . Si $q < l$ alors $\varphi(q) - \varphi(l) = \overline{q - l}$ est la classe de la suite constante $q - l$ qui est un élément strictement positif de $\mathbb{Q}$. Nous avons donc $\overline{q - l} \in \mathbb{R}^+$, et donc $\varphi(q) < \varphi(l)$. $\square$

Remarque 1.36.

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 1.37.

Si $x, y, z \in \mathbb{R}$ avec $y > 0$ sont tels que $z > x/y$ alors $zy > x$.

Démonstration. Nous savons que

$$z - \frac{x}{y} \in \mathcal{E}^+ \setminus \{0\}. \tag{1.53}$$

Vu que $y \in \mathcal{E}^+$, multiplier par y fait rester dans $\mathcal{E}^{++}$:

$$zy = y \frac{x}{y} \in \mathcal{E}^{++}. \tag{1.54}$$

Un représentant de $y \frac{x}{y}$ est la suite $n \mapsto y_n \frac{x_n}{y_n} = x_n$. Donc $y \frac{x}{y} = x$. Cela signifie que $zy - x \in \mathcal{E}^{++}$ et donc que $zy > x$. $\square$

Lemme 1.38.

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.

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 supérieurement, c'est à dire qu'il existe $m, q \in \mathbb{N}$ tels que $|a_n| \leq m/q$ pour tout n (proposition 1.20(2)). Soit M un naturel strictement plus grand que m/q .

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 positif¹³. Par définition de la relation d'ordre, $M \geq a$.

Seconde façon La suite (a_n) est majorée par $\frac{m}{q}$, donc on a dans $\mathbb{Q}$ et pour tout n :

$$a_n \leq \frac{m}{q} = M \leq qM. \quad (1.55)$$

L'application $\varphi: \mathbb{Q} \rightarrow \mathbb{R}$ est croissante, donc

$$\varphi((a_n)) \leq \varphi(qM). \quad (1.56)$$

□

Théorème 1.39 ([11]).

*Le corps $\mathbb{R}$ est archimédien*¹⁴.

Démonstration. Soient $x, y \in \mathbb{R}$ avec $x > 0$ et trouvons $s \in \mathbb{N}$ tel que $px > y$. Nous posons $a = \frac{y}{x}$ et le lemme 1.38 nous donne un $p > a$ dans $\mathbb{N}$. Par le lemme 1.37. □

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 1.40.

Si $x, y \in \mathbb{R}$ sont tels que $x < y$, il existe $s \in \mathbb{Q}$ tel que $x < s < y$

Démonstration. Nous avons par hypothèse que $y - x > 0$ et donc le fait que $\mathbb{R}$ soit archimédien (théorème 1.39) nous donne $q \in \mathbb{N}$ tel que $q(y - x) > 1$. Soit

$$E = \{n \in \mathbb{Z} \text{ tel que } \frac{n}{q} \leq x\}. \quad (1.57)$$

Cet ensemble n'est pas vide parce que $1/q > 0$, ce qui donne $n_0 \in \mathbb{N}$ tel que $n_0/q \geq |x|$. Dans ce cas, $-n_0 \in E$. De plus E est majoré par n_0 . Donc E possède un plus grand élément p qui vérifie

$$\frac{p}{q} \leq x < \frac{p+1}{q}. \quad (1.58)$$

De plus $(p+1)/q < y$. En effet nous avons

$$\frac{p+1}{q} = \frac{p}{q} + \frac{1}{q} \leq x + \frac{1}{q} < x + y - x = y \quad (1.59)$$

où nous avons utilisé l'inégalité stricte $y - x > \frac{1}{q}$.

Le nombre $s \in \mathbb{Q}$ que nous recherchions est $s = \frac{p+1}{q}$. □

Nous avons terminé avec la construction des réels. Les propriétés topologiques arrivent en 5.1.6.

1.7 Les complexes

1.7.1 Définitions

Un nombre complexe s'écrit sous la forme $z = a + bi$, où a et b sont des nombres réels appelés (et notés) respectivement partie réelle ($a = \Re(z)$) et partie imaginaire ($b = \Im(z)$) de z . L'ensemble des nombres de cette forme s'appelle l'ensemble des nombres complexes; cet ensemble porte une structure de corps et est noté $\mathbb{C}$. Le nombre complexe $i = 0 + 1i$ est un nombre imaginaire qui a la particularité que $i^2 = -1$.

13. Et nous allons d'ailleurs arrêter de toujours préciser «la classe de» lorsque ce n'est pas nécessaire.

14. Définition 1.17(5).

Deux nombres complexes $a + bi$ et $c + di$ sont égaux si et seulement si $a = c$ et $b = d$, c'est-à-dire leurs parties réelles sont égales, et leurs parties imaginaires sont égales.

Un nombre complexe étant représenté par deux nombres, on peut le représenter dans un plan appelé « plan de Gauss ». La plupart des opérations sur les nombres complexes ont leur interprétation géométrique dans ce plan.

Pour $z = a + bi$ un nombre complexe, on note $\bar{z} = a - bi$ le *complexe conjugué* de z . Dans le plan de Gauss, il s'agit du symétrique de z par rapport à la droite réelle (généralement dessinée horizontalement).

On définit le module du complexe z par $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$. Dans le plan de Gauss, il s'agit de la distance entre 0 et z .

Proposition 1.41.

Pour tout $z = a + bi$ et z' nombres complexes, on a

$$(1) \quad z\bar{z} = a^2 + b^2;$$

$$(2) \quad \bar{\bar{z}} = z;$$

$$(3) \quad |z| = |\bar{z}|;$$

$$(4) \quad |zz'| = |z||z'|;$$

$$(5) \quad |z + z'| \leq |z| + |z'|.$$

Chapitre 2

Théorie des groupes

2.1 Groupes

Définition 2.1 ([14]).

Soit G un groupe. Le **centralisateur** de $H \subset G$ est

$$Z_G(H) = \{g \in G \text{ tel que } hg = gh \forall h \in H\} \quad (2.1)$$

Si H est un sous-groupe, son **normalisateur** est

$$N_G(H) = \{g \in G \text{ tel que } gH = Hg\}. \quad (2.2)$$

Le **centre** du groupe G est l'ensemble

$$Z_G = \{z \in G \text{ tel que } gz = zg \forall g \in G\}. \quad (2.3)$$

Définition 2.2.

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 $N \triangleleft G$.

Un sous-groupe H de G est un sous-groupe **caractéristique** si $\alpha(H) = H$ pour tout $\alpha \in \text{Aut}(G)$.

Définition 2.3.

Soit G , un groupe et A une partie de G . Nous notons $\text{gr}(A)$ l'intersection de tous les sous-groupes de G contenant A . C'est le plus petit (pour l'inclusion) groupe de G contenant A . Si $\text{gr}(A) = G$, alors nous disons que A est une **partie génératrice** le groupe G .

Un groupe est **monogène** si il a une partie génératrice réduite à un seul élément.

Définition 2.4 (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**.

Définition 2.5 (Sous-groupe engendré).

Soit A une partie du groupe G . Le sous-groupe **engendré** est l'intersection de tous les sous-groupes de G contenant A .

Lemme 2.6.

Si A est une partie du groupe G , alors le sous-groupe engendré¹ 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).

Démonstration. Nous nommons K le groupe engendré par A et par H l'ensemble de tous les produits finis d'éléments de A et de A^{-1} . Cela est un sous-groupe de G contenant A . Donc $K \subset H$ parce que K est une intersection dont un des éléments est H .

1. Définition 2.5.

Par ailleurs tout groupe contenant A doit contenir les inverses et les produits finis, donc $H \subset K$.
Au final, $H = K$, ce qu'il fallait. $\square$

Exemple 2.7

Soit G le groupe des rotations d'angle $2k\pi/10$. La rotation d'angle $\pi/2$ n'est pas génératrice parce qu'elle n'engendre que $\pi/2, \pi, 3\pi/2$ et l'identité. La rotation d'angle $2\pi/10$ par contre est génératrice. $\triangle$

2.2 Sous groupe normal

Proposition 2.8.

Soit N un sous-groupe de G . Les propriétés suivantes sont équivalentes :

- (1) $gNg^{-1} \subseteq N$ pour tout $g \in G$,
- (2) $gNg^{-1} = N$ pour tout $g \in G$,
- (3) $gN = Ng$ pour tout $g \in G$,
- (4) N est une union de classes de conjugaison de G ,
- (5) N est normal.

Définition 2.9.

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 $g^n = (g^{-1})^{-n}$.

Définition 2.10.

Si G est un groupe, l'**ordre** est la cardinalité de G et est noté $|G|$. L'**ordre** d'un élément g de G est le naturel

$$\min\{n \in \mathbb{N} \text{ tel que } g^n = e\}. \quad (2.4)$$

Si le minimum n'existe pas, nous disons que l'ordre de g est infini.

Nous verrons que le corollaire 2.40 au théorème de Lagrange dira que l'ordre d'un élément divise l'ordre du groupe.

Lemme 2.11 ([15]).

Si H et K sont normaux dans le groupe G et si $H \cap K = \{e\}$ alors $HK \simeq H \times K$.

Définition 2.12.

L'**exposant** du groupe G est le plus petit entier non nul n tel que $g^n = e$ pour tout $g \in G$. Si il n'existe pas, nous disons que l'exposant du groupe est infini.

Si l'ordre de tous les éléments acceptent un majorant commun, alors l'exposant du groupe est le plus petit commun multiple des ordres des éléments. En particulier pour un groupe fini, l'exposant est le ppcm des ordres des éléments du groupe.

Le théorème de Burnside 6.357 nous donnera un bon paquet d'exemples de groupes d'exposant fini dans $GL(n, \mathbb{C})$.

Proposition 2.13.

Soit H un sous-groupe normal de G et $\psi: G \rightarrow K$ un homomorphisme.

- (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

$$[\psi(g_1)][\psi(g_2)] = [\psi(g_1)\psi(g_2)] \quad (2.5a)$$

$$= [\psi(g_1g_2)] \quad (2.5b)$$

$$= \{\psi(g_1g_2)\psi(h) \text{ tel que } h \in H\} \quad (2.5c)$$

$$= \{\psi(g_1g_2h) \text{ tel que } h \in H\} \quad (2.5d)$$

$$= \psi\left(\{g_1g_2h \text{ tel que } h \in H\}\right) \quad (2.5e)$$

$$= \psi(\overline{g_1g_2}) \quad (2.5f)$$

$$= \psi(\overline{g_2g_1}) \quad (2.5g)$$

$$= \text{refaire à l'envers} \quad (2.5h)$$

$$= [\psi(g_2)][\psi(g_1)]. \quad (2.5i)$$

Par conséquent $\psi(G)/\psi(H)$ est abélien. $\square$

2.3 Groupe dérivé

Définition 2.14.

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 . Le **groupe dérivé** de G est le sous-groupe noté $D(G)$ ou $[G, G]$ engendré par les commutateurs.

Autrement dit, $D(G)$ est l'intersection de tous les sous-groupes de G contenant tous les commutateurs. Intersection non vide parce que G lui-même en fait partie.

En vertu du lemme 2.6, 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

$$D(G) = \bigcup_{m=1}^{\infty} S_m. \quad (2.6)$$

Lemme 2.15.

Le groupe dérivé est un sous-groupe caractéristique, et un sous-groupe normal.

Démonstration. Il est évident que si $\alpha \in \text{Aut}(G)$ alors

$$\alpha([g, h]) = [\alpha(g), \alpha(h)], \quad (2.7)$$

c'est à dire que $D(G)$ est un sous-groupe caractéristique. En particulier si c est un commutateur, alors xcx^{-1} en est encore un, ce qui montre que $D(G)$ est normal dans G . Plus spécifiquement,

$$x(ghg^{-1}h^{-1})x^{-1} = (xgx^{-1})(xhx^{-1})(xg^{-1}x^{-1})(xh^{-1}x^{-1}) = (xgx^{-1})(xhx^{-1})(xgx^{-1})^{-1}(xhx^{-1})^{-1}. \quad (2.8)$$

$\square$

Proposition 2.16.

Le groupe quotient $G/D(G)$ est abélien.

Démonstration. En ce qui concerne le fait que $G/D(G)$ soit abélien, nous savons que pour tout $g, h \in G$ nous avons $h^{-1}g^{-1}hg \in D(G)$ et donc

$$[g][h] = [gh] = [ghh^{-1}g^{-1}hg] = [hg] = [h][g]. \quad (2.9)$$

$\square$

Le groupe quotient $G/D(G)$ est appelé l'**abélianisé** de G et est parfois noté G^{ab} .

Si $f: G \rightarrow A$ est un homomorphisme entre le groupe G et un groupe abélien A , alors $f(D(G)) = \{0\}$. Du coup f passe au quotient de G par $D(G)$, et il existe une unique application $\bar{f}: G/D(G) \rightarrow A$ telle que $f = \bar{f} \circ \pi$ où $\pi: G \rightarrow G/D(G)$ est la projection canonique.

2.4 Théorèmes d'isomorphismes

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 $\pi: G \rightarrow G/N$ est un homomorphisme surjectif de noyau N .

Théorème 2.17 (premier théorème d'isomorphisme).

Soit $\theta: G \rightarrow H$ un homomorphisme de groupe. Alors

- (1) $\text{Ker } \theta$ est normal dans G ,
- (2) $\text{Image } \theta$ est un sous-groupe de H
- (3) nous avons un isomorphisme naturel

$$G/\text{Ker } \theta \simeq \text{Image } \theta \quad (2.10)$$

Démonstration. (1)

(2)

(3) Si $[g]$ représente la classe de g dans $G/\text{Ker } \theta$, l'isomorphisme est donné par $\varphi[g] = \theta(g)$. $\square$

Théorème 2.18 (Deuxième théorème d'isomorphisme).

Soient H et N deux sous-groupes de G et supposons que N soit normal. 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

$$\frac{HN}{N} \simeq \frac{H}{H \cap N}. \quad (2.11)$$

(5) L'isomorphisme du point (4) est encore valable si N n'est pas normal mais si seulement H normalise N , c'est à dire si $hNh^{-1} \in N$ pour tout $h \in H$.

Démonstration. (1)

(2)

(3)

(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

$$\begin{aligned} j: H &\rightarrow HN \\ h &\mapsto h \end{aligned} \quad (2.12)$$

et la surjection canonique

$$\sigma: HN \rightarrow HN/N \quad (2.13)$$

Nous considérons ensuite l'application composée

$$\begin{aligned} f: H &\rightarrow HN/N \\ h &\mapsto hN. \end{aligned} \quad (2.14)$$

L'application f est surjective parce que l'élément $hnN \in HN/N$ est l'image de h , étant donné que $hnN = hN$.

Le noyau de f est $\text{Ker } f = H \cap N$. En effet si $a \in H \cap N$, nous avons $f(a) = \sigma(a) \in K$. Par conséquent $H \cap N \subset \text{Ker } f$. D'autre part si $h \in H$ vérifie $h \in \text{Ker } f$, alors $f(h) = hN = N$, ce qui est uniquement possible si $h \in N$.

Le premier théorème d'isomorphisme implique alors que $H/\text{Ker } f \simeq \text{Image } f$, c'est à dire

$$H/N \cap H \simeq HN/N. \quad (2.15)$$

$\square$

Théorème 2.19 (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

$$(G/M)/(N/M) \simeq G/N. \quad (2.16)$$

Démonstration. Afin de montrer que N/M est normal dans G/M , nous considérons $g \in G$, $nM \in N/M$ et nous calculons

$$gnMg^{-1} = gng^{-1} \underbrace{gMg^{-1}}_{=M} = \underbrace{gng^{-1}}_{\in N} M \in N/M. \quad (2.17)$$

Pour prouver l'isomorphisme nous considérons le morphisme

$$\begin{aligned} \varphi: G/M &\rightarrow G/N \\ gM &\mapsto gN. \end{aligned} \quad (2.18)$$

C'est surjectif et le 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

$$(G/M)/\text{Ker } \varphi \simeq \text{Image } \varphi, \quad (2.19)$$

c'est à dire

$$(G/M)/(N/M) \simeq G/N. \quad (2.20)$$

□

2.5 Le groupe et anneau des entiers

Certes $\mathbb{Z}$ est un groupe pour l'addition, mais c'est également un anneau² parce que nous avons les deux opérations d'addition et de multiplication. Nous n'allons pas nous priver de cette belle structure juste parce que le titre du chapitre est «groupes».

Proposition 2.20.

Une partie H du groupe $(\mathbb{Z}, +)$ est un sous-groupe si et seulement si il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

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 $x \in H$, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}_{n-1}$ tels que $x = nq + r$.

Problèmes et choses à faire

Justification par la division euclidienne à venir.

Nous savons déjà que $nq \in H$, donc $r \in H$ parce que x est également dans H . Mais nous avons décidé que n serait le plus petit naturel de $H \cap \mathbb{N}^*$. Par conséquent $r = 0$ et $x = nq \in n\mathbb{Z}$. □

Notons que si un sous-groupe H de $\mathbb{Z}$ est donné, alors le nombre n tel que $H = n\mathbb{Z}$ est unique. En effet si $n\mathbb{Z} = m\mathbb{Z}$ nous avons que n divise m (parce que $m \in m\mathbb{Z} \subset n\mathbb{Z}$) et que m divise n parce que $n \in m\mathbb{Z}$. Par conséquent $n = m$.

Lemme 2.21.

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 .

2. Définition 1.13.

2.5.1 Division euclidienne

Théorème 2.22 (Division euclidienne).

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \quad (2.21)$$

avec $0 \leq r < b$.

L'opération $(a, b) \mapsto (a, r)$ donnée par le théorème 2.22 est la **division euclidienne**. Le nombre q est le **quotient** et r est le **reste** de la division de a par b .

2.5.2 PGCD, PPCM et Bézout

Pour des versions plus générales, nous avons Bézout dans un anneau principal au théorème 3.69 et les définitions de PGCD et PPCM dans un anneau intègre à la définition 3.46. Voir également le théorème de Bézout pour les polynômes, théorème 3.105.

Soient $p, q \in \mathbb{Z}^*$. Les ensembles $p\mathbb{Z} \cap q\mathbb{Z}$ et $p\mathbb{Z} + q\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Par conséquent il existe des entiers $\text{ppcm}(p, q)$ et $\text{pgcd}(p, q)$ tels que

$$p\mathbb{Z} \cap q\mathbb{Z} = \text{ppcm}(p, q)\mathbb{Z} \quad (2.22a)$$

$$p\mathbb{Z} + q\mathbb{Z} = \text{pgcd}(p, q)\mathbb{Z}. \quad (2.22b)$$

Définition 2.23.

Si $\text{pgcd}(p, q) = 1$, nous disons que p et q sont **premiers entre eux**. 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 à tout le monde.

Théorème 2.24 (Théorème de Bézout³[16]).

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

$$au + bv = 1 \quad (2.23)$$

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

$$E = \{au + bv \text{ tel que } u, v \in \mathbb{Z}\} \cap \mathbb{N}^*. \quad (2.24)$$

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

$$m = au_1 + bv_1. \quad (2.25)$$

Écrivons la division euclidienne de a par m , c'est à dire

$$a = mq + r \quad (2.26)$$

avec $0 \leq r < m$. En remplaçant m par sa valeur (2.25), $a = (au_1 + bv_1)q + r$ et

$$r = a(1 - u_1q) - bv_1q, \quad (2.27)$$

c'est à dire que $r \in \mathbb{Z}a + \mathbb{Z}b$ en même temps que $0 \leq r < m$, donc $r = 0$ par minimalité de m . Donc a est divisible par m .

De la même façon nous prouvons que b est divisible par m . Vu que m divise à la fois a et b nous avons $m = 1$. □

3. Il y a une super application ici : https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/mauvais_prix.pdf.

Corollaire 2.25.

Soient p et q deux entiers premiers entre eux. Nous avons

$$p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}. \quad (2.28)$$

Notons que l'application $p\mathbb{Z} + q\mathbb{Z}$ vers $\mathbb{Z}$ n'est évidemment pas injective.

Démonstration. Soit $x \in \mathbb{Z}$. Le théorème de Bézout nous donne k et l tels que $kp + lq = 1$. Du coup, $(xk)p + (xl)q = x$. $\square$

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 chaîne de Markov peuvent être atteints à tout moments (assez grand), voir la définition 28.41 et ce qui suit.

Proposition 2.26.

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 $x \in \mathbb{N}$. Soit p positif tel que

$$\begin{cases} pa + pb \geq x \\ p(a+b) - x \leq a+b. \end{cases} \quad (2.29a)$$

$$(2.29b)$$

C'est à dire que $p(a+b)$ est le multiple supérieur de $a+b$ le plus proche de x . Nous avons alors

$$p(a+b) - ra - sb = x \quad (2.30)$$

où r et s sont donnés par le théorème de Bézout. Il s'agit maintenant de savoir si nous pouvons être assuré d'avoir $p > r$ et $q > s$ dès que x est assez grand. Pour cela nous considérons les nombres r_i et s_i définis par

$$r_i a + s_i b = i \quad (2.31)$$

pour $i = 1, \dots, a+b$. Nous posons $r^* = \max\{r_i\}$, $s^* = \max\{s_i\}$, et $p^* = \max\{r^*, s^*\}$. Maintenant si $x > p^*(a+b)$, alors

$$x = p(a+b) - r_k a - s_k b \quad (2.32)$$

où $k = x - p(a+b)$. $\square$

Exemple 2.27

Écrivons $1000 = a \cdot 7 + b \cdot 5$ avec $a, b \in \mathbb{N}$. D'abord $72 \cdot 7 = 504$ et $100 \cdot 5 = 500$. Nous avons donc

$$1004 = 72 \cdot 7 + 100 \cdot 5. \quad (2.33)$$

Ensuite $4 = 25 - 21 = -3 \cdot 7 + 5 \cdot 5$. Au final,

$$1000 = 75 \cdot 7 + 95 \cdot 5. \quad (2.34)$$

$\triangle$

Proposition 2.28.

soient $a, b \in \mathbb{Z}^*$. Si

$$a = \epsilon \prod_{p \text{ premiers}} p^{\mu(p)} \quad b = \epsilon' \prod_{p \text{ premier}} p^{\nu(p)}, \quad (2.35)$$

alors

$$\text{pgcd}(a, b) = \prod p^{\min\{\mu(p), \nu(p)\}} \quad (2.36a)$$

$$\text{ppcm}(a, b) = \prod p^{\max\{\mu(p), \nu(p)\}} \quad (2.36b)$$

Cette proposition implique que $m \leq p^n$ et $\text{pgcd}(m, p^n) \neq 1$ si et seulement si $m = qp$ avec $q \leq p^{n-1}$.

2.5.3 Calcul effectif du PGCD et de Bézout

Source : [17].

Soient A et B , deux entiers disons positifs. Nous allons voir maintenant l'algorithme de **Euclide étendu** qui est capable, pour A et B donnés, de calculer le $\text{pgcd}(A, B)$ et un couple de Bézout (u, v) tel que $uA + vB = \text{pgcd}(A, B)$. Ce calcul est indispensable si on veut implémenter RSA (12.8).

Cela se base sur le lemme suivant.

Lemme 2.29.

Soient $A, B \in \mathbb{N}$ et des nombres q et r tels que $A = qB + r$ avec $r < B$. Alors $\text{pgcd}(A, B) = \text{pgcd}(r, B)$.

Démonstration. Il suffit de voir que les diviseurs communs de A et B sont diviseurs de r et que les diviseurs communs de r et B divisent A .

Si s divise A et B , alors dans l'équation $\frac{A}{s} = \frac{qB}{s} + \frac{r}{s}$, les termes A/s et qB/s sont entiers, donc r/s doit aussi être entier.

Inversement, si s divise r et B , alors il divise $qB + r$ et donc A . □

Remarque 2.30.

Ce lemme est surtout intéressant lorsque $A = qB + r$ est la division euclidienne de A par B .

2.5.3.1 L'idée

L'algorithme pour calculer $\text{pgcd}(A, B)$ consiste à écrire la division euclidienne de A par B puis celle de B par r :

$$A = qB + r \quad r < B \quad (2.37a)$$

$$B = q'r + r' \quad r' < r \quad (2.37b)$$

et donc $\text{pgcd}(A, B) = \text{pgcd}(B, r) = \text{pgcd}(r, r')$. Étant donné que les inégalités $r < B$ et $r' < r$ sont strictes, en continuant ainsi nous finissons sur zéro, c'est à dire

$$r_{n-1} = q_n r_n, \quad (2.38)$$

et à ce moment nous avons $\text{pgcd}(A, B) = \text{pgcd}(r_{n-1}, r_n) = r_n$.

2.5.3.2 Pour le PGCD

Écrivons cela en détail (parce que Bézout, ça va être la même chose en cinq fois plus compliqué). On pose

$$r_0 = A \quad (2.39a)$$

$$r_1 = B. \quad (2.39b)$$

Ensuite on écrit la division euclidienne $A = q_1 B + r_2$, c'est à dire $r_0 = q_1 r_1 + r_2$. Cela donne r_2 et q_1 en termes de r_0 et r_1 :

$$r_2 = r_0 - q_1 r_1. \quad (2.40)$$

Ensuite, sachant r_2 nous pouvons continuer :

$$r_1 = q_2 r_2 + r_3 \quad (2.41)$$

donne q_2 et $r_3 = r_1 - q_2 r_2$. On continue avec $r_2 = q_3 r_3 + r_4$. Tout cela pour poser la suite

$$\begin{aligned} r_0 &= A \\ r_1 &= B \end{aligned} \quad (2.42)$$

$$r_k = q_{k+1} r_{k+1} + r_{k+2}$$

où la troisième ligne est la définition de r_{k+2} et de q_{k+1} en fonction de r_k et r_{k+1} . La suite (r_k) ainsi construite est strictement décroissante et à chaque étape le lemme 2.29 et le principe de l'algorithme d'Euclide nous donnent

$$\begin{cases} \text{pgcd}(r_k, r_{k+1}) = \text{pgcd}(r_{k+1}, r_{k+2}) = \text{pgcd}(A, B) \\ 0 \leq r_{k+1} < r_k. \end{cases} \quad (2.43a)$$

$$(2.43b)$$

La suite étant strictement décroissante, nous prenons r_n , le dernier non nul : $r_{n+1} = 0$. Dans ce cas la dernière équation sera

$$r_{n-1} = q_n r_n \quad (2.44)$$

avec $\text{pgcd}(A, B) = \text{pgcd}(r_n, r_{n-1}) = r_n$.

Exemple 2.31

Calculons le PGCD de 18 et 231. Pour cela nous écrivons les divisions euclidiennes en chaîne :

$$231 = 18 \cdot 12 + 15 \quad (2.45a)$$

$$18 = 1 \cdot 15 + 3 \quad (2.45b)$$

$$15 = 5 \cdot 3 + 0. \quad (2.45c)$$

Donc le PGCD est 3. △

2.5.3.3 Bézout : calcul effectif

La difficulté est de construire la suite qui donne Bézout. Elle va être construite à l'envers. Nous supposons déjà connaître la liste complète des r_k jusqu'à $r_n = \text{pgcd}(A, B)$, ainsi que la liste complète des divisions euclidiennes

$$r_k = q_{k+1} r_{k+1} + r_{k+2}. \quad (2.46)$$

Nous voulons trouver les couples (u_k, v_k) de telle façon à avoir à chaque étape

$$r_n = u_k r_k + v_k r_{k-1}. \quad (2.47)$$

Notons que c'est à chaque fois r_n que nous construisons. La première équation de type Bézout à résoudre est

$$r_n = u_n r_n + v_n r_{n-1}, \quad (2.48)$$

sachant que $r_{n-1} = q_n r_n$. On pose $v_n = 0$ et $u_n = 1$ et c'est bon. Pour la récurrence, nous égalisons les deux expressions pour r_n :

$$r_n = u_k r_k + v_k r_{k-1} = u_{k-1} r_{k-1} + v_{k-1} r_{k-2} \quad (2.49)$$

dans laquelle nous substituons $r_{k-2} = q_{k-1} r_{k-1} + r_k$ et nous égalisons les coefficients de r_k et r_{k-1} :

$$u_k r_k + v_k r_{k-1} = u_{k-1} r_{k-1} + v_{k-1} (q_{k-1} r_{k-1} + r_k), \quad (2.50)$$

cela donne

$$\begin{cases} v_{k-1} = u_k \\ u_{k-1} = v_k - v_{k-1} q_{k-1}. \end{cases} \quad (2.51a)$$

$$(2.51b)$$

Dès que u_k et v_k ainsi que q_{k-1} sont connus, on peut calculer u_{k-1} et v_{k-1} .

La dernière équation, celle avec $k = 1$, est

$$r_n = u_1 r_1 + v_1 r_0, \quad (2.52)$$

c'est à dire

$$\text{pgcd}(A, B) = u_1 B + v_1 A. \quad (2.53)$$

Nous avons ainsi résolu Bézout.

Lemme 2.32 (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. Vu que a est premier avec c , nous avons $\text{pgcd}(a, c) = 1$ et Bézout (2.24) 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 . $\square$

Lemme 2.33 (Lemme d'Euclide[18]).

Si un nombre premier p divise le produit de deux nombres entiers b et c , alors p divise b ou c .

Démonstration. Vu que p est premier, si il ne divise pas a c'est que $\text{pgcd}(a, p) = 1$. Dans ce cas le lemme de Gauss 2.32 implique que p divise b . $\square$

2.5.4 Écriture des fractions

Théorème 2.34.

Tout élément de $\mathbb{Q}^+$ s'écrit de façon unique comme quotient de deux entiers premiers entre eux.

Démonstration. En deux parties

Unicité Supposons avoir $\frac{a}{b} = \frac{c}{d}$ avec $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. Nous avons

$$ad = bc \quad (2.54)$$

donc

(1) a divise bc mais est premier avec b donc a divise c par le lemme de Gauss 2.32.

(2) c divise ad mais est premier avec d donc c divise a par le lemme de Gauss 2.32.

En conclusion a divise c et c divise a , ergo $a = c$. L'égalité $b = d$ est alors immédiate.

Existence Soit le quotient $\frac{a}{b}$. Nous avons

$$\frac{a}{b} = \frac{a/\text{pgcd}(a, b)}{b/\text{pgcd}(a, b)}, \quad (2.55)$$

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. $\square$

Proposition 2.35.

Les entiers p et q sont premiers entre eux si et seulement si p^2 et q^2 sont premiers entre eux.

Démonstration. Si p^2 et q^2 sont premiers entre eux, par le théorème de Bézout 2.24 il exist $ea, b \in \mathbb{Z}$ tels que

$$ap^2 + bq^2 = 1 \quad (2.56)$$

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.

Réciproquement, supposons que p et q ne sont pas premiers entre eux. Alors $\text{pgcd}(p, q) = k \neq 1$. L'entier k divise p et donc p^2 ; et l'entier k divise q et donc q^2 . Au final, k divise p^2 et q^2 , ce qui montre que p^2 et q^2 ne sont pas premiers entre eux. $\square$

Une des conséquences de ces résultats sera le fait que $\sqrt{n}$ est irrationnelle dès que n n'est pas un carré parfait, théorème 11.53.

2.5.5 Équation diophantienne linéaire à deux inconnues

Soient a , b et c des entiers naturels donnés. Nous considérons l'équation

$$ax + by = c \quad (2.57)$$

à résoudre[19] pour $(x, y) \in \mathbb{N}^2$.

Si a ou b est nul, c'est facile ; nous supposons donc que a et b sont tout 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

$$d(a'x + b'y) = c, \quad (2.58)$$

et donc si c n'est pas un multiple de d , il n'y a pas de solutions⁴. Si par contre c est un multiple de d alors nous écrivons $c = c'd$ et l'équation devient

$$a'x + b'y = c' \quad (2.59)$$

C'est maintenant que nous utilisons le théorème de Bézout 2.24 : vu que a' et b' sont premiers entre eux, nous avons la relation $a'u + b'v = 1$ pour certains⁵ 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 :

$$a'(x - c'u) = b'(c'v - y). \quad (2.60)$$

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 forcément⁶ diviser $c'v - y$. Disons $c'v - y = ka'$. Alors $a'(x - c'u) = b'ka'$ et donc

$$x = b'k + c'u. \quad (2.61)$$

Nous trouvons alors une expression pour y en injectant cela dans $a'x + b'y = c'$ et en utilisant Bézout : $a'c'u = (1 - b'v)c'$. Au final nous avons prouvé que toutes les solutions sont de la forme

$$\begin{cases} x = b'k + c'u \\ y = v'c' - a'k \end{cases} \quad \begin{matrix} (2.62a) \\ (2.62b) \end{matrix}$$

avec $k \in \mathbb{Z}$. Si nous voulons réellement seulement des 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 (2.62) sont solutions.

Exemple 2.36

Résoudre l'équation $2x + 6y = 52$.

Nous pouvons factoriser 2 dans le membre de gauche et simplifier alors toute l'équation par 2 :

$$x + 3y = 26. \quad (2.63)$$

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

$$x + 3y = 26 \times (-5 + 3 \times 2), \quad (2.64)$$

et donc $x + 5 \times 26 = 3(y - 26 \times 6)$, et en posant $k = y - 26 \times 6$ nous avons

$$x = 3k - 130. \quad (2.65)$$

En injectant nous trouvons l'équation $3k - 130 + 3y = 26$ et donc

$$y = 52 - k. \quad (2.66)$$

△

4. Exemple : $8x + 2y = 9$. Le membre de gauche est certainement un nombre pair et il n'y a donc pas de solutions.

5. Nous avons décrit un algorithme pour les trouver en démontrant l'équation 2.53.

6. C'est Gauss 2.32 qui le dit, et vous savez que lorsque Gauss dit, c'est *forcément* vrai.

2.5.6 Quotients

Nous écrivons $a = b \pmod p$ essentiellement si il existe $k \in \mathbb{Z}$ tel que $b + kp = a$. Plus généralement nous notons $[a]_p = \{a + kp \mid k \in \mathbb{Z}\}$ et l'écriture « $a = n \pmod p$ » peut tout autant signifier $a = [b]_p$ que $a \in [b]_p$. La différence entre les deux est subtile mais peut de temps en temps valoir son pesant d'or.

Proposition 2.37.

Soit $n \in \mathbb{N}$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est monogène. Si $n \neq 0$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n .

Démonstration. Nous considérons la surjection canonique $\mu: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. Si $a \in \mathbb{Z}$, alors $\mu(a) = a\mu(1)$. Par conséquent $\mathbb{Z}/n\mathbb{Z} = \text{gr}(\mu(1))$ 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 2.22 donne l'existence de q et r avec $0 \leq r < n$ et $q \geq 0$ tels que

$$x_0 = nq + r. \quad (2.67)$$

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

$$\mathbb{Z}/n\mathbb{Z} = \mu(\mathbb{Z}) = \mu(\mathbb{N}_{n-1}). \quad (2.68)$$

La restriction $\mu: \mathbb{N}_{n-1} \rightarrow \mathbb{Z}/n\mathbb{Z}$ 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. $\square$

Lemme 2.38 ([1]).

Soit $q \in \mathbb{N}$ avec $q \geq 2$. Soient $n, d \in \mathbb{N}$ tels que $q^d - 1 \mid q^n - 1$. Alors $d \mid n$.

Démonstration. Par la divisions euclidienne 2.22 il existe $a, b \in \mathbb{Z}$ tels que $n = ad + b$ avec $0 \leq b < d$. En remarquant que $q^d \in [1]_{q^d-1}$ nous avons

$$q^n = (q^d)^a q^b \in [1]_{q^d-1} q^b = [q^b]_{q^d-1}. \quad (2.69)$$

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

$$q^n \in [1]_{q^d-1}. \quad (2.70)$$

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

$$[1]_{q^d-1} = [q^b]_{q^d-1}, \quad (2.71)$$

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 $q \geq 2$, 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. $\square$

2.6 Indice d'un sous-groupe et ordre des éléments

Soit G un groupe fini et H , un sous-groupe. 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 4.43).

Théorème 2.39 (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

$$|G/H| = \frac{|G|}{|H|}. \quad (2.72)$$

Démonstration. Nous commençons par montrer que les classes de H ont toutes les même nombre d'éléments que H . En effet pour chaque $g \in G$ nous avons la bijection

$$\begin{aligned} \varphi: H &\rightarrow gH \\ h &\mapsto gh. \end{aligned} \quad (2.73)$$

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 :

$$|G| = |H| \cdot \text{nombre de classes}. \quad (2.74)$$

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 . $\square$

Corollaire 2.40.

L'ordre d'un élément d'un groupe fini divise l'ordre du groupe. En particulier dans un groupe d'ordre n tous les éléments vérifient $q^n = e$.

Démonstration. Soit G un groupe fini et considérons le sous-groupe

$$H = \{g^k \text{ tel que } k \in \mathbb{N}\}. \quad (2.75)$$

Par le théorème de Lagrange, 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 . $\square$

Le lemme suivant indique que sous hypothèse de commutativité, l'ordre d'un élément est une notion multiplicative.

Lemme 2.41 ([20]).

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 vu que 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

$$a^{r_1s_1}b^{r_1s_1} = (ab)^{r_1s_1} = 1, \quad (2.76)$$

que nous élevons à la puissance r_2 où r_2 est défini en posant $r = r_1r_2$:

$$a^{rs_1}b^{rs_1} = 1. \quad (2.77)$$

Et comme $a^{rs_1} = 1$, nous concluons que $b^{rs_1} = 1$. Donc $s \mid rs_1$. Par le lemme de Gauss (2.32), nous avons en fait $s \mid s_1$. Vu qu'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 $r_1s_1 = rs$. $\square$

Lemme 2.42.

L'ensemble des ordres d'un groupe commutatif est stable par PPCM.

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 :

$$r = \prod_{i=1}^k p_i^{\alpha_i} \quad (2.78a)$$

$$s = \prod_{i=1}^k p_i^{\beta_i} \quad (2.78b)$$

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

$$r' = \prod_{\substack{i=1 \\ \alpha_i > \beta_i}}^k p_i^{\alpha_i} \quad (2.79a)$$

$$s' = \prod_{\substack{i=1 \\ \alpha_i \leq \beta_i}}^k p_i^{\beta_i}, \quad (2.79b)$$

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 2.41 pour conclure que l'ordre de $x^{r/r'}y^{s/s'}$ est $r's' = m$. $\square$

Lemme 2.43 ([21]).

Un sous-groupe d'indice 2 est un sous-groupe normal.

Lemme 2.44 ([22]).

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 $a^m \in H$. $\square$

Proposition 2.45 ([22]).

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 .

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'autres.

Démonstration. Soit H' un sous-groupe d'ordre n . Si $h \in H'$ alors $h^n = 1$ et $h^m \in H$ (lemme 2.44). Étant donné que m et n sont premiers entre eux, il existe $a, b \in \mathbb{Z}$ tels que (Bézout, théorème 2.24)

$$am + bn = 1. \quad (2.80)$$

Du coup $h = h^1 = (h^m)^a (h^n)^b$. En tenant compte du fait que $a^n = 1$ 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 $|H'| = |H| = |G|/m$. $\square$

2.7 Suite de composition

Sources : [23, 24].

Définition 2.46.

Soit G un groupe. Une **suite de composition** pour G est une suite finie de sous-groupes $(G_i)_{i=0,\dots,n}$ telle que

$$\{e\} = G_n \subseteq G_{n-1} \subseteq \dots \subseteq G_1 \subseteq G_0 = G \quad (2.81)$$

et telle que G_{i+1} est normal⁷ dans G_i . Les groupes G_i/G_{i+1} sont les **quotients** de la suite de composition.

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 2.51).

Lemme 2.47 (du papillon[23]).

Soit G un groupe et des sous-groupes A et B . Soit 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

$$\frac{A'(A \cap B)}{A'(A \cap B')} \simeq \frac{(A \cap B)B'}{(A' \cap B)B'} \simeq \frac{B'(A \cap B)}{B'(A' \cap B)}. \quad (2.82)$$

Démonstration. Nous n'allons pas démontrer chacun des points ; nous renvoyons au fameux «preuve très similaire dans les autres cas» pour plus de justifications.

Commençons par montrer que $A'(A \cap B')$ est un groupe. Si $a, b \in A'$ et $x, y \in A \cap B'$,

$$axby = xx^{-1}axbx^{-1}xy \quad (2.83)$$

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

$$x^{-1}a^{-1} = \underbrace{x^{-1}a^{-1}x}_{\in A'} x^{-1}. \quad (2.84)$$

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

$$(bf)^{-1}(ax)(bf) = (bf)^{-1}(a \underbrace{xbx^{-1}}_{\in A'})xf \quad (2.85a)$$

$$= f^{-1}b^{-1}acxf \quad (2.85b)$$

$$= f^{-1}b^{-1}acf \underbrace{f^{-1}xf}_{\in A \cap B'} \quad (2.85c)$$

$$= \underbrace{f^{-1}b^{-1}acf}_{\in A'} y \quad (2.85d)$$

$$\in A'(A \cap B'). \quad (2.85e)$$

Pour prouver l'isomorphisme

$$\frac{A'(A \cap B)}{A'(A \cap B')} = \frac{(A \cap B)B'}{(A' \cap B)B'}, \quad (2.86)$$

nous allons utiliser le deuxième théorème d'isomorphisme (2.19(5)). 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

$$\frac{A'(A \cap B')(A \cap B)}{A'(A \cap B')} \simeq \frac{A \cap B}{A \cap B \cap A'(A \cap B')}. \quad (2.87)$$

7. Nous rappelons au cas où que «normal» signifie «distingué».

Pour simplifier un peu cette expression nous prouvons d'abord que

$$(A \cap B) \cap A'(A \cap B') = (A' \cap B)(A \cap B'). \quad (2.88)$$

L'inclusion $\supset$ est facile. Pour l'autre sens, étant donné que $A'(A \cap B') \subset A$ nous avons

$$A \cap B \cap A'(A \cap B) = B \cap A'(A \cap B). \quad (2.89)$$

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 $x^{-1} \in B'$. Par conséquent $a \in B$ et donc $a \in A' \cap B$. Nous avons donc

$$(A \cap B) \cap A'(A \cap B') = B \cap A'(A \cap B) \subset (A' \cap B)(A \cap B'), \quad (2.90)$$

et donc l'égalité (2.88). Toujours dans l'idée de simplifier (2.87) 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

$$\frac{A'(A \cap B)}{A'(A \cap B')} = \frac{A \cap B}{(A' \cap B)(A \cap B')}. \quad (2.91)$$

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

$$\frac{B'(A \cap B)}{B'(A' \cap B)} = \frac{A'(A \cap B)}{A'(A \cap B')}. \quad (2.92)$$

Nous devons encore justifier $B'(A \cap B) = (A \cap B)B'$ et $B'(A' \cap B) = (A' \cap B)B'$. Faisons le premier et laissons le second au lecteur. Si $b \in B'$ et $x \in A \cap B$, alors

$$bx = x \underbrace{x^{-1}bx}_{\in B'} \in (A \cap B)B'. \quad (2.93)$$

□

Proposition 2.48.

Si G est un groupe fini et que (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 (2.39) s'applique et nous avons à chaque pas de la suite de composition nous avons

$$\left| \frac{G_i}{G_{i+1}} \right| = \frac{|G_i|}{|G_{i+1}|} \quad (2.94)$$

et il suffit d'écrire $|G|$ de façon télescopique :

$$|G| = \prod_{0 \leq i \leq n-1} \frac{|G_i|}{|G_{i+1}|} \quad (2.95)$$

□

Nous disons que les deux suites de composition $(G_i)_{0 \leq i \leq r}$ et $(G_j)_{0 \leq j \leq s}$ sont **équivalentes** si $r = s$ et si il existe une permutation $\sigma \in S_{r-1}$ telle que

$$\frac{G_i}{G_{i+1}} \simeq \frac{H_{\sigma(i)}}{H_{\sigma(i)+1}}. \quad (2.96)$$

Proposition 2.49 (Schreider).

Deux suites de composition d'un même groupe admettent des raffinements équivalents.

Démonstration. Soient les suites de composition

$$\{e\} = G_m \subseteq \dots \subseteq G_1 \subseteq G_0 = G \quad (2.97a)$$

$$\{e\} = H_m \subseteq \dots \subseteq H_1 \subseteq H_0 = G \quad (2.97b)$$

Nous raffinons la suite (G_i) en remplaçant $G_{i+1} \subseteq G_i$ par

$$G_{i+1} = G_{i+1}(G_i \cap H_n) \subset G_{i+1}(G_i \cap H_{n-1}) \subseteq \dots \subseteq G_{i+1}(G_i \cap H_0) = G_i, \quad (2.98)$$

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 2.47 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 de 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

$$\frac{G_{i+1}(G_i \cap H_k)}{G_{i+1}(G_i \cap H_{k+1})} \simeq \frac{H_{k+1}(H_k \cap G_i)}{H_{k+1}(H_k \cap G_{i+1})} \quad (2.99)$$

en vertu du lemme du papillon (2.47). Le membre de droite de (2.99) est un des quotients du raffinement de (H_j) . $\square$

Lemme 2.50 (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. $\square$

Théorème 2.51 (Jordan-Hölder).

Tout groupe fini admet une suite de Jordan-Hölder.

Deux suites de Jordan-Hölder sont équivalentes.

Démonstration. Nous ne prouvons que le second point.

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 2.50. 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. $\square$

2.8 Groupes résolubles

Définition 2.52.

*Le groupe G est **résoluble** si il existe une suite finie de sous-groupes G_i*

$$\{e\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G \quad (2.100)$$

avec G_i normal dans G_{i+1} et G_i/G_{i+1} abélien.

Il s'agit d'un groupe qui admet une suite de composition⁸ dont les quotients sont abéliens.

8. Voir définition 2.46.

Lemme 2.53 ([25]).

Soit G un groupe et H un sous-groupe normal. Le groupe G/H est abélien si et seulement si $D(G) \subset H$.

Démonstration. Les proposition suivantes sont équivalentes :

- Le groupe G/H est abélien
- pour tout $x, y \in G$, $\bar{x}\bar{y} = \bar{y}\bar{x}$
- $\overline{\bar{x}\bar{y}x^{-1}\bar{y}^{-1}} = \bar{e}$
- $\overline{xyx^{-1}y^{-1}} = \bar{e}$
- $[x, y] \in H$
- $D(G) \subset H$.

□

Proposition 2.54 ([25]).

Un groupe est résoluble si et seulement si sa suite dérivée termine sur $\{e\}$.

Démonstration. Grâce au lemme 2.15 et à la proposition 2.16, si la suite dérivée termine sur $\{e\}$ alors la suite dérivée est une suite qui répond aux conditions de la définition 2.52 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

$$\{e\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G \quad (2.101)$$

avec G_i/G_{i+1} abélien et G_{i+1} normal dans G_i . Nous allons prouver par récurrence que $D^i(G) \subset G_i$.

Pour $i = 0$ nous avons bien $G \subset G_0$. Notre hypothèse de récurrence est :

$$D^i(G) \subset G_i \quad (2.102)$$

Par le lemme 2.53 nous avons aussi

$$D(G_i) \subset G_{i+1}. \quad (2.103)$$

En dérivant (2.102) et en tenant compte de (2.103), $D^{i+1}(G) \subset D(G_i) \subset G_{i+1}$. Donc par récurrence nous avons bien $D^k(G) \subset G_k$ pour tout k . Mais $G_r = \{e\}$ pour un certain r , donc pour ce r nous avons $D^r(G) = \{e\}$, ce qu'il fallait. □

Proposition 2.55.

Soient des groupes G et H . Nous supposons que G est résoluble et nous considérons un homomorphisme $\psi: G \rightarrow H$. Alors $\psi(G)$ est résoluble.

Démonstration. Vu que G est résoluble, il existe une suite de sous-groupes G_i tels que

$$\{e\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G \quad (2.104)$$

avec G_i normal dans G_{i+1} et G_i/G_{i+1} abélien. Nous posons $\psi(G)_i = \psi(G_i)$ et nous avons $\psi(G)_n = \psi(\{e\}) = \{e\}$ ainsi que $\psi(G)_0 = \psi(G)$; donc

$$\{e\} = \psi(G)_n \subset \psi(G)_{n-1} \subset \dots \subset \psi(G)_1 \subset \psi(G)_0 = \psi(G). \quad (2.105)$$

Les faits que $\psi(G)_i$ soit normal dans $\psi(G)_{i+1}$ et que $\psi(G)_i/\psi(G)_{i+1}$ soit abélien est directement la proposition 2.13. □

2.9 Action de groupes

Si G agit sur un ensemble E , nous notons $G \cdot x$ l'orbite de $x \in E$ sous l'action de G . Nous notons G_x ou $\text{Stab}(x)$ le stabilisateur de x :

$$G_x = \text{Stab}(x) = \{g \in G \text{ tel que } g \cdot x = x\}. \quad (2.106)$$

Pour $g \in G$, nous notons aussi $\text{Fix}(g)$ le **fixateur** de g :

$$\text{Fix}(g) = \{x \in E \text{ tel que } g \cdot x = x\}. \quad (2.107)$$

Définition 2.56.

L'action de G sur E est **fidèle** si l'identité est le seul élément de G à fixer tous les points de E , c'est à dire si $gx = x \forall x \in E \Rightarrow g = e$.

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 10.33.

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 2.57.

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 $\mathbf{Ad}(g): G \rightarrow G$ 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

$$x \sim_g y \Leftrightarrow xh = y \quad (2.108)$$

pour un certain $h \in H$. Ensuite

$$x \sim_d y \Leftrightarrow hx = y \quad (2.109)$$

pour un certain $h \in H$.

Le lemme suivant est une généralisation du théorème de Lagrange 2.39.

Lemme 2.58.

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

$$\begin{aligned} f: (G/H)_g &\rightarrow (G/H)_d \\ [x]_g &\mapsto [x^{-1}]_d \end{aligned} \quad (2.110)$$

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, soit

$$f([x]_g) = f([y]_h). \quad (2.111)$$

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

$$\begin{aligned} f: [x]_g &\rightarrow [y]_g \\ xh &\mapsto yh. \end{aligned} \quad (2.112)$$

- (3) Le nombre d'éléments dans une classe est égal à $|H|$ par la bijection

$$\begin{aligned} g: [x]_g &\rightarrow H \\ xh &\mapsto h. \end{aligned} \quad (2.113)$$

Par conséquent

$$|G| = |H| \cdot \text{nombre de classes} = |H| \cdot \text{cardinal de } (G/H)_g, \quad (2.114)$$

et nous avons bien

$$\text{cardinal de } (G/H)_g = \frac{|G|}{|H|} = |G : H|. \quad (2.115)$$

□

Proposition 2.59 (Orbite-stabilisateur[21]).

Soit 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 G_x est finie si et seulement si G_x est d'indice fini dans G . Dans ce cas nous avons

$$\text{Card}(G \cdot x) = |G : G_x|. \quad (2.116)$$

Une autre façon d'écrire la même formule :

$$|G| = |\text{Stab}(x)| |\mathcal{O}_x|. \quad (2.117)$$

C'est la formule (2.116) qui est nommée formule des classes sur wikipédia.

Démonstration. (1) Soit l'application

$$\begin{aligned} \psi : G \cdot x &\rightarrow G/G_x \\ a \cdot x &\mapsto [a]. \end{aligned} \quad (2.118)$$

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 $A_y = \{g \in G \text{ tel que } g \cdot x = y\}$. L'ensemble A_y est une classe à gauche de $\text{Stab}(x)$, par conséquent $|A_y| = |\text{Stab}(x)|$ pour tout $y \in \mathcal{O}_x$. Les A_y pour différents y sont disjoints et nous avons de plus

$$\bigcup_{y \in \mathcal{O}_x} A_y = G. \quad (2.119)$$

Les ensemble A_y divisent donc G en $|\mathcal{O}_x|$ paquets de $|\text{Stab}(x)|$ éléments. D'où la formule (2.117).

□

Corollaire 2.60.

Soit C_g la classe de conjugaison de l'élément g du groupe fini G . Alors

$$\text{Card}(C_g) = |G : Z_g| \quad (2.120)$$

Démonstration. Cela est une application directe de la proposition 2.59 dans le cas de l'action adjointe de G sur lui-même. □

Lemme 2.61.

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 .

Corollaire 2.62 (Équation des orbites).

Soit 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) $\text{Card}(E) = \sum_i \text{Card}(\mathcal{O}_i)$.

Définition 2.63.

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 forment une partition de l'ensemble :

$$E = \bigsqcup_{g \in G} f(F), \quad (2.121)$$

union disjointe, c'est à dire que si $g \neq g'$, alors $g(F) \cap g'(F) = \emptyset$.

Proposition 2.64 (Équation des classes[26]).

Soit G , un groupe fini opérant sur un ensemble E . Si E'' est un ensemble contenant exactement un élément de chaque orbite dans $E \setminus \text{Stab}_G(E)$, alors

$$|G| = |\text{Stab}_G(E)| + \sum_{x \in E''} \frac{|G|}{|\text{Stab}_G(x)|}. \quad (2.122)$$

Si de plus G est un p -groupe, alors

$$|E| = |\text{Stab}_G(E)| \pmod{p}. \quad (2.123)$$

Démonstration. Par le corollaire 2.62, 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,

$$|G| = \text{Card}(\text{Stab}_G(E)) + \sum_{x \in E''} \frac{|G|}{|\text{Stab}_G(x)|} \quad (2.124)$$

où nous avons utilisé le fait que $|G| = |\text{Stab}_G(x)| |\mathcal{O}_x|$.

Si G est un p -groupe alors si $x \in E''$, $\text{Stab}_G(x)$ est un sous-groupe propre de G et donc $|\text{Stab}_G(x)|$ est un diviseur propre de $|G|$. Du coup la fraction $|G|/|\text{Stab}_G(x)|$ est une puissance non nulle de p et l'équation (2.122) devient immédiatement (2.123). $\square$

Corollaire 2.65 (Équation des classes).

Soit G , un groupe et $C_1, \dots, C_l$ la liste de ses classes de conjugaison contenant plus d'un éléments. Alors

$$\text{Card}(G) = \text{Card}(Z(G)) + \sum_i |G : Z_{g_i}| = \text{Card}(Z(G)) + \sum_i \frac{\text{Card}(G)}{\text{Card}(\text{Stab}(g_i))} \quad (2.125)$$

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, $\text{Card}(C_{g_i}) = |G : Z_{g_i}|$ par le théorème orbite-stabilisateur (proposition 2.59). $\square$

Théorème 2.66 (Formule de Burnside).

Si G est un groupe fini agissant sur l'ensemble fini E et si Ω est l'ensemble des orbites, alors

$$\text{Card}(\Omega) = \frac{1}{|G|} \sum_{g \in G} \text{Card}(\text{Fix}(g)). \quad (2.126)$$

Démonstration. Nous considérons l'ensemble

$$A = \{(g, x) \in G \times E \text{ tel que } gx = x\}, \quad (2.127)$$

et nous en calculons le cardinal de deux façons. D'abord

$$\text{Card}(A) = \sum_{x \in E} \text{Card}\{g \in G \text{ tel que } gx = x\} \quad (2.128a)$$

$$= \sum_{x \in E} \text{Card}(\text{Stab}(x)) \quad (2.128b)$$

$$= \sum_{\omega \in \Omega} \sum_{x \in \omega} \text{Card}(\text{Stab}(x)) \quad (2.128c)$$

$$= \sum_{x \in \omega} \frac{|G|}{\text{Card}(\omega)} \quad (2.128d)$$

$$= |G|. \quad (2.128e)$$

Pour obtenir (2.128d) nous avons utilisé l'équation des classes (2.117). L'autre façon de calculer $\text{Card}(A)$ est de regrouper ainsi :

$$\text{Card}(A) = \sum_{g \in G} \text{Card}\{x \in E \text{ tel que } gx = x\} = \sum_{g \in G} \text{Card}(\text{Fix}(g)). \quad (2.129)$$

En égalisant les deux expressions de $\text{Card}(A)$ nous trouvons

$$|G| \text{Card}(\Omega) = \sum_{g \in G} \text{Card}(\text{Fix}(g)). \quad (2.130)$$

□

Liens internes vers des applications :

— Le jeu de la roulette et l'affaire du collier, 12.4.8.1 et 12.4.8.2.

Proposition 2.67.

Soit 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.
- (3) Si G est fini de centre Z , alors $|G : H|$ n'est pas premier.

Théorème 2.68.

Soit G un groupe cyclique d'ordre n .

- (1) Tout sous-groupe de G est cyclique.
- (2) Pour chaque diviseur d de n , il existe un unique sous-groupe H_d de G d'ordre d .

Si a est un générateur de G , alors H_d peut être décrit des façons suivantes :

$$H_d = \{x \in G \text{ tel que } x^d = e\} = \{x \in G \text{ tel que } \exists y \in G \text{ tel que } y^{n/d} = x\} = \langle a^{n/d} \rangle. \quad (2.131)$$

Exemple 2.69

Si E est un espace vectoriel alors $(E, +)$ est un groupe commutatif. L'inverse de x est $-x$. △

Définition 2.70.

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 $g = g'$.

2.10 Le groupe symétrique

Définition 2.71.

Le **groupe symétrique** S_n est le groupe des permutations de l'ensemble $\{1, \dots, n\}$. C'est donc l'ensemble des bijections $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$.

Plus généralement le groupe symétrique d'un ensemble est le groupe des bijections de cet ensemble sur lui-même.

Nous disons qu'un élément $s \in S_n$ **inverse** les nombres $i < j$ si $s(i) > s(j)$. Soit N_s le nombre d'inversions que $s \in S_n$ possède (c'est le nombre de couples (i, j) avec $i < j$ tels que $s(i) > s(j)$). L'entier

$$\epsilon(s) = (-1)^{N_s} \quad (2.132)$$

est la **signature** de s .

Un élément du groupe symétrique S_n peut être décomposé en produit de cycles de support disjoints de la façon suivante. D'abord écrire le cycle qui correspond à l'orbite de 1. Ce sera le cycle

$$(1, \sigma 1, \sigma^2 1, \dots, \sigma^k 1) \quad (2.133)$$

avec $\sigma^{k+1} 1 = 1$. Ensuite nous recommençons avec le plus petit élément de $\{1, \dots, n\}$ à ne pas être dans ce cycle, et puis le suivant, etc. La *structure* d'une telle décomposition est la donnée des nombres k_i donnant le nombre de cycles de longueur i .

Lemme 2.72 ([21]).

Soit $c = (i_1, \dots, i_k) \in S_n$, un cycle de longueur k et $s \in S_n$. Alors

$$csc^{-1} = (s(i_1), \dots, s(i_k)). \quad (2.134)$$

Tous les cycles de longueur k sont conjugués entre eux.

Proposition 2.73 (Classes de conjugaison et structure en cycles[27]).

Une classe de conjugaison dans S_n est formée des permutations ayant une décomposition en cycle disjoints de même structure. Autrement dit, deux permutations σ et σ' sont conjuguées si et seulement si le nombre k_i de cycles de longueur i dans σ est le même que le nombre k'_i de cycles de longueur i dans σ' .

Démonstration. Soit $\sigma = c_1 \dots c_m$ la décomposition de σ en cycles de supports disjoints. Les c_i sont des cycles de supports disjoints. Si τ est une permutation, alors

$$\sigma' = \tau \sigma \tau^{-1} = (\tau c_1 \tau^{-1}) \dots (\tau c_m \tau^{-1}), \quad (2.135)$$

mais $\tau c_i \tau^{-1}$ est un cycle de même longueur que c_i parce que si $c_i = (a_1, \dots, a_k)$, alors $\tau c_i \tau^{-1} = (\tau(a_1), \dots, \tau(a_k))$. 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 de σ .

Réciproquement, si $\sigma' = c'_1 \dots c'_m$ est une décomposition de σ' en cycles disjoints tels que la longueur de c_i est la même que la longueur de c'_i , alors il suffit de prendre des permutations τ_i telles que $\tau_i c_i \tau_i^{-1} = c'_i$. Vu que les supports sont disjoints, la permutation $\tau_1 \dots \tau_m$ conjugue σ et σ' . $\square$

Exemple 2.74

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

$$C_1 = \{\text{Id}\} \quad (2.136a)$$

$$C_2 = \{(1, 2), (1, 3), (2, 3)\} \quad (2.136b)$$

$$C_3 = \{(1, 2, 3), (2, 1, 3)\}. \quad (2.136c)$$

△

Exemple 2.75

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 2.73). 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 permutations 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.
- (5) Les doubles permutations, du type $(a, b)(c, d)$. Il y a 6 éléments dans cette classe parce qu'un élément est fixé par le choix de deux nombres parmi 4 dans la première des deux permutations.

△

Lemme 2.76 ([15]).

Un k -cycle est une permutation impaire si k est pair et paire si k est impair.

Proposition 2.77.

Tout élément de S_n peut être écrit sous la forme d'un produit fini de transpositions.

Cette décomposition n'est pas à confondre avec celle en cycles de support disjoints. Par exemple $(1, 2, 3) = (1, 3)(1, 2)$.

Proposition 2.78 ([21]).

Soit S_n le groupe symétrique.

- (1) L'application $\epsilon: S_n \rightarrow \{1, -1\}$ 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 $s, t \in S_n$. Afin de montrer que $\epsilon(st) = \epsilon(s)\epsilon(t)$, nous divisons les couples (i, j) tels que $i \neq j$ en 4 groupes suivant que $t(i) \geq t(j)$ et $s(t(i)) \geq s(t(j))$. Nous notons N_1, N_2, N_3 et N_4 le nombre de couples dans chacun des quatre groupes :

(i, j)	$s(t(i)) < s(t(j))$	$s(t(i)) > s(t(j))$
$t(i) < t(j)$	N_1	N_2
$t(i) > t(j)$	N_3	N_4

Nous avons immédiatement $N_t = N_3 + N_4$ et $N_{st} = N_2 + N_4$. Les éléments qui participent à N_s sont ceux où $t(i)$ et $t(j)$ sont dans l'ordre inverse de $s(t(i))$ et $s(t(j))$ (parce que t est une bijection). Donc $N_s = N_2 + N_3$. Par conséquent nous avons

$$\epsilon(s)\epsilon(t)(-1)^{N_2+N_3}(-1)^{N_3+N_4} = (-1)^{N_2+N_4} = (-1)^{N_{st}} = \epsilon(st). \quad (2.137)$$

Nous avons prouvé que ϵ est un homomorphisme. Pour montrer que ϵ est surjectif sur $\{-1, 1\}$ nous devons trouver un élément $t \in S_n$ tel que $\epsilon(t) = -1$. Si t est la transposition $1 \leftrightarrow 2$ alors le couple $(1, 2)$ est le seul à être inversé par t et nous avons $\epsilon(t) = -1$.

Avant de montrer l'unicité, nous montrons que si $s = t_1 \cdots t_k$ alors $\epsilon(s) = (-1)^k$. Pour cela il faut montrer que $\epsilon(t) = -1$ dès que t est une transposition. Soit t , la transposition (i, j) et $c = (i, i+1, \dots, j-1)$ alors le lemme 2.72 dit que

$$t_{ij} = ct_{j-1,j}c^{-1}. \quad (2.138)$$

La signature étant un homomorphisme,

$$\epsilon(t_{ij}) = \epsilon(c)\epsilon(t_{j-1,j})\epsilon(c)^{-1} = \epsilon(t_{j-1,j}) = 1. \quad (2.139)$$

Nous passons maintenant à la prouver l'unicité de la proposition. Soit un homomorphisme surjectif $\varphi: S_n \rightarrow \{-1, 1\}$ et t , une transposition telle que $\varphi(t) = -1$ (qui existe parce que sinon φ ne serait pas surjectif⁹). Si t' est une autre transposition, il existe $s \in S_n$ tel que $t' = sts^{-1}$ (lemme 2.72). Dans ce cas, $\varphi(t') = \varphi(t) = -1$, et si $s = t_1 \dots t_k$,

$$\varphi(s) = (-1)^k = \epsilon(s). \quad (2.140)$$

□

Le groupe A_n des permutations paires est le **groupe alterné**.

Proposition 2.79.

Le groupe alterné est un sous-groupe caractéristique de S_n d'indice 2. C'est le seul sous-groupe d'indice 2 dans S_n .

Démonstration. Soit $\alpha \in \text{Aut}(S_n)$. Étant donné que $\alpha \circ \alpha$ est un homomorphisme surjectif sur $\{-1, 1\}$ nous avons $\alpha \circ \alpha = \epsilon$, et donc $\alpha(A_n) = A_n$. Par le premier théorème d'isomorphisme, il existe un isomorphisme

$$f: S_n / \ker \epsilon \rightarrow \text{Image}(\epsilon). \quad (2.141)$$

En égalisant 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 2.43, 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. Si nous notons φ le morphisme canonique $\varphi: S_n \rightarrow S_n/H$:

$$S_n \xrightarrow{\varphi} S_n/H \xrightarrow{\theta} \{-1, 1\}. \quad (2.142)$$

La composition $\varphi \circ \theta$ est alors un homomorphisme surjectif de S_n sur $\{-1, 1\}$ et nous avons $\varphi \circ \theta = \epsilon$ par la proposition 2.78. L'enchaînement (2.142) nous montre que $H = \ker(\theta \circ \varphi) = \ker(\epsilon) = A_n$. □

Lemme 2.80.

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 2.81 ([28]).

Soit $n \geq 3$. 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

$$c_i = (1, 2, i) = (1, 2)(2, i), \quad (2.143)$$

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 $A_3 = \{\text{Id}, c_3, c_3^2\}$. 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. □

9. Nous utilisons ici le fait que tous les éléments de S_n sont des produits de transpositions, proposition 2.77.

Proposition 2.82.

Lorsque $n \geq 5$, 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. Vu que $n \geq 5$, nous pouvons prendre s et t , des éléments distincts dans $\{1, \dots, n\} \setminus \{j_1, j_2, j_3\}$ et poser $\tau = (st)$. Vu que la signature est un homomorphisme et que τ et α sont impairs, l'élément $\tau\alpha$ est pair (lemme et proposition 2.76 et 2.77) et est donc dans A_n . Les supports de τ et φ étant disjoints, ces derniers commutent et nous avons

$$(\tau\alpha)\sigma(\tau\alpha)^{-1} = \tau(\alpha\sigma\alpha^{-1})\tau^{-1} = \varphi. \quad (2.144)$$

Donc σ et φ sont conjugués par $\tau\alpha$ qui est dans A_n . $\square$

Théorème 2.83 ([15]).

Le groupe alterné A_n est simple pour $n \geq 5$.

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 2.81) et que tous les 3-cycles sont conjugués dans A_n (proposition 2.82), il suffit de montrer que N contient un 3-cycle. En effet si N contient un 3-cycle, le fait qu'il soit normal implique (par conjugaison) qu'il les contienne tous et donc qu'il contient une partie génératrice de A_n .

Soit donc $\sigma \in N$ différent de l'identité. Nous prenons i dans le support de σ et $j = \sigma(i)$. Nous choisissons ensuite $k \in \{1, \dots, n\} \setminus \{i, j, \sigma^{-1}(i)\}$ et $m = \sigma(k)$. Nous considérons la permutation $\alpha = (ijk)$. Étant donné que N est normal l'élément

$$\theta = \alpha^{-1}\sigma\alpha\sigma^{-1} \quad (2.145)$$

est dans N . De plus en utilisant le lemme 2.72 et le fait que $\alpha^{-1} = (ikj)$ nous avons

$$\theta = (ijk)(j\sigma(j)m). \quad (2.146)$$

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 $j \neq \sigma(j)$ parce que i est dans le support de σ ; $m \neq i$ parce que $k \neq \sigma^{-1}(i)$; $i \neq m$ parce que $k \neq \sigma^{-1}(i)$. Les seules possibilités d'égalités sont $i = \sigma(j)$, $\sigma(j) = k$ et $m = k$ (et les combinaisons, mais toutes ne sont pas possibles).

Si $i, j, k, \sigma(j)$ et m sont cinq nombres différents, alors

$$\theta = (i, j, \sigma(j), m, k) \quad (2.147)$$

est un 5-cycle.

Si $i = \sigma(j)$, alors

$$\theta = (imk) \quad (2.148)$$

qui est un 3-cycle. Notons que i, m et k sont bien trois éléments différents.

Si $\sigma(j) = k$, alors

$$\theta = (ikm) \quad (2.149)$$

qui est encore un 3-cycle.

Si $m = k$, nous avons

$$\theta = (ik)(j\sigma(j)). \quad (2.150)$$

C'est a priori un 2×2 -cycle. Mais si de plus $i = \sigma(j)$, alors

$$\theta = (ijk) \quad (2.151)$$

qui est un 3-cycle. Et si $k = \sigma(j)$, alors

$$\theta = (ikj) \quad (2.152)$$

qui est un autre 3-cycle.

Bref nous avons montré que θ est soit un 3-cycle, soit un 5-cycle, soit un 2×2 -cycle. Si θ est un 3-cycle, la preuve est terminée.

Si $\theta = (ab)(cd)$, alors on considère $e \in \{1, \dots, n\} \setminus \{a, b, c, d\}$ et nous avons

$$\underbrace{(abe)^{-1} \theta (abe)}_{\in N} \theta^{-1} = (aeb)(ab)(cd)(abe)(an)(cd) = (abe) \in N. \quad (2.153)$$

Si θ est le 5-cycle $(abcde)$, alors l'élément suivant est dans N :

$$(abc)^{-1} \theta (abc) \theta^{-1} = (acb)(abcde)(abc)(aedcb) = (acd). \quad (2.154)$$

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. $\square$

Nous en déduisons immédiatement que si $n \geq 5$, le groupe dérivé de A_n est A_n parce que A_n ne contient pas d'autres sous-groupes non triviaux.

Le théorème suivant montre que tout groupe peut être vu, en agissant sur lui-même, comme une partie du groupe symétrique.

Théorème 2.84.

Un groupe G est isomorphe à un sous-groupe de son groupe symétrique $S(G)$.

Démonstration. Nous considérons φ , la translation à gauche :

$$\begin{aligned} \varphi: G &\rightarrow S(G) \\ g &\mapsto t_g \end{aligned} \quad (2.155)$$

où $f_g(h) = gh$. Étant donné que

$$\varphi(gh) = ghx = g(t_h x) = t_g \circ t_h(x), \quad (2.156)$$

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 $\text{Image}(\varphi)$ est donc un sous-groupe de $S(G)$, et φ est un isomorphisme vers ce groupe. $\square$

2.11 Produit semi-direct de groupes

Une **suite exacte** est une suite d'applications comme suit :

$$\dots \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots \quad (2.157)$$

où pour chaque i , les application 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 de homomorphismes.

Très souvent nous sommes confrontés à des suites exactes de la forme

$$1 \longrightarrow A \xrightarrow{f} G \xrightarrow{g} B \longrightarrow 1 \quad (2.158)$$

où G , A et B sont des groupes, 1 est l'identité. La première flèche est l'application $\{1\} \rightarrow A$ qui à 1 fait correspondre 1. La dernière est l'application $B \rightarrow 1$ 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 2.85.

Soient N et H deux groupes et un morphisme de groupes $\phi: H \rightarrow \text{Aut}(N)$. Le **produit semi-direct** de N et H relativement à ϕ , noté $N \rtimes_{\phi} H$ est l'ensemble $N \times H$ muni de la loi (que l'on vérifiera être de groupe)

$$(n, h) \cdot (n', h') = (n\phi_h(n'), hh'). \quad (2.159)$$

Attention à l'ordre quelque peu contre intuitif. Lorsque nous notons $N \rtimes_{\phi} H$, c'est bien $\phi: H \rightarrow \text{Aut}(N)$, 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 2.57.

Le théorème suivant permet de reconnaître des produits semi-directs lorsqu'on en voit un.

Théorème 2.86 ([29]).

Soit une suite exacte de groupes

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{s} H \longrightarrow 1 \quad (2.160)$$

Si il existe un sous-groupe $\tilde{H}$ de G à partir duquel s est un isomorphisme, alors

$$G \simeq i(N) \rtimes_{\sigma} \tilde{H} \quad (2.161)$$

où σ est l'action adjointe¹⁰ 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 $\ker(s)$.
- (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 aurions $h = h'$ et immédiatement après $n = n'$.
- (5) L'application

$$\begin{aligned} \phi: G &\rightarrow \tilde{N} \times \tilde{H} \\ nh &\mapsto (n, h) \end{aligned} \quad (2.162)$$

est une bijection. C'est une conséquence des points (3) et (4).

- (6) Si sur $\tilde{N} \times \tilde{H}$ nous mettons le produit

$$(n, h) \cdot (n', h') = (n\sigma_h(n'), hh') \quad (2.163)$$

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

$$\phi(nhn'h') = \phi(n \underbrace{hn'h^{-1}}_{\in \tilde{N}} hh') \quad (2.164a)$$

$$= \phi((nhn'h^{-1})(hh')) \quad (2.164b)$$

$$= (nhn'h^{-1}, hh') \quad (2.164c)$$

$$= (n, h) \cdot (n', h') \quad (2.164d)$$

$$= \phi(nh)\phi(n'h'). \quad (2.164e)$$

10. Le fait que H agisse sur $i(N)$ fait partie du théorème.

□

Corollaire 2.87.

Soit G un groupe, et N, H des sous-groupes de G tels que

- (1) H normalise N (c'est à dire que $hnh^{-1} \in N$ pour tout $h \in H$ et $n \in N$ ¹¹),
- (2) $H \cap N = \{e\}$,
- (3) $HN = G$.

Alors l'application

$$\begin{aligned} \psi: N \times_{\sigma} H &\rightarrow G \\ (n, h) &\mapsto nh \end{aligned} \quad (2.165)$$

est un isomorphisme de groupes.

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 .

2.12 Isométries du cube

Les isométries du cube proviennent de [1].

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-groupes de G constitué des éléments de déterminant positif. Nous notons

$$\mathcal{D} = \{D_1, \dots, D_4\} \quad (2.166)$$

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

$$\rho: G \rightarrow S_4. \quad (2.167)$$

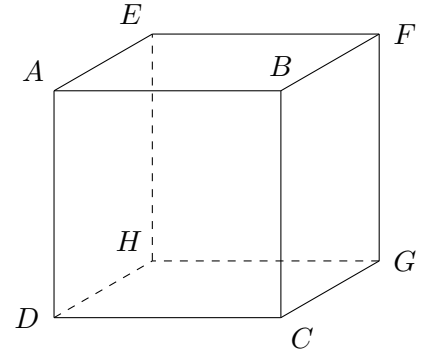
Nous montrons ce que morphisme est surjectif en montrant qu'il contient les transpositions. Le groupe G contient la symétrie axiale passant par le milieu M de $[AE]$ et le milieu N de $[CG]$. Il est facile de voir que cette symétrie permute $[AG]$ avec $[EC]$. De plus elle laisse $[FD]$ inchangée. En effet, aussi incroyable que cela paraisse en regardant le dessin, nous avons $FD \perp MN$, parce qu'en termes de vecteurs directeurs,

$$\overrightarrow{ON} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \quad \overrightarrow{OF} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}. \quad (2.168)$$

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, $d(f(B), f(G)) = d(B, G)$, 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 :

$$\ker(\rho) = \{\text{Id}, s_0\}. \quad (2.169)$$

11. Ou encore que H agit sur N par automorphismes internes.



Le premier théorème d'isomorphisme 2.17 nous permet d'écrire le quotient de groupes :

$$\frac{G}{\{\text{Id}, s_0\}} \simeq S_4. \quad (2.170)$$

Une classe d'équivalence modulo $\ker(\rho)$ dans G est donc toujours de la forme $\{f, f \circ s_0\}$. Et vu que 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 que en tant que matrice, $s_0 = -\mathbb{I}$, donc les problèmes de commutativité ne se posent pas. L'application

$$\begin{aligned} \varphi: \frac{G}{\{\text{Id}, s_0\}} &\rightarrow G^+ \\ [g] &\mapsto \begin{cases} g & \text{si } \det(g) > 0 \\ g \circ s_0 & \text{sinon} \end{cases} \end{aligned} \quad (2.171)$$

est un isomorphisme de groupes. Et enfin nous pouvons écrire

$$G^+ \simeq S_4. \quad (2.172)$$

Nous allons maintenant utiliser le corollaire 2.87 pour montrer que $G = G^+ \times_{\sigma} \ker(\rho)$. Les conditions sont remplies :

- $\ker(\rho)$ normalise G^+ parce que $\ker(\rho)$ ne contient que $\pm \mathbb{I}$.
- $\ker(\rho) \cap G^+ = \{\text{Id}\}$.
- $\ker(\rho)G^+ = G$ parce que les classes d'équivalence de G modulo $\ker(\rho)$ sont composées de $\{f, f \circ s_0\}$.

Vu que $G^+ \simeq S_4$ et $\ker(\rho) \simeq \mathbb{Z}/2\mathbb{Z}$ nous pouvons écrire de façon plus brillante que

$$G \simeq S_4 \times_{\sigma} \mathbb{Z}/2\mathbb{Z}. \quad (2.173)$$

Mais étant donné que la conjugaison par s_0 est triviale, le produit semi-direct est un produit direct :

$$G \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}. \quad (2.174)$$

Il est maintenant du meilleur goût de pouvoir identifier géométriquement ces éléments. Les éléments de $\mathbb{Z}/2\mathbb{Z} = \{\text{Id}, s_0\}$ ne font pas de mystères. Dans S_4 nous avons les classes de conjugaison des éléments Id , (12) , (123) , (1234) et $(12)(34)$ déterminées durant l'exemple 2.75.

- (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 :

$$B \rightarrow D \rightarrow E \rightarrow B. \quad (2.175)$$

C'est une rotation est d'angle $\frac{2\pi}{3}$. Cela sont 8 rotations d'ordre 3.

Notons à ce propos que la différence entre (234) et (243) est que la première fait une rotation d'angle $2\pi/3$ tandis que la seconde fait 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 précédente¹², c'est à dire les rotations d'angle π autour des mêmes axes. Cela fait 3 éléments d'ordre 2.

12. En fait c'est $(13)(24)$, le carré de la précédente, mais c'est la même classe de conjugaison.

2.13 Groupe de torsion

Soit G un groupe. Un élément $g \in G$ est un **élément de torsion** si il est d'ordre fini. La **torsion** de G est l'ensemble de ses éléments de torsion. Nous disons qu'un groupe est un **groupe de torsion** si tous ses éléments sont de torsion.

Exemple 2.88

Le groupe additif $\mathbb{Q}/\mathbb{Z}$ est un groupe de torsion parce que si $[x] = [p/q]$, alors $q[x] = [p] = [0]$.

△

2.14 Famille presque nulle

Soit $(G, +)$ un groupe abélien et $\mathcal{F} = \{g_i\}_{i \in I}$ une famille d'éléments de G indicés par un ensemble I . Le **support** de $\mathcal{F}$ est l'ensemble $\{i \in I \text{ tel que } g_i \neq 0\}$. La famille est dite **presque nulle** si le support est fini.

Nous disons que $\mathcal{F}$ est une **suite** si $I = \mathbb{N}$.

Chapitre 3

Anneaux

3.1 Généralités

Soit X un ensemble et A un anneau. Nous considérons $\mathbf{Fun}(X, A)$ l'ensemble des applications $X \rightarrow A$. Cet ensemble devient un anneau avec les définitions

$$(f + g)(x) = f(x) + g(x) \quad (3.1a)$$

$$(fg)(x) = f(x)g(x). \quad (3.1b)$$

Cela est la **structure canonique** d'anneau sur $\mathbf{Fun}(X, A)$.

Le **centralisateur** de $x \in A$ dans A est l'ensemble

$$\{y \in A \text{ tel que } xy = yx\}, \quad (3.2)$$

le **centre** de A est

$$\{y \in A \text{ tel que } xy = yx \forall x \in A\}. \quad (3.3)$$

Un élément $a \in A$ est **régulier à droite** $ba = 0$ implique $b = 0$. Il est régulier à gauche si $ab = 0$ implique $b = 0$.

L'ensemble $U(A)$ des éléments inversibles de A est un groupe pour la multiplication. Nous notons $A^* = A \setminus \{0\}$.

Lemme 3.1.

Si a et b commutent, nous avons la formule

$$a^{r+1} - b^{r+1} = (a - b) \left(\sum_{k=0}^r a^{r-k} b^k \right). \quad (3.4)$$

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 (3.4) nous avons

$$1 = 1 - a^n = (1 - a)(1 + a + \dots + a^{n-1}) = (1 + a + \dots + a^{n-1})(1 - a). \quad (3.5)$$

La somme $1 + a + \dots + a^{n-1}$ est donc un inverse de $(1 - a)$. $\square$

Définition 3.3.

Soit $\mathbb{A}$ un anneau et $a, b \in \mathbb{A}$. Nous disons que d est un pgcd de a et b si tout diviseur commun de a et b divise d .

Définition 3.4.

*Si A et B sont des anneaux, un **morphisme** est une application $f: A \rightarrow B$ telle que pour tout $x, y \in A$ nous ayons*

- (1) $f(x + y) = f(x) + f(y)$
- (2) $f(xy) = f(x)f(y)$
- (3) $f(1) = 1$

Si f est un morphisme, nous avons $f(0) = 0$ et $f(x)^{-1} = f(x^{-1})$.

3.2 Binôme de Newton et morphisme de Frobenius

Proposition 3.5.

Pour tout $x, y \in \mathbb{R}$ et $n \in \mathbb{N}$, nous avons

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \quad (3.6)$$

où

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (3.7)$$

sont les **coefficients binomiaux**.

La preuve qui suit provient de wikipédia.

Démonstration. La preuve se fait par récurrence. La vérification pour $n = 0$ et $n = 1$ sont faciles. Supposons que la formule (3.6) soit vraie pour n , et prouvons la pour $n + 1$. Nous avons

$$\begin{aligned} (x + y)^{n+1} &= (x + y) \cdot \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\ &= \sum_{k=0}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^n \binom{n}{k} x^{n-k} y^{k+1} \\ &= x^{n+1} + \sum_{k=1}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} + y^{n+1}. \end{aligned} \quad (3.8)$$

La seconde grande somme peut être transformée en posant $i = k + 1$:

$$\sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} = \sum_{i=1}^n \binom{n}{i-1} x^{n-(i-1)} y^{i-1+1}, \quad (3.9)$$

dans lequel nous pouvons immédiatement renommer i par k . En remplaçant dans la dernière expression de (3.8), nous trouvons

$$(x + y)^{n+1} = x^{n+1} + y^{n+1} + \sum_{k=1}^n \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n-k+1} y^k. \quad (3.10)$$

La thèse découle maintenant de la formule

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \quad (3.11)$$

qui est vraie parce que

$$\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)(n-k+1)!} = \frac{n!(n-k+1) + n!k}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n-k+1)!}, \quad (3.12)$$

par simple mise au même dénominateur. □

3.3 Décomposition en facteurs premiers

Le théorème fondamental de l'arithmétique permet de décomposer des nombres en facteurs premiers.

Théorème 3.6 ([30]).

Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

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.

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. La le lemme d'Euclide 2.33, 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. $\square$

En d'autres termes, pour tout entier $n > 1$, il existe une suite finie unique $(p_1, k_1), \dots, (p_r, k_r)$ 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) $n = \prod_{i=1}^r p_i^{k_i}$.

3.4 Le groupe des racines de l'unité

Définition 3.7.

Une **racine n^e de l'unité** est une racine du polynôme $X^n - 1$.

Dans $\mathbb{C}$ nous avons au maximum n telles racines, et il est facile de voir qu'il y en a effectivement n distinctes données par les éléments du groupe multiplicatif

$$U_n = \{e^{2i\pi k/n} \text{ tel que } k = 0, \dots, n-1\} \quad (3.13)$$

Un des intérêts du groupe des racines est qu'il permet de factoriser $X^n - 1$, comme nous le verrons via les polynômes cyclotomiques dans le lemme 4.108.

Lemme 3.8.

L'ensemble U_n est un groupe cyclique¹ d'ordre n généré par $\xi = e^{2i\pi/n}$.

Démonstration. Il y a les trois propriétés à vérifier pour que ce soit un groupe.

Neutre Le nombre 1 est une racine de l'unité.

Inverse Si $\omega \in U_n$ alors $\omega^n = 1$ et donc $\omega\omega^{n-1} = 1$, ce qui signifie que ω^{n-1} est un inverse de ω . Il reste à voir que $\omega^{n-1} \in U_n$. En effet $(\omega^{n-1})^n = (\omega^n)^{n-1} = 1^{n-1} = 1$.

1. Définition 2.4.

Associativité Cas particulier de l'associativité dans $\mathbb{C}$.

Le fait que ce soit un groupe cyclique contenant n éléments est la définition. $\square$

Le lemme suivant donne les autres générateurs.

Lemme 3.9.

Le nombre ξ^a est un générateur de U_n si et seulement si $\text{pgcd}(a, n) = 1$.

Démonstration. Si $\text{pgcd}(a, n) = 1$ alors le théorème de Bézout 2.24 nous fournit des entiers u et v tels que $ua + vn = 1$. Alors nous avons

$$e^{2i\pi/n} = e^{2(ua+vn)i\pi/n} = (e^{2ai\pi/n})^u, \quad (3.14)$$

ce qui signifie que ξ est dans le groupe engendré par ξ^a , et par conséquent tout U_n est engendré.

Pour l'implication inverse, nous utilisons Bézout dans le sens inverse. Soit ξ^a un générateur de U_n . Alors il existe u tel que $(\xi^a)^u = \xi$, donc $\xi^{au-1} = 1$, c'est à dire qu'il existe v tel que $au - 1 = vn$. Cette dernière égalité implique que $\text{pgcd}(a, n) = 1$. $\square$

Exemple 3.10

Une conséquence tout à fait extraordinaire de ce lemme est que 7 est générateur de $\mathbb{Z}/12\mathbb{Z}$ (parce que $\text{pgcd}(7, 12) = 1$). Or en solfège, une quinte fait 7 demi-tons, et une gamme en fait 12. Le cycle des quintes est donc générateur de la gamme[31]. Cela est un fait connu des pianistes² depuis des siècles. $\triangle$

Proposition 3.11 (Intersection par deux).

Les ensembles U_α et U_β ont une intersection non réduite à $\{1\}$ si et seulement si α et β ne sont pas premiers entre eux.

Démonstration. Nous rappelons qu'une racine α^e de l'unité peut s'écrire sous la forme $e^{2i\pi k/\alpha}$ avec $0 \leq k < \alpha$.

Sens direct Nous supposons que $z \in U_\alpha \cap U_\beta$. Le fait que z soit une racine α^e de l'unité implique qu'il existe un $k < \alpha$ tel que $z = e^{2i\pi k/\alpha}$. Mais si z est également une racine β^e de l'unité, alors $z^\beta = 1$, c'est à dire que $k\beta/\alpha$ doit être un entier, soit l cet entier. Nous avons

$$k\beta = l\alpha. \quad (3.15)$$

Le nombre α divise $k\beta$; et si nous supposons que α et β étaient premiers entre eux, cela conduirait via le lemme de Gauss 2.32 à dire que α divise k . Mais α ne peut pas diviser k parce que nous avons supposé que k était strictement plus petit que α .

Sens réciproque Nous supposons maintenant que α et β ne sont pas premiers entre eux, et nous notons d leur pgcd. Nous nommons $\alpha = d\alpha'$ et $\beta = d\beta'$. Pour trouver une intersection entre U_α et U_β nous devons trouver une valeur de $k < \alpha$ telle que

$$(e^{2i\pi k/\alpha})^\beta = e^{2i\pi k\beta/\alpha} = 1, \quad (3.16)$$

c'est à dire une valeur de k telle que $k\beta/\alpha$ soit un entier. Mais $k\beta/\alpha = k\beta'/\alpha'$ et par conséquent prendre $k = \alpha'$ fonctionne. Surtout que par hypothèse $d > 1$ et donc $k = \alpha' < \alpha$. $\square$

Proposition 3.12 (Intersection : le cas général[8]).

Soient des entiers positifs $\alpha_1, \dots, \alpha_p$. Nous avons

$$\bigcup_{i=1}^p U_{\alpha_i} = \{1\} \quad (3.17)$$

si et seulement si $\text{pgcd}(\alpha_1, \dots, \alpha_p) = 1$ (c'est à dire que les α_i sont premiers dans leur ensemble).

2. Même ceux qui ignorent le théorème de Bézout.

Démonstration. Nous le décomposons les α_i en facteurs premiers³ de la façon suivante : $\alpha_i = \prod_{k \in \mathbb{N}} p_k^{\alpha_i^{(k)}}$ où les p_k sont les nombres premiers.

Caractérisation par une décomposition en facteurs premiers Les éléments z différents de 1 dans U_{α_1} s'écrivent sous la forme

$$z = e^{2i\pi k/\alpha_1} \quad (3.18)$$

avec $0 < k < \alpha_1$.

Pour tout $i \neq 1$, le fait que $z \in U_{\alpha_i} \cap U_{\alpha_1}$ se traduit par le fait que $(e^{2i\pi k/\alpha_1})^{\alpha_i} = 1$, c'est à dire que $\alpha_i k/\alpha_1$ est entier, donc que α_1 divise $k\alpha_i$. Par conséquent il existera un élément différent de 1 dans l'intersection des U_{α_i} si et seulement si il existe un entier k strictement compris entre 0 et α_1 pour lequel α_1 divise tous les $k\alpha_i$.

Un entier $0 < k < \alpha_1$ convient si et seulement si pour tout l , la puissance de p_l dans la décomposition de k est au moins égale à

$$\alpha_1^{(l)} - \alpha_i^{(l)} \quad (3.19)$$

pour tout l .

Sens direct L'hypothèse $\text{pgcd}(\alpha_1, \dots, \alpha_p) \neq 1$ implique qu'il existe un l pour lequel tous les $\alpha_i^{(l)}$ sont non nuls. Nous construisons le k voulu en prenant pour tout p_i la même puissance que celle dans α_1 , sauf pour p_l pour lequel nous prenons la puissance $\alpha_1^{(l)} - \min_i \{\alpha_i^{(l)}\}$. Le minimum en question est strictement positif, ce qui donne un k strictement inférieur à α_1 .

Sens réciproque Si $\text{pgcd}(\alpha_1, \dots, \alpha_p) = 1$ alors pour tout l , il existe un i tel que $\alpha_i^{(l)} = 0$. Donc pour tout l , la puissance de p_l dans la décomposition de k est au moins $\alpha_1^{(l)}$. Cela implique que $k \geq \alpha_1$, ce qui est impossible.

□

Définition 3.13.

Les générateurs de U_n sont les **racines primitives**⁴ de l'unité dans $\mathbb{C}$. Nous nommons Δ_n leur ensemble :

$$\Delta_n = \{e^{2ki\pi/n} \text{ tel que } 0 \leq k \leq n-1, \text{pgcd}(k, n) = 1\}. \quad (3.20)$$

Nous avons par exemple

$$\Delta_1 = \{1\} \quad (3.21a)$$

$$\Delta_2 = \{e^{\pi i}\} \quad (3.21b)$$

$$\Delta_4 = \{e^{\pi i/2}, e^{3\pi i/2}\}. \quad (3.21c)$$

Notons que $1 \in \Delta_d$ seulement avec $d = 1$.

3.5 Fonction indicatrice d'Euler (première partie)

Nous introduisons ici la fonction indicatrice d'Euler et ses liens basiques avec les racines de l'unité. Pour les propriétés plus avancées, voir 12.6.5.

3. Théorème 3.6.

4. parce qu'en prenant les puissances successives de l'une d'entre elles, nous retrouvons toutes les racines de l'unité, voir aussi la définition 4.146.

3.5.1 Introduction par les racines de l'unité

Définition 3.14.

La fonction φ donnée par

$$\varphi(n) = \text{Card}(\Delta_n) \quad (3.22)$$

est l'*indicatrice d'Euler*.

Si p est un nombre premier, alors $\varphi(p) = p - 1$.

Lemme 3.15.

Nous avons

$$U_n = \bigcup_{d|n} \Delta_d \quad (3.23)$$

et l'union est disjointe. Nous avons aussi la formule

$$n = \sum_{d|n} \varphi(d). \quad (3.24)$$

Démonstration. À l'application $x \mapsto e^{2i\pi x}$ près, nous pouvons considérer

$$\Delta_d = \left\{ \frac{k}{d} \text{ tel que } k = 0, \dots, d-1, \text{pgcd}(k, d) = 1 \right\}, \quad (3.25)$$

c'est à dire l'ensemble des fractions irréductibles dont le dénominateur est d . L'union des Δ_d sera donc disjointe.

Toujours à l'application $x \mapsto e^{2i\pi x}$ près, le groupe U_n est donné par

$$U_n = \left\{ \frac{k}{n} \text{ tel que } k = 0, \dots, n-1 \right\}. \quad (3.26)$$

L'égalité (3.23) revient maintenant à dire que toute fraction de la forme $\frac{k}{n}$ s'écrit de façon irréductible avec un dénominateur qui divise n .

La relation (3.24) consiste à prendre le cardinal des deux côtés de (3.23). Nous avons $\text{Card}(U_n) = n$ et l'union étant disjointe, à droite nous avons la somme des cardinaux.

Pour chaque diviseur d de n nous considérons l'ensemble

$$\Phi_n(d) = \left\{ n \in \mathbb{N} \text{ tel que } \text{pgcd}(n, n) = \frac{n}{d} \right\}. \quad (3.27)$$

Étant donné que tous les entiers entre 0 et n ont un pgcd avec n qui est automatiquement un quotient de n nous avons

$$\{0, \dots, n\} = \bigcup_{d|n} \Phi_n(d) \quad (3.28)$$

où l'union est disjointe. Par ailleurs nous savons que si $\text{pgcd}(a, b) = 1$, alors $\text{pgcd}(ka, kb) = k$. Donc si $n \in \Delta(d)$, alors $n \cdot \frac{n}{d}$ appartient à $\Phi_n(d)$. En d'autres termes, $a \mapsto \frac{n}{d}a$ est une bijection entre $\Delta(d)$ et $\Phi_n(d)$.

Nous avons donc $\text{Card}(\Phi_n(d)) = \text{Card}(\Delta(d)) = \varphi(d)$ et finalement

$$\text{Card}\{1, \dots, n\} = \sum_{d|n} \text{Card}(\Phi_n(d)) = \sum_{d|n} \varphi(d). \quad (3.29)$$

□

Lemme 3.16.

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 $q \leq p^{n-1}$. Il y a évidemment p^{n-1} tels nombres.

Par conséquent le cardinal de P_{p^n} est $\varphi(p^n) = p^n - p^{n-1}$. □

3.5.2 Générateurs

Proposition 3.17.

Soit $n \in \mathbb{N}^*$ 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 $\text{gr}([1]_n) = \mathbb{Z}/n\mathbb{Z}$. L'élément $[x]_n$ sera générateur si et seulement si il génère $[1]_n$, c'est à dire si il existe p tel que $p[x]_n = [1]_n$. Cette dernière égalité étant une égalité de classes dans $\mathbb{Z}/n\mathbb{Z}$, elle sera vraie si et seulement si il existe q tel que

$$px + qn = 1. \quad (3.30)$$

Cela signifie entre autres que $x\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$, c'est à dire que $\text{pgcd}(x, n) = 1$ et que $x \in P_n$. $\square$

3.6 Idéal dans un anneau

La définition d'un idéal dans un anneau est la définition 1.15.

Définition 3.18.

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.

Lorsqu'un ensemble est idéal à gauche et à droite, nous disons que c'est un **idéal bilatère**. Lorsque nous parlons d'idéal sans précisions, nous parlons d'idéal bilatère.

Remarque 3.19.

Un idéal n'est pas toujours un anneau parce que l'identité pourrait manquer. Un idéal qui contient l'identité est l'anneau complet.

Exemple 3.20

L'ensemble $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$. $\triangle$

Soit A , un anneau, I un idéal bilatère⁵ de A . Nous considérons la relation d'équivalence $x \sim y$ si et seulement si $x - y \in I$. Dans ce cas, le quotient

$$A/\sim = A/I \quad (3.31)$$

est un anneau appelé **anneau quotient**. La surjection $A \rightarrow A/I$ est un morphisme.

Proposition 3.21.

Soient A et B des anneaux et un homomorphisme $f: A \rightarrow B$. Nous considérons l'injection canonique $j: f(A) \rightarrow B$ et la surjection canonique $\phi: A \rightarrow A/\ker f$. Alors il existe un unique isomorphisme

$$\tilde{f}: A/\ker f \rightarrow f(A) \quad (3.32)$$

tel que $f = j \circ \tilde{f} \circ \phi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \phi \downarrow & & \downarrow j \\ A/\ker f & \xrightarrow{\tilde{f}} & f(A) \subset B \end{array} \quad (3.33)$$

5. Définition 1.15.

Proposition 3.22.

Soit I , un idéal de A et $\phi: A \rightarrow A/I$ la surjection canonique. Les idéaux de A/I sont les $\phi(J)$ où J est un idéal de A contenant I . De plus cette relation est bijective :

$$\{\text{idéaux de } A \text{ contenant } I\} \simeq \{\text{idéaux de } A/I\}. \quad (3.34)$$

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

$$\phi(i)\phi(j) = \phi(ij) \in \phi(J). \quad (3.35)$$

Soit maintenant K , un idéal dans A/I . 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 $I \subset \phi^{-1}(K)$. $\square$

Corollaire 3.23.

Les quotients de $\mathbb{Z}$ sont $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Tous les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$. En effet en vertu de la proposition 2.20, 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 : si $a \in n\mathbb{Z}$ et si $k \in \mathbb{Z}$ alors $ak \in n\mathbb{Z}$. Cela est donc un idéal. $\square$

Proposition 3.24.

Soit $n \geq 2$ un entier et $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, la surjection canonique. Nous noterons $\tilde{a} = \phi(a)$. Alors l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donné par

$$U(\mathbb{Z}/n\mathbb{Z}) = \phi(P_n) = \{\tilde{x} \text{ tel que } 0 \leq x \leq n \text{ tel que } \text{pgcd}(x, n) = 1\}. \quad (3.36)$$

où P_n est l'ensemble $P_n = \{x \in \{0, \dots, n-1\} \text{ tel que } \text{pgcd}(x, n) = 1\}$. En particulier, $\text{Card}(U(\mathbb{Z}/n\mathbb{Z})) = \varphi(n)$.

Démonstration. Soit $0 \leq x \leq n$ tel que $\text{pgcd}(x, n) = 1$. Il existe donc $p, q \in \mathbb{Z}$ tels que $px + qn = 1$. En passant aux classes,

$$\tilde{p}\tilde{x} = \tilde{1}, \quad (3.37)$$

donc $\tilde{p}$ est l'inverse de $\tilde{x}$. Cela prouve que $\phi(P_n) \subset U(\mathbb{Z}/n\mathbb{Z})$.

Nous prouvons maintenant l'inclusion inverse. Soit $\tilde{x}$ et $\tilde{y}$ inverses l'un de l'autre : $\tilde{x}\tilde{y} = \tilde{1}$. Il existe donc $q \in \mathbb{Z}$ tel que $xy - qn = 1$, ce qui prouve que $\text{pgcd}(x, n) = 1$. $\square$

3.7 Caractéristique

L'application

$$\begin{aligned} \mu: \mathbb{Z} &\rightarrow A \\ n &\mapsto n \cdot 1_A \end{aligned} \quad (3.38)$$

est un morphisme d'anneaux. Le noyau de μ étant un sous-groupe de $\mathbb{Z}$, il existe un et un seul $p \in \mathbb{Z}$ tel que $\ker \mu = p\mathbb{Z}$. Ce p est la **caractéristique** de A .

Par exemple la caractéristique que $\mathbb{Q}$ est zéro parce qu'aucun multiple de l'unité n'est nul.

À propos de diagonalisation en caractéristique 2, voir l'exemple 6.285.

Lemme 3.25.

Si A est de caractéristique nulle, alors A est infini.

Démonstration. En effet, $\ker \mu = 0$ implique que $n1_A \neq m1_A$ et par conséquent A est infini. $\square$

Lemme 3.26.

Si p est la caractéristique de l'anneau A , alors nous avons l'isomorphisme d'anneaux

$$\mathbb{Z}1_A \simeq \mathbb{Z}/p\mathbb{Z}. \quad (3.39)$$

Démonstration. L'isomorphisme est donné par l'application $n1_A \mapsto \phi(n)$ si ϕ est la projection canonique $\mathbb{Z} \rightarrow \mathbb{Z}_p$. $\square$

Proposition 3.27.

La caractéristique d'un anneau fini divise son cardinal.

Démonstration. Si $\mathbb{A}$ est un anneau, le groupe $\mathbb{Z}$ agit sur $\mathbb{A}$ par

$$n \cdot a = a + n1_A. \quad (3.40)$$

Chaque orbite de cette action est de la forme

$$\mathcal{O}_a = \{a + n1_A \text{ tel que } n = 0, \dots, p-1\} \quad (3.41)$$

où p est la caractéristique de $\mathbb{A}$. Les orbites ont p éléments et forment une partition de $\mathbb{A}$, donc le cardinal de $\mathbb{A}$ est un multiple de p . $\square$

L'ensemble typique de caractéristique p est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Exemple 3.28

Soit à factoriser $X^p - 1$ dans $\mathbb{F}_p$. Grâce au morphisme de Frobenius, nous avons immédiatement

$$X^p - 1 = (X - 1)^p. \quad (3.42)$$

$\triangle$

Définition 3.29.

Un élément a d'un anneau est dit **nilpotent** si $a^r = 0$ pour un certain r . Il est dit **unipotent** si $a - 1$ est nilpotent, c'est à dire si $(a - 1)^r = 0$ pour un certain r .

Proposition 3.30.

Soit $\mathbb{A}$ un anneau commutatif de caractéristique première p . Alors $\sigma(x) = x^p$ est un automorphisme de l'anneau $\mathbb{A}$. Nous avons la formule

$$(a + b)^p = a^p + b^p \quad (3.43)$$

pour tout $a, b \in \mathbb{A}$.

Démonstration. Nous utilisons la formule du binôme de la proposition 3.5 et le fait que les coefficients binomiaux non extrêmes sont divisibles par p et donc nuls. $\square$

Proposition 3.31.

Soit $\mathbb{A}$ un anneau commutatif unitaire de caractéristique p . L'application

$$\begin{aligned} \text{Frob}_{\mathbb{A}} : \mathbb{A} &\rightarrow \mathbb{A} \\ x &\mapsto x^p \end{aligned} \quad (3.44)$$

est un automorphisme d'anneau unitaire.

Nous le nommons le **morphisme de Frobenius**. Nous utiliserons aussi les itérés du morphisme de Frobenius : $\text{Frob}^k : x \mapsto x^{p^k}$.

3.8 Modules

Si $\mathbb{A}$ est un anneau et si $(\mathcal{E}, +)$ est un groupe commutatif, nous disons que $\mathcal{E}$ est un **module** à gauche sur $\mathbb{A}$ si nous avons une application $\mathbb{A} \times M \rightarrow M$ notée $a \cdot x$ telle que

- (1) $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$ (distributivité de $\cdot$ par rapport à l'addition dans M)

- (2) $(a+b) \cdot x = a \cdot x + b \cdot x$ (distributivité de $\cdot$ par rapport à l'addition dans $\mathbb{A}$). Remarque : la loi $+$ du membre de gauche est celle de l'anneau A et la loi $+$ du membre de droite est celle du groupe M
- (3) $(ab) \cdot x = a \cdot (b \cdot x)$
- (4) $1 \cdot x = x$

Soit $\mathcal{E}$ un A -module et $x = (x_i)_{i \in I}$ une famille d'éléments de $\mathcal{E}$, paramétrée par l'ensemble I . Nous considérons l'application

$$\begin{aligned} \mu_x: A^{(I)} &\rightarrow \mathcal{E} \\ (a_i)_{i \in I} &\mapsto \sum_{i \in I} a_i x_i. \end{aligned} \quad (3.45)$$

Ici $A^{(I)}$ désigne l'ensemble de toutes les applications $I \rightarrow A$ de support fini.

Définition 3.32.

À l'instar des espaces vectoriels, les modules ont une notion de partie libre, génératrice et de bases :

- (1) Si μ_x est surjective, nous disons que x est une partie **génératrice**.
- (2) Si μ_x est injective, nous disons que la partie x est **libre**.
- (3) Si μ_x est bijective, nous disons que la partie x est une **base**.

Définition 3.33.

Soit $\mathcal{E}$ un module sur un anneau commutatif A . Un **projecteur** est une application linéaire $p: \mathcal{E} \rightarrow \mathcal{E}$ telle que $p^2 = p$.

Une famille $(p_i)_{i \in I}$ sur $\mathcal{E}$ est **orthogonale** si $p_i \circ p_j = 0$ pour tout $i \neq j$. La famille est **complète** si $\sum_{i \in I} p_i = \text{Id}$.

Théorème 3.34.

Soient des sous modules $\mathcal{E}_1, \dots, \mathcal{E}_n$ du module $\mathcal{E}$ tels que $\mathcal{E} = \mathcal{E}_1 \oplus \dots \oplus \mathcal{E}_n$. Les applications p_i définies par

$$p_i(x_1 + x_n) = x_i \quad (3.46)$$

forment une famille orthogonale de projecteurs et $p_1 + \dots + p_n = \text{Id}$.

Inversement, si $(p_1, \dots, p_n)$ est une famille orthogonale de projecteurs dans un module $\mathcal{E}$ tel que $\sum_{i=1}^n p_i = \text{Id}$, alors

$$\mathcal{E} = \bigoplus_{i=1}^n p_i(\mathcal{E}). \quad (3.47)$$

Un sous-ensemble $\mathcal{F} \subset \mathcal{E}$ est un **sous-module** si $(\mathcal{F}, +)$ est un sous-groupe de $(\mathcal{E}, +)$ et si $a \cdot x \in \mathcal{F}$ pour tout $x \in \mathcal{F}$ et pour tout $a \in \mathbb{A}$.

Exemple 3.35

Un anneau $\mathbb{A}$ est lui-même un $\mathbb{A}$ -module et ses sous-modules sont les idéaux. △

Un module est **simple** ou **irréductible** si il n'a pas d'autre sous-modules que $\{0\}$ et lui-même. Un module est **indécomposable** si il ne peut pas être écrit comme somme directe de sous-modules.

Un module simple est a fortiori indécomposable. L'inverse n'est pas vrai comme le montre l'exemple suivant.

Exemple 3.36

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 $\mathcal{E}$. △

3.9 Anneau intègre

Un élément $a \neq 0$ est un **diviseur de zéro à gauche** si il existe $x \neq 0$ tel que $xa = 0$. L'élément a est un diviseur de zéro **à droite** si il existe b tel que $ab = 0$. Un anneau est **intègre** si il est non nul et ne possède pas de diviseurs de zéro.

Autrement dit, un anneau intègre est un anneau qui possède la propriété du produit nul : si $ab = 0$, alors soit a soit b est nul. Nous verrons en temps et en heure (proposition 4.2) qu'un corps est un anneau intègre.

Exemple 3.37

L'ensemble $\mathbb{Z}$ avec les opérations usuelles est un anneau intègre. △

Exemple 3.38

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. △

Exemple 3.39

Nous verrons au théorème 3.90 que si $\mathbb{A}$ est intègre, alors l'anneau des polynômes sur $\mathbb{A}$ est intègre. △

Corollaire 3.40.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.

Démonstration. Si n est premier, tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles parce que tous les éléments rentrent dans $\phi(P_n)$. Donc $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Si n n'est pas premier, il existe $p, q \in \mathbb{N}^*$ tels que $pq = n$. Dans ce cas au niveau des classes nous avons $\tilde{p}\tilde{q} = 0$ avec $\tilde{p} \neq 0 \neq \tilde{q}$, ce qui montre que $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro et n'est pas intègre. □

Lemme 3.41.

La caractéristique d'un anneau intègre est zéro ou un nombre premier.

Démonstration. Si A est intègre, alors $\mathbb{Z}1_A$ est intègre (a fortiori), et $\mathbb{Z}_p$ est intègre parce qu'il est isomorphe à $\mathbb{Z}1_A$. Mais nous savons que $\mathbb{Z}_p$ est intègre si et seulement si p est premier (proposition 3.40). □

Exemple 3.42

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 :

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = 0. \quad (3.48)$$

△

Exemple 3.43

Si $\mathbb{K}$ est un corps de caractéristique 2, alors l'égalité $x = -x$ n'implique pas $x = 0$, vu que $2x = 0$ est vérifiée pour tout x . Cela se répercute sur un certain nombre de résultats. En caractéristique deux, une forme antisymétrique n'est pas toujours alternée. Voir le lemme 6.41. △

Lemme 3.44.

Si $\mathbb{A}$ est un anneau intègre et si $a, b \in \mathbb{A}$ sont tels que $a \mid b$ et $b \mid a$, alors il existe un inversible $u \in \mathbb{A}$ tel que $a = ub$.

Démonstration. Les hypothèses à propos de la divisibilité nous indiquent que $a = xb$ et $b = ya$ pour certains $x, y \in \mathbb{A}$. Du coup,

$$b(1 - yx) = 0. \quad (3.49)$$

Étant donné que $\mathbb{A}$ 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. $\square$

Exemple 3.45

Si $\mathbb{A}$ est un anneau intègre, l'anneau $\mathbb{A}[X]$ des polynômes sur $\mathbb{A}$ est également intègre. En effet si P et Q sont deux polynômes non nuls, alors le coefficient du terme de plus haut degré de PQ est donné par le produit des coefficients de plus haut degré de P et Q qui est non nul parce que $\mathbb{A}$ est intègre. $\triangle$

3.9.1 PGCD et PPCM

Source : [32].

Le théorème de Bézout aura lieu dans les anneaux principaux, corollaire 3.69.

Dans un anneau intègre, la relation de divisibilité s'exprime en termes d'idéaux par

$$a \mid b \Leftrightarrow (b) \subset (a). \quad (3.50)$$

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 $\mathbb{A}$, nous notons $a \mid S$ pour exprimer que $a \mid x$ pour tout $x \in S$.

Définition 3.46.

Soit $\mathbb{A}$, un anneau intègre et $S \subset \mathbb{A}$. Nous disons que $\delta \in \mathbb{A}$ est un **PGCD** de S si

- (1) $\delta \mid S$
- (2) si $d \mid S$ alors $d \mid \delta$.

Nous disons que $\mu \in \mathbb{A}$ est un **PPCM** de S si

- (1) $S \mid \mu$,
- (2) si $S \mid m$, alors $\mu \mid m$.

Notons qu'il n'y a en général pas unicité du PGCD ou du PPCM d'un ensemble.

Lemme 3.47.

Soit $\mathbb{A}$ un anneau intègre et $S \subset \mathbb{A}$. 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. Soit δ un PGCD de S et u un inversible dans $\mathbb{A}$. 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 une autre PGCD de S , alors il existe un inversible $u \in \mathbb{A}$ tel que $\delta' = u\delta$. Vu que δ' divise x pour tout $x \in S$, nous avons $\delta' \mid \delta$, et symétriquement nous trouvons $\delta \mid \delta'$. Par conséquent (lemme 3.44), il existe un inversible u tel que $\delta = u\delta'$.

Le même type de raisonnement tient pour le PPCM. $\square$

Si δ est un PGCD de S , nous dirons *par abus de langage* que δ est le PGCD de S , gardant en tête qu'en réalité toute sa classe d'association est PGCD. Nous noterons aussi, toujours par abus que $\delta = \text{pgcd}(S)$.

6. Il me semble qu'à ce niveau il y a une faute de frappe dans [32].

Remarque 3.48.

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.

3.9.2 Contenu d'un polynôme**Définition 3.49.**

Le **contenu** du polynôme $P = \sum_i a_i X^i \in \mathbb{K}[X]$

$$c(P) = \text{pgcd}(a_i). \quad (3.51)$$

Une polynôme est dit **primitif** si $c(P) = 1$.

Lemme 3.50 (de Gauss[1, 33]).

Soient $P, Q \in \mathbb{Z}[X]$. Alors $c(PQ) = c(P)c(Q)$.

Démonstration. Afin de fixer les notations, nous posons $P = \sum_i a_i X^i$ et $Q = \sum_j b_j X^j$.

Pour les polynômes primitifs Nous commençons par supposer que $c(P) = c(Q) = 1$. Dans ce cas si $c(PQ) \neq 1$, nous considérons un nombre premier p divisant $c(PQ)$. Vu que le contenu de P et de Q sont 1, le nombre p ne peut pas diviser tous leurs coefficients. Nous définissons i_0 de façon que a_{i_0} soit le premier à ne pas être divisible par p et j_0 de telle façon que b_{j_0} soit le premier à ne pas être divisible par p . Autrement dit :

$$p \mid a_0, p \mid a_1, \dots, p \mid a_{i_0-1}, p \nmid a_{i_0} \quad (3.52)$$

et similaire pour j_0 . Donc p ne divise ni a_{i_0} ni b_{j_0} . Nous nous demandons alors avec malice quel est le coefficient de $X^{i_0+j_0}$ dans PQ . La réponse est :

$$a_{i_0}b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i < i_0 \text{ ou } j < j_0}} a_i b_j. \quad (3.53)$$

Par définition p divise soit a_i soit b_j pour chacun des termes de la grande somme. Vu que p ne divise pas $a_{i_0}b_{j_0}$, il ne divise pas le coefficient de $X^{i_0+j_0}$ dans PQ , alors que nous étions partis en disant que p divisait tous les coefficients de PQ .

Nous concluons donc que $c(PQ) = 1$.

Cas général Si P et Q sont maintenant des polynômes sans conditions particulières dans $\mathbb{Z}[X]$, nous considérons $P_1 = \frac{P}{c(P)}$ et $Q_1 = \frac{Q}{c(Q)}$; ces deux polynômes sont primitifs et nous avons alors, en utilisant la première partie :

$$c(P_1Q_1) = 1. \quad (3.54)$$

Étant donné que

$$P_1Q_1 = \frac{1}{c(P)c(Q)}PQ, \quad (3.55)$$

nous avons

$$c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q). \quad (3.56)$$

□

3.10 Anneau factoriel

Définition 3.51.

On dit que les éléments a et b d'un anneau sont **associés** si il existe un élément u inversible dans $\mathbb{A}$ tel que $a = ub$.

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, le nombre $7 + 6i$ est divisible par $2 + i$ dans $\mathbb{Z}[i]$. En effet :

$$(2 + i)(4 + i) = 7 + 6i. \quad (3.57)$$

△

Définition 3.53.

Soit $\mathbb{A}$ un anneau commutatif intègre. Un élément $a \in \mathbb{A}$ est **irréductible** si a n'est pas inversible, mais si $a = xy$, alors soit x soit y est inversible. Nous notons $U(\mathbb{A})$ l'ensemble des éléments inversibles de $\mathbb{A}$.

Remarque 3.54.

Un corps n'a pas d'éléments irréductibles parce qu'à part zéro tous les éléments sont inversibles alors que 0 n'est certainement pas irréductible vu que $0 = 0 \cdot 0$.

Exemple 3.55

Les éléments irréductibles de l'anneau $\mathbb{Z}$ sont les nombres premiers. En effet 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 $b = \pm 1$.

△

Définition 3.56.

Un anneau commutatif unitaire $\mathbb{A}$ est **factoriel** si il vérifie les propriétés suivantes.

- (1) L'anneau $\mathbb{A}$ est intègre (pas de diviseurs de zéro).
- (2) Si $a \in \mathbb{A}$ est non nul et non inversible alors il admet une décomposition $a = p_1 \dots p_k$ où les p_i sont irréductibles.
- (3) Si $a = q_1 \dots q_m$ est une autre décomposition de a en irréductibles, alors $m = k$ et il existe une permutation $\sigma \in S_k$ telle que p_i et $q_{\sigma(i)}$ soient associés.

Un anneau factoriel permet de définir le pgcd et le ppcm de nombres. Soit une famille $\{a_n\}$ d'éléments de $\mathbb{A}$ qui se décomposent en irréductibles comme

$$a_i = \prod_k p_k^{\alpha_{k,i}}. \quad (3.58)$$

Nous définissons

$$\text{pgcd}\{a_n\} = \prod_k p_k^{\min_i \{\alpha_{k,i}\}}. \quad (3.59)$$

Proposition 3.57.

L'élément $\text{pgcd}\{a_n\}$ est l'unique diviseur commun des a_i à être un multiple des autres.

Nous définissons aussi

$$\text{ppcm}\{a_i\} = \prod_k p_k^{\max_i \{\alpha_{k,i}\}}. \quad (3.60)$$

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 : $a < b$ si et seulement si $(b) \subset (a)$.

Exemple 3.58

L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel parce que

$$4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3}) \quad (3.61)$$

donnent deux décompositions distinctes de 4 en irréductibles. $\triangle$ Nous allons voir dans l'exemple 3.76 que $\mathbb{Z}[i\sqrt{2}]$ est factoriel parce qu'il sera euclidien.

3.11 Anneau principal

Nous parlons de l'idéal des polynôme annulateurs dans le théorème 3.110.

Définition 3.59.

Un idéal I dans $\mathbb{A}$ est **principal à gauche** si il existe $a \in I$ tel que $I = \mathbb{A}a$. Il est **principal à droite** si il existe $a \in I$ tel que $I = a\mathbb{A}$. Nous disons qu'il est **principal** si il est principal à gauche et à droite.

Un anneau commutatif intègre est **principal** si tous ses idéaux sont principaux.

Un idéal I dans l'anneau $\mathbb{A}$ est **maximal** si les seuls idéaux de $\mathbb{A}$ contenant I sont I et $\mathbb{A}$.

Souvent pour prouver qu'un anneau est principal, nous prouvons qu'il est euclidien (définition 3.73) et nous utilisons la proposition 3.75 qui dit qu'un anneau euclidien est principal.

Définition 3.60.

Nous disons qu'un idéal I dans $\mathbb{A}$ est **premier** si $\mathbb{A}$ est un anneau commutatif intègre et si $\mathbb{A}/I$ est intègre.

Définition 3.61 (Idéal engendré par un élément).

Si p est un élément d'un anneau $\mathbb{A}$ alors nous notons (p) l'idéal dans $\mathbb{A}$ **engendré** par p , c'est à dire $p\mathbb{A}$.

Proposition 3.62.

Soit $\mathbb{A}$ un anneau principal qui n'est pas un corps. Pour un idéal $I \subset \mathbb{A}$, les conditions suivantes sont équivalentes :

- (1) I est un idéal maximum ;
- (2) I est un idéal premier non nul ;
- (3) il existe p irréductible dans $\mathbb{A}$ tel que $I = (p)$.

Proposition 3.63.

Un idéal I dans $\mathbb{A}$ est premier si et seulement si I est strictement inclus dans $\mathbb{A}$ et si pour tout $a, b \in \mathbb{A}$ tels que $ab \in I$ nous avons $a \in I$ ou $b \in I$.

Proposition 3.64.

Si $\mathbb{A}$ est un anneau principal et si p est irréductible, alors $\mathbb{A}/p$ est un corps.

Exemple 3.65

L'anneau $\mathbb{Z}$ est principal parce que ses seuls idéaux sont les $n\mathbb{Z}$ qui sont principaux : $n\mathbb{Z}$ est engendré par n . $\triangle$

Exemple 3.66

Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont principaux. En effet les idéaux de $\mathbb{Z}/n\mathbb{Z}$ seraient par la proposition 3.22 des quotients d'idéaux de $\mathbb{Z}$ par (n) . Donc les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les anneaux $(\mathbb{Z}/m\mathbb{Z})$ avec m divisant n .

Par exemple si $I = 4\mathbb{Z}$, on peut considérer l'idéal $J = 2\mathbb{Z}$ qui contient $4\mathbb{Z}$. Donc $\mathbb{Z}/2\mathbb{Z}$ est un idéal de $\mathbb{Z}/4\mathbb{Z}$. $\triangle$

Théorème 3.67.

Si $\mathbb{A}$ est un anneau principal et si p et q sont premiers entre eux dans $\mathbb{A}$, alors on a l'isomorphisme d'anneaux

$$\mathbb{A}/pq\mathbb{A} \simeq \mathbb{A}/p\mathbb{A} \times \mathbb{A}/q\mathbb{A}. \quad (3.62)$$

3.11.1 Bézout**Théorème 3.68** ([32]).

Toute partie S d'un anneau principal admet un PGCD et un PPCM. De plus

$$\delta = \text{pgcd}(S) \Leftrightarrow (\delta) = \sum_{s \in S} (s) \mu = \text{ppcm}(S) \Leftrightarrow (\mu) = \bigcap_{s \in S} (s) \quad (3.63)$$

Démonstration. Vu que l'anneau $\mathbb{A}$ est principal, tous ses idéaux sont principaux et donc engendrés par un seul élément. En particulier il existe $\delta, \mu \in \mathbb{A}$ tels que

$$(\delta) = \sum_{s \in S} (s) \quad (3.64a)$$

$$(\mu) = \bigcap_{s \in S} (s) \quad (3.64b)$$

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

$$\sum_{x \in S} (x) \subset (d), \quad (3.65)$$

puis $(\delta) \subset (d)$ et finalement $d \mid \delta$.

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 $\mu \mid m$.

□

Nous disons que deux éléments d'un anneau principal sont **premiers entre eux** si leur PGCD est 1.

Corollaire 3.69 (Théorème de Bézout[32]).

Soit $\mathbb{A}$ un anneau principal. Deux éléments $a, b \in \mathbb{A}$ sont premiers entre eux si et seulement si il existe un couple $u, v \in \mathbb{A}$ tel que

$$ua + vb = 1. \quad (3.66)$$

À la place de 1 on aurait pu écrire n'importe quel inversible.

Démonstration. Pour cette preuve, nous allons écrire $\text{pgcd}(a, b)$ 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

$$1 \in \text{pgcd}(a, b) = \sum_{x=a,b} (x) = (a) + (b). \quad (3.67)$$

À l'inverse, si nous avons $ua + vb = 1$, alors $1 \in (a) + (b)$, mais vu que $(a) + (b)$ est un idéal principal, $(1) = (a) + (b)$ et donc $1 \in \text{pgcd}(a, b)$. □

Le lemme de Gauss est une application immédiate de Bézout. Il y aura aussi un lemme de Gauss à propos de polynômes (lemme 4.18), et une généralisation directe au théorème de Gauss, théorème 4.17.

Lemme 3.70 (lemme de Gauss).

Soit $\mathbb{A}$ un anneau principal et $a, b, c \in \mathbb{A}$ tels que a divise bc . Si a est premier avec c , alors a divise b .

Démonstration. Vu que a est premier avec c , nous avons $\text{pgcd}(a, c) = 1$ et Bézout (2.24) nous donne donc $s, t \in \mathbb{A}$ tels que $sa + tc = 1$. En multipliant par b ,

$$sab + tbc = b. \quad (3.68)$$

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 . $\square$

Un cas usuel d'utilisation est le cas de $\mathbb{A} = \mathbb{N}^*$.

3.11.2 Anneau noetherien

Un anneau est dit **noetherien** si toute suite croissante d'idéaux est stationnaire (à partir d'un certain rang). Montrer que tout anneau principal est noetherien est le premier pas pour montrer que tout anneau principal est factoriel.

Lemme 3.71.

Tout anneau principal est noetherien.

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 emboîtés. 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 $n \geq N$ nous avons

$$J \subset J_N \subset J_n \subset J. \quad (3.69)$$

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 $n \geq N$ nous avons $J_N = J_n = J$. La suite est par conséquent stationnaire. $\square$

Théorème 3.72 ([34]).

Tout anneau principal est factoriel.

3.12 Anneau euclidien

Définition 3.73 (Wikipédia).

Soit $\mathbb{A}$ un anneau intègre. Un **stathme euclidien** sur $\mathbb{A}$ est une application $\alpha: \mathbb{A} \setminus \{0\} \rightarrow \mathbb{N}$ tel que

(1) $\forall a, b \in \mathbb{A} \setminus \{0\}$, il existe $q, r \in \mathbb{A}$ tel que

$$a = bq + r \quad (3.70)$$

et $\alpha(r) < \alpha(b)$.

(2) Pour tout $a, b \in \mathbb{A} \setminus \{0\}$, $\alpha(b) \leq \alpha(ab)$.

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.

Exemple 3.74

Le stathme de $\mathbb{N}$ pour la division euclidienne usuelle est $\alpha(n) = n$. Si $a, b \in \mathbb{N}$ nous écrivons

$$a = bq + r \quad (3.71)$$

où q est l'entier le plus proche *inférieur* à a/b (on veut que le reste soit positif) et $r = a - bq$. Nous avons donc

$$r - b = a - b(q + 1) < a - b\frac{a}{b} = 0, \quad (3.72)$$

ce qui montre que $r < b$. $\triangle$

Proposition 3.75 (Wikipédia).

Un anneau euclidien est principal.

Démonstration. Soit $\mathbb{A}$ un anneau principal et α un stathme sur $\mathbb{A}$. Nous considérons un idéal I non nul de $\mathbb{A}$. Nous devons montrer que I est généré par un élément. En l'occurrence nous allons montrer que l'élément $a \in I \setminus \{0\}$ qui minimise $\alpha(a)$ va générer. Soit $x \in I$. Par construction, il existe $q, r \in \mathbb{A}$ 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. $\square$

Exemple 3.76

Prouvons que $\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien. Pour cela nous démontrons que

$$\begin{aligned} N: \mathbb{Z}[i\sqrt{2}] &\rightarrow \mathbb{N} \\ a + bi\sqrt{2} &\mapsto a^2 + 2b^2 \end{aligned} \quad (3.73)$$

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

$$\frac{z}{t} = \alpha + \beta i\sqrt{2}. \quad (3.74)$$

Nous désignons par $\alpha + \epsilon_1$ et $\beta + \epsilon_2$ les entiers les plus proches de α et β . Nous avons $|\alpha|, |\beta| \leq \frac{1}{2}$. Nous posons alors naturellement

$$q = (\alpha + \epsilon_1) + (\beta + \epsilon_2)i\sqrt{2} \quad (3.75)$$

et nous calculons $r = z - qt$:

$$2b'\epsilon_2 - a'\epsilon_1 + i\sqrt{2}(\epsilon_1b' - a'\epsilon_2). \quad (3.76)$$

Nous trouvons

$$N(r) = a'^2\epsilon_1^2 + 4b'^2\epsilon_2^2 + 2a'^2\epsilon_1^2 + 2b'^2\epsilon_2^2 \leq \frac{3}{4}a'^2 + \frac{3}{2}b'^2. \quad (3.77)$$

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

$$N(z) = (a^2 + 2b^2)(a'^2 + 2b'^2), \quad (3.78)$$

et tant que $t \neq 0$ nous avons bien $N(z) > N(r)$. $\triangle$

Notons en particulier que $\mathbb{Z}[i\sqrt{2}]$ est factoriel et principal.

Exemple 3.77

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 3.51) si et seulement si $a = \pm b$.

De plus si p est irréductible, alors $-p$ est irréductible. Les éléments irréductibles de $\mathbb{Z}[i\sqrt{2}]$ arrivent donc par paires 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 $x = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n}$. Ce fait va être pratique pour comparer des décomposition en facteurs irréductibles d'éléments. $\triangle$

Le lemme suivant fait en pratique partie de l'exemple 3.80, mais nous l'isolons pour plus de clarté⁷.

Lemme 3.78.

Si a et b sont deux éléments premiers entre eux de $\mathbb{Z}[i\sqrt{2}]$ tels que $ab = y^3$ alors a et b sont des cubes (dans $\mathbb{Z}[i\sqrt{2}]$).

7. Merci à Marvoir pour m'avoir souligné le manque.

Démonstration. D'après l'exemple 3.77 nous pouvons écrire

$$y = \pm p_1^{\sigma_1} \dots p_n^{\sigma_n} \quad (3.79a)$$

$$a = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n} \quad (3.79b)$$

$$b = \pm p_1^{\beta_1} \dots p_n^{\beta_n} \quad (3.79c)$$

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. $\square$

3.12.1 Équations diophantiennes

Exemple 3.79

L'équation diophantienne

$$x^2 = 3y^2 + 8 \quad (3.80)$$

n'a pas de solutions. En effet si nous prenons l'équation modulo 3 nous obtenons

$$x^2 \pmod 3 = 8 \pmod 3 = 2 \pmod 3. \quad (3.81)$$

Or dans $\mathbb{Z}/3\mathbb{Z}$, aucun élément ne vérifie $x^2 = 2 : 0^2 = 0 \neq 2, 1^2 = 1 \neq 2$ et $2^2 = 4 = 1 \neq 2$. $\triangle$

Exemple 3.80

Résolvons l'équation diophantienne

$$x^2 + 2 = y^3. \quad (3.82)$$

Une première remarque est que x doit être impair. En effet si $x = 2k$, nous devons avoir y^3 pair. Mais si un cube pair est divisible par 8, donc $y^3 = 8l$. L'équation devient $4k^2 + 2 = 8l^3$, c'est à dire $2k^2 + 1 = 4l^3$. 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 (3.73).

L'élément $i\sqrt{2}$ est irréductible parce que $N(i\sqrt{2}) = 2$. Si nous avons $i\sqrt{2} = pq$, alors nous aurions $N(p)N(q) = 2$, ce qui n'est possible que si $N(p)$ ou $N(q)$ égal à 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 $(-i\sqrt{2})$. Du coup nous devrions avoir $d = (i\sqrt{2})^\alpha$ et donc

$$x = (i\sqrt{2})^\beta q \quad (3.83)$$

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 $d = 1$.

Vu que 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 3.78). 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: 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

$$\begin{cases} x = a^3 - 6ab^2 \\ 1 = 3a^2b - 2b^3 \end{cases} \quad \begin{matrix} (3.84a) \\ (3.84b) \end{matrix}$$

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

$$(x, z) = (-5, 1 + i\sqrt{2}) \quad (3.85a)$$

$$(x, z) = (5, -1 + i\sqrt{2}) \quad (3.85b)$$

$$(3.85c)$$

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 $(-5, 3)$. $\triangle$

3.12.2 Triplet pythagoriciens et équation de Fermat pour $n = 4$

Proposition 3.81 (Triplets pythagoriciens[35, 36]).

Un triple $(x, y, z) \in (\mathbb{N}^*)^3$ 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

$$\begin{cases} x = d(u^2 - v^2) \\ y = 2duv \end{cases} \quad \begin{matrix} (3.86a) \\ (3.86b) \end{matrix}$$

$$\begin{cases} z = d(u^2 + v^2) \end{cases} \quad (3.86c)$$

ou

$$\begin{cases} x = 2duv \\ y = d(u^2 - v^2) \end{cases} \quad \begin{matrix} (3.87a) \\ (3.87b) \end{matrix}$$

$$\begin{cases} z = d(u^2 + v^2) \end{cases} \quad (3.87c)$$

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 (3.86) :

$$x^2 + y^2 = d^2(u^2 - v^2)^2 + 4d^2u^2v^2 = d^2(u^2 + v^2)^2, \quad (3.88)$$

qui correspond bien au z^2 proposé.

Nous allons maintenant prouver la réciproque : toute solution est d'une des deux formes proposées. D'abord une solution *primitive* est un triplet (x, y, z) d'entiers premiers dans leur ensemble. Déterminer ces solutions suffira parce que si (x, y, z) n'est pas une solution primitive, alors en posant $k = \text{pgcd}(x, y, z)$, le triplet $(\frac{x}{k}, \frac{y}{k}, \frac{z}{k})$ est primitif. Connaissant les triplet primitifs, nous obtenons tous les autres par simple multiplication.

Soit donc (x, y, z) un triplet pythagorien primitif. D'abord nous remarquons que si deux parmi x , y et z sont divisible par un nombre, alors tous les trois sont divisibles par ce nombre⁸, donc les nombres x , y et z sont premiers deux à deux.

8. Parce que si k et k^2 ont les mêmes facteurs premiers.

De plus les nombres x et y ne sont pas tous les deux impairs. En effet si $x = 2a + 1$ nous avons $x^2 = 4a^2 + 4a + 1 \in [1]_4$ (et idem pour y). Si $x = 4a + 1$ et $y = 4b + 1$ alors $z^2 = x^2 + y^2 \in [2]_4$, ce qui signifierait que z^2 est pair et donc que z est pair. Et enfin si z est pair, $z = 2c$ alors $z^2 = 4c^2 \in [0]_4$. Contradiction.

Au final, quitte à inverser les rôles de x et y , nous avons x pair, y impair, z impair.

Cela dit, nous nous attaquons à l'équation. Nous avons $x^2 = (z + y)(z - y)$ et donc

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)^2 \left(\frac{z-y}{2}\right)^2. \quad (3.89)$$

Vu que z et y sont premiers entre eux, les nombres $z - y$ et $z + y$ sont également premiers entre eux⁹. Donc les facteurs premiers (qui arrivent au moins au carré) de $(x/2)^2$ sont chacun soit dans $(z + y)/2$ soit dans $(z - y)/2$. Nous en déduisons que ces derniers sont des carrés d'entiers. Nous posons

$$\frac{z-y}{2} = u^2 \quad \frac{z+y}{2} = v^2. \quad (3.90)$$

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 $(x/2)^2 = u^2 v^2$ et donc $x = 2uv$ puis par somme et différence :

$$\begin{cases} x = 2yv & (3.91a) \\ y = v^2 - u^2 & (3.91b) \\ z = m^2 + n^2, & (3.91c) \end{cases}$$

ce qu'il fallait. □

Remarque 3.82.

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.

Remarque 3.83.

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.

Proposition 3.84 ([35]).

Les équations $x^4 + y^4 = z^2$ et $x^2 + y^4 = z^4$ n'ont pas de solutions dans $(\mathbb{N}^*)^3$.

Démonstration. Si la première équation n'a pas de solutions, alors la seconde n'en n'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 une solution (x, y, z) dans $(\mathbb{N}^*)^3$ que nous prenons avec z minimum. Du coup, les trois nombres x , y et z sont premiers dans leur ensembles parce que 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 3.81, il existe $u, v \in \mathbb{N}^*$ premiers entre eux tels que

$$\begin{cases} \bar{x} = 2uv & (3.92a) \\ \bar{y} = u^2 - v^2 & (3.92b) \\ z = u^2 + v^2. & (3.92c) \end{cases}$$

Si u est pair, alors v est impair (et inversement) parce que $\text{pgcd}(u, v) = 1$.a. 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 et v pair.

9. Si $z - y = kn$ et $z + y = km$, faisant la somme et la différence on voit que y et z sont divisibles par k .

Nous pouvons donc écrire l'équation $v^2 + \bar{y} = u^2$ où u , v et $\bar{y}$ sont premiers dans leur ensemble (dans une égalité $a + b = c$, si deux des nombres ont un diviseur commun, le troisième l'a aussi). Vu que $\bar{y} = y^2$, le triplet (v, y, u) est un triplet pythagoriciens élémentaire. Il existe donc deux nombres r et s premiers entre eux tels que

$$\begin{cases} v = 2rs & (3.93a) \end{cases}$$

$$\begin{cases} y = r^2 - s^2 & (3.93b) \end{cases}$$

$$\begin{cases} u = r^2 + s^2. & (3.93c) \end{cases}$$

Avec cela, $\bar{x} = 2uv = 2rs(r^2 + s^2)$. Vu que $\bar{x}$ est un carré et que r , s et $r^2 + s^2$ sont premiers entre eux, ils doivent séparément être des carrés, ou alors $rs(r^2 + s^2) = 2$. Voyons que cette deuxième possibilité est impossible. Un produit de deux entiers qui vaut 2, c'est soit 1×2 , soit 2×1 . D'une part $r^2 + s^2 = 1$ est impossible parce que r et s sont non nuls, et d'autre part, demander $r^2 + s^2 = 2$ avec $rs = 1$, c'est demander $r = s = 1$, mais alors $v = 2$, $y = 0$ et $u = 2$, ce qui contredit le fait que u et v sont premiers entre eux. Bref, les nombres r , s et $r^2 + s^2$ sont séparément des carrés :

$$\begin{cases} r = \alpha^2 & (3.94a) \end{cases}$$

$$\begin{cases} s = \beta^2 & (3.94b) \end{cases}$$

$$\begin{cases} r^2 + s^2 = \gamma^2. & (3.94c) \end{cases}$$

En mettant les deux premiers dans la troisième, nous avons $\alpha^2 + \beta^4 = \gamma^2$. Donc (α, β, γ) est une solution. Nous allons prouver que $\gamma < z$, ce qui terminera la preuve. Nous avons :

$$z = u^2 + v^2 = r^2 + s^2 + 4r^2s^2 = \gamma^2 + 4r^2s^2. \quad (3.95)$$

Cela prouve que $\gamma^2 < z$ et a fortiori que $\gamma < z$. □

3.12.3 Lignes et colonnes de matrices

Nous nommons E_{ij} la matrice remplie de zéros sauf à la case ij qui vaut 1. Autrement dit

$$(E_{ij})_{kl} = \delta_{ik}\delta_{jl}. \quad (3.96)$$

Définition 3.85.

Une **matrice de transvection** est une matrice de la forme

$$T_{ij}(\lambda) = \text{Id} + \lambda E_{ij} \quad (3.97)$$

avec $i \neq j$.

Une **matrice de dilatation** est une matrice de la forme

$$D_i(\lambda) = \text{Id} + (\lambda - 1)E_{ii}. \quad (3.98)$$

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 permutations** associée est la matrice d'entrées

$$(P_\sigma)_{ij} = \delta_{i\sigma(j)}. \quad (3.99)$$

Lemme 3.86.

La matrice $T_{ij}(\lambda)A = (\mathbb{1} + \lambda E_{ij})A$ est la matrice A à qui on a effectué la substitution

$$L_i \rightarrow L_i + \lambda L_j. \quad (3.100)$$

La matrice $AT_{ij}(\lambda)$ est la substitution

$$C_j \rightarrow C_j + \lambda C_i. \quad (3.101)$$

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 kl de la matrice $E_{ij}A$:

$$(E_{ij}A)_{kl} = \sum_m (E_{ij})_k m A_{ml} \quad (3.102a)$$

$$= \sum_m \delta_{ik} \delta_{jm} A_{ml} \quad (3.102b)$$

$$= \delta_{ik} A_{jl}. \quad (3.102c)$$

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

$$A + \lambda E_{ij}A \quad (3.103)$$

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

$$(AE_{ij}) = A_{ki} \delta_{jl}. \quad (3.104)$$

Pour les matrices de permutations, nous avons

$$(AP_\sigma)_{kl} = A_{k\sigma(l)} \quad (3.105)$$

et

$$(P_\sigma A)_{kl} = \sum_m \delta_{k\sigma(m)} A_{ml} = \sum_m \delta_{\sigma^{-1}(k)m} A_{ml} = A_{\sigma^{-1}(k)l}. \quad (3.106)$$

□

3.12.4 Algorithme des facteurs invariants

Proposition 3.87 (Algorithme des facteurs invariants[1]).

Soit $(\mathbb{A}, \delta)$ un anneau euclidien muni de son stathme et $U \in \mathbb{M}(n, m, \mathbb{A})$. Alors il existe $d_1, \dots, d_s \in \mathbb{A}^*$ et des matrices $P \in \text{GL}(m, \mathbb{A})$, $Q \in \text{GL}(n, \mathbb{A})$ tels que nous ayons

$$U = P \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_s & \\ & 0 & & 0 \end{pmatrix} Q \quad (3.107)$$

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'aménons en $(1, 1)$ par les permutations

$$\begin{aligned} C_1 &\leftrightarrow C_{j_0} \\ L_1 &\leftrightarrow L_{i_0} \end{aligned} \quad (3.108)$$

Ensuite nous traitons la première colonne jusqu'à amener des zéros partout en dessous de u_{11} de la façon suivante : pour chaque ligne successivement nous calculons la division euclidienne

$$u_{i1} = qu_{11} + r_i, \quad (3.109)$$

et nous faisons

$$L_i \rightarrow L_i - qL_1, \quad (3.110)$$

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

content¹⁰. Dans ce cas nous permutons $L_1 \leftrightarrow L_i$, ce qui aura pour effet de strictement diminuer le stathme de u_{11} parce qu'on va mettre en u_{11} le nombre r_i dont le stathme est strictement plus petit que celui de u_{11} .

En faisant ce jeu de division euclidienne puis échange, on diminue toujours le stathme de u_{11} , donc ça fini par s'arrêter, c'est à dire qu'à un certain moment la division euclidienne de u_{i1} par u_{11} va donner un reste zéro et nous serons content.

Une fois la première colonne ramenée à la forme

$$C_1 = \begin{pmatrix} u_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad (3.111)$$

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 matrice¹¹

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix} \quad (3.112)$$

Si l'élément u_{11} ne divise pas un des éléments de A , disons a_{ij} , alors nous faisons

$$C_1 \rightarrow C_1 - C_j. \quad (3.113)$$

Cela nous détruit un peu la première colonne, mais ne change pas u_{11} . Nous avons maintenant

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ * & & & \\ u_{ij} & & A & \\ * & & & \\ 0 & & & \end{pmatrix} \quad (3.114)$$

Et nous refaisons tout le jeu depuis le début. Cependant lorsque nous allons nous attaquer à la ligne i , u_{11} ne divisera pas u_{ij} , ce qui donnera lieu à une division euclidienne et un échange $L_1 \leftrightarrow L_i$. Cet échange mettra r_i à la place de u_{11} et donc diminuera encore strictement le stathme. Encore une fois nous allons travailler jusqu'à avoir la matrice sous la forme

$$U = \begin{pmatrix} u_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix}, \quad (3.115)$$

saut que cette fois le stathme de u_{11} est strictement plus petit que la fois précédente. Si u_{11} 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 (3.115) avec u_{11} 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

$$U = \begin{pmatrix} u_{11} & & 0 \\ & u_{22} & \\ & 0 & B \end{pmatrix}. \quad (3.116)$$

10. Si il est zéro, nous passons à la ligne suivante

11. Nous nommons toujours par la même lettre U la matrice originale et la modifiée, comme il est d'usage en informatique.

Sous cette forme nous avons $u_{11} \mid u_{22}$ et u_{11} divise tous les éléments de B . En effet u_{11} 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 3.86). $\square$

3.13 Anneaux des polynômes

Soit A un anneau commutatif. Nous considérons $\mathcal{P}$ l'ensemble des suites presque nulles d'éléments de A , ce sont les suites $(a_n)_{n \in \mathbb{N}}$ telles que il existe N tel que $a_i = 0$ pour tout $i > N$.

Cela est un A -module libre de base (définition 3.32)

$$(e_n)_k = \delta_{nk}. \quad (3.117)$$

Si $(a_n)_{n \in \mathbb{N}}$ et $(b_n)_{n \in \mathbb{N}}$ sont des éléments de $\mathcal{P}$, nous définissons le produit ab par

$$(ab)_n = \sum_{p+q=n} a_p b_q. \quad (3.118)$$

Cela est bien un élément de $\mathcal{P}$ parce qu'il existe $N \in \mathbb{N}$ tel que $a_n = b_n = 0$ pour tout $n \geq N$. Avec la somme et le produit par un scalaire, le module $\mathcal{P}$ devient une A -algèbre commutative unitaire. L'unité est

$$e_0 = (1, 0, \dots). \quad (3.119)$$

Définition 3.88.

En tant que A -algèbre, l'ensemble $\mathcal{P}$ est l'algèbre des polynômes en une indéterminée à coefficients dans A .

Si nous posons que $X = e_1$, et que nous prenons la convention $X^0 = 1$, alors nous avons $e_k = X^k$ et nous notons $A[X]$ l'anneau $\mathcal{P}$ exprimé avec X . Les éléments de la forme λX^k avec $\lambda \in A$ et $k \in \mathbb{N}$ sont des **monômes**. Nous allons aussi considérer

$$A_n[X] = \{P \in A[X] \text{ tel que } \deg(P) \leq n\}. \quad (3.120)$$

Cela est un sous module libre.

Remarque 3.89.

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 a 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 4.58 et l'exemple 4.125.

Théorème 3.90.

L'anneau A est intègre si et seulement si $A[X]$ est intègre.

Démonstration. Soient P et Q des éléments non nuls de $A[X]$. Vu que l'anneau A est intègre, nous avons

$$\deg(PQ) = \deg(P) + \deg(Q) \quad (3.121)$$

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 vu comme sous anneau. $\square$

Remarque 3.91.

Si A n'est pas intègre, soit $\alpha\beta = 0$, alors $(\alpha X)(\beta x) = 0$ et le degré du produit n'est pas la somme des degrés.

Corollaire 3.92.

Si A est intègre, les inversibles de $A[X]$ sont les éléments de $U(A)$.

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 degrés zéro et il faut que $P, Q \in A$. Enfin pour qu'ils soient inversibles, ils doivent être dans $U(A)$. $\square$

La **valuation** de P du polynôme $P = \sum_n a_n X^n$, notée $\text{val}(P)$, est

$$\text{val}(P) = \min\{n \text{ tel que } a_n \neq 0\}. \quad (3.122)$$

Nous avons $\text{val}(P) \leq \deg(P)$ et $\text{val}(P) = \deg(P)$ si et seulement si P est un monôme. Si $P = 0$, nous convenons que $\text{val}(0) = \infty$ et $\deg(0) = -\infty$.

Proposition 3.93.

L'anneau $\mathbb{K}[X]$ des polynômes sur un corps commutatif $\mathbb{K}$ est factoriel.

Le théorème suivant est une particularisation à $\mathbb{K}[X]$ du théorème chinois 3.67.

Théorème 3.94 (Théorème chinois).

Si P et Q sont deux polynômes premiers entre eux, alors nous avons l'isomorphisme

$$\mathbb{K}[X]/(P, Q) \simeq \mathbb{K}[X]/(P) \times \mathbb{K}[X]/(Q). \quad (3.123)$$

3.13.1 Irréductibilité**Théorème 3.95** (d'Alembert-Gauss).

Tout polynôme non constant à coefficients complexes possède au moins une racine complexe.

Définition 3.96.

Un polynôme est **irréductible** lorsqu'il ne peut pas être écrit sous la forme de produits de polynômes de degré supérieurs à 1.

Exemple 3.97

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

$$P = (X^2 + 1)(X^2 + 2), \quad (3.124)$$

mais n'a pas de racines dans $\mathbb{Z}$. Par contre, il est vrai que si on veut réduire plus, il faut sortir de $\mathbb{Z}$.

$\triangle$

Proposition 3.98.

Un polynôme irréductible à coefficients réels est soit de degré un soit de degré 2 avec un discriminant négatif.

Démonstration. Soit un polynôme P à coefficients réels de degré plus grand que 1. Alors le théorème de d'Alembert-Gauss (théorème 3.95) implique l'existence d'une racine α . Il est facile de montrer que le conjugué complexe $\bar{\alpha}$ est également racine. Par conséquent les polynômes $(X - \alpha)$ et $(X - \bar{\alpha})$ divisent P .

Ces deux polynômes sont premiers entre eux parce que

$$a(X - \alpha) + b(X - \bar{\alpha}) = 0 \quad (3.125)$$

implique $a = b = 0$. Par conséquent le produit

$$X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} \quad (3.126)$$

divise également P . Ce dernier est un polynôme à coefficients réels de degré 2. Donc tout polynôme de degré 3 ou plus est réductible. $\square$

Définition 3.99.

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 polynôme scindés.

Théorème 3.100 (Conséquence du lemme de Gauss).

Soit $\mathbb{A}$ un anneau factoriel et $\text{Frac}(\mathbb{A})$ son corps des fractions. Un polynôme non constant $P \in \mathbb{A}[X]$ est irréductible (sur $\mathbb{A}$) si et seulement si il est irréductible et primitif sur $\text{Frac}(\mathbb{A})[X]$.

Dans cet énoncé, un polynôme primitif est un polynôme dont le pgcd des coefficients est 1. Voir la remarque 4.140. Notons qu'ici nous considérons des polynômes dont les coefficients sont dans un anneau et non dans un corps comme nous en avons l'habitude.

3.13.2 Division euclidienne

Le théorème suivant établit la **division euclidienne** dans $\mathbb{A}[X]$ du polynôme A par B .

Théorème 3.101.

Soit $B \neq 0$ dans $\mathbb{A}[X]$ de coefficient dominant inversible dans $\mathbb{A}$. Pour tout $A \in \mathbb{A}[X]$, il existe $Q, R \in \mathbb{A}[X]$ tels que

$$A = BQ + R \quad (3.127)$$

avec $\deg(R) < \deg(B)$.

Les polynômes Q et R sont déterminés de façon univoque par cette condition.

Définition 3.102.

Le polynôme Q est le **quotient** et R est le **reste** de la division euclidienne de A par B . Si le reste de la division de A par B est nul on dit que B **divise** A et on note $B \mid A$. Autrement dit B divise A si il existe Q tel que $A = BQ$.

Corollaire 3.103.

Si $\mathbb{A}$ est un anneau intègre, l'anneau des polynômes à coefficients dans $\mathbb{A}$ est un anneau euclidien et principal.

Démonstration. Le théorème 3.101 montre que le degré est un stathme euclidien (définition 3.73), ce qui fait que l'anneau des polynômes est un anneau euclidien et en particulier un anneau principal par la proposition 3.75. $\square$

Définition 3.104.

Deux polynômes P et Q sont dits **étrangers** entre eux si 1 est un pgcd 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.

3.13.3 Bézout

Théorème 3.105 (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

$$P_1Q_1 + \dots + P_nQ_n = 1. \quad (3.128)$$

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 :

$$xP + yQ = 0; \quad (3.129)$$

cette dernière pourra être écrite en termes de la matrice de Sylvester, voir sous-section 6.5.7.

Lemme 3.106.

Soient $(P_i)_{i=1,\dots,n} \in \mathbb{K}[X]$ des polynômes étrangers deux à deux. Alors les polynômes

$$Q_i = \prod_{j \neq i} P_j \quad (3.130)$$

sont étrangers entre eux¹².

Lemme 3.107 ([37]).

Soit $\mathbb{K}$ un corps commutatif et $\mathbb{A} \subset \mathbb{K}$ un sous anneau de $\mathbb{K}$. Soit $\phi \in \mathbb{K}[X]$. Si il existe $Q \in \mathbb{A}[X]$ unitaire tel que $\phi Q \in \mathbb{A}[X]$, alors $\phi \in \mathbb{A}[X]$.

Lemme 3.108.

Quelques propriétés du PGCD dans les polynômes.

(1) Soit $P, Q, R \in \mathbb{K}[X]$ des polynômes tels que P soit premier avec Q . Alors

$$\text{pgcd}(P, QR) = \text{pgcd}(P, Q) \text{pgcd}(P, R) \quad (3.131)$$

(2) En analogie avec le lemme 2.29, nous avons

$$\text{pgcd}(P, PQ + R) = \text{pgcd}(P, R). \quad (3.132)$$

Problèmes et choses à faire

Est-ce que ce lemme 3.108 est correct ? J'aimerais en voir une preuve.

3.13.4 Idéaux

Soit $P \in \mathbb{K}[X]$ un polynôme. Nous notons (P) l'idéal engendré par P :

$$(P) = \{PR \text{ tel que } R \in \mathbb{K}[X]\}. \quad (3.133)$$

Lemme 3.109.

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. $\square$

Théorème 3.110.

Soit $\mathbb{K}$ un corps commutatif.

- (1) L'anneau $\mathbb{K}[X]$ est principal.
- (2) Si I est un idéal dans $\mathbb{K}[X]$ et si P est de degré minimal, alors $(P) = I$.
- (3) De plus si $I \neq \{0\}$, il existe un unique polynôme unitaire μ tel que $I = (\mu)$.

12. Et non juste deux à deux.

Démonstration. L'anneau $\mathbb{K}[X]$ est commutatif et intègre (pas de diviseurs de zéro). Nous devons encore montrer que tous les idéaux 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 $A \in I$. Par le théorème 3.101 de la division euclidienne¹³, il existe Q et R dans $\mathbb{K}[X]$ tels que $A = PQ + R$ avec $\deg(R) < \deg(P)$. Étant donné que $R = A - PQ$ nous avons $R \in I$ et par conséquent $R = 0$ parce que P a été choisit de degré minimum dans I . Nous avons donc $A = PQ$ et $I \subset (P)$.

L'existence d'un polynôme unitaire qui génère I est obtenu en choisissant $U = P/a_n$ où a_n est le coefficient du terme de plus haut degré. $\square$

Nous voyons que n'importe quel polynôme de degré minimum dans un idéal génère l'idéal. Une importante conséquence du théorème 3.110 que nous verrons plus bas est que tout polynôme annulateur d'un endomorphisme est divisé par le polynôme minimal (proposition 6.245).

3.13.5 Racines des polynômes

Proposition 3.111.

Soit $\mathbb{A}$ un anneau et P un polynôme non nul dans $\mathbb{A}[X]$. Si $\alpha \in \mathbb{A}$ est une racine de P alors $X - \alpha$ divise P .

Démonstration. Nous notons le polynôme $\mu = X - \alpha$ par analogie avec le polynôme minimal dont il sera question dans la très semblable proposition 4.55. Vu que P possède une racine, il est de degré au moins égal à 1 et nous pouvons effectuer la division euclidienne¹⁴ de P par μ : il existe des polynômes Q et R tels que

$$P = Q\mu + R \quad (3.134)$$

avec $\deg(R) < \deg(\mu)$. Donc $\deg(R) = 0$ et il est constant. Il existe donc $a \in \mathbb{A}$ tel que $S = Q\mu + a$. En évaluant cela en α ,

$$S(\alpha) = Q(\alpha)\mu(\alpha) + a, \quad (3.135)$$

nous voyons que $a = 0$, ce qui montre que $S = Q\mu$ et que μ divise S . $\square$

Définition 3.112 (Racine simple et multiple d'un polynôme).

Soit $\mathbb{A}$ un anneau ainsi qu'un polynôme $P \in \mathbb{A}[X]$ et $\alpha \in \mathbb{A}$. 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 .

Pour une définition générale d'une racine simple de l'équation $f(x) = 0$, voir la définition 25.57.

La proposition 3.111 nous indique que toute racine est de multiplicité au moins 1.

Proposition 3.113.

L'élément $\alpha \in \mathbb{A}$ est une racine de multiplicité h du polynôme P si et seulement si il existe $Q \in \mathbb{A}[X]$ tel que $P = (X - \alpha)^h Q$ avec $Q(\alpha) \neq 0$.

Lemme 3.114.

Soient P et Q des polynômes non nuls de $\mathbb{A}[X]$ et $\alpha \in \mathbb{A}$ de multiplicité p pour P et de multiplicité q pour Q . Alors

- (1) $\theta_\alpha(P + Q) \geq \min\{\theta_\alpha(P), \theta_\alpha(Q)\}$
- (2) si $\theta_\alpha(P) \neq \theta_\alpha(Q)$, alors $\theta_\alpha(P + Q) = \min\{\theta_\alpha(P), \theta_\alpha(Q)\}$
- (3) $\theta_\alpha(PQ) \geq \theta_\alpha(P) + \theta_\alpha(Q)$;
- (4) si $\mathbb{A}$ est intègre alors $\theta_\alpha(PQ) = \theta_\alpha(P) + \theta_\alpha(Q)$;

13. Ici $\mathbb{K}$ est un corps et donc l'hypothèse d'inversibilité est automatiquement vérifiée.

14. Théorème 3.101.

Théorème 3.115.

Soit $\mathbb{A}$ un anneau intègre et $P \in \mathbb{A}[X] \setminus \{0\}$, un polynôme de degré n . Si $\alpha_1, \dots, \alpha_p \in \mathbb{A}$ sont des racines deux à deux distinctes de multiplicités $k_1, \dots, k_p$, alors il existe $Q \in \mathbb{A}[X]$ tel que

- (1) $Q(\alpha_i) \neq 0$;
- (2) $P = Q \prod_{i=1}^p (X - \alpha_i)^{k_i}$;
- (3) Le degré de Q est $n - p$.

De plus 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 $Q \in \mathbb{A}[X]$ tel que $P = Q(X - \alpha)^k$. Il reste à voir que $Q(\alpha) \neq 0$. Cela est une conséquence de la proposition 3.111 : 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 $p \geq 2$ et nous effectuons une récurrence sur p . Nous considérons donc les $p - 1$ premières racines $\alpha_1, \dots, \alpha_{p-1}$ et un polynôme $R \in \mathbb{A}[X]$ tel que $R(\alpha_i) \neq 0$ pour $i = 1, \dots, p - 1$ et

$$P = \underbrace{(X - \alpha_1)^{k_1} \dots (X - \alpha_{p-1})^{k_{p-1}}}_S R. \quad (3.136)$$

Par hypothèse $P(\alpha_p) = S(\alpha_p)R(\alpha_p) = 0$. L'anneau $\mathbb{A}$ 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 (4) du lemme 3.114 afin de dire que le degré de α_p pour $P = SR$ est k_p . Par conséquent

$$R = (X - \alpha_p)^{k_p} T \quad (3.137)$$

avec $T(\alpha_p) \neq 0$ et enfin

$$P = \prod_{i=1}^p (X - \alpha_i)^{k_i} T. \quad (3.138)$$

De plus $T(\alpha_i) \neq 0$, sinon $R(\alpha_i)$ serait nul. □

Proposition 3.116 (Critère d'Eisenstein).

Soit le polynôme $P(X) = \sum_{k=0}^n a_k X^k$ 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 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 (3.70) 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 est primitif au sens du pgcd. Il est donc irréductible et primitif sur $\mathbb{Q}[X]$ et une conséquence du lemme de Gauss (3.100) nous dit alors que P est irréductible sur $\mathbb{Z}[X]$. □

Exemple 3.117

Soit le polynôme $P(X) = 3X^4 + 15X^2 + 10$. Pour faire fonctionner 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. C'est vite vu que $p = 5$ fait l'affaire. Le polynôme P est donc irréductible sur $\mathbb{Q}[X]$. $\triangle$

3.13.6 Quelques identités**Lemme 3.118.**

Quelques identités de polynômes.

(1) Si n est impair, alors $1 + X$ divise $1 + X^n$.

(2) Pour tout n nous avons $X^n - 1 = (X - 1)(1 + X + \dots + X^{n-1})$.

(3) $z^n - z_0^n = (z - z_0) \sum_{i=0}^{n-1} z^i z_0^{n-1-i}$.

Démonstration. Le cas $n = 1$ est évident. Procédons alors par récurrence en considérant un nombre entier impair n :

$$1 + X^{n+2} = 1 + X^n + X^{n+2} - X^n \quad (3.139a)$$

$$= (1 + X)P + X^n(X^2 - 1) \quad (3.139b)$$

$$= (1 + X)P + X^n(X + 1)(X - 1) \quad (3.139c)$$

$$= (1 + X)(P + X^n(X - 1)). \quad (3.139d)$$

□

Chapitre 4

Corps

4.1 Généralités

4.1.

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 4.119 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 [1] 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.

Dans tous les cas, un corps dans lequel l'élément nul est inversible est appelé un mensonge, comme le prouve le lemme suivant.

Lemme 4.2.

En tant que anneau, un corps est un anneau intègre : il n'a pas de diviseurs zéro.

Démonstration. En effet si a est un diviseur de zéro, alors $ax = 0$ pour un certain $x \neq 0$. Si a était inversible, nous aurions $x = a^{-1}ax = 0$, ce qui est impossible. $\square$

Conséquence : dans un corps nous avons toujours la règle du produit nul.

Définition 4.3 (Algèbre[38]).

Si $\mathbb{K}$ est un corps commutatif¹, une $\mathbb{K}$ -**algèbre** A est un espace vectoriel muni d'une opération bilinéaire $\times : A \times A \rightarrow A$, 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 $f : A \rightarrow B$ est un **morphisme** 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 $x \times y$.

Définition 4.4.

Si X est une partie d'une algèbre A , alors l'**algèbre engendrée** par X est l'intersection de toutes les sous-algèbres de A contenant X .

1. Définition 1.16

Par le lemme 3.41, un anneau sans diviseur de zéro est de caractéristique zéro ou première. Le fait d'être intègre pour un anneau n'assure cependant pas le fait d'être un corps. Nous avons cependant ce résultat pour les anneaux finis.

Proposition 4.5.

Un anneau fini intègre est un corps.

Démonstration. Soit A un tel anneau. Soit $a \neq 0$. Les applications

$$l_a: x \rightarrow ax \quad (4.1a)$$

$$r_a: x \rightarrow xa \quad (4.1b)$$

sont injectives. En tant que applications injectives entre ensembles finis, elles sont surjectives. Il existe donc b et c tels que $1 = ba = ac$. Il se fait que b et c sont égaux parce que

$$b = b(ac) = (ba)c = c. \quad (4.2)$$

Par conséquent b est un inverse de a . □

Proposition 4.6.

Soit $n \in \mathbb{N}^*$. Les conditions suivantes sont équivalentes :

- (1) n est premier.
- (2) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
- (3) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Démonstration. L'équivalence entre les deux premiers points est le contenu du corollaire 3.40. Le fait que $\mathbb{Z}/n\mathbb{Z}$ soit un corps lorsque $\mathbb{Z}/n\mathbb{Z}$ est intègre est la proposition 4.5. 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 4.2). □

Proposition 4.7.

Si A est un anneau, nous avons les équivalences

- (1) A est un corps.
- (2) A est non nul et ses seuls idéaux à gauche sont $\{0\}$ et A .
- (3) A est non nul et ses seuls idéaux à droite sont $\{0\}$ et A .

Proposition 4.8.

Soit A , un anneau commutatif non nul et I , un idéal dans A . L'ensemble I est un idéal maximum de A si et seulement si A/I est un corps.

Démonstration. Par la proposition 4.7, le fait pour A/I d'être un corps signifie qu'il n'a pas d'idéaux non triviaux. Si ϕ est la projection canonique $A \mapsto A/I$, nous savons que les idéaux de A/I sont les $\phi(J)$ où J est un idéal de A contenant I (proposition 3.22). Si I est un idéal maximum de A , un tel J n'existe pas. Inversement si A/I n'a pas d'autres idéaux que A/I et $\phi(0)$, c'est que I est un idéal maximum. □

4.1.1 Corps des fractions

Théorème 4.9.

Soit $\mathbb{A}$ un anneau commutatif intègre. Il existe un corps commutatif $\mathbb{K}$ et un morphisme injectif (d'anneaux) $\epsilon: \mathbb{A} \rightarrow \mathbb{K}$ tels que pour tout $\lambda \in \mathbb{K}$, il existe $(a, b) \in \mathbb{A} \times \mathbb{A}^*$ tels que

$$\lambda = \epsilon(a)(\epsilon(b))^{-1} \quad (4.3)$$

De plus 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 $\mathbb{A}$ est le **corps des fractions** de $\mathbb{A}$, et sera noté $\text{Frac}(\mathbb{A})$.

Notons que l'application $\mathbb{A} \times \mathbb{A}^* \rightarrow \mathbb{K}$ donnée par $(a, b) \mapsto \epsilon(a)(\epsilon(b))^{-1}$ envoie (xa, xb) sur le même que (a, b) .

L'ensemble $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. Cet ensemble n'est pas l'ensemble de tous les réels.

Proposition 4.10 (Irrationalité de $\sqrt{2}$).

Il n'existe pas de fractions de nombres entiers dont le carré soit 2.

Démonstration. La preuve repose sur deux idées :

- Il n'existe pas de suite strictement décroissante d'entiers positifs.
- Si x est un nombre tel que x^2 est pair, alors x est pair. En effet si x est impair, alors $x = 2n + 1$ et $x^2 = 4n^2 + 4n + 1$ qui est impair.

Nous allons maintenant prouver la proposition par l'absurde². Soient des entiers positifs a_0, b_0 tels que $a_0/b_0 = \sqrt{2}$, c'est à dire

$$\frac{a_0^2}{b_0^2} = 2. \quad (4.4)$$

Dans ce cas, $a_0^2 = 2b_0^2$ est pair, donc a_0 est pair. Nous avons alors $a_0^2 = 4n$ pour un certain entier positif n . L'égalité

$$4n = 2b_0^2 \quad (4.5)$$

dit alors que b_0^2 est pair et donc que b_0 est pair.

Nous construisons alors $a_1 = a_0/2$ et $b_1 = b_0/2$ qui sont encore des entiers strictement positifs, mais strictement inférieurs à a_0 et b_0 . De plus,

$$\frac{a_1^2}{b_1^2} = 2 \quad (4.6)$$

et nous pouvons continuer.

Nous construisons ainsi par récurrence une suite strictement décroissante d'entiers positifs, ce qui est impossible. $\square$

4.1.2 Corps premier

Définition 4.11.

*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 4.12.

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. $\square$

Définition 4.13.

Soit p un nombre premier. Nous notons $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Nous verrons plus loin (section 4.6) comment nous pouvons définir $\mathbb{F}_{p^n}$ lorsque p est premier, ainsi que l'unicité d'un tel corps.

Nous avons par exemple

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\} \quad (4.7)$$

avec la loi $2 = 0$.

Notons que $\mathbb{F}_p$ est un corps possédant p éléments. L'ensemble $\mathbb{F}_p^*$ est un groupe d'ordre $p - 1$.

2. Vraiment par l'absurde : en supposant le contraire de la thèse nous allons construire quelque chose d'impossible.

Lemme 4.14.

Les corps $\mathbb{Q}$ et $\mathbb{F}_p$ (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 4.6 que $\mathbb{F}_p$ est un corps lorsque p est premier. $\square$

Proposition 4.15.

Soit $\mathbb{K}$ un corps de caractéristique p et $\mathbb{P}$ son sous corps premier. Si $p = 0$ alors $\mathbb{P} = \mathbb{Q}$. Si $p > 0$, alors $\mathbb{P} = \mathbb{F}_p$.

Démonstration. Notons d'abord que la caractéristique d'un corps est toujours un nombre premier parce qu'un corps est en particulier un anneau intègre (proposition 3.41).

Étant donné que 1 est dans tout sous corps, nous devons avoir $\mathbb{Z}1 \subseteq \mathbb{P}$. Si $p = 0$, alors $\mathbb{Z}1 \simeq \mathbb{Z}$, et nous avons

$$\mathbb{Z}1_{\mathbb{A}} \subset \mathbb{P} \subset \mathbb{K}. \quad (4.8)$$

Pour chaque $(n, m) \in \mathbb{Z}1_{\mathbb{A}} \times (\mathbb{Z}1_{\mathbb{A}})^*$ l'élément $nm^{-1} \in \mathbb{K}$ est dans $\mathbb{P}$ parce que $\mathbb{P}$ est un corps. Nous en déduisons que le corps des fractions de $\mathbb{Z}$ est contenu dans $\mathbb{P}$ par conséquent $\mathbb{P} = \mathbb{Q}$ (théorème 4.9).

Si par contre la caractéristique de $\mathbb{K}$ est $p \neq 0$, nous avons $\mathbb{Z}1_{\mathbb{A}} \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ par le lemme 3.26. L'ensemble $\mathbb{F}_p$ étant un corps, c'est le corps premier de $\mathbb{K}$. $\square$

Proposition 4.16.

Soit $\mathbb{K}$ un corps et $\mathbb{P}$ son sous corps premier. Si $\sigma \in \text{Aut}(\mathbb{K})$ alors $\sigma|_{\mathbb{P}} = \text{Id}$, c'est à dire que

$$\sigma(x) = x \quad (4.9)$$

pour tout $x \in \mathbb{P}$.

Théorème 4.17 (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 Bézout³ 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

$$R = PUR + QVR = PUR + VPS = P(UR + VS), \quad (4.10)$$

ce qui signifie que P divise R . $\square$

Le lemme suivant est une généralisation du lemme de Gauss dans $\mathbb{Z}$ (lemme 3.70).

Lemme 4.18 (Lemme de Gauss[35]).

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

$$\pi_p: \mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X]. \quad (4.11)$$

3. théorème 3.105.

Par définition $abPQ = P_1Q_1 \in \mathbb{Z}[X]$; en prenant la projection,

$$\pi_p(P_1)\pi_p(Q_1) = \pi_p(P_1Q_1) = \pi_P(ab)\pi_p(PQ) = 0 \quad (4.12)$$

parce que $\pi_p(ab) = 0$. Étant donné que $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre (exemple 3.45), 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 . $\square$

4.1.3 Petit théorème de Fermat

Théorème 4.19 (Petit théorème de Fermat).

Soit p un nombre premier. Si $x \in \mathbb{F}_p$ alors $x^p = x$. Si $x \in (\mathbb{F}_p)^*$, alors $x^{p-1} = 1$.

En particulier si $x \in \mathbb{F}_p^*$ alors $x^{-1} = x^{p-2}$.

Démonstration. Étant donné que $\mathbb{F}_p$ est un corps commutatif et que p est premier, la proposition 3.30 nous indique que $\sigma(x) = x^p$ est un automorphisme. La proposition 4.16 nous indique alors que

$$a^p = a. \quad (4.13)$$

Si a est inversible alors $a^{p-1} = a^p a^{-1} = 1$. $\square$

Remarque 4.20.

Une autre façon d'énoncer le petit théorème de Fermat 4.19 est que si p est premier et si a est premier avec a , alors $a^{p-1} \in [1]_p$. Le nombre a n'est pas premier avec p uniquement lorsque a est multiple de p . Dans ce cas c'est $a = 0$ dans $\mathbb{F}_p$ et donc $a^{p-1}=0$.

Exemple 4.21

Soit $\mathbb{K} = \mathbb{F}_{29}^*$. Le nombre 29 étant premier, $\mathbb{K}$ est un corps premier. C'est le corps des entier modulo 29. Nous avons donc

$$-142 = -113 = -84 = -55 = -26 = 3 = 32 = 61 = 90 = 119. \quad (4.14)$$

Le petit théorème de Fermat nous permet aussi de calculer des exposants et des inverses. Nous avons

$$x^{-a} = (x^a)^{27} = x^{27a}. \quad (4.15)$$

Le nombre $27a$ peut être grand par rapport à 29. Étant donné que $1 = x^{28}$ nous avons

$$x^{-a} = x^{27a \mod 28}. \quad (4.16)$$

Dans les exposants nous calculons modulo 28. $\triangle$

4.2 Théorème des deux carrés

Proposition 4.22.

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. $\square$

4.2.1 Un peu de structure dans $\mathbb{Z}[i]$

Lemme 4.23.

L'application

$$\begin{aligned} N: \mathbb{Z}[i] &\rightarrow \mathbb{N} \\ a + bi &\mapsto a^2 + b^2 \end{aligned} \quad (4.17)$$

est un stathme euclidien pour $\mathbb{Z}[i]$.

Démonstration. Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$ et

$$\frac{z}{t} = x + iy \quad (4.18)$$

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 hasard⁴. Alors nous avons

$$\left| \frac{z}{t} - q \right| \leq \frac{|1 + i|}{2} = \frac{\sqrt{2}}{2} < 1. \quad (4.19)$$

On pose $r = z - qt$ qui est bien un élément de $\mathbb{Z}[i]$. De plus

$$|r| = |z - qt| = |t| \left| \frac{z}{t} - q \right| < |t|, \quad (4.20)$$

c'est à dire que $|r|^2 < |t|^2$ et donc $N(r) < N(t)$. □

Étant donné que $\mathbb{Z}[i]$ est euclidien, il est principal (proposition 3.75).

Lemme 4.24.

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

$$1 = N(zz') = N(z)N(z'), \quad (4.21)$$

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

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}. \quad (4.22)$$

□

Nous notons $\Sigma = \{a^2 + b^2 \text{ tel que } a, b \in \mathbb{N}\}$.

Lemme 4.25.

L'ensemble Σ est un sous-monoïde de $\mathbb{N}$.

Démonstration. Il suffit de prouver que si $m, n \in \Sigma$, alors le produit mn est également dans Σ . Si N est le stathme euclidien sur $\mathbb{Z}[i]$, alors $n \in \Sigma$ si et seulement si il existe $z \in \mathbb{Z}[i]$ tel que $N(z) = n$. Si $z, z' \in \mathbb{Z}[i]$, alors $zz' \in \mathbb{Z}[i]$ et de plus

$$N(zz') = N(z)N(z') = nm. \quad (4.23)$$

Donc nm est l'image de zz' par N , ce qui prouve que $nm \in \Sigma$. □

Théorème 4.26 (Théorème des deux carrés, version faible).

Un nombre premier est somme de deux carrés si et seulement si $p = 2$ ou $p \in [1]_4$.

4. Dans l'exemple 3.74, nous prenions toujours l'inférieur parce que le stathme tenait compte de la positivité.

Remarque 4.27.

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 $[1]_4$.

Démonstration. Soit p un nombre premier dans Σ . Si $a = 2k$, alors $a^2 = 4k^2$ et $a^2 \equiv 0 \pmod{4}$. Si au contraire a est impair, $a = 2k + 1$ et $a^2 = 4k^2 + 1 + 4k \equiv 1 \pmod{4}$. 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 $0 \pmod{4}$ ne sont pas premiers ; parmi les $2 \pmod{4}$, 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 $p \equiv 1 \pmod{4}$. Il reste à faire le contraire : démontrer que si un nombre premier p vaut $1 \pmod{4}$, alors il est premier. Nous considérons l'anneau

$$\mathbb{Z}[i] = \{a + bi \text{ tel que } a, b \in \mathbb{Z}\}. \quad (4.24)$$

puis l'application

$$\begin{aligned} N: \mathbb{Z}[i] &\rightarrow \mathbb{N} \\ a + bi &\mapsto a^2 + b^2. \end{aligned} \quad (4.25)$$

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 4.24).

Le lemme 4.23 montre que $\mathbb{Z}[i]$ est un anneau euclidien parce que N est un stathme. L'anneau $\mathbb{Z}[i]$ étant euclidien, il est principal (proposition 3.75).

Pour la suite, nous allons d'abord montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$, puis nous allons voir quels sont les irréductibles de $\mathbb{Z}[i]$.

Soit p , un nombre premier dans Σ . Si $p = a^2 + b^2$, alors nous avons $p = (a + ib)(a - bi)$, mais étant donné que p est premier, nous avons $a \neq 0$ et $b \neq 0$. Du coup p n'est pas inversible dans $\mathbb{Z}[i]$, mais il peut être écrit comme le produit de deux non inversibles. Le nombre p est donc non irréductible dans $\mathbb{Z}[i]$.

Dans l'autre sens, nous supposons que p est un nombre premier non irréductible dans $\mathbb{Z}[i]$. Nous avons alors $p = zz'$ avec ni z ni z' dans $\{\pm 1, \pm i\}$. En appliquant N nous avons

$$p^2 = N(p) = N(z)N(z'). \quad (4.26)$$

Vu que p est premier, cela est uniquement possible avec $N(z) = N(z') = p$ (avoir $N(z) = 1$ est impossible parce que cela dirait que z est inversible). Si $z = a + ib$, alors $p = N(z) = a^2 + b^2$, et donc $p \in \Sigma$.

Nous savons déjà que $\mathbb{Z}[i]$ est un anneau principal et n'est pas un corps ; la proposition 3.62 s'applique donc et p sera non irréductible si et seulement si l'idéal (p) sera non premier. Le fait que (p) soit un idéal non premier implique que le quotient $\mathbb{Z}[i]/(p)$ est non intègre (c'est la définition d'un idéal premier). Nous cherchons donc les nombres premiers pour lesquels le quotient $\mathbb{Z}[i]/(p)$ n'est pas intègre.

Nous commençons par écrire le quotient $\mathbb{Z}[i]/(p)$ sous d'autres formes. D'abord en remarquant que si I et J sont deux idéaux, on a $(\mathbb{A}/I)/J \simeq (\mathbb{A}/J)/I$, du coup, en tenant compte du fait que $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2 + 1)$, nous avons

$$\mathbb{Z}[i]/(p) = (\mathbb{Z}[X]/(p))/(X^2 + 1) = \mathbb{F}_p[X]/(X^2 + 1). \quad (4.27)$$

Nous avons donc équivalence des propositions suivantes :

$$p \in \Sigma \quad (4.28a)$$

$$\mathbb{F}_p[X]/(X^2 + 1) \text{ n'est pas intègre} \quad (4.28b)$$

$$X^2 + 1 \text{ n'est pas irréductible dans } \mathbb{F}_p \quad (4.28c)$$

$$X^2 + 1 \text{ admet une racine dans } \mathbb{F}_p \quad (4.28d)$$

$$-1 \in (\mathbb{F}_p^*)^2 \quad (4.28e)$$

$$\exists y \in \mathbb{F}_p^* \text{ tel que } y^2 = -1. \quad (4.28f)$$

Le point (4.28c) vient de la proposition 4.22. 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,

$$(-1)^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1 \quad (4.29)$$

parce que dans $\mathbb{F}_p$ nous avons $y^{(p-1)} = 1$ par le petit théorème de Fermat (théorème 4.19). Du coup p doit vérifier

$$1 = (-1)^{(p-1)/2}, \quad (4.30)$$

c'est à dire $\frac{p-1}{2} = 0 \pmod{2}$ ou encore $p = 1 \pmod{4}$. $\square$

Théorème 4.28 (Théorème des deux carrés[1]).

Soit $n \geq 2$ un nombre dont nous notons

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \quad (4.31)$$

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. **Condition suffisante.** Le produit (4.31) 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

$$\prod_{p \in \mathcal{P} \cap [1]_4} p^{v_p(n)} \in \Sigma. \quad (4.32)$$

— Le seul nombre premier dans $[2]_4$ est 2. C'est un élément de Σ .

— Le produit

$$\prod_{p \in \mathcal{P} \cap [3]_4} p^{v_p(n)} \quad (4.33)$$

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 4.25.

Condition nécessaire. Soit p , un nombre premier. Nous voulons montrer que

$$\{v_p(n) \text{ tel que } n \in \Sigma\} \subset [2]_2. \quad (4.34)$$

Pour montrer cela nous allons procéder par récurrence sur les ensembles

$$E_k = \{v_p(n) \text{ tel que } n \in \Sigma\} \cap \{0, \dots, k\}. \quad (4.35)$$

Il est évident que les éléments de E_0 sont pairs, vu qu'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 $v_p(n) \leq k+1$ 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

$$n = a^2 + b^2 = (a + bi)(a - bi) \quad (4.36)$$

Vu que $\mathbb{Z}[i]$ est principal, le lemme de Gauss 3.70 nous dit que si p divise n , alors il doit diviser soit $a + bi$, soit $a - bi$ (et du coup en fait les deux). Nous avons alors $p \mid a$ et $p \mid b$ en même temps. Du coup

$$p^2 \mid a^2 + b^2 = n. \quad (4.37)$$

Posons $a = pa'$ et $b = pb'$ avec $a', b' \in \mathbb{N}$. Nous avons

$$\frac{n}{p^2} = \frac{p^2 a'^2 + p^2 b'^2}{p^2} = a'^2 + b'^2 \in \Sigma. \quad (4.38)$$

Mais par construction,

$$v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 < k. \quad (4.39)$$

Donc $v_p(\frac{n}{p^2})$ est pair et du coup $v_p(n)$ doit également être pair.

□

4.2.2 Résultats chinois

Nous allons maintenant parler du système d'équations

$$\begin{cases} x = a_1 \pmod{p} \\ x = a_2 \pmod{q} \end{cases} \quad (4.40a)$$

$$(4.40b)$$

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 corollaire qui établira l'isomorphisme d'anneaux $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Voir les-mathematiques.net.

Lemme 4.29 (Lemme chinois [39]).

Soient n_1, n_2 deux entiers premiers entre eux. Soient $a_1, a_2 \in \mathbb{Z}$. Les solutions du système

$$\begin{cases} x = a_1 \pmod{n_1} \\ x = a_2 \pmod{n_2} \end{cases} \quad (4.41a)$$

$$(4.41b)$$

pour $x \in \mathbb{Z}/n_1 n_2 \mathbb{Z}$ sont données de la façon suivante. Soient u_1, u_2 deux entiers qui satisfont la relation de Bézout⁵

$$u_1 n_1 + u_2 n_2 = 1, \quad (4.42)$$

et

$$a = (a_1 u_2 n_2 + a_2 u_1 n_1) \pmod{(n_1 n_2)}. \quad (4.43)$$

Alors $x = a \pmod{(n_1 n_2)}$.

Démonstration. Vérifions que le x donné par $x = a \pmod{(n_1 n_2)}$ est bien une solution. D'abord

$$a \pmod{n_2} = a_1 u_2 n_2 \pmod{n_1} \quad (4.44a)$$

$$= a_1 (1 - u_1 n_1) \pmod{n_1} \quad (4.44b)$$

$$= a_1 \pmod{n_1} \quad (4.44c)$$

où nous avons utilisé l'identité de Bézout (4.42). La vérification de $a \pmod{n_2} = a_2 \pmod{n_2}$ est la même.

Soit maintenant $x \in \mathbb{Z}/n_1 n_2 \mathbb{Z}$ une solution du système (4.41) et a donné par la formule (4.43). Alors

$$(x - a) \pmod{n_1} = \left(a_1 - (a_1 n_2 u_2 + a_2 u_1 n_1) \right) \pmod{n_1} \quad (4.45a)$$

$$= a_1 - a_1 u_2 n_2 \pmod{n_1} \quad (4.45b)$$

$$= 0, \quad (4.45c)$$

donc $(x - a) \pmod{n_1} = 0$, ce qui signifie que $x - a$ est divisible par n_1 . De la même façon, $(x - a) \pmod{n_2} = 0$ et $x - a$ est divisible par n_2 . Nous savons maintenant que $x - a$ est divisible par n_1 et n_2 . Étant donné que n_1 et n_2 sont premiers entre eux, nous en déduisons que $x - a$ est divisible par $n_1 n_2$, ou encore que $x = a \pmod{n_1 n_2}$. □

5. voir le théorème 2.24

Théorème 4.30 (Théorème chinois).

Soient p, q deux naturels premiers entre eux. Si $p, q \geq 2$ alors l'application

$$\begin{aligned}\phi: \mathbb{Z}/pq\mathbb{Z} &\rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ [x]_{pq} &\mapsto ([x]_p, [x]_q)\end{aligned}\tag{4.46}$$

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,

$$\phi([q]_{pq} + [y]_{pq}) = \phi((x + y) \bmod pq) \tag{4.47a}$$

$$= ([x + y]_p, [x + y]_q) \tag{4.47b}$$

$$= ([x]_p + [y]_p, [x]_q + [y]_q) \tag{4.47c}$$

$$= ([x]_p, [x]_q) + ([y]_p, [y]_q) \tag{4.47d}$$

$$= \phi(x) + \phi(y). \tag{4.47e}$$

En ce qui concerne le produit, c'est le même jeu : nous obtenons

$$\phi([xy]_{pq}) = \phi([x]_{pq})\phi([y]_{pq}) \tag{4.48}$$

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

$$\phi([x]_{pq}) = ([y_1]_p, [y_2]_q) \tag{4.49}$$

revient à demander que $[x]_p = [y_1]_p$ et $[x]_q = [y_2]_q$, c'est à dire que x résolve le système

$$\begin{cases} x = y_1 \bmod p \\ x = y_2 \bmod q. \end{cases} \tag{4.50a}$$

$$\tag{4.50b}$$

Le lemme chinois 4.29 nous assure qu'une solution existe.

En ce qui concerne l'injectivité, nous supposons que x et y soient deux entiers tels que

$$\phi([x]_{pq}) = \phi([y]_{pq}). \tag{4.51}$$

Nous en déduisons le système

$$\begin{cases} x \bmod p = y \bmod p \\ x \bmod q = y \bmod q \end{cases} \tag{4.52a}$$

$$\tag{4.52b}$$

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

$$kp + lq = 0. \tag{4.53}$$

Étant donné que p et q sont premiers entre eux, la seule possibilité est $k = l = 0$, c'est à dire $x = y$. $\square$

Théorème 4.31 (Théorème chinois).

Soit A un anneau commutatif, $n \geq 2$, 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 $1 \leq i \leq n$.

Démonstration. Pour $i \in \{1, \dots, n\}$ nous notons J_i le produit $J_i = \prod_{k \neq i} I_k$. Étant donné que chaque I_i est un idéal, nous avons $I_k \in J_i$ lorsque $i \neq k$.

Soit i fixé, et considérons $j \neq i$. Nous pouvons trouver $a_j \in I_i$ et $b_j \in I_j$ tel que $a_j + b_j = 1$. Nous avons alors

$$1 = \prod_{j \neq i} (a_j + b_j). \tag{4.54}$$

Par ailleurs $I_i + J_i = A$ parce que J_i contient I_k avec $k \neq i$ et $I_i + I_k = A$. Nous pouvons donc prendre $\alpha_i \in I_i$ et $\beta_i \in J_i$ tels que

$$\prod_{j \neq i} (a_j + b_j) = \alpha_i + \beta_i. \quad (4.55)$$

Nous considérons alors l'élément $x = \beta_1 x_1 + \dots + \beta_n x_n$ et nous avons

$$x - x_1 = (\beta_1 - 1)x_1 + \beta_2 x_2 + \dots + \beta_n x_n \quad (4.56a)$$

$$= -\alpha_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n \quad (4.56b)$$

Mais $\alpha_1 \in I_1$ et tous les autres termes sont dans les J_i avec $i \neq 1$. Par conséquent le tout est dans I_1 . Ici nous utilisons par exemple le fait que $\beta_2 \in J_2 \subset I_1$ parce que les éléments de J_2 sont des produits d'éléments dont un facteur est dans I_1 . $\square$

Remarque 4.32.

Ce théorème chinois est bien une généralisation du lemme chinois 4.29. En effet, l'élément x dont il est question est solution du problème $x = x_i \pmod{I_i}$. 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 corollaire 2.25.

4.2.3 Anneaux principaux et polynômes

Nous supposons que $\mathbb{K}$ est un corps commutatif, et nous étudions l'anneau $\mathbb{K}[X]$. Étant donné que $\mathbb{K}$ est commutatif pour tout polynôme que l'idéal engendré par P est $(P) = \mathbb{K}[X]P$, voir la notation (3.133).

Remarque 4.33.

Un polynôme est irréductible dans $\mathbb{K}[X]$ au sens de la définition 3.53 si et seulement si il est irréductible au sens de la définition 3.96 parce que seules les constantes (non nulles) sont inversibles dans $\mathbb{K}[X]$.

Corollaire 4.34.

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 3.110, par conséquent la proposition 3.64 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 $\sum_{k=0}^{n-1} a_k \bar{X}^k = 0$ alors un représentant de cette classe doit être de la forme SP dans $\mathbb{K}[X]$, c'est à dire

$$\sum_{k=0}^{n-1} a_k X^k = SP, \quad (4.57)$$

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

$$\bar{X}^{n+l} = \bar{X}^n \bar{X}^l = (\bar{P} - \bar{Q}) \bar{X}^l = \bar{Q} \bar{X}^l. \quad (4.58)$$

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 . $\square$

Remarque 4.35.

Ce corollaire prendra une nouvelle jeunesse lorsque nous parlerons de polynômes d'endomorphismes, en particulier la proposition 6.255 va donner des précisions.

4.3 Extension de corps

Lemme 4.36.

Soit $\mathbb{L}$ un corps fini et $\mathbb{K}$ un sous corps de $\mathbb{K}$. Alors il existe $s \in \mathbb{N}$ tel que

$$\text{Card}(\mathbb{K}) = \text{Card}(\mathbb{L})^s. \quad (4.59)$$

Démonstration. Le corps $\mathbb{L}$ est un $\mathbb{K}$ -espace vectoriel de dimension finie. Si s est la dimension alors nous avons la formule (4.59) parce que chaque élément de $\mathbb{L}$ est un s -uplet d'éléments de $\mathbb{K}$. $\square$

Définition 4.37.

Soit $\mathbb{K}$ un corps commutatif. Une **extension** de $\mathbb{K}$ est un corps $\mathbb{L}$ muni d'un morphisme $i: \mathbb{K} \rightarrow \mathbb{L}$. Nous identifions le plus souvent $\mathbb{K}$ avec $i(\mathbb{K}) \subset \mathbb{L}$.

Une extension est **algébrique** de $\mathbb{K}$ est une extension dont tous les éléments sont racines de polynômes dans $\mathbb{K}[X]$.

Notons que $\mathbb{R}$ 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*.

4.3.1 Polynôme minimal

Définition 4.38 (Polynôme minimal).

Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $a \in \mathbb{L}$. Nous considérons l'idéal

$$I_a = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\}. \quad (4.60)$$

Étant donné que $\mathbb{K}[X]$ est principal, cet idéal est principal et donc accepte un générateur unitaire. Nous nommons ce dernier **polynôme minimal** de a sur $\mathbb{K}$.

Exemple 4.39

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 $\mathbb{Q}[X]$. $\triangle$

Proposition 4.40 ([8]).

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 irréductible⁶ sur $\mathbb{K}$;
- (2) si $Q \in \mathbb{K}[X]$ est un polynôme non annulateur de a alors Q et μ_a sont premiers⁷ entre eux.

Démonstration. (1) Si μ_a était réductible sur $\mathbb{K}$, il existerait des polynômes P et Q dans $\mathbb{K}[X]$ tels que $\mu_a = PQ$; en évaluant cela en a nous obtenons $0 = P(a)Q(a)$, ce qui signifie que soit P soit Q est annulateur de a . Mais P et Q sont tous deux de degré supérieur à 1 (et donc de degré inférieur à celui de μ_a). Cela contredit la minimalité de μ_a : le polynôme minimal doit diviser tout polynôme annulateur.

- (2) Soit Q un polynôme non annulateur de a . Si Q et μ_a ne sont pas premiers entre eux dans $\mathbb{K}[X]$ alors ils ont un diviseur commun. Mais μ_a étant irréductible sur $\mathbb{K}$ par (1), ce diviseur commun ne peut être que μ_a lui-même. Mais dans ce cas Q serait annulateur de a . $\square$

Deux éléments α et β dans $\mathbb{L}$ sont dit **conjugués** si ils ont même polynôme minimal. Par exemple i et $-i$ sont conjugués dans $\mathbb{C}$ vu comme extension de $\mathbb{Q}$.

Lemme 4.41 ([40]).

Un nombre complexe algébrique dont tous les conjugués sont de module 1 est une racine de l'unité.

6. Définition 3.96.

7. Définition 3.104.

Lemme 4.42.

Si $(\mathbb{L}, i)$ est une extension de $\mathbb{K}$, alors $\mathbb{L}$ est un espace vectoriel sur $\mathbb{K}$.

Démonstration. Il faut définir le produit d'un élément de $\mathbb{L}$ par un élément de $\mathbb{K}$; si $\lambda \in \mathbb{K}$ et $x \in \mathbb{L}$ nous la définissons par

$$\lambda \cdot x = i(\lambda)x \quad (4.61)$$

où la multiplication du membre de droite est celle du corps $\mathbb{L}$. $\square$

Définition 4.43.

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 4.44

L'ensemble $\mathbb{C}$ est une extension de $\mathbb{R}$ et son degré est $[\mathbb{C} : \mathbb{R}] = 2$. $\triangle$

Proposition 4.45 ([41]).

Si $\mathbb{L}$ est une extension du corps $\mathbb{K}$ et si $\mathbb{M}$ est une extension de $\mathbb{L}$, alors les degrés se multiplient :

$$[\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}] = [\mathbb{M} : \mathbb{K}]. \quad (4.62)$$

Démonstration. Soit $\{l_i\}$ une base de $\mathbb{L}$ sur $\mathbb{K}$ et $\{m_j\}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Un élément de $\mathbb{M}$ se note

$$\sum_j b_j m_j \quad (4.63)$$

pour des $b_j \in \mathbb{L}$. Chacun de ces b_j s'écrit comme une combinaison des l_i :

$$\sum_j b_j m_j = \sum_{ij} (a_{ji} l_i) m_j, \quad (4.64)$$

donc nous voyons que les éléments $l_i m_j$ de $\mathbb{M}$ sont une base de $\mathbb{M}$ sur $\mathbb{K}$. $\square$

Lemme 4.46 ([42]).

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 $\mathbb{L}$.

Définition 4.47.

Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $A \subset \mathbb{L}$.

- (1) Nous notons $\mathbb{K}(A)$ le plus petit sous corps de $\mathbb{L}$ contenant $\mathbb{K}$ et A . C'est l'intersection de tous les sous-corps de $\mathbb{L}$ contenant A .
- (2) Nous notons $\mathbb{K}[A]$ le plus petit sous anneau de $\mathbb{L}$ contenant $\mathbb{K}$ et A . C'est l'intersection de tous les sous-anneaux de $\mathbb{L}$ contenant A .

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.

Remarque 4.48.

Les ensembles $\mathbb{K}(A)$ et $\mathbb{K}[A]$ sont aussi appelés corps et anneaux **engendré** par A . Cependant il faut bien remarquer que ce sont les parties de $\mathbb{L}$ engendrées par A . Il n'est pas question a priori de parler de corps engendré par A sans dire dans quel corps plus grand nous nous plaçons.

Exemple 4.49

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 . $\triangle$

Exemple 4.50

Nous avons déjà vu à l'occasion de la définition 3.88 que $A[X]$ est l'anneau de tous les polynômes

de degré fini en X . Cela rentre dans le cadre de la définition 4.47 parce un anneau contenant X doit contenir tous les X^n .

Notons que même si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ reste un anneau parce que A/X n'est pas dedans. Par contre, $\mathbb{K}(X)$ est un corps parce qu'il contient également les fractions rationnelles. $\triangle$

Exemple 4.51

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 étendus $\mathbb{F}_p$ 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 $x \in \mathbb{F}_p$. $\triangle$

Lemme 4.52.

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 . Cela est un corps par le corollaire 4.34. Nous identifions $\mathbb{K}$ avec $\phi(\mathbb{K})$ où

$$\phi: \mathbb{K}[X] \rightarrow \mathbb{L} \quad (4.65)$$

est la projection canonique. Nous considérons également $a = \phi(X)$.

Nous avons alors $P(a) = 0$ dans $\mathbb{L}$. En effet $P(a) = P(\phi(X))$ 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 $Q = \sum_i Q_i a^i$. $\square$

Proposition 4.53.

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

$$I_a = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}; \quad (4.66a)$$

$$I_b = \{Q \in \mathbb{K}[X] \text{ tel que } Q(b) = 0\}; \quad (4.66b)$$

même si $Q(a)$ est calculé dans $\mathbb{L}$, ce sont des idéaux de $\mathbb{K}[X]$. Le polynôme μ_a est par définition le générateur unitaire de I_a , et vu que a est une racine de P , nous avons $P \in I_a$ et il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = \mu_a Q. \quad (4.67)$$

Montrons que $\mu_a(b) \neq 0$. En effet supposons que $\mu_a(b) = 0$. Nous avons alors $\mu_a \in I_b$ et il existe $R \in \mathbb{K}[X]$ tel que $\mu_a = \mu_b R$. Étant donné que μ_b divise μ_a et que $\mu_b \neq \mu_a$, nous ne pouvons pas avoir $\mu_b(a) = 0$ parce que μ_b divise μ_a et que μ_a est minimal. Du coup nous devons avoir $R(a) = 0$, ce qui contredirait la minimalité de μ_a .

Étant donné que $\mu_a(b) \neq 0$, l'évaluation de (4.67) 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 . $\square$

Exemple 4.54

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 considérons les racines $a = i$ et $b = -i$, nous aurions $\mu_a = \mu_b = X^2 + 1$, et les polynôme μ_a^2 ne divise pas P . $\triangle$

4.3.2 Racines de polynômes**Proposition 4.55.**

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 divise⁸ tout polynôme annulateur.

Autrement dit, l'idéal engendré par le polynôme minimal est l'idéal des polynômes annulateurs.

Démonstration. Nous considérons l'idéal

$$I = \{Q \in \mathbb{K}[X] \text{ tel que } Q(a) = 0\}. \quad (4.68)$$

Le fait que cela soit un idéal est simplement dû à la définition du produit : $(PQ)(a) = P(a)Q(a)$. Par le théorème 3.110, 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 . $\square$

Corollaire 4.56 (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 4.55 : 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. $\square$

Corollaire 4.57.

Soit $\mathbb{K}$ un corps commutatif et $\mathbb{L}$ une extension de $\mathbb{K}$. Si $P \in \mathbb{K}[X]$ est unitaire, annulateur et irréductible, alors il est le polynôme minimal⁹ de α sur $\mathbb{K}$.

Démonstration. Par la proposition 4.55, le polynôme P est divisé par le polynôme minimal, mais P étant irréductible et unitaire c'est que P est le polynôme minimal. $\square$

Théorème 4.58 (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 $\alpha_1, \dots, \alpha_{n+1}$, alors $P = 0$.

Voir la remarque 3.89 pour savoir ce qu'est un polynôme nul.

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

$$\begin{cases} a\alpha + b = 0 \\ a\beta + b = 0. \end{cases} \quad \begin{matrix} (4.69a) \\ (4.69b) \end{matrix}$$

La différence entre les deux donne $a(\alpha - \beta) = 0$. Vu que $\alpha \neq \beta$, la règle du produit nul (lemme 4.2) nous donne $a = 0$. Maintenant que $a = 0$, l'annulation de b est alors immédiate.

8. Définition 3.102.

9. Définition 4.38.

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. Vu que $P(\alpha_1) = 0$, le corollaire 4.56 nous donne un polynôme Q de degré n tel que

$$P(X) = (X - \alpha_1)Q. \quad (4.70)$$

Étant donné que pour tout $i \neq 1$ nous avons $\alpha_i \neq \alpha_1$,

$$0 = P(\alpha_i) = \underbrace{(\alpha_i - \alpha_1)}_{\neq 0} Q(\alpha_i), \quad (4.71)$$

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 (4.70) sont alors également nuls. $\square$

Remarque 4.59.

Dans le cas des polynôme à plusieurs indéterminées, le résultat n'est plus vrai¹⁰, mais nous avons la proposition 4.105.

Remarque 4.60.

L'intérêt du théorème 4.58 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 12.24.

4.3.3 Corps de rupture

Définition 4.61.

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 $\mathbb{L} = \mathbb{K}(a)$.

Exemple 4.62

Soit $\mathbb{K} = \mathbb{Q}$ et $P(X) = X^2 - 2$. On pose $a = \sqrt{2}$ et $\mathbb{L} = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. De cette façon P est scindé :

$$P = (X - \sqrt{2})(X + \sqrt{2}). \quad (4.72)$$

Le corps $\mathbb{Q}(\sqrt{2})$ est donc un corps de rupture pour P . $\triangle$

Exemple 4.63

Dans l'exemple 4.62, le polynôme P était scindé dans son corps de rupture. Il n'en est pas toujours ainsi. Prenons

$$P(X) = X^3 - 2 \quad (4.73)$$

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. $\triangle$

Exemple 4.64

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 degrés 1 en $\sqrt{s}$. Le cardinal en est p^2 . $\triangle$

Proposition 4.65 (Propriétés d'extensions algébriques[8]).

Soit $\mathbb{K}$ un corps commutatif¹¹ et a un élément algébrique sur $\mathbb{K}$, de polynôme minimal μ_a de degré n . Alors

¹⁰. Exemple 4.106.

¹¹. Juste en passant nous rappelons que tous les corps considérés ici sont commutatifs

(1) En considérant l'application d'évaluation

$$\begin{aligned}\varphi_a: \mathbb{K}[X] &\rightarrow \mathbb{L} \\ Q &\mapsto Q(a),\end{aligned}\tag{4.74}$$

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 :

$$[\mathbb{K}[a] : \mathbb{K}] = n.\tag{4.75}$$

(4) L'anneau $\mathbb{K}[a]$ est l'ensemble des polynômes en a de degré $n-1$ à coefficient dans $\mathbb{K}$.

(5) $\mathbb{K}(a) = \mathbb{K}[a]$.

(6) $\mathbb{K}[a] \simeq \mathbb{K}[X]/(\mu_a)$ (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 $n-1$ en a . Un tel polynôme ne peut pas être nul parce que nous avons mis comme hypothèse que le polynôme minimal de a est n .

Rappelons qu'en vertu de la définition 4.38, le polynôme minimal μ_a est unitaire ; donc le polynôme $\mu_a(X) - X^n$ est un polynôme de degré $n-1$. Par conséquent en posant $S(X) = X^n - \mu_a(X)$, le polynôme S est de degré $n-1$ et vérifie $a^n = S(a)$.

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 :

$$Q(X) = Q_1(X) + X^n Q_2(X)\tag{4.76}$$

où Q_1 est de degré $n-1$ et Q_2 de degré $p-n$. Nous évaluons cette égalité en a :

$$Q(a) = Q_1(a) + S(a)Q_2(a).\tag{4.77}$$

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 4.40). Donc le théorème de Bézout 3.105 affirme l'existence d'éléments $U, V \in \mathbb{K}[X]$ tels que

$$U\mu_a + VQ = 1\tag{4.78}$$

dans $\mathbb{K}[X]$. Nous évaluons cette égalité en a en tenant compte de $\mu_a(a) = 0$ dans $\mathbb{K}[a]$:

$$U(a)\mu_a(a) + V(a)Q(a) = 1\tag{4.79}$$

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

$$\begin{aligned}\psi: \mathbb{K}[X]/(\mu_a) &\rightarrow \mathbb{K}[a] \\ \bar{R} &\mapsto R(a)\end{aligned}\tag{4.80}$$

et nous montrons qu'elle convient. Pour cela, nous nous souvenons que la proposition 4.55 nous enseigne que (μ_a) , l'idéal engendré par μ_a , est égal à l'idéal des polynômes annulateurs de a dans $\mathbb{K}[X]$. Le polynôme μ_a divise tous les éléments de cet idéal ; voir aussi la définition 3.61 de l'idéal (μ_a) . Cela étant mis au point, nous passons à la preuve.

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 $Q(a) = 0$.

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 $x = \psi(\bar{Q})$.

Injective Si $\psi(\bar{R}) = 0$ alors $R(a) = 0$, mais comme mentionné plus haut, μ_a engendre l'idéal est polynômes annulateurs de a . Donc $R \in (\mu_a)$ et nous avons $\bar{R} = 0$ dans $\mathbb{K}[X]/(\mu_a)$. $\square$

Exemple 4.66

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 4.65. Du point de vue de Bézout, $\mu_{\sqrt{2}}(X) = X^2 - 2$, et nous cherchons des polynômes U et V tels que

$$U(X^2 - 2) + VX = 1.\tag{4.81}$$

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 $\sqrt{2}$:

$$V(\sqrt{2}) = \frac{1}{2}\sqrt{2}.\tag{4.82}$$

$\triangle$

4.3.4 Corps de décomposition

Définition 4.67.

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 $R = \bigcup_{i \in I} \{x \in \mathbb{L} \text{ tel que } P_i(x) = 0\}$.

C'est à dire que $\mathbb{L}$ étend $\mathbb{K}$ par toutes les racines de tous les polynômes de F .

L'unicité est due à la proposition suivante.

Proposition 4.68.

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 $f: \mathbb{L} \rightarrow \mathbb{F}$ tel que $f|_{\mathbb{K}} = \text{Id}$.

Nous pouvons donc parler du corps de décomposition d'un polynôme.

Soit $\mathbb{K}$, un corps et $\mathbb{L}$, une extension de $\mathbb{K}$. Un élément $a \in \mathbb{L}$ est **algébrique** sur $\mathbb{K}$ si il existe un polynôme $P \in \mathbb{K}[X]$ tel que $P(a) = 0$.

Une **clôture algébrique** du corps $\mathbb{K}$ est une extension algébriquement close de $\mathbb{K}$ dont tous les éléments sont algébriques sur $\mathbb{K}$.

Remarque 4.69.

L'ensemble $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$ parce qu'il existe des éléments de $\mathbb{C}$ qui ne sont pas des racines de polynômes à coefficients rationnels.

L'existence d'une clôture algébrique pour tout corps est le théorème de Steinitz.

Exemple 4.70

Soit p un nombre premier. Montrons que le polynôme

$$Q(X) = X^p - X + 1 \quad (4.83)$$

est irréductible dans $\mathbb{F}_p$.

Nous supposons qu'il n'est pas irréductible, c'est à dire que

$$Q(X) = R(X)S(X) \quad (4.84)$$

avec R et S , des polynômes de degrés ≥ 1 dans $\mathbb{F}_p[X]$

Soit $\bar{\mathbb{F}}_p$ une clôture algébrique 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

$$Q(\alpha + a) = (\alpha + a)^p - (\alpha + a) + 1 \quad (4.85a)$$

$$= \alpha^p + a^p - \alpha - a + 1 \quad (4.85b)$$

$$= \alpha^p - \alpha + 1 \quad (4.85c)$$

$$= Q(\alpha) \quad (4.85d)$$

$$= 0 \quad (4.85e)$$

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

$$R(X) = \prod_{i=1}^k (X - (\alpha + a_i)) \quad (4.86)$$

où les a_i sont les éléments de $\mathbb{F}_p$. En développant un peu,

$$R(X) = X^k - \sum_{i=1}^k (\alpha + a_i^{k-1}) + \text{termes de degré plus bas en } X. \quad (4.87)$$

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 :

$$Q(\alpha) = \alpha^p - \alpha + 1 = 1 \neq 0. \quad (4.88)$$

Le polynôme $X^p - X + 1$ est donc irréductible sur $\mathbb{F}_p$. $\triangle$

4.3.5 Clôture algébrique

Théorème 4.71.

Tout corps $\mathbb{K}$ possède une clôture algébrique 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 4.72.

Les polynômes $P, Q \in \mathbb{K}[X]$ ne sont pas premiers entre eux si et seulement si 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. $\square$

4.3.6 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 (4.85).

Définition 4.73.

Soit $\mathbb{K}$ un corps. Un polynôme irréductible $P \in \mathbb{K}[X]$ est **séparable** sur $\mathbb{K}$ si dans un corps de décomposition, ses racines sont distinctes.

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.

La proposition suivante donne un sens à la définition de polynôme irréductible séparable.

Proposition 4.74.

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 4.68 qui donne l'unicité du corps de décomposition à $\mathbb{K}$ -isomorphisme près. Soit donc $\psi: \mathbb{L} \rightarrow \mathbb{L}'$ 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

$$P = a(X - \alpha_1) \dots (X - \alpha_n) \quad (4.89)$$

avec $a \in \mathbb{K}$ et $\alpha_i \in \mathbb{L}$. Nous avons donc

$$P = \psi(P) = a(X - \psi(\alpha_1)) \dots (X - \psi(\alpha_n)). \quad (4.90)$$

Donc les racines de P dans $\mathbb{L}'$ sont les éléments $\psi(\alpha_i)$ qui sont distincts. $\square$

Exemple 4.75

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

$$P = X^p - T^p \quad (4.91)$$

dans $\mathbb{K}[X]$. Par le morphisme de Frobenius nous avons

$$P = (X - T)^p \quad (4.92)$$

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. $\triangle$

Exemple 4.76

Le polynôme $(X - 1)^3$ est séparable sur $\mathbb{Q}$ parce que ses facteurs irréductibles dans $\mathbb{Q}[X]$ sont $X - 1$ qui ont des racines simples. $\triangle$

Exemple 4.77

Le polynôme $(X^2 + 1)^2$ est séparable dans $\mathbb{Q}[X]$. En effet, il a pour facteurs irréductibles le polynôme $X^2 + 1$ dont les racines sont $\pm i$ dans l'extension $\mathbb{Q}(i)$. $\triangle$

Proposition 4.78 ([43]).

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Les propriétés suivantes sont équivalentes.

- (1) P a une racine multiple dans une extension de $\mathbb{K}$. C'est à dire qu'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 $\text{pgcd}(P, P')$ est ≥ 1 .

Démonstration. (1) $\Rightarrow$ (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 une 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 $\psi: \mathbb{E} \rightarrow \mathbb{E}'$. 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

$$P(\psi(a)) = \psi(P(a)). \quad (4.93)$$

(1) $\Rightarrow$ (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,

$$P' = 2(X - a)Q + (X - a)^2 Q', \quad (4.94)$$

et donc a est également une racine de P' .

(3) $\Rightarrow$ (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

$$AP + BP' = D. \quad (4.95)$$

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 $\deg(D) \geq 1$.

(4) $\Rightarrow$ (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

$$P = (X - a)Q, \quad (4.96)$$

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.

Proposition 4.79.

Soit $P \in \mathbb{K}[X]$ irréductible. Le polynôme P est séparable si et seulement si $P' \neq 0$.

Démonstration. Soit $D = \text{pgcd}(P, P')$ et nous voudrions prouver que $\deg(D) \geq 1$ si et seulement si $P' = 0$. Si $P' = 0$, alors $\text{pgcd}(P, P') = P$ est donc $\deg(D) \geq 1$.

Dans l'autre sens, si P est irréductible, il est associé à D parce qu'il n'a pas d'autres diviseurs que lui-même (à part 1). Nous avons donc $P = \lambda D$ avec $\lambda \in \mathbb{K}$ et donc $\deg(P) \geq 1$. Cela prouve immédiatement que $P' \neq 0$. □

Corollaire 4.80.

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 4.78. $\square$

Définition 4.81.

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 $\mathbb{K}$.
- (2) L'extension $\mathbb{L}$ est **séparable** si tous ses éléments sont séparables.

Proposition 4.82.

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. Soit P un polynôme irréductible dans $\mathbb{K}[X]$. Soient a et b des racines de P dans un corps de décomposition $\mathbb{L}$. Par hypothèse, $\mathbb{L}$ est séparable, donc les polynômes minimaux μ_a et μ_b sont séparables dans $\mathbb{K}[X]$. Étant donné que P est irréductible, il est le seul à se diviser lui-même et donc $\mu_a = \mu_b = P$. Donc P est séparable sur $\mathbb{K}$.

Dans l'autre sens, soit $\mathbb{L}$ une extension algébrique de $\mathbb{K}$, soit $a \in \mathbb{L}$ et le polynôme minimal $\mu_a \in \mathbb{K}[X]$. Par définition il est irréductible et donc séparable (par hypothèse). Donc a est séparable et $\mathbb{L}$ est une extension séparable.

La dernière phrase est une conséquence du corollaire 4.80. $\square$

Exemple 4.83

Une des conséquences les plus intéressantes de la proposition 4.82 est que toutes les extensions algébriques de $\mathbb{Q}$ sont séparables. $\triangle$

Théorème 4.84 ([20]).

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

$$x^\omega = 1 \tag{4.97}$$

pour tout $x \in G$. Mais ce polynôme possède au plus ω racines dans $\mathbb{K}$. Du coup $|G| \leq \omega$. 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 2.42. $\square$

Théorème 4.85 (Théorème de l'élément primitif[20]).

Toute extension de corps séparable finie admet un élément primitif.

Plus explicitement, soient $\alpha_1, \dots, \alpha_n$ des éléments algébriques séparables sur $\mathbb{K}$; alors $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ admet un élément primitif.

Démonstration. Si le corps $\mathbb{K}$ est fini, alors $\mathbb{L}$ est également fini. Donc $\mathbb{L}^*$ est cyclique par le théorème 4.84. 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

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n), \tag{4.98}$$

et donc si $\mathbb{K}(\alpha_1, \dots, \alpha_{n-1}) = \mathbb{K}(\theta)$, nous avons

$$\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\theta, \alpha_n) \quad (4.99)$$

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

$$\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r \quad (4.100)$$

de P dans $\mathbb{E}$ et les racines

$$\beta_1 = \beta, \beta_2, \dots, \beta_s \quad (4.101)$$

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 $s \geq 2$.

Pour chaque $(i, j) \in \llbracket 1, r \rrbracket \times \llbracket 2, s \rrbracket$, l'équation $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ pour $x \in \mathbb{K}$ a au plus¹² une solution donnée le cas échéant par

$$x = (\alpha_i - \alpha_1)(\beta_1 - \beta_k)^{-1} \quad (4.102)$$

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 (4.102) :

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1. \quad (4.103)$$

Nous posons $\theta = \alpha + c\beta$ et nous prétendons que $\mathbb{L} = \mathbb{K}(\theta)$. Montrons que $\beta \in \mathbb{K}(\theta)$. Soit dans $\mathbb{K}(\theta)[T]$ les polynômes $Q(T)$ et $S(T) = P(\theta - cT)$. Nous nommons R le PGCD de ces deux polynômes.

D'une part, une racine de R doit être une racine de Q , et donc être un des β_i . D'autre part, le choix de c fait que β est une racine de R parce que

$$S(\beta) = P(\alpha + c\beta - c\beta) = P(\alpha) = 0. \quad (4.104)$$

Enfin si $k \geq 2$, alors

$$S(\beta_k) = P(\alpha_1 + c(\beta - \beta_k)) \neq 0 \quad (4.105)$$

parce que $\alpha_1 + c(\beta - \beta_k)$ n'est aucun des α_i . Nous concluons que β est l'unique racine de R et donc que

$$R = X - \beta \in \mathbb{K}(\theta)[T], \quad (4.106)$$

et donc $\beta \in \mathbb{K}(\theta)$.

De plus $\alpha = \theta - c\beta$ est alors immédiatement dans $\mathbb{K}(\theta)$. À partir du moment où α et β sont dans $\mathbb{K}(\theta)$, nous avons obtenu $\mathbb{L} = \mathbb{K}(\alpha, \beta) = \mathbb{K}(\theta)$. □

Exemple 4.86

Le théorème de l'élément primitif 4.85 ne tient pas pour les corps non commutatifs. Par exemple si nous considérons pour $\mathbb{K}$ le corps des quaternions et comme G le groupe à 8 éléments $\{\pm 1, \pm i, \pm j, \pm k\}$. Ce dernier groupe n'est pas cyclique alors qu'il est un groupe fini dans $\mathbb{K}^*$. △

Exemple 4.87

Il est aussi possible pour un groupe fini d'avoir $\omega(G) = |G|$ sans pour autant que G soit cyclique.

¹². La solution (4.102) peut être dans $\mathbb{L}$ et non dans $\mathbb{K}$. L'équation peut donc très bien ne pas avoir de solutions $x \in \mathbb{K}$.

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. $\triangle$

Remarque 4.88.

Il est prouvé dans [20] que $\mathbb{C}$ est algébriquement clos à partir du théorème de l'élément primitif 4.85, mais c'est encore un petit peu de travail.

4.3.7 Idéal maximum

Définition 4.89.

Un nombre (dans $\mathbb{C}$) est **transcendant** si il n'est racine d'aucun polynôme non nul à coefficients entiers. Plus généralement si $\mathbb{L}$ est une extension du corps $\mathbb{K}$ alors si $t \in \mathbb{L}$ est une racine d'un polynôme dans $\mathbb{K}[X]$ nous disons que t est **algébrique** sur $\mathbb{K}$; sinon nous disons que t est **transcendant** sur $\mathbb{K}$.

Définition 4.90.

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 4.91 (wikipédia).

un idéal I d'un anneau commutatif $\mathbb{A}$ est maximal si et seulement si le quotient $\mathbb{A}/I$ est un corps.

Théorème 4.92 ([44]).

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 4.93 ([44]).

Si $\mathbb{K}$ est un corps algébriquement clos, les idéaux maximaux de $\mathbb{K}[X_1, \dots, X_n]$ sont de la forme

$$(X_1 - a_1, \dots, X_n - a_n) \quad (4.107)$$

où les a_i sont des éléments de $\mathbb{K}$.

Démonstration. Nous commençons par montrer que

$$J = (X_1 - a_1, \dots, X_n - a_n) \quad (4.108)$$

est un idéal maximum. Pour cela nous considérons le morphisme surjectif d'anneaux

$$\begin{aligned} \phi: \mathbb{K}[X_1, \dots, X_n] &\rightarrow \mathbb{K} \\ P &\mapsto P(a_1, \dots, a_n). \end{aligned} \quad (4.109)$$

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 :

$$P = (X - a_1)Q_1 + \dots + (X_n - a_n)Q_n + R \quad (4.110)$$

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 (4.110) à $(a_1, \dots, a_n)$ et en nous rappelant que $P \in \ker(\phi)$ nous obtenons

$$0 = P(a_1, \dots, a_n) = R, \quad (4.111)$$

donc $R = 0$ et $P = (X_1 - a_1)Q_1 + \dots + (X_n - a_n)Q_n$, 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 $\mathbb{K}[X_1, \dots, X_n] \rightarrow \mathbb{K}$, nous avons

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{J} = \mathbb{K}. \quad (4.112)$$

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

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{I} \quad (4.113)$$

est une $\mathbb{K}$ -algèbre de type fini (définition 4.90). De plus c'est un corps par le théorème 4.91. C'est donc une extension algébrique finie de $\mathbb{K}$ par le théorème 4.92. Mais $\mathbb{K}$ étant algébriquement clos, il est sa propre et unique extension algébrique ; nous en déduisons que

$$\frac{\mathbb{K}[X_1, \dots, X_n]}{I} = \mathbb{K}. \quad (4.114)$$

Donc pour tout $1 \leq i \leq n$, 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 $I = J$. $\square$

Corollaire 4.94.

Soit $\mathbb{K}$ un corps algébriquement clos et I , un idéal de $\mathbb{K}[X_1, \dots, X_n]$. Si nous notons

$$V(I) = \{x \in \mathbb{K}^n \text{ tel que } P(x_1, \dots, x_n) = 0\} \quad (4.115)$$

l'ensemble des racines communes à tous les éléments de I , on a $V(I) = \emptyset$ 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 $V(I) = \emptyset$. 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 contenu dans I . Nous savons déjà par le théorème 4.93 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

$$P(a_1, \dots, a_n) = 0, \quad (4.116)$$

c'est à dire que $(a_1, \dots, a_n) \in V(I)$ et donc que $V(I) \neq \emptyset$. $\square$

4.4 Espaces de polynômes

Dans cette section nous abandonnons pour quelques minutes l'espace $\mathbb{R}^m$ et considérons plus attentivement l'espace des fonctions polynômiales $\mathcal{P}_{\mathbb{R}}$ et de ses sous-espaces $\mathcal{P}_{\mathbb{R}}^k$, pour k dans $\mathbb{N}_0$.

Attention : les polynômes en soi sont définis par la définition 3.88.

Pour chaque $k > 0$ donné nous définissons

$$\mathcal{P}_{\mathbb{R}}^k = \{p : \mathbb{R} \rightarrow \mathbb{R} \mid p : x \mapsto a_0 + a_1x + a_2x^2 + \dots + a_kx^k, a_i \in \mathbb{R}, \forall i = 0, \dots, k\}. \quad (4.117)$$

Il est facile de se convaincre que la somme de deux polynômes de degré inférieur ou égal à k est encore un polynôme de degré inférieur ou égal à k . En outre il est clair que la multiplication par un scalaire ne peut pas augmenter le degré d'un polynôme. L'ensemble $\mathcal{P}_{\mathbb{R}}^k$ est donc un espace vectoriel muni des opérations héritées de $\mathcal{P}_{\mathbb{R}}$.

La base canonique de l'espace $\mathcal{P}_{\mathbb{R}}^k$ est donné par les monômes $\mathcal{B} = \{x \mapsto x^j \mid j = 0, \dots, k\}$. 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 $\mathcal{P}_{\mathbb{R}}^k$ vers des autres espaces vectoriels

L'isomorphisme canonique $\phi : \mathcal{P}_{\mathbb{R}}^k \rightarrow \mathbb{R}^{k+1}$ Nous définissons ϕ par les relations suivantes

$$\phi(x^j) = e_{j+1}, \quad \forall j \in \{0, \dots, k\}.$$

Cela veut dire que pour tout p dans $\mathcal{P}_{\mathbb{R}}^k$, avec $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_kx^k$, 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 4.95

Soit $k = 5$ on a

$$\phi(-8 - 7x - 4x^2 + 4x^3 + 2x^5) = \begin{pmatrix} -8 \\ -7 \\ -4 \\ 4 \\ 0 \\ 2 \end{pmatrix}. \quad (4.118)$$

△

Cette application est clairement bijective et respecte les opérations d'espace vectoriel, donc elle est un isomorphisme d'espaces vectoriels. L'existence d'un isomorphisme entre $\mathcal{P}_{\mathbb{R}}^k$ 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 $d : \mathcal{P}_{\mathbb{R}}^k \rightarrow \mathcal{P}_{\mathbb{R}}^{k-1}$ L'application de dérivation d fait exactement ce qu'on s'attend d'elle

$$d(x^0) = d(1) = 0, \quad d(x^j) = jx^{j-1}, \quad \forall j \in \{1, \dots, k\}.$$

Cette application n'est pas injective, parce que l'image de p ne dépend pas de la valeur de a_0 , donc si deux polynômes sont les mêmes à une constante près ils auront la même image par d .

Exemple 4.96

Soit $k = 3$ on a

$$d(-8 - 12x + 4x^3) = -12(1) + 4(3x^2) = -12 + 12x^2. \quad (4.119)$$

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 $I : \mathcal{P}_{\mathbb{R}}^k \rightarrow \mathcal{P}_{\mathbb{R}}^{k+1}$ Nous pouvons définir une application que est «à une constante près» l'application inverse de la dérivation

$$I(p) = \int_0^x p(t) dt. \quad (4.120)$$

Il faut comprendre que dans l'intégral la variable t est simplement la variable d'intégration. La «vraie» variable de la fonction image de p sera x !

Comme d'habitude nous écrivons explicitement l'action de I sur les éléments de la base canonique

$$I(x^j) = \int_0^x t^j dt = \frac{x^{j+1}}{j+1}. \quad (4.121)$$

Exemple 4.97

Soit $k = 4$ on a

$$I(6 + 2x + x^2 + x^4) = 6x + x^2 + \frac{x^3}{3} + \frac{x^5}{5}. \quad (4.122)$$

△

Remarquez que, étant donné que dans la définition de I nous avons décidé d'intégrer entre zéro et x , tous les polynômes dans $\mathcal{P}_{\mathbb{R}}^{k+1}$ qui sont l'image par I d'un polynôme de $\mathcal{P}_{\mathbb{R}}^k$ 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 $\mathcal{P}_{\mathbb{R}}^{k+1}$, en particulier $\mathcal{B}_1 = \{x \mapsto x^j \mid j = 1, \dots, k\} \subset \mathcal{B}$ 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 6.12.2, nous verrons que toutes les normes ne sont pas équivalentes sur l'espace des polynômes.

4.4.1 Polynômes symétriques, alternés ou semi-symétriques

[35].

Soit $\mathbb{K}$ un corps de caractéristique différente ¹³ de 2. Le groupe S_n agit sur l'anneau $\mathbb{K}[T_1, \dots, T_n]$ par

$$(\sigma \cdot f)(T_1, \dots, T_n) = f(T_{\sigma(1)}, \dots, T_{\sigma(n)}). \quad (4.123)$$

On peut vérifier que c'est une action.

Définition 4.98.

Un polynôme Q en n indéterminées est

- (1) **symétrique** si $Q = \sigma \cdot Q$ pour tout $\sigma \in S_n$;
- (2) **alterné** si $\sigma \cdot Q = \epsilon(\sigma)Q$ pour tout $\sigma \in S_n$;
- (3) **semi-symétrique** si $\sigma \cdot Q = Q$ pour tout $\sigma \in A_n$

Le polynôme $T_1 + T_2$ est symétrique ; le polynôme $T_1 + T_2^2$ ne l'est pas.

4.4.2 Polynôme symétrique élémentaire

Définition 4.99.

Le k ème **polynôme symétrique élémentaire** à n inconnues est le polynôme est

$$\sigma_k(T_1, \dots, T_n) = \sum_{s \in F_k} \prod_{i=1}^k T_{s(i)} \quad (4.124)$$

où F_k est l'ensemble des fonctions strictement croissantes $\{1, 2, \dots, k\} \rightarrow \{1, 2, \dots, n\}$.

Une autre façon de décrire ces polynômes élémentaires est

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}. \quad (4.125)$$

Par exemple

$$\sigma_1(T_1, \dots, T_n) = T_1 + T_2 + \dots + T_n \quad (4.126a)$$

$$\sigma_2(T_1, \dots, T_n) = T_1 T_2 + \dots + T_1 T_n + T_2 T_3 + \dots + T_2 T_n + \dots + T_{n-1} T_n \quad (4.126b)$$

$$\sigma_n(T_1, \dots, T_n) = T_1 \dots T_n. \quad (4.126c)$$

En particulier, $\sigma_2(x, y, z) = xy + yz + xz$.

13. Le truc de la caractéristique deux est que $a = -a$ n'implique pas $a = 0$.

Théorème 4.100 ([45]).

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

$$Q(T_1, \dots, T_n) = P(\sigma_1(T_1, \dots, T_n), \dots, \sigma_n(T_1, \dots, T_n)). \quad (4.127)$$

Exemple 4.101

Nous voulons décomposer $P(x, y, z) = x^3 + y^3 + z^3$ en polynômes symétriques élémentaires, c'est à dire en

$$\begin{cases} \sigma_1 = x + y + z & (4.128a) \\ \sigma_2 = xy + xz + yz & (4.128b) \\ \sigma_3 = xyz. & (4.128c) \end{cases}$$

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

$$P = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \quad (4.129)$$

△

Lemme 4.102 ([35]).

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 4.82 et de l'exemple 4.83, $\mathbb{K}$ est une extension séparable de $\mathbb{Q}$, et donc vérifie le théorème de l'élément primitif (4.85). 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

$$\{1, \theta, \dots, \theta^{\delta-1}\}. \quad (4.130)$$

Mais par ailleurs la proposition 4.65(2) nous indique qu'une base de $\mathbb{Q}(\theta)$ sur $\mathbb{Q}$ est donnée par

$$\{1, \theta, \dots, \theta^{n-1}\} \quad (4.131)$$

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

$$\begin{aligned} \sigma_k: \mathbb{Q}(\theta) &\rightarrow \mathbb{Q}(\theta_k) \\ \sum_i q_i \theta^i &\mapsto \sum_i q_i \theta_k^i \end{aligned} \quad (4.132)$$

Nous avons $\sigma_1: \mathbb{K} \rightarrow \mathbb{K}$ qui est l'identité.

Notons N le degré du polynôme $P \in \mathbb{K}[T_1, \dots, T_m]$ dont il est question dans l'énoncé. Nous le décomposons alors en

$$P = \sum_{l=0}^N \sum_{i=1}^m c_{il} T_i^l \quad (4.133)$$

avec $c_{il} \in \mathbb{K}$. Nous voyons $c_{i,\cdot}$ comme un élément de $\mathbb{K}^m$ et donc nous écrivons¹⁴

$$P = \sum_{l=0}^N \sum_{i=1}^m c_l(\theta)_i T_i^l \quad (4.134)$$

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

$$P^{\sigma_k} = \sum_{l,i} c_l(\theta_k)_i T_i^l \in \mathbb{Q}(\theta_k)[T_1, \dots, T_m], \quad (4.135)$$

et $\bar{P} = PP^{\sigma_2} \dots P^{\sigma_k}$. Le coefficient de T_i^l dans $\bar{P}$ est

$$\bar{c}_l(\theta_1, \dots, \theta_\delta)_i = \sum_{l_1 + \dots + l_\delta = l} c_{l_1}(\theta_1)_i \dots c_{l_\delta}(\theta_\delta)_i. \quad (4.136)$$

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 4.100 à propos des polynômes symétriques élémentaires qui nous dit que les coefficients de $\bar{P}$ sont en réalité des polynômes en ceux de P_θ qui sont dans $\mathbb{Q}$. Donc $\bar{P} \in \mathbb{Q}[T_1, \dots, T_m]$. Par ailleurs nous avons que

$$\deg(\bar{P}) = \delta \deg(P) \quad (4.137)$$

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. $\square$

14. Il me semble qu'il manque la somme sur i dans [35].

4.4.3 Relations coefficients racines

Théorème 4.103 (Relations coefficients-racines).

Soit le polynôme $P = a_n X^n + \dots + a_1 X + a_0$ et r_i ses n racines. Alors nous avons pour chaque $1 \leq k \leq n$ la relation

$$\sigma_k(r_1, \dots, r_n) = (-1)^k \frac{a_{n-k}}{a_n} \quad (4.138)$$

où σ_k est le k^e polynôme symétrique défini en 4.99.

Exemple 4.104

Soit le polynôme

$$P(x) = x^3 + 2x^2 + 3x + 4 \quad (4.139)$$

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 (théorème 4.103) nous donnent $\sigma_1(a, b, c) = -2$ et $\sigma_2(a, b, c) = 3$, donc

$$a^2 + b^2 + c^2 = (-2)^2 - 2 \cdot 3 = -2. \quad (4.140)$$

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) :

```

1 sage: P(x)=x**3+2*x**2+3*x+4
2 sage: S=solve( P(x)==0,x )
3 sage: sols=[ s.rhs() for s in S ]
4 sage: Q=[ s**2 for s in sols ]
5 sage: s=sum(Q)
6 sage: s.simplify_full()
7 -2

```

VAYVmNRpolynomeSym.py

Notez qu'il faut un peu chipoter pour isoler les solutions depuis la réponse de la fonction `solve`. $\triangle$

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 4.105 (Annulation de fonctions polynômiales[46]).

Soit $\mathbb{K}$ un corps et P un polynôme à n indéterminées. Nous supposons que P s'annule sur un ensemble de la forme $A_1 \times \dots \times A_n$ 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 nuls¹⁵.

Démonstration. Nous prouvons le résultat par récurrence sur le nombre n d'indéterminées. Si $n = 1$, cela est le théorème 4.58. Nous classons les monômes du polynôme P par ordre de puissance de X_n et nous le factorisons :

$$P = \sum_{i=1}^m P_i X_n^i \quad (4.141)$$

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

$$Q(T) = P(a_1, \dots, a_{n-1}, T) = \sum_{i=1}^m P_i(a_1, \dots, a_{n-1}) T^i. \quad (4.142)$$

¹⁵. 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.

Le polynôme Q s'annule sur A_n avec $\deg(Q) = \deg_{X_n}(P) < \text{Card}(A_n)$ et le théorème 4.58 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

$$\deg_{X_j}(P_i) \leq \deg_{X_j} P < \text{Card}(A_j), \quad (4.143)$$

donc l'hypothèse de récurrence donne $P_i = 0$. Par suite, $P = 0$ également. $\square$

Exemple 4.106

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. $\triangle$

4.5 Polynômes cyclotomiques

4.5.1 Définitions et propriétés

Définition 4.107.

Le *polynôme cyclotomique* d'indice n est le polynôme

$$\phi_n(X) = \prod_{z \in \Delta_n} (X - z) \quad (4.144)$$

où Δ_n est l'ensemble des racines primitives de l'unité de la définition 3.13 :

$$\Delta_n = \{e^{2ik\pi/n} \text{ tel que } 0 \leq k \leq n-1 \text{ tel que } \text{pgcd}(k, n) = 1\}, \quad (4.145)$$

Le polynôme ϕ_n est un polynôme unitaire de degré $\varphi(n)$ où φ est l'indicatrice d'Euler¹⁶ $\varphi(n)$. Nous avons par exemple

$$\Delta_1 = \{1\} \quad (4.146a)$$

$$\Delta_2 = \{-1\} \quad (4.146b)$$

$$\Delta_3 = \{e^{2\pi i/3}, e^{4\pi i/3}\} \quad (4.146c)$$

et les premiers polynômes cyclotomiques sont donnés par

$$\phi_1(X) = X - 1 \quad (4.147a)$$

$$\phi_2(X) = X + 1 \quad (4.147b)$$

$$\phi_3(X) = X^2 + X + 1. \quad (4.147c)$$

Pour le dernier nous avons utilisé le fait que $e^{6\pi i/3} = 1$ et $e^{4\pi i/3 + e^{2\pi i/3}} = -1$.

Lemme 4.108.

Le polynôme $X^n - 1$ se factorise des diverses manières suivantes :

$$X^n - 1 = \prod_{z \in U_n} (X - z) = \prod_{d|n} \prod_{z \in \Delta_d} (X - z) = \prod_{d|n} \phi_d(X) \quad (4.148)$$

Démonstration. En ce qui concerne la première égalité, tous les éléments de U_n sont des racines simples de $X^n - 1$. Donc le théorème 3.115 dit qu'il existe un nombre k (polynôme de degré zéro) tel que $X^n - 1 = k \prod_{z \in U_n} (X - z)$. Vu le coefficient du terme de plus haut degré, ce k ne peut être que 1.

Pour la suite nous utilisons l'union disjointe $U_n = \bigcup_{d|n} \Delta_d$ du lemme 3.15 et la définition (4.144) des polynômes cyclotomiques. $\square$

16. Définie par l'équation 3.22.

Remarque 4.109.

Notons juste pour le plaisir que dans le produit $\prod_{d|n} \prod_{z \in \Delta_d}$, il y a bien n termes parce que $\text{Card}(\Delta_d) = \varphi(d)$ et $\sum_{d|n} \varphi(d) = n$ (définition 3.13 et lemme 3.15).

Proposition 4.110.

Les polynômes cyclotomiques sont à coefficients entiers : $\phi_n \in \mathbb{Z}[X]$.

Démonstration. Nous devons démontrer que les coefficients de ϕ_n sont dans $\mathbb{Z}$ alors qu'ils sont a priori dans $\mathbb{C}$. Nous démontrons cela par récurrence. D'abord $\phi_1(X) = X - 1$, d'accord. Ensuite

$$X^{n+1} - 1 = \prod_{d|n+1} \phi_d(X) = \phi_{n+1}(X) \cdot \underbrace{\prod_{\substack{d|n+1 \\ d \leq n}} \phi_d(X)}_{\in \mathbb{Z}[X] \text{ par récurrence}} \quad (4.149)$$

Le lemme 3.107 conclut que $\phi_{n+1} \in \mathbb{Z}[X]$. Nous avons vu $\mathbb{Z}$ comme sous anneau du corps $\mathbb{C}$. $\square$

Proposition 4.111.

Soient $1 \leq m \leq n$ deux entiers et

$$T(X) = \frac{X^n - 1}{X^m - 1} \in \mathbb{Z}[X]. \quad (4.150)$$

Alors :

- (1) si $m \mid n$ alors $T \in \mathbb{Z}[X]$,
- (2) si $m \mid n$ et si $m < n$ alors ϕ_n divise T dans $\mathbb{Z}[X]$.

Démonstration. Nous prouvons point par point.

- (1) Si m divise n alors les diviseurs de n sont l'union des diviseurs de m et des diviseurs de n qui ne divisent pas m . Soit

$$Q = \{\text{diviseurs de } n \text{ ne divisant pas } m\}. \quad (4.151)$$

Nous avons alors

$$X^n - 1 = \prod_{d|n} \phi_d(X) = \prod_{d|m} \phi_d(X) \cdot \prod_{q \in Q} \phi_q(X) = (X^m - 1) \cdot \prod_{q \in Q} \phi_q(X). \quad (4.152)$$

Nous avons donc

$$T(X) = \frac{X^n - 1}{X^m - 1} = \prod_{q \in Q} \phi_q(X) \in \mathbb{Z}[X]. \quad (4.153)$$

- (2) Nous venons de montrer que

$$T = \prod_{q \in Q} \phi_q \in \mathbb{Z}[X]. \quad (4.154)$$

Étant donné que $m < n$ nous avons $n \in Q$ et donc

$$T = \phi_n \cdot \prod_{q \in Q \setminus \{n\}} \phi_q. \quad (4.155)$$

Par conséquent ϕ_n divise T dans $\mathbb{Z}[X]$. $\square$

Corollaire 4.112.

Si p est premier alors le polynôme cyclotomique ϕ_p a une bonne tête :

$$\phi_p(X) = 1 + X + \dots + X^{p-1}. \quad (4.156)$$

Démonstration. Nous utilisons la formule du lemme 4.108 en remarquant que seuls p et 1 divisent p :

$$X^p - 1 = \prod_{d|p} \phi_d(X) = \phi_1(X)\phi_p(X) = (X-1)\phi_p(X). \quad (4.157)$$

Nous pouvons simplifier par $X-1$ en utilisant la formule du lemme 3.118(2) :

$$1 + X + \dots + X^{p-1} = \phi_p(X) \quad (4.158)$$

□

Proposition 4.113 (Irréductibilité des polynômes cyclotomiques[47]).

Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$.

Démonstration. Pour rappel, nous savons déjà que pour tout $n \in \mathbb{N}$, $\phi_n \in \mathbb{Z}[X]$. Vu que les racines de ϕ_n sont les racines primitives de l'unité, nous devons montrer que toutes les racines primitives de l'unité ont même polynôme minimal (qui sera alors ϕ_n) ; en effet vu que ces polynômes divisent ϕ_n , si ils sont distincts, la proposition 4.53 s'applique et le produit des polynômes minimaux diviserait ϕ_n . Dans le cas inverse, ϕ_n est polynôme minimal des racines primitives de l'unité et est donc irréductible. Soit donc ξ , une telle racine primitive. Une autre racine primitive est de la forme ξ^l où l est un nombre premier tel que $\text{pgcd}(l, n) = 1$.

Soient f et g , les polynômes minimaux dans $\mathbb{Z}[X]$ de ξ et ξ^l . Nous allons montrer que $f = g$ et donc que $f = g = \phi_n$. Supposons par l'absurde que $f \neq g$. Dans ce cas ils seraient des facteurs irréductibles distincts de ϕ_n et il existerait un polynôme h tel que $\phi_n = fgh$. A priori, $h \in \mathbb{Q}[X]$ parce que nous sommes justement en train de prouver que ϕ_n est irréductible dans $\mathbb{Q}[X]$. Quoi qu'il en soit, le lemme de Gauss 4.18 nous montre que $h \in \mathbb{Z}[X]$ parce que ϕ_n , f et g ont des coefficients entiers. Nous avons

$$f(\xi) = g(\xi^l) = 0. \quad (4.159)$$

Considérons le polynôme $\psi(X) = g(X^l)$. Ce polynôme ψ est dans $\mathbb{Z}[X]$ et ψ est annulateur de ξ , donc f divise ψ en tant que polynôme minimal de ξ . Il y a un polynôme unitaire à coefficients entiers (lemme de Gauss forever) k tel que

$$\psi = fk \quad (4.160)$$

Nous considérons maintenant les projections sur $\mathbb{F}_l[X]$: étant donné que $\phi_n = fgh$, nous savons que $\bar{f}\bar{g}$ divise $\bar{\phi}_n$. En même temps, $\bar{f}$ divise $\bar{\psi}$. En utilisant le morphisme de Frobenius (c'est ici que la projection sur $\mathbb{F}_l$ joue), nous avons aussi

$$\bar{\psi}(X) = \bar{g}(X^l) = \bar{g}(X)^l. \quad (4.161)$$

Par conséquent dire que $\bar{f}$ divise $\bar{\psi}$ revient à dire que $\bar{f}(X)$ divise $\bar{g}(X)^l$. En particulier tous facteur irréductible de $\bar{f}$ divise $\bar{g}$. Un facteur irréductible de $\bar{f}$ serait donc à la fois dans $\bar{f}$ et dans $\bar{g}$ et donc deux fois (au moins) dans $\bar{\phi}_n$ parce que $\bar{f}\bar{g}$ divise $\bar{\phi}_n$. Dans un corps de décomposition de ce facteur, ϕ_n aurait une racine double, alors que ce n'est pas le cas. Contradiction. Nous concluons que $f = g$. □

Le corollaire suivant va être utilisé pour déterminer les polygones constructibles à la règle et au compas, théorème de Gauss-Wantzel 4.173.

Corollaire 4.114.

Soit p un nombre premier et α un entier non nul. Nous posons $q = p^\alpha$. Alors le polynôme minimal de $e^{2i\pi/q}$ sur $\mathbb{Q}$ est le polynôme cyclotomique ϕ_q .

Démonstration. Le polynôme ϕ_q est irréductible par la proposition 4.113, il est unitaire par définition et contient le monôme $X - e^{2i\pi/q}$, donc il est annulateur. Annulateur, irréductible et unitaire, le corollaire 4.57 en fait le polynôme minimal de ω . □

Théorème 4.115.

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible non constant tel que toutes les racines dans $\mathbb{C}$ soient de module ≤ 1 . Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration. Nous supposons que $X \neq 0$, et nous notons $P = \sum_i a_i X^i$. Étant donné que P est irréductible et différent de X , nous avons $a_0 \neq 0$ (sinon $x = 0$ serait une racine). Nous allons montrer que les racines de P sont toutes des racines N -ièmes de l'unité (avec le même N pour toutes).

Soient $\{\xi_i\}_{i=1,\dots,d}$ les racines de P ; on a

$$P = \prod_{i=1}^d (X - \xi_i) \quad (4.162)$$

avec $\prod_{i=1}^d \xi_i = a_0$. Par hypothèse, $|\xi_i| \leq 1$ et donc $0 < |a_0| \leq 1$. Vu que $P \in \mathbb{Z}[X]$ nous avons donc $a_0 = 1$ et donc $|\xi_i| = 1$ pour tout i .

Nous introduisons les polynômes

$$g_q(X) = \prod_{i=1}^d (X - (\xi_i)^q), \quad (4.163)$$

et en particulier $g_1 = P$, et nous développons

$$g_q(X) = X^n + C_{1,q}X^{n-1} + \dots + C_{n,q} \quad (4.164)$$

où

$$C_{k,q} = (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq d} (\xi_{i_1} \dots \xi_{i_k})^q. \quad (4.165)$$

Nous introduisons aussi les polynômes

$$F_{k,q}(X_1, \dots, X_n) = (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq d} (X_{i_1} \dots X_{i_k})^q \quad (4.166)$$

qui sont des polynômes symétriques. Ils vérifient deux propriétés. La première est que

$$C_{r,q} = F_{r,q}(\xi_1, \dots, \xi_n), \quad (4.167)$$

et la seconde est que les polynômes $F_{r,1}$ sont les polynômes symétriques élémentaires à un coefficients près. Le théorème 4.100 nous donne alors des polynômes $G_{k,q} \in \mathbb{Z}[X_1, \dots, X_n]$ tels que

$$F_{k,q}(X_1, \dots, X_n) = G_{k,q}(F_{1,1}(X_1, \dots, X_n), \dots, F_{k,1}(X_1, \dots, X_n)). \quad (4.168)$$

Nous savons que

$$|C_{k,q}| \leq \sum_{1 \leq i_1 < \dots < i_k \leq d} 1 = \binom{d}{k}. \quad (4.169)$$

Donc g_q fait partie de l'ensemble fini des polynômes dans $\mathbb{Z}[q]$ dont tous les coefficients sont bornée en valeur absolue par

$$\max_{k=1,\dots,d} \binom{d}{k}. \quad (4.170)$$

Il existe un certain nombre d'ensembles $\{\xi_i\}$ qui sont racines de polynômes vérifiant les conditions du théorème. À chacun de ces ensembles est associé une suite de polynômes g_q et donc des coefficients $C_{k,q}$. Ce que nous avons vu est que l'ensemble de tous les coefficients $C_{k,q}$ possibles (pour un choix donné des $\{\xi_i\}$) est fini, en particulier, vu que $C_{1,q} = \sum_i \xi_i^q$, pour chaque k , l'ensemble

$$\{\xi_k^q \text{ tel que } q \in \mathbb{N}\}. \quad (4.171)$$

Par le principe des tiroirs, il existe q_1 et q_2 tels que $\xi_k^{q_1} = \xi_k^{q_2}$. Ici, q_1 et q_2 dépendent de k et nous notons $N_k = q_1 - q_2$; nous avons donc $\xi_k^{N_k} = 1$.

En posant $N = \text{ppcm}(N_1, \dots, N_d)$, nous avons

$$\xi_k^N = 1 \quad (4.172)$$

pour tout k .

Mais P est irréductible dans $\mathbb{Z}[X]$; si il a ± 1 comme racines, alors c'est que $P = X + 1$ ou $P = X - 1$ et ce sont des polynômes cyclotomiques. Si P n'a pas ± 1 parmi ses racines, alors P n'a pas de racines dans $\mathbb{Q}$ parce que ± 1 sont les seules racines de $X^N - 1$ dans $\mathbb{Q}$.

Par conséquent P est un facteur irréductible de $X^N - 1$ dans $\mathbb{Q}[X]$. Mais étant donné que

$$X^N - 1 = \prod_{d|N} \phi_d(X), \quad (4.173)$$

les polynômes cyclotomiques sont les seuls facteurs irréductibles de $X^N - 1$. Donc P est un polynôme cyclotomique. $\square$

4.5.2 Nombres premiers

Lemme 4.116 ([48]).

Soit $n \geq 1$. Il existe un nombre premier p et un entier a tels que

- (1) p divise $\phi_n(a)$,
- (2) p ne divise aucun de $\phi_d(a)$ avec $d \mid n$ et $d \neq n$.

De tels p et a vérifient automatiquement

- (1) p divise $a^n - 1$,
- (2) p ne divise aucun des $a^d - 1$ pour $d \mid n$, $d \neq n$.

Démonstration. Nous posons

$$B(X) = \prod_{\substack{d \mid n \\ d \neq n}} \phi_d(X), \quad (4.174)$$

et nous commençons par montrer que ϕ_n est premier avec B . Nous avons $X^n - 1 = B\phi_n$, donc B et ϕ_n n'ont pas de racines communes (même pas dans $\mathbb{C}$) parce que ce serait une racine double de $X^n - 1$. Notons que par définition 4.144, les polynômes cyclotomiques sont scindés (dans $\mathbb{C}$), donc en particulier les polynômes ϕ_n et B sont scindés et donc premiers entre eux, dans $\mathbb{C}$ et a fortiori dans $\mathbb{Q}$. Par Bézout (corollaire 3.69), il existe $U, V \in \mathbb{Q}[X]$ tels que

$$U\phi_n + VB = 1. \quad (4.175)$$

Si nous prenons $a \in \mathbb{Z}$ tel que $U' = aU$ et $V' = aV$ soient tous deux dans $\mathbb{Z}[X]$, alors nous avons

$$U'\phi_n + V'B = a, \quad (4.176)$$

égalité dans $\mathbb{Z}[X]$. Quitte à prendre un multiple assez grand de a , nous pouvons choisir a de telle sorte que $|\phi_n(a)| \geq 2$. Nous prenons alors un nombre premier p divisant $\phi_n(a)$.

Montrons que le a et le p ainsi construits satisfont aux exigences.

Vu que $X^n - 1 = B\phi_n$, si p divise $\phi_n(a)$, il divise automatiquement $a^n - 1$ et donc $[a^n]_p = 1$, ce qui signifie entre autres que a et p sont premiers entre eux. Évaluons l'équation (4.176) en a :

$$U'(a)\phi_n(a) + V'(a)B(a) = a. \quad (4.177)$$

Le nombre p ne divisant pas a , mais divisant $\phi_n(a)$, il ne peut pas diviser $B(a)$ ¹⁷. Étant donné que p ne divise pas $B(a)$, il ne divise aucun des $\phi_d(a)$ avec $d \mid n$ et $d \neq n$.

17. C'est pour pouvoir dire ça que l'on a choisi $V' \in \mathbb{Z}[X]$ de telle sorte que $V'(a)$ soit dans $\mathbb{Z}$

Nous passons maintenant à la seconde partie de la preuve. Nous supposons avoir a et p tels que p soit un nombre premier divisant $\phi_n(a)$ et tels que p ne divise aucun des $\phi_d(a)$ avec $d \mid n$, $d \neq n$. Le fait de diviser $\phi_n(a)$ entraîne le fait de diviser $a^n - 1$ parce que ϕ_n est un des facteurs de $X^n - 1$. Soit maintenant $d \neq n$ divisant n ; nous avons

$$X^d - 1 = \prod_{d' \mid d} \phi_{d'}, \quad (4.178)$$

et cela est une partie du produit

$$\prod_{\substack{d \mid n \\ d \neq n}} \phi_d. \quad (4.179)$$

Vu que p ne divise aucun des $\phi_d(a)$ de ce dernier produit, a fortiori, il ne divise pas le produit 4.178, et donc pas $a^d - 1$. $\square$

Lemme 4.117.

Si $n \geq 1$, alors il existe un nombre premier dans $[1]_n$, c'est à dire un nombre premier de la forme $1 + kn$ avec $k \in \mathbb{N}^*$.

Démonstration. Soit $n \geq 1$ et les nombres p, a donnés par le lemme 4.116. Vu que p divise $\phi_n(a)$, p divise $a^n - 1$ et donc $[a]_p$ a un ordre qui divise n dans $(\mathbb{Z}/p\mathbb{Z})^*$ parce que $[a]_p^n = [1]_p$.

Prenons $d \neq n$ divisant n . Nous savons que

$$a^d - 1 = \prod_{d' \mid d} \phi_{d'}(a). \quad (4.180)$$

Par construction de a et p , nous avons

$$[\phi_{d'}(a)]_p \neq 0 \quad (4.181)$$

Vu que $\mathbb{Z}/p\mathbb{Z}$ est intègre, le produit est également non nul, c'est à dire

$$\left[\prod_{d' \mid d} \phi_{d'}(a) \right]_p \neq 0, \quad (4.182)$$

et donc $[a]_p^d \neq 1$. Nous avons donc montré que si $d \neq n$ divise n , alors nous avons en même temps

$$[a]_p^n = 1 \quad (4.183)$$

et

$$[a]_p^d \neq 1. \quad (4.184)$$

Cela prouve que $[a]_p$ est d'ordre exactement n . Oui, mais l'ordre de $[a]_p$ doit diviser l'ordre du groupe $\mathbb{Z}/p\mathbb{Z}$ qui est $p - 1$, donc n divise $p - 1$ et nous écrivons $p = kn + 1$ avec k entier. $\square$

Théorème 4.118 (Forme faible du théorème de Dirichlet [35]).

Pour tout $n \geq 1$, il existe une infinité de nombres premiers dans $[1]_n$.

Démonstration. Le lemme 4.117 nous donne déjà l'existence de nombres premiers dans $[1]_n$. Il faut maintenant voir qu'il y en a une infinité. Nous supposons qu'il y en ait seulement un nombre fini : $p_1, \dots, p_r$, et nous notons

$$N = np_1 \dots p_r. \quad (4.185)$$

Nous utilisons maintenant le lemme 4.117 avec ce N , c'est à dire qu'on a un nombre premier de la forme

$$p = 1 + kN = 1 + knp_1 \dots p_r. \quad (4.186)$$

Cela est un nombre premier plus grand que tous les p_i et de la forme $1 + \lambda n$. Cela contredit l'exhaustivité de la liste $p_1, \dots, p_r$. $\square$

4.5.3 Théorème de Wedderburn

Théorème 4.119 (Théorème de Wedderburn[37]).

Tout corps fini est commutatif.

Démonstration. Soit $\mathbb{K}$ un corps fini et Z , le centre de $\mathbb{K}$. Ce dernier est un corps fini et un sous corps de $\mathbb{K}$. Si $q = \text{Card}(Z)$ alors par le lemme 4.36 nous avons

$$\text{Card}(\mathbb{K}) = q^n \quad (4.187)$$

pour un certain n .

Nous supposons maintenant que $\mathbb{K}$ est non commutatif. Dans ce cas $Z \neq \mathbb{K}$ et nous avons $n \geq 2$. Nous considérons aussi

$$Z_x = \{a \in \mathbb{K} \text{ tel que } ax = xa\}. \quad (4.188)$$

Le centre Z est un sous corps de Z_x , donc il existe $d(x)$ tel que

$$\text{Card}(Z_x) = q^{d(x)}. \quad (4.189)$$

De la même manière, Z_x est un sous corps de $\mathbb{K}$, donc il existe $m(x)$ tel que

$$\text{Card}(\mathbb{K}) = \text{Card}(Z_x)^{m(x)}. \quad (4.190)$$

En mettant bout à bout nous avons

$$q^n = \text{Card}(Z_x)^{m(x)} = q^{d(x)m(x)}, \quad (4.191)$$

et par conséquent $n = d(x)m(x)$. Le point important à retenir est que $d(x)$ divise n pour tout $x \in \mathbb{K}$.

Nous considérons maintenant l'action adjointe du groupe $\mathbb{K}^*$ sur lui-même :

$$\varphi(k)x = kxk^{-1}. \quad (4.192)$$

Nous notons $\mathcal{O}_x$ l'orbite de $x \in \mathbb{K}^*$ pour cette action, et $\text{Stab}(x)$ son stabilisateur. Nous avons

$$Z_y = \text{Stab}(y) \cup \{0\} \quad (4.193)$$

parce que Z_y et $\text{Stab}(y)$ ont les mêmes définitions, sauf que $\text{Stab}(y)$ est dans $\mathbb{K}^*$ alors que Z_y est dans $\mathbb{K}$. Nous avons donc

$$\text{Card}(\text{Stab}(y)) = \text{Card}(Z_y) - 1 = q^{d(y)} - 1. \quad (4.194)$$

Nous avons $\text{Card}(\mathcal{O}_x) = 1$ si et seulement si $\mathcal{O}_x = \{x\}$ si et seulement si $\text{Stab}(x) = \mathbb{K}^*$ si et seulement si $z \in Z^*$. Soient $z_0, \dots, z_{q-1}$ les éléments de Z avec $z_0 = 0$. Ce sont les éléments qui auront une orbite réduite à un point. Les orbites qui coupent Z^* sont

$$\{z_1\}, \dots, \{z_{q-1}\} \quad (4.195)$$

et il y en a $q - 1$. Soient $\mathcal{O}_{y_1}, \dots, \mathcal{O}_{y_r}$, les autres orbites. Nous utilisons l'équation des classes (2.125) :

$$\text{Card}(\mathbb{K}^*) = \text{Card}(Z^*) + \sum_{i=1}^r \frac{\text{Card}(\mathbb{K}^*)}{\text{Card}(\text{Stab}(y_i))}, \quad (4.196)$$

mais $\text{Card}(Z^*) = q - 1$, $\text{Card}(\mathbb{K}^*) = q^n - 1$ et $\text{Card}(\text{Stab}(y_i)) = q^{d(y_i)} - 1$, donc

$$q^n - 1 = (q - 1) + \sum_{i=1}^r \frac{q^n - 1}{q^{d(y_i)} - 1}. \quad (4.197)$$

Nous considérons la fraction rationnelle

$$F(X) = (X^n - 1) - \sum_{i=1}^r \frac{X^n - 1}{X^{d(y_i)} - 1}. \quad (4.198)$$

Étant donné que $d(y_i)$ divise n , nous avons, contrairement aux apparences, que $F \in \mathbb{Z}[X]$ par la proposition 4.111(1).

Nous pouvons exploiter un peu mieux la proposition 4.111 en remarquant que $d(y_i) < n$ parce que sinon $\text{Card}(Z_{y_i}) = \text{Card}(\mathbb{K})$, ce qui signifierait que $y_i \in Z$, ce qui nous avons exclu. Par conséquent le polynôme cyclotomique ϕ_n divise

$$\frac{X^n - 1}{X^{d(y_i)} - 1} \quad (4.199)$$

dans $\mathbb{Z}[X]$. Le polynôme cyclotomique ϕ_n divise également $X^n - 1$ et par conséquent ϕ_n divise F . Il existe donc $Q \in \mathbb{Z}[X]$ tel que $F = Q\phi_n$. En particulier en évaluant en q :

$$F(q) = Q(q)\phi_n(q) = q - 1. \quad (4.200)$$

En effet nous avons $F(q) = q - 1$ par construction : comparer (4.197) avec (4.198). Évidemment $q \neq 1$ parce que si $q = 1$ alors $\text{Card}(\mathbb{K}) = 1$ et le théorème est trivial. Par ailleurs $Q(q)$ est un entier (parce que $Q \in \mathbb{Z}[X]$ et $q \in \mathbb{N}$) et $Q(q) \neq 0$, parce qu'à droite de (4.200) nous avons $q - 1 \neq 0$. Nous avons donc $|Q(q)| \geq 1$ et donc

$$|\phi_n(q)| \leq q - 1. \quad (4.201)$$

Par définition du polynôme cyclotomique nous avons

$$|\phi_n(q)| = \prod_{z \in \Delta_n} |q - z|. \quad (4.202)$$

Étant donné que ce produit doit être inférieur à $q - 1$, au moins un des termes doit l'être : il existe $z_0 \in \Delta_n$ tel que $|z_0 - q| \leq q - 1$. Étant donné que $n \geq 2$ nous avons $z_0 \neq 1$.

Mais d'autre part, comme indiqué sur la figure 4.1, la distance entre z_0 et q doit être strictement plus grande que $q - 1$ parce que $q - 1$ est le minimum de la distance entre le cercle trigonométrique et q , et n'est atteint qu'en $z = 1$.

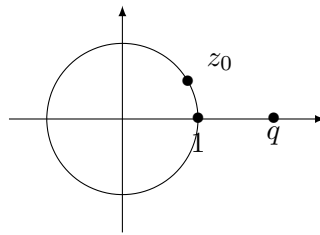


FIGURE 4.1 – Nous devons avoir $|z_0 - q| > q - 1$.

Nous avons ainsi obtenu une contradiction, et nous concluons que le corps $\mathbb{K}$ est commutatif. $\square$

4.6 Corps finis

Si vous cherchez des choses à propos de RSA, c'est à la section 12.8.

4.6.1 Existence, unicité

Nous avons déjà défini le corps fini $\mathbb{F}_p$ lorsque p est un nombre premier dans la section 4.1.2. Le théorème suivant sert à définir $\mathbb{F}_{p^n}$ lorsque p est premier.

Théorème 4.120.

Soit p un nombre premier, soit $n \in \mathbb{N}^*$ et $q = p^n$. Alors il existe un unique corps $\mathbb{K}$ de cardinal q . Ce corps est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.

Démonstration. Montrons l'unicité. Soit $\mathbb{K}$ un corps fini de cardinal $q = p^n$. Le groupe multiplicatif $\mathbb{K}^*$ est de cardinal $q - 1$, et par le corollaire 2.40 tous les éléments de $\mathbb{K}^*$ vérifient $g^{q-1} = e$, c'est à dire que dans $\mathbb{K}[X]$, les éléments de $\mathbb{K}^*$ sont des racines du polynôme

$$X^{q-1} - 1 \quad (4.203)$$

Par conséquent $\mathbb{K}$ est un corps de décomposition pour le polynôme $Q(X) = X^q - X = X(X^{q-1} - 1)$ parce que $Q(X) = 0$ dans $\mathbb{K}$. Il est unique par la proposition 4.68.

Montrons maintenant que le corps de décomposition de $P = X^q - X$ sur $\mathbb{F}_p$ est un corps de cardinal q . Pour ce faire nous considérons $\mathbb{K}$ ce corps de décomposition et $\mathbb{E}$, l'ensemble des racines de P dans $\mathbb{K}$. Nous allons montrer que $\mathbb{E} = \mathbb{K}$ et que $\mathbb{E}$ est un corps contenant q éléments.

Montrons que $\mathbb{E}$ est un corps. Pour $\alpha, \beta \in \mathbb{E}$ nous avons

$$(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta \quad (4.204)$$

parce que $\alpha^q = \alpha$. Le produit $\alpha\beta$ est donc encore dans $\mathbb{E}$. Pour la somme,

$$(\alpha + \beta)^q = (\alpha + \beta)^{p^n} = \left((\alpha + \beta)^p\right)^{p^{n-1}} = (\alpha^p + \beta^p)^{p^{n-1}} = \dots = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta. \quad (4.205)$$

En ce qui concerne l'inverse,

$$(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}. \quad (4.206)$$

Donc $\mathbb{E}$ est un corps. Évidemment $\mathbb{E}$ est un corps de décomposition de P au sens où $\mathbb{E}$ est une extension de $\mathbb{F}_p$ sur lequel P est scindé (parce qu'il est scindé sur $\mathbb{K}$ et $\mathbb{E}$ est le sous corps de $\mathbb{K}$ contenant les racines de P) et tel que $\mathbb{E} = \mathbb{F}_p(\{\alpha_i\})$ où les α_i sont les racines de P . Notons que $\mathbb{F}_p \subset \mathbb{E}$ parce que dans $\mathbb{F}_p$ on a $x^q = x$.

Par unicité, nous avons $\mathbb{K} = \mathbb{E}$. Nous devons montrer que P possède exactement q racines distinctes, afin d'avoir $\text{Card}(\mathbb{E}) = q$. Pour cela remarquons que

$$P'(X) = qX^{q-1} - 1 = -1 \quad (4.207)$$

dans $\mathbb{F}_p$. En effet $P \in \mathbb{F}_p$ et $q = 0$ dans $\mathbb{F}_p$. Par conséquent P' ne s'annule pas et P n'a pas de racines doubles. Toutes les racines étant simples, il y en a exactement q . □

Le théorème 4.120 ne permet pas de *construire* le corps à $q = p^n$ éléments. Nous allons maintenant voir un certain nombre de résultats donnant des façons de construire. Ces résultats proviennent de [49, 50, 51] et de wikipedia

Proposition 4.121 ([51]).

Soit $\mathbb{K}$ un corps fini. Alors le groupe multiplicatif $\mathbb{K}^*$ est cyclique.

Démonstration. Soit $\mathbb{K}$ un corps ayant q éléments. Le groupe $\mathbb{K}^*$ en a $q - 1$; ergo l'ordre des éléments de $\mathbb{K}^*$ sont des diviseurs de $q - 1$; c'est le corollaire 2.40. Soit d un diviseur de $q - 1$ et

$$H_d^* = \{x \text{ d'ordre } d \text{ dans } \mathbb{K}^*\} \quad (4.208a)$$

$$H_d = \{\text{racines de } X^d - 1 \text{ dans } \mathbb{K}\}. \quad (4.208b)$$

Ici le polynôme $X^d - 1$ est vu dans $\mathbb{K}[X]$. Notons que nous avons automatiquement $H_d^* \subset H_d$, mais l'inclusion inverse n'est pas assurée parce que les éléments d'ordre $d/2$ par exemple sont aussi dans H_d . Supposons $H_d^* \neq \emptyset$ et considérons $a \in H_d^*$. Alors l'application

$$\begin{aligned} \phi: \mathbb{Z}/d\mathbb{Z} &\rightarrow H_d \\ n &\mapsto a^n \end{aligned} \quad (4.209)$$

est un isomorphisme d'anneaux. En effet étant donné que $a \in H_d^* \subset H_d$, l'ensemble H_d contient le groupe cyclique engendré par a . Ce dernier contient, par construction, d éléments. Mais $\text{Card}(H_d) \leq d$ parce que H_d est l'ensemble des racines d'un polynôme de degré d . Par conséquent $\text{Card}(H_d) = d$ et l'ensemble H_d est bien engendré par a et ϕ est bien un isomorphisme. Par conséquent tous les éléments de H_d^* sont des générateurs de H_d .

Inversement soit x un générateur de H_d . L'ordre de H_d étant d , l'ordre de x doit être un diviseur de d . Supposons donc que x soit d'ordre d/k . Dans ce cas nous devrions avoir $\text{Card}(H_d) = d/k$, ce qui contredit l'isomorphisme ϕ .

En conclusion, H_d^* est l'ensemble des générateurs du groupe H_d . Le nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$ étant $\varphi(d)$ par la proposition 3.17, et H_d étant isomorphe à $\mathbb{Z}/d\mathbb{Z}$ nous avons

$$\text{Card}(H_d^*) = \varphi(d). \quad (4.210)$$

Par conséquent si H_d^* n'est pas vide, son cardinal est $\varphi(d)$. Nous avons

$$q - 1 = \text{Card}(\mathbb{K}^*) \quad (4.211a)$$

$$= \text{Card} \left(\bigcup_{d|q-1} H_d^* \right) \quad (4.211b)$$

$$= \sum_{d|q-1} \text{Card}(H_d^*) \quad (4.211c)$$

$$\leq \sum_{d|q-1} \varphi(d) \quad (4.211d)$$

$$= q - 1 \quad (4.211e)$$

où nous avons utilisé le lemme 3.15. Par conséquent pour tout d divisant $q - 1$ nous avons $\text{Card}(H_d^*) = \varphi(d)$ et il y a au moins un élément d'ordre $q - 1$ dans $\mathbb{K}$. Cet élément engendre $\mathbb{K}^*$ parce que $\mathbb{K}^*$ contient exactement $q - 1$ éléments. Par conséquent $\mathbb{K}$ est cyclique. $\square$

Corollaire 4.122.

Si p est un nombre premier, alors

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}. \quad (4.212)$$

L'isomorphisme est un isomorphisme de groupe (abéliens). À gauche multiplicatif et à droite additif.

Démonstration. La proposition 4.121 nous enseigne que le le groupe multiplicatif d'un corps fini est cyclique et donc isomorphe à un certain $\mathbb{Z}/n\mathbb{Z}$. Donc $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique d'ordre p , et donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n = p - 1$. $\square$

Lorsque $\mathbb{K}$ est un corps les éléments du groupe $\mathbb{K}^*$ sont les **éléments primitifs** de $\mathbb{K}$.

Proposition 4.123.

Soit $\mathbb{K}$ un corps contenant q éléments. Alors

- (1) $x^q = x$ pour tout $x \in \mathbb{K}$,
- (2) $X^q - X = \prod_{a \in \mathbb{K}} (X - a)$.

Démonstration. Le groupe $\mathbb{K}^*$ ayant $q - 1$ éléments, ses éléments vérifient $a^{q-1} = 1$ par le corollaire 2.40 et par conséquent $a^q = aa^{q-1} = a$.

Soit $a \in \mathbb{K}$. Étant donné que $a^q - a = 0$, le polynôme $(X - a)$ divise $X^q - X$ dans $\mathbb{K}[X]$. Par conséquent

$$\prod_{a \in \mathbb{K}} (X - a) \quad (4.213)$$

divise également $X^q - X$. Les polynômes $X^q - X$ et $\prod_{a \in \mathbb{K}} (X - a)$ étant deux polynômes unitaires de même degré, le fait que l'un divise l'autre montre qu'ils sont égaux. $\square$

Exemple 4.124

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 . $\triangle$

Une conséquence du fait que $x^q = x$ est qu'il ne fait pas regarder le théorème 4.58 trop rapidement en disant «si il s'annule partout, alors c'est le polynôme nul». En effet dans un corps fini, «partout» n'est pas forcément très grand.

Exemple 4.125

Si $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ est le ¹⁸ corps à 3 éléments, alors le polynôme $P(X) = X^3 - X$ s'évalue à zéro pour tout $x \in \mathbb{F}_3$ (proposition 4.123.) mais il n'est pas le polynôme nul. $\triangle$

4.6.2 Symboles de Legendre et carrés

Source : [52].

Nous disons que $a \in \mathbb{F}_p$ est un **carré** si il existe $b \in \mathbb{F}_p$ tel que $a = b^2$.

Définition 4.126.

Soit $n \in \mathbb{N}$ et $p > 2$ un nombre premier. Le **symbole de Legendre** par

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } n \\ 1 & \text{si } n \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon.} \end{cases} \quad (4.214)$$

Note que -1 peut être un carré, et pas que dans $\mathbb{C}$. Par exemple dans $\mathbb{F}_5$ nous avons $4 = -1$ et donc -1 est un carré.

Proposition 4.127.

Soit un nombre premier $p > 2$. Le corps $\mathbb{F}_p^*$ contient autant de carrés que de non carrés. De plus pour tout $n \in \mathbb{N}$ nous avons

$$\left(\frac{n}{p}\right) = n^{(p-1)/2} \pmod{p}. \quad (4.215)$$

Démonstration. Nous considérons l'application

$$\begin{aligned} \psi: \mathbb{F}_p^* &\rightarrow \mathbb{F}_p^* \\ x &\mapsto x^2. \end{aligned} \quad (4.216)$$

C'est un morphisme de groupes multiplicatifs et $\ker \psi = \{-1, 1\}$. Étant donné que $p > 2$, nous avons alors

$$\text{Card}(\ker \psi) = 2 \quad (4.217)$$

parce que $1 \neq -1$. Évidemment l'ensemble des carrés dans $\mathbb{F}_p^*$ est l'image de ψ . Le premier théorème d'isomorphisme 2.17(3) nous permet alors de conclure que

$$\text{Card}(\text{Image}(\psi)) = \frac{\text{Card}(\mathbb{F}_p^*)}{2}. \quad (4.218)$$

Ceci prouve la première assertion.

Par le petit théorème de Fermat (théorème 4.19), nous avons $x^{p-1} = 1$ pour tout $x \in \mathbb{F}_p^*$. Les $(p-1)$ éléments de $\mathbb{F}_p^*$ sont donc tous racines d'un des deux polynômes

$$X^{(p-1)/2} = \pm 1. \quad (4.219)$$

Mais chacun des deux ne peut avoir, au maximum, que $(p-1)/2$ solutions. Ils ont donc chacun exactement $(p-1)/2$ racines.

18. Le singulier est justifié par le théorème 4.120, mais ça n'a pas d'importance ici.

Nous pouvons maintenant prouver la formule (4.215). D'abord si $n = 0$, elle est évidente. Si n est un carré dans $\mathbb{F}_p$, nous posons $n = x^2$ et nous avons

$$n^{(p-1)/2} = n^{p-1} = 1 = \left(\frac{n}{p}\right). \quad (4.220)$$

Si n n'est pas un carré, c'est que n n'est pas une racine de $X^{(p-1)/2} = 1$. Le nombre n est alors une racine de $X^{(p-1)/2} = -1$. Nous avons alors

$$n^{(p-1)/2} = -1 = \left(\frac{n}{p}\right). \quad (4.221)$$

□

Corollaire 4.128.

Si $a, b \in \mathbb{N}$ et si $p > 2$ est un nombre premier, alors

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right). \quad (4.222)$$

Démonstration. Par la formule (4.215),

$$\left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right). \quad (4.223)$$

□

Soit un nombre premier $q > 2$ et $\mathbb{A}$, un anneau de caractéristique p . Si $\alpha \in \mathbb{A}$ vérifie

$$1 + \alpha + \dots + \alpha^{q-1} = 0, \quad (4.224)$$

nous définissons la **somme de Gauss** par

$$\tau = \sum_{x \in \mathbb{F}_q} \left(\frac{i}{q}\right) \alpha^i = \sum_{x=1}^{q-1} \left(\frac{x}{q}\right) \alpha^i. \quad (4.225)$$

Notons que la somme de Gauss dépend de q et du α choisis.

Proposition 4.129.

Les sommes de gauss vérifient les propriétés suivantes.

(1) $\tau^2 = \left(\frac{-1}{q}\right) q$. Nous allons noter $\epsilon(q) = \left(\frac{-1}{q}\right)$.

(2) Si $\mathbb{A}$ est de caractéristique $p \geq 3$ et si $p \neq q$ alors

$$\tau^p = \left(\frac{p}{q}\right) \tau. \quad (4.226)$$

(3) Si $\mathbb{A}$ est de caractéristique p et si q est premier avec p , alors τ est inversible dans $\mathbb{A}$.

Démonstration. D'abord nous notons que

$$\alpha^q - 1 = (\alpha - 1)(1 + \alpha + \dots + \alpha^{q-1}) = 0 \quad (4.227)$$

par définition de α . Nous calculons

$$\epsilon(q) \tau^2 = \epsilon(q) \sum_{x, y \in \mathbb{F}_q} \left(\frac{x}{q}\right) \left(\frac{y}{q}\right) \alpha^{x+y} \quad (4.228a)$$

$$= \sum_{x, y \in \mathbb{F}_q} \left(\frac{-xy}{q}\right) \alpha^{x+y}. \quad (4.228b)$$

$$= \sum_{z \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \left(\frac{-(z-y)y}{q}\right) \alpha^z \quad (4.228c)$$

$$= \sum_{z \in \mathbb{F}_q} s_z \alpha^z \quad (4.228d)$$

Justifications :

- Pour obtenir (4.228b) nous avons utilisé le corollaire 4.128.
- (4.228c) est un changement de variable $z = x + y$ dans la somme sur x .
- Pour (4.228d) nous avons posé

$$s_z = \sum_{y \in \mathbb{F}_q} \left(\frac{-(z-y)y}{q} \right). \quad (4.229)$$

Nous avons

$$s_0 = \sum_{y \in \mathbb{F}_q} \left(\frac{y^2}{q} \right). \quad (4.230)$$

Dans cette somme, tous les termes sont 1 sauf celui avec $y = 0$ qui vaut zéro. Nous avons donc $s_0 = q - 1$. Voyons maintenant s_y avec $y \neq 0$. L'application

$$\begin{aligned} \mathbb{F}_q^* &\rightarrow \mathbb{F}_q \setminus \{1\} \\ k &\mapsto 1 - zy^{-1} \end{aligned} \quad (4.231)$$

étant une bijection nous pouvons effectuer le changement de variables $t = y^{-1}z - 1$ pour la somme sur y en notant y^{-1} l'inverse de y dans $\mathbb{F}_q^*$, nous trouvons alors

$$\sum_{y \in \mathbb{F}_q} \left(\frac{y(z-y)}{q} \right) = \sum_{y \in \mathbb{F}_q} \left(\frac{y^2(y^{-1}z - 1)}{q} \right) \quad (4.232a)$$

$$= \sum_{y \in \mathbb{F}_q} \left(\frac{y^{-1}z - 1}{q} \right) \quad (4.232b)$$

$$= \sum_{t \in \mathbb{F}_q \setminus \{1\}} \left(\frac{t}{q} \right) \quad (4.232c)$$

$$= \underbrace{\sum_{t \in \mathbb{F}_q} \left(\frac{t}{q} \right) - \left(\frac{1}{q} \right)}_{=0} \quad (4.232d)$$

$$= -1 \quad (4.232e)$$

parce qu'il y a autant de carrés que de non carrés dans $\mathbb{F}_q^*$ (proposition 4.127). En résumé nous avons

$$\epsilon(q)\tau^2 = \sum_{z \in \mathbb{F}_q} s_z \alpha^z \quad (4.233)$$

où

$$s_z = \begin{cases} q-1 & \text{si } z = 0 \\ -1 & \text{sinon.} \end{cases} \quad (4.234)$$

Cela donne

$$\epsilon(q)\tau^2 = (q-1) - \underbrace{(\alpha + \dots + \alpha^{q-1})}_{=-1} = q \quad (4.235)$$

où nous avons utilisé l'hypothèse sur α . Donc $\epsilon(q)\tau^2 = q$, et étant donné que $\epsilon(q) = \pm 1$ nous concluons

$$\tau^2 = \epsilon(q)q. \quad (4.236)$$

Nous prouvons maintenant la seconde partie. Vu que $\mathbb{A}$ est de caractéristique p en utilisant le fait que le morphisme de Frobenius est un morphisme,

$$\tau^p = \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q} \right) \alpha^x \right)^p = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q} \right)^p \alpha^{px}. \quad (4.237)$$

Étant donné que $\left(\frac{x}{q}\right) = \pm 1$ et que p est impair, nous avons

$$\left(\frac{x}{q}\right)^p = \left(\frac{x}{q}\right). \quad (4.238)$$

Du coup nous avons

$$\left(\frac{p}{q}\right) \tau^p = \sum_{x \in \mathbb{F}_p} \left(\frac{xp}{q}\right) \alpha^{px}. \quad (4.239)$$

Mais p étant inversible dans $\mathbb{F}_q$, l'application $x \mapsto px$ est une bijection et nous pouvons sommer sur px au lieu de x :

$$\left(\frac{p}{q}\right) \tau^p = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{q}\right) \alpha^x = \tau. \quad (4.240)$$

Nous trouvons alors que

$$\tau^p = \left(\frac{p}{q}\right) \tau. \quad (4.241)$$

Étant donné la formule du τ^2 que nous venons de démontrer, nous avons $\tau^2 = \pm q$. Les nombres p et q étant premiers entre eux, la relation de Bézout (théorème 2.24) nous donne a et b tels que

$$ap + ba = 1. \quad (4.242)$$

Cela montre que b est un inverse de q modulo p . Donc τ^2 est inversible, et il en découle que τ lui-même est inversible. $\square$

Théorème 4.130 (Loi de réciprocité quadratique).

Soient deux nombres premiers distincts $p, q \geq 3$. Alors

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right). \quad (4.243)$$

Démonstration. Soit ϕ_q le polynôme $A + X + \dots + X^{q-1}$ et l'anneau

$$\mathbb{A} = \mathbb{F}_p[X]/(\phi_q). \quad (4.244)$$

Cela est un anneau de caractéristique p parce que son unité est le polynôme constant 1. Nous nommons $\alpha = X/(\phi_q)$, c'est à dire que $\phi_q(\alpha) = 0$ dans $\mathbb{A}$, et nous pouvons considérer la somme de Gauss

$$\tau = \sum_{i \in \mathbb{F}_q} \left(\frac{i}{q}\right) \alpha^i. \quad (4.245)$$

Notons que cela est un élément de $\mathbb{A}$ et plus précisément une (classe de) polynôme de degré zéro dans $\mathbb{A}$. Donc les coefficients de α doivent être compris comme des éléments de $\mathbb{F}_p$. Nous savons (proposition 4.129) que

$$\tau^2 = \left(\frac{-1}{q}\right), \quad (4.246)$$

et en utilisant la formule (4.215) nous trouvons

$$\left(\frac{\tau^2}{p}\right) = (\tau^2)^{(p-1)/2} \mod p = \tau^{p-1} \mod p \quad (4.247)$$

En réalité sur cette dernière ligne, nous ne devrions pas préciser le « mod p » parce que, comme mentionné plus haut, ce sont des éléments de $\mathbb{F}_p$. En utilisant cela ainsi que (4.226) nous avons

$$\underbrace{\left(\frac{\tau^2}{p}\right)}_{\tau^{p-1}} \tau = \tau^p = \left(\frac{p}{q}\right) \tau \quad (4.248)$$

Vu que τ est inversible, nous écrivons

$$\left(\frac{\tau^2}{p}\right) = \left(\frac{p}{q}\right) \quad (4.249)$$

Nous utilisons maintenant la formule (4.215) sur le membre de gauche avec $n = \tau^2 = \left(\frac{-1}{q}\right)$:

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right). \quad (4.250)$$

Toujours avec la même formule nous pouvons substituer $\left(\frac{-1}{q}\right)$ par $(-1)^{(q-1)/2}$ et obtenir

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(q-1)}{2} \frac{(p-1)}{2}}. \quad (4.251)$$

□

Lemme 4.131.

Si p est un nombre premier $p \geq 3$, alors le symbole de Legendre $x \mapsto \left(\frac{x}{p}\right)$ est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{-1, 1\}$.

Démonstration. Le fait que le symbole de Legendre soit non trivial est simplement le fait qu'il y ait des carrés et des non carrés dans $\mathbb{F}_p^*$; voir la proposition 4.127. Pour l'unicité, soit $\alpha: \mathbb{F}_p^* \rightarrow \{-1, 1\}$ un morphisme surjectif (c'est à dire non trivial). Étant donné que

$$\mathbb{F}_p^* = \ker(\alpha) \cup -\ker(\alpha), \quad (4.252)$$

le groupe $\mathbb{F}_p^*/\ker(\alpha)$ ne contient que deux éléments : $[1]$ et $[-1]$. Autrement dit, $\ker(\alpha)$ est d'indice 2 dans $\mathbb{F}_p^*$.

Or $\mathbb{F}_p^*$ ne possède qu'un seul sous-groupe d'indice 2. En effet soit S un tel sous-groupe et a , un générateur de $\mathbb{F}_p^*$ (qui est cyclique par la proposition 4.121), alors $a^2 \in S$ par le lemme 2.44. Par conséquent S contient le groupe des puissances paires de a . Le groupe S ne peut rien contenir de plus parce qu'il est d'indice 2 et que l'ordre de $\mathbb{F}_p^*$ est pair.

Bref, le sous-groupe $\ker(\alpha)$ est l'unique sous-groupe d'indice 2 dans $\mathbb{F}_p^*$. Mais la proposition 4.127 nous indique que $|(\mathbb{F}_p^*)^2| = \frac{p-1}{2}$, c'est à dire que le groupe des carrés est d'indice 2. Nous avons donc, par l'unicité,

$$\ker(\alpha) = (\mathbb{F}_p^*)^2. \quad (4.253)$$

Au final, pour $y \in \mathbb{F}_p^*$,

$$\alpha(y) = \begin{cases} 1 & \text{si } y \text{ est un carré} \\ -1 & \text{sinon.} \end{cases} \quad (4.254)$$

Cela est bien la définition des symboles de Legendre. □

Proposition 4.132.

Pour p premier nous avons

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \in [1]_8 \text{ ou } p \in [7]_8 \\ -1 & \text{sinon.} \end{cases} \quad (4.255)$$

Démonstration. Soit le polynôme

$$X^4 + 1 \in \mathbb{F}_p[X] \quad (4.256)$$

et α , une racine dans une fermeture de $\mathbb{F}_p$. Nous posons $\theta = \alpha + \alpha^{-1}$ et nous calculons

$$\theta^2 = (\alpha + \alpha^{-1})(\alpha + \alpha^{-1}) = \alpha^2 + 2 + (\alpha^2)^{-1} = \alpha^2 + 2 - \alpha^2 = 2 \quad (4.257)$$

parce que α^2 étant -1 , nous avons $(\alpha^2)^{-1} = -\alpha^2$. Bref, $\theta^2 = 2$.

Dire que 2 est un carré modulo p revient à dire que θ est dans $\mathbb{F}_p$. C'est à dire que pour calculer le symbole de Legendre $\left(\frac{2}{p}\right)$, nous étudions pour quels p , l'élément θ est vraiment dans $\mathbb{F}_p$ et non seulement dans l'extension $\mathbb{F}_p(\alpha)$. En tenant compte de l'exemple 4.51, il faut distinguer deux cas : $\alpha^p = \alpha$ et $\alpha^p \neq \alpha$. Autrement dit, si $\alpha^k = \alpha$ pour un certain nombre premier k , alors le cas $p = k$ est à traiter à part. La liste des puissances de α est :

$$1, \alpha, \alpha^2, \alpha^3, -1, -\alpha, -\alpha^2, -\alpha^3, 1, \alpha, \dots \quad (4.258)$$

Nous avons donc automatiquement $\alpha^{9k} = \alpha$, mais $p = 9k$ est exclu parce que p est premier. Nous devons donc vérifier si une des possibilités

$$\alpha^2 = \alpha \quad (4.259a)$$

$$\alpha^3 = \alpha \quad (4.259b)$$

$$-\alpha = \alpha \quad (4.259c)$$

$$-\alpha^3 = \alpha \quad (4.259d)$$

est possible. Il est aisément vérifiable, au cas par cas, que ces possibilités sont toutes incompatibles avec $\alpha^4 = -1$. Nous avons donc certainement $\alpha^p \neq \alpha$ et compte tenu de l'exemple 4.51, l'équation $x^p = x$ caractérise les éléments de $\mathbb{F}_p$ dans $\mathbb{F}_p(\alpha)$.

L'équation $X^2 = 2$ a exactement deux solutions qui sont $\pm\theta$. Nous avons donc $2 \in \mathbb{F}_p^2$ si et seulement si $\theta \in \mathbb{F}_p$ si et seulement si $\theta^p = \theta$. Nous avons réduit notre problème à déterminer pour quels p nous avons $\theta^p = \theta$. D'abord nous avons, par le morphisme de Frobenius,

$$\theta^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p}. \quad (4.260)$$

Nous pouvons maintenant conclure facilement. Un nombre premier étant impair (sauf $p = 2$ qui peut être traité à part), p est automatiquement dans un des ensembles $[1]_8$, $[3]_8$, $[5]_8$ ou $[7]_8$. Nous avons quatre petites vérifications à faire. Dans tous les cas $\alpha^{8k} = 1$. Si $p = 1 + 8k$, alors

$$\theta^p = \alpha^{1+8k} + (\alpha^{-1})^{1+8k} = \alpha + \alpha^{-1} = \theta, \quad (4.261)$$

donc 2 est un carré dans $\mathbb{F}_p$. Si $p \in [3]_8$, alors $\theta^p = \alpha^3 + \alpha^{-3}$. Si cela était égal à $\alpha + \alpha^{-1}$, alors nous aurions

$$\alpha^6 + 1 = \alpha^4 + \alpha^2, \quad (4.262)$$

et donc $\alpha^2 = 1$, ce qui est impossible. Les vérifications pour $p \in [5]_8$ et $p \in [7]_8$ sont du même style. $\square$

4.6.3 Théorème de Chevalley-Warning

Lemme 4.133.

Soit $\mathbb{K}$ un corps de caractéristique p et de cardinal q . Pour $m \in \mathbb{N}$ nous définissons

$$S_m = \sum_{x \in \mathbb{K}} x^m. \quad (4.263)$$

Alors nous avons

$$S_m \mod p = \begin{cases} -1 & \text{si } m \geq 1 \text{ et } m \text{ divisible par } q-1 \\ 0 & \text{sinon.} \end{cases} \quad (4.264)$$

Démonstration. Si $m = 0$, alors $x^0 = 1$ et $S_m = q$. Par conséquent $S_m \mod p = 0$ parce que la caractéristique d'un corps divise son ordre (proposition 3.27).

Nous prenons maintenant $m \geq 1$ et nous voyons séparément les cas où $q-1$ divise m ou non. Si $q-1$ divise m , alors pour tout $x \neq 0$ nous avons

$$x^m = x^{k(q-1)} = 1 \quad (4.265)$$

parce que $\mathbb{K}^*$ est cyclique et $x^{q-1} = 1$ par le petit théorème de Fermat (théorème 4.19). Par conséquent nous avons

$$\sum_{x \in \mathbb{K}} x^m = \sum_{x \in \mathbb{K}^*} 1 = q - 1. \quad (4.266)$$

Si le nombre $m \geq 1$ n'est pas divisible par $q - 1$ alors nous prenons un générateur y du groupe $\mathbb{K}^*$. Un tel élément vérifie $y^m \neq 1$. En effet, si y vérifiait $y^m = 1$ alors cela signifierait que l'ordre de $\mathbb{K}^*$ est un diviseur de m , ce qui n'est pas le cas ici parce que l'ordre de $\mathbb{K}^*$ est $q - 1$. Pour un tel y , l'application

$$\begin{aligned} \varphi: \mathbb{K}^* &\rightarrow \mathbb{K}^* \\ x &\mapsto yx \end{aligned} \quad (4.267)$$

est une bijection¹⁹. En ce qui concerne l'injectivité, $ya = yb$ implique $a = b$. En ce qui concerne la surjectivité, si a est un générateur, si $z = a^l$ et si $y = a^k$, alors

$$z = \varphi(a^{l-k}). \quad (4.268)$$

Nous pouvons maintenant faire le calcul.

$$S_m = \sum_{x \in \mathbb{K}^*} x^n = \sum_{x \in \mathbb{K}^*} (yx)^m = y^m \sum_{x \in \mathbb{K}^*} x^m = y^m S_m. \quad (4.269)$$

Étant donné que $y^m \neq 1$, la seule solution est $S_m = 0$. □

Théorème 4.134 (Chevalley-Waring).

Soit $\mathbb{K}$ un corps fini de cardinal q et de caractéristique p . Soient $P_1, \dots, P_r$ des éléments de $\mathbb{K}[X_1, \dots, X_n]$ tels que $\sum_{i=1}^r \deg(P_i) < n$. Nous considérons l'ensemble des zéros communs à tous les polynômes :

$$V = \{x \in \mathbb{K}^n \text{ tel que } P_1(x) = \dots = P_r(x) = 0\}. \quad (4.270)$$

Alors $\text{Card}(V) \equiv 0 \pmod{p}$.

Démonstration. Nous considérons le polynôme

$$P = \prod_{i=1}^r (1 - P_i^{q-1}). \quad (4.271)$$

Montrons que

$$P(x) = \begin{cases} 1 & \text{si } x \in V \\ 0 & \text{sinon.} \end{cases} \quad (4.272)$$

La première ligne est facile : étant donné que tous les $P_i(x)$ sont nuls pour $x \in V$, nous avons $P(x) = 1$. Si x n'est pas dans V , alors nous avons un i tel que $P_i(x) \in \mathbb{K}^*$. Mais dans ce cas (toujours la cyclicité de $\mathbb{K}^*$) nous avons $P_i(x)^{q-1} = 1$ et donc le produit est nul.

En utilisant l'hypothèse sur le degré des P_i , nous trouvons que

$$\deg(P) = \sum_{i=1}^r (q-1) \deg(P_i) < n(q-1). \quad (4.273)$$

Pour un polynôme $Q \in \mathbb{K}[X_1, \dots, X_n]$, nous définissons

$$\int Q = \sum_{x \in \mathbb{K}^n} Q(x). \quad (4.274)$$

Nous avons immédiatement

$$\int P = \sum_{x \in \mathbb{K}^n} P(x) = \sum_{x \in V} 1 = \text{Card}(V) \pmod{p}. \quad (4.275)$$

¹⁹. Notons que nous n'avons pas réellement besoin que y soit un générateur. Nous n'utilisons seulement le fait que $y^m \neq 1$ et $y \neq 0$.

Nous insistons sur le «modulo p » parce que dans la formule $P(x) = 1$, le membre de droite est le 1 de $\mathbb{K}$; il est donc automatiquement modulo la caractéristique de $\mathbb{K}$.

Il nous reste à prouver que $\int P = 0$. Pour cela nous décomposons

$$P = \sum_m c_m X_1^{m_1} \dots X_n^{m_n} \quad (4.276)$$

où la somme s'étend sur les $m \in \mathbb{N}^n$ tels que $c_m \neq 0$. Nous avons

$$\int P = \sum_{m \in \mathbb{N}^n} \sum_m c_m x_1^{m_1} \dots x_n^{m_n} \quad (4.277a)$$

$$= \sum_m c_m \left(\sum_{x \in \mathbb{K}^n} x_1^{m_1} \dots x_n^{m_n} \right) \quad (4.277b)$$

$$= \sum_m c_m S_{m_1} \dots S_{m_n}. \quad (4.277c)$$

Le terme de plus haut degré dans la décomposition (4.276) est celui du m tel que $\sum_i m_i$ est le plus grand, mais étant donné que nous savons que ce degré est plus petit que $n(q-1)$, nous avons pour tous les m entrant dans la somme que

$$\sum_{i=1}^n m_i < n(q-1). \quad (4.278)$$

En particulier pour tout $m \in \mathbb{N}^n$, il existe i tel que $m_i < q-1$, et dans ce cas $S_{m_i} = 0$. Donc tous les termes de la somme

$$\sum_{m \in \mathbb{N}^n} c_m S_{m_1} \dots S_{m_n} \quad (4.279)$$

ont un facteur nul. □

Corollaire 4.135.

Soit P_i des polynômes à n variables avec $\sum_{i=1}^r \deg(P_i) < n$. Si les P_i n'ont pas de termes constants, alors ils ont un zéro commun non trivial.

Démonstration. Nous reprenons les notations du théorème 4.134. Étant donné que les P_i n'ont pas de termes constants, $0 \in V$, mais $\text{Card}(V) = 0 \pmod{p}$. Par conséquent nous devons avoir $\text{Card}(V) > p$. □

Exemple 4.136

Nous considérons les polynômes

$$P_1(x, y, t, u) = xy + x + ux \quad (4.280a)$$

$$P_2(x, y, t, u) = x + y - 3t. \quad (4.280b)$$

La somme de leurs degrés est 3 et ce sont des polynômes à 4 variables. Nous devons donc avoir, en vertu du corollaire 4.135, des autres racines que la racine triviale $(x, y, t, u) = (0, 0, 0, 0)$.

Le corollaire nous donne aussi une borne inférieure nombre de racines à chercher : plus que la caractéristique du corps sur lequel nous travaillons. Nous pouvons dire cela sans avoir la moindre idée de la façon dont on pourrait résoudre le système $P_1 = P_2 = 0$. △

4.6.4 Théorème de l'élément primitif

Définition 4.137.

Soit $\mathbb{K}$ un corps. Une extension $\mathbb{L}$ de $\mathbb{K}$ est dite **finie** si $\mathbb{L}$ est un espace vectoriel de dimension finie sur $\mathbb{K}$.

Notez que la définition d'extension finie ne suppose ni que $\mathbb{K}$ ni que $\mathbb{L}$ soient finis en tant qu'ensembles.

Théorème 4.138 (de l'élément primitif).

Si $\mathbb{K}$ est un corps fini, toute extension finie de $\mathbb{K}$ est simple²⁰.

Si $\mathbb{K}$ est un corps quelconque alors toute extension séparable finie est simple.

Démonstration. Nous ne donnons la preuve que dans le cas où $\mathbb{K}$ est fini. Dans ce cas nous savons par la proposition 4.121 que le groupe $\mathbb{K}^*$ est cyclique. Si de plus $\mathbb{L}$ est une extension finie alors $\mathbb{L}$ est fini en tant qu'ensemble. Par conséquent $\mathbb{L}^*$ est un groupe cyclique. Si α est un générateur de $\mathbb{L}$ alors $\mathbb{L} = \mathbb{K}(\alpha)$ et l'extension est donc simple.

Une preuve de l'assertion dans le cas où $\mathbb{K}$ est infini peut être trouvée sur wikipédia. $\square$

Définition 4.139.

Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p[X]$. L'ordre de P est

$$\min\{k \text{ tel que } P \mid X^k - 1\}. \quad (4.281)$$

*Soit p , un nombre premier et P un polynôme unitaire irréductible de degré n dans $\mathbb{F}_p[X]$. Nous disons que P est **primitif** si les racines de P sont d'ordre $p^n - 1$ dans $\mathbb{F}_p[X]/P$.*

Remarque 4.140.

Si $\mathbb{A}$ est un anneau factoriel, il est souvent dit qu'un polynôme $P \in \mathbb{A}[X]$ est primitif si le pgcd de ses coefficients est 1. Cette notion de primitivité n'est apparemment pas reliée à celle de la définition 4.139 qui sera celle que nous retiendrons pour la suite. Notons au passage que dans un corps, tous les polynômes non nuls et unitaires sont primitifs au sens du pgcd des coefficients ; cette notions de primitivité n'a donc pas d'intérêt dans notre cadre.

Lorsque nous utiliserons la notion de polynôme primitif au sens du pgcd, nous le mentionnerons explicitement. C'est pas exemple le cas pour le théorème 3.100.

Proposition 4.141.

L'ordre d'un polynôme P vérifie les propriétés suivantes :

- (1) *L'ordre de P est l'ordre multiplicatif de ses racines*
- (2) *L'ordre de P divise $p^n - 1$.*

Lemme 4.142.

Soit p un nombre premier et P un polynôme irréductible unitaire de degré n . Si $\alpha, \beta \in \mathbb{F}_p[X]/P$, alors $(\alpha + \beta)^p = \alpha^p + \beta^p$.

Démonstration. La preuve est exactement la preuve classique :

$$(\alpha + \beta)^p = \sum_k \binom{p}{k} \alpha^k \beta^{p-k} \quad (4.282)$$

où les coefficients binomiaux sont dans $\mathbb{F}_p$ et donc nuls pour les k différents de p et de 0. $\square$

Cette proposition est encore vraie avec $\alpha, \beta \in \mathbb{F}_{p^n}$ et $(\alpha + \beta)^{p^n}$.

Lemme 4.143.

Si $\alpha \in \mathbb{F}_q$ est une racine d'ordre k de P (de degré n) alors les racines de $X^k - 1$ sont $\{\alpha^i \text{ tel que } i = 0, \dots, k-1\}$.

Nous serions donc intéressé à construire $\mathbb{F}_q$ comme quotient de $\mathbb{F}_p[X]$ par un polynôme primitif. Le théorème suivant donne une description abstraite de $\mathbb{F}_q$ qui va nous servir de point de départ pour la construction.

20. Définition 4.47.

Théorème 4.144 (Théorème de l'élément primitif).

Soit p un nombre premier, $n \in \mathbb{N}$ et $q = p^n$. Soit $\mathbb{K}$ un corps à q éléments. Alors

- (1) Il existe $\alpha \in \mathbb{K}$ tel que $\mathbb{K} = \mathbb{F}_p[\alpha]$.
- (2) Il existe une polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n tel que

$$\begin{aligned} \phi: \mathbb{F}_p[X]/(P) &\rightarrow \mathbb{K} \\ \bar{X} &\mapsto \alpha \end{aligned} \quad (4.283)$$

soit un isomorphisme de corps.

Soit α et P choisis pour avoir les propriétés citées plus haut. Alors nous avons les propriétés suivantes.

- (1) P est primitif.
- (2) P est scindé dans $\mathbb{K}$.
- (3) L'ensemble des racines de P est $\{\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}\}$.
- (4) Le polynôme P divise $X^q - X$ dans $\mathbb{F}_p[X]$.

Démonstration. Le corps $\mathbb{K}$ étant fini, il est cyclique par la proposition 4.121. Si α un générateur de $\mathbb{K}^*$ alors

$$\mathbb{K} = \mathbb{F}_p[\alpha]. \quad (4.284)$$

Soit ℓ le plus grand entier tel que l'ensemble

$$\{1, \alpha, \dots, \alpha^{\ell-1}\} \subset \mathbb{K} \quad (4.285)$$

soit libre. Pour rappel $\mathbb{K}$ est un espace vectoriel sur $\mathbb{F}_p$. Il existe des $a_i \in \mathbb{F}_p$ tels que

$$\alpha^\ell + a_{\ell-1}\alpha^{\ell-1} + \dots + a_0 = 0. \quad (4.286)$$

De façon équivalente, il existe un polynôme unitaire $P \in \mathbb{F}_p[X]$ de degré ℓ tel que $P(\alpha) = 0$. Étant donné que α est générateur de $\mathbb{K}$,

$$\mathbb{K} = \text{Span}\{1, \alpha, \dots, \alpha^{\ell-1}\} \quad (4.287)$$

parce que $\mathbb{K}$ est généré par les puissances de α alors que les puissances de α plus hautes que $\ell - 1$ peuvent être générées par $1, \alpha, \dots, \alpha^{\ell-1}$. L'espace $\mathbb{K}$ est donc un $\mathbb{F}_p$ -espace vectoriel de dimension ℓ ; par conséquent

$$\text{Card}(\mathbb{K}) = p^\ell = q \quad (4.288)$$

et $\ell = n$.

Montrons que P est irréductible dans $\mathbb{F}_p$. Si P était réductible dans $\mathbb{F}_p$, l'élément $\alpha \in \mathbb{K}$ serait une racine d'un des facteurs, c'est à dire qu'il serait racine d'un polynôme de degré inférieur à n , ce qui contredirait le fait que

$$\{\alpha^{\ell-1}, \dots, 1\} \quad (4.289)$$

est libre.

Montrons que l'application

$$\begin{aligned} \phi: \mathbb{F}_p[X]/(P) &\rightarrow \mathbb{K} \\ \bar{X} &\mapsto \alpha \end{aligned} \quad (4.290)$$

est un isomorphisme. Pour l'injectivité, deux éléments $Q_1, Q_2 \in \mathbb{F}_p[X]/(P)$ s'écrivent

$$Q_1 = \sum_{k=0}^{n-1} a_k \bar{X}^k \quad (4.291a)$$

$$Q_2 = \sum_{k=0}^{n-1} b_k \bar{X}^k. \quad (4.291b)$$

Dans ce cas si $\phi(Q_1) = \phi(Q_2)$ alors

$$\phi(Q_1) = \sum_{k=0}^{n-1} a_k \alpha^k = \phi(Q_2) = \sum_{k=0}^{n-1} b_k \alpha^k. \quad (4.292)$$

Mais l'ensemble $\{1, \alpha, \dots, \alpha^{n-1}\}$ étant libre sur $\mathbb{F}_p$, cela implique $a_k = b_k$. La surjectivité de ϕ provient du fait que α génère $\mathbb{K}$.

Nous passons maintenant à la seconde partie de la démonstration. Soient $\alpha \in \mathbb{K}$ tel que $\mathbb{K} = \mathbb{F}_p[\alpha]$ et $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n tel que $\alpha \mapsto \bar{X}$ soit un isomorphisme entre $\mathbb{K}$ et $\mathbb{F}_p[X]/(P)$.

Le polynôme P est primitif parce que α est d'ordre p^n dans $\mathbb{K}$ alors que $\bar{X} \mapsto \alpha$ est un isomorphisme. Par conséquent $\bar{X}$ est d'ordre p^n dans $\mathbb{F}_p[X]/(P)$.

Nous commençons par prouver que l'ensemble

$$\{\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{n-1}}\} \quad (4.293)$$

est l'ensemble des racines distinctes de P . Pour cela nous posons

$$P(X) = \sum_{k=0}^n a_k X^k \quad (4.294)$$

avec $a_k \in \mathbb{F}_p$. D'abord α est une racine de P . En effet

$$P(\bar{X}) = \sum_k a_k \bar{X}^k = 0 \quad (4.295)$$

parce que cette somme est calculée dans $\mathbb{F}_p[X]/(P)$. En appliquant l'isomorphisme ϕ à l'égalité (4.295) nous trouvons

$$0 = \phi(P(\bar{X})) = \sum_k a_k \phi(\bar{X}^k) = \sum_k a_k \alpha^k. \quad (4.296)$$

Donc α est bien une racine de P dans $\mathbb{F}_p[X]$. Nous devons montrer qu'il en est de même pour les autres puissances dans l'ensemble (4.293). Étant donné que pour tout x dans $\mathbb{F}_p$ nous avons $x^p = x$, nous avons aussi

$$P(X^p) = \sum_k a_k (X^p)^k = \sum_k a_k^p (X^p)^k = \sum_k (a_k X^k)^p \quad (4.297)$$

alors que nous savons que $x \mapsto x^p$ est un automorphisme de $\mathbb{F}_p$ par la proposition 3.31. Par conséquent

$$P(X^p) = \sum_k (a_k X^k)^p = \left(\sum_k a_k X^k \right)^p = P(X)^p. \quad (4.298)$$

Nous avons montré que si β est une racine de P , alors β^p est également une racine de P . Nous savons déjà que α est une racine de P , et que α est également générateur de $\mathbb{K}$, c'est à dire que α est d'ordre $q-1$. Les puissances

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{n-1}} \quad (4.299)$$

sont donc distinctes ($\alpha^{p^n} = \alpha^q = 1$) et sont toutes des racines de P . Étant donné que P est de degré n il ne peut pas y avoir d'autres racines. Nous concluons que l'ensemble

$$\{\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{n-1}}\} \quad (4.300)$$

est l'ensemble des racines distinctes de P dans $\mathbb{K}$. Le polynôme P est alors scindé dans $\mathbb{K}[X]$.

Le dernier point du théorème est de montrer que P divise $X^q - X$. Pour cela nous allons montrer que toutes les racines de P sont des racines de $X^q - X$. Soit β une racine de P ; il s'écrit

$\beta = \alpha^k$ pour un certain k . Étant donné que $\alpha^{q-1} = e = \alpha^{p^n-1}$,

$$\beta^q = (\alpha^{p^n})^k \quad (4.301a)$$

$$= (\alpha^{p^n-1}\alpha)^k \quad (4.301b)$$

$$= (\alpha^{q-1}\alpha)^k \quad (4.301c)$$

$$= \alpha^k \quad (4.301d)$$

$$= \beta. \quad (4.301e)$$

Cela signifie que $\beta^q = \beta$ et donc que β est racine de $X^q - X$. $\square$

Corollaire 4.145.

Le corps fini à $q = p^n$ éléments est de caractéristique p .

Démonstration. Nous considérons le corps fini $\mathbb{K}$ à q éléments sous la forme $\mathbb{K} = \mathbb{F}_p[X]/P$ comme indiqué par l'équation (4.283). Soit 1_q la classe du polynôme 1 modulo P , nous considérons le morphisme

$$\begin{aligned} \mu: \mathbb{Z} &\rightarrow \mathbb{F}_q \\ n &\mapsto n1_q. \end{aligned} \quad (4.302)$$

Le noyau de cette application est $\ker \mu = \mathbb{Z}_p$ parce que $p1_q = 0$, les coefficients étant à comprendre dans $\mathbb{F}_p$. $\square$

Définition 4.146.

Soit P , un polynôme de degré n et p , un nombre premier. Un élément $\alpha \in \mathbb{F}_p[X]/(P)$ est une **racine primitive** si les puissances de α parcourent tout le groupe multiplicatif $(\mathbb{F}_p[X]/P)^*$.

Lemme 4.147.

Soit p un nombre premier et P , un polynôme de degré n . Si $\alpha \in \mathbb{F}_p[X]/P$ est une racine primitive de P alors les autres racines de P sont également primitives.

Démonstration. Soit $\alpha \in \mathbb{F}_p[X]/P$ une racine primitive de P . L'élément α^p est également une racine parce que si $P = \sum_k a_k X^k$,

$$P(\alpha^p) = \sum_k (a_k \alpha^k)^p = \left(\sum_k a_k \alpha^k \right)^p = 0 \quad (4.303)$$

où nous avons utilisé le fait que $a_k^p = a_k$ étant donné que $a_k \in \mathbb{F}_p$. Par hypothèse α est une racine primitive; cela implique que les éléments $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^n-1}$ sont distincts dans $\mathbb{F}_p[X]/P$. Ces éléments constituent donc toutes les racines de P .

Soit $\beta = \alpha^{p^k}$ une racine de P . Montrons que α est une puissance de β . Étant donné que $(\mathbb{F}_p[X]/P)^*$ est un groupe à $p^n - 1$ éléments, le corollaire 2.40 indique que $\alpha^{p^n} = \alpha$. En particulier avec $r = p^n - k$ nous avons

$$\beta^r = \alpha^{rp^k} = \alpha^{p^n} = \alpha. \quad (4.304)$$

Par suite toutes les puissances de α sont des puissances de β , ce qui implique que β est générateur du groupe cyclique $(\mathbb{F}_p[X]/P)^*$. $\square$

Lemme 4.148.

Soit p un nombre premier et n , un entier. Un polynôme de degré d irréductible dans $\mathbb{F}_p[X]$ divise $X^{p^n} - X$ si et seulement si d divise n .

Théorème 4.149.

Soient P et Q deux polynômes irréductibles de degré n dans $\mathbb{F}_p[X]$. Alors les quotients $\mathbb{F}_p[X]/P$ et $\mathbb{F}_p[X]/Q$ sont isomorphes en tant que corps.

En guise de démonstration de ce théorème, nous allons démontrer la proposition suivante.

Proposition 4.150.

Si $\mathbb{K}$ et $\mathbb{L}$ sont deux corps à $q = p^n$ éléments, alors ils sont isomorphes.

Démonstration. Soit a un élément primitif de $\mathbb{K}$ et P son polynôme minimal. Nous savons que $\mathbb{K} \simeq \mathbb{F}_p[X]/P$ par le théorème de l'élément primitif 4.144. L'élément a est en particulier une racine de $X^q - X$. Par ailleurs P divise $X^q - X$ par le lemme 4.148.

Nous avons aussi

$$X^q - X = \prod_{b \in \mathbb{L}} (X - b) \quad (4.305)$$

par la proposition 4.123. Étant donné que P divise $X^q - X$, un des éléments de $\mathbb{L}$ annule P . Soit $b \in \mathbb{L}$ tel que $P(b) = 0$. Soit Q le polynôme minimal de b . Par définition nous avons que Q divise P , mais P étant irréductible et unitaire nous avons immédiatement $P = Q$. En particulier nous avons

$$\mathbb{F}_p[X]/P \simeq \mathbb{F}_p[X]/Q \simeq \mathbb{K}. \quad (4.306)$$

Nous montrons maintenant que $\mathbb{F}_p[X]/Q \simeq \mathbb{L}$ par l'application

$$\begin{aligned} \phi: \mathbb{F}_p[X]/Q &\rightarrow \mathbb{L} \\ \bar{X} &\mapsto b \end{aligned} \quad (4.307)$$

qui se prolonge en $R(\bar{X}) \mapsto R(b)$ pour tout $R \in \mathbb{F}_p[X]$. Cette application est bien définie parce que $Q(b) = 0$. Elle est injective parce que $R(b) = 0$ ne peut pas avoir lieu avec $R \in \mathbb{F}_p[X]/Q$ parce que Q est le polynôme minimal de b . La surjectivité vient alors du fait que les deux corps ont le même nombre d'éléments. $\square$

4.6.5 Construction de $\mathbb{F}_q$

Soit p un nombre premier et $n \in \mathbb{N}$. Nous souhaitons construire un corps à $q = p^n$ éléments. Nous savons déjà que ce corps est unique (théorème 4.120) et que nous le notons $\mathbb{F}_q$. Le théorème 4.144 nous incite à l'écrire sous la forme

$$\mathbb{F}_q = \mathbb{F}_p[X]/(P) \quad (4.308)$$

pour un certain polynôme irréductible $P \in \mathbb{F}_p[X]$.

4.6.5.1 La version du faignant

Nous pouvons construire le corps à p^n éléments en prenant le quotient de $\mathbb{F}_p[X]$ par n'importe quel polynôme irréductible de degré n . Le résultat est le suivant.

Proposition 4.151.

Soit P une polynôme unitaire irréductible dans $\mathbb{F}_p[X]$. Nous posons $\mathbb{K} = \mathbb{F}_p[X]/(P)$. Alors

- (1) $\mathbb{K}$ est un corps à q éléments.
- (2) $\alpha = \bar{X}$ est une racine de P dans $\mathbb{K}$.
- (3) $\mathbb{K} = \mathbb{F}_p[\alpha]$.

Démonstration. (1) En vertu du corollaire 4.34, $\mathbb{K}$ est un corps. Il est aussi un espace vectoriel de dimension n sur $\mathbb{F}_p$, et contient donc $p^n = q$ éléments.

(2) Nous avons $P(\bar{X}) = 0$ par construction de $\mathbb{K} = \mathbb{F}_p[X]/(P)$.

(3) En tant que quotient de $\mathbb{F}_p[X]$, les éléments de $\mathbb{K}$ sont des polynômes en $\bar{X}$. $\square$

4.6.5.2 La version plus élaborée

Construire $\mathbb{F}_q$ comme quotient de $\mathbb{F}_p[X]$ par un polynôme irréductible quelconque ne donne pas d'informations sur les générateurs de $\mathbb{F}_q^*$, et en particulier il n'est pas toujours vrai que $\bar{X}$ est générateur.

Exemple 4.152

Construisons $\mathbb{F}_4$. Le polynôme $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2$ parce qu'il n'a pas de racines (c'est vite vu : dans $\mathbb{F}_2$ il n'y a que deux candidats). Donc $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$. $\triangle$

Remarque 4.153.

Le corps $\mathbb{F}_2$ n'est pas un sous-corps de $\mathbb{C}$ parce que leurs caractéristiques ne sont pas les mêmes. Une conséquence est que les racines de polynômes peuvent être très différentes. Par exemple le polynôme $X^2 + 1$ accepte $x = 1$ comme racine dans $\mathbb{F}_2$ tandis qu'il a pour racines $\pm i$ dans $\mathbb{C}$.

En changeant de corps, les racines peuvent donc complètement changer. Ce n'est pas juste qu'il y a des racines dans l'un et pas dans l'autre.

Exemple 4.154

Cherchons à construire $\mathbb{F}_{16}$ comme quotient de $\mathbb{F}_2$ par un polynôme de degré 4.

```
-----
| Sage Version 4.7.1, Release Date: 2011-08-11                |
| Type notebook() for the GUI, and license() for information. |
|-----|
sage: x=polygen(GF(2))
sage: -x-1
x + 1
sage: Q=x**15-1
sage: Q.factor()
(x + 1) * (x^2 + x + 1) * (x^4 + x + 1) * (x^4 + x^3 + 1) * (x^4 + x^3 + x^2 + x + 1)
```

Les polynômes candidats à avoir des racines génératrices sont donc au nombre de 3 :

$$P_1 = X^4 + X + 1 \quad (4.309a)$$

$$P_2 = X^4 + X^3 + 1 \quad (4.309b)$$

$$P_3 = X^4 + X^3 + X^2 + X + 1. \quad (4.309c)$$

Dans le quotient $\mathbb{F}_2[X]/P_3$, l'élément $\bar{X}$ n'est pas générateur. En effet nous avons $X^4 = X^3 + X^2 + X + 1$ et par conséquent les puissances successives de X sont

$$X \quad (4.310a)$$

$$X^2 \quad (4.310b)$$

$$X^3 \quad (4.310c)$$

$$X^4 = X^3 + X^2 + X + 1 \quad (4.310d)$$

$$1. \quad (4.310e)$$

La classe de X dans $\mathbb{F}_2[X]/P_3$ n'est donc pas génératrice du groupe $(\mathbb{F}_2[X]/P_3)^*$.

Le polynôme $P_1 = X^4 + X + 1$ par contre est primitif parce que les puissances de X dans

$\mathbb{F}_2[X]/P_1$ sont

$$X \quad (4.311a)$$

$$X^2 \quad (4.311b)$$

$$X^3 \quad (4.311c)$$

$$X + 1 \quad (4.311d)$$

$$X^2 + X \quad (4.311e)$$

$$X^3 + X^2 \quad (4.311f)$$

$$X + 1 + X^3 \quad (4.311g)$$

$$X^2 + 1 \quad (4.311h)$$

$$X^3 + X \quad (4.311i)$$

$$X + 1 + X^2 \quad (4.311j)$$

$$X^2 + X + X^3 \quad (4.311k)$$

$$X^3 + X^2 + X + 1 \quad (4.311l)$$

$$1 + X^2 + X^2 \quad (4.311m)$$

$$1 + X^3 \quad (4.311n)$$

$$1 \quad (4.311o)$$

Cela fait 15 puissances distinctes, ce qui prouve que P_1 est primitif. Nous verrons plus loin comment alléger un peu la vérification de la primitivité de P_1 . $\triangle$

Proposition 4.155.

Soit P un polynôme irréductible unitaire primitif dans $\mathbb{F}_p[X]$. Nous considérons $\mathbb{K} = \mathbb{F}_p[X]/P$ et $\alpha = \bar{X} \in \mathbb{K}$. Alors

(1) Les racines de P sont $\{\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}\}$ et $\alpha^q = \alpha$.

(2) P est le polynôme minimal de α .

(3) P est scindé dans $\mathbb{K}$.

(4) P divise $X^q - X$ dans $\mathbb{K}$.

(5) La famille $\{1, \alpha, \alpha^2, \dots, \alpha^{q-1}\}$ est une base de $\mathbb{K}$ en tant qu'espace vectoriel sur $\mathbb{F}_p$.

(6) En tant qu'ensemble,

$$\mathbb{F}_q = \{0, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{q-1}\}, \quad (4.312)$$

et les α^k sont distincts pour $k = 1, \dots, q-1$.

Démonstration. La plupart des assertions sont des corollaires ou des paraphrases de résultats contenus dans les propositions précédentes.

- (1) L'assertion à propos des racines de P est contenue dans le lemme 4.147. D'autre part le groupe $(\mathbb{F}_p[X]/P)^*$ est cyclique d'ordre $q-1$. Par conséquent le corollaire 2.40 indique que $\alpha^{q-1} = 1$ et donc $\alpha^q = \alpha$.
- (2) Soit $\tilde{P}$ un polynôme annulateur de α . Nous voyons que si β est racine de $\tilde{P}$ alors β^p est également racine de $\tilde{P}$ en utilisant les techniques habituelles. Par conséquent toutes les racines de P sont racines de $\tilde{P}$, ce qui implique que $\tilde{P}$ est de degré au moins égal à celui de P .
- (3) Possédant n racines distinctes dans $\mathbb{K}$, le polynôme P est scindé.
- (4) D'après le lemme 4.123 un polynôme irréductible de degré n divise le polynôme $X^{p^n} - X$. Une autre façon de montrer ce point est de remarquer que le polynôme P est scindé et que toutes ses racines sont également racines de $X^q - X$.

- (5) Une combinaison linéaire nulle entre les éléments de $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ serait un polynôme annulateur de degré $n-1$ de α . Cet ensemble est donc libre. Par ailleurs un ensemble libre de n éléments dans un espace vectoriel de dimension n est générateur.
- (6) Si $\alpha^l = \alpha^k$ avec $k < l$ et $k, l \leq q$ alors nous avons $\alpha^r = 1$ avec $r = l - k < q$, ce qui contredirait la primitivité de P . Les éléments $0, \alpha, \dots, \alpha^{q-1}$ étant distincts et au nombre de q , ils forment tout l'ensemble $\mathbb{F}_q$.

□

4.6.6 Exemple : étude de $\mathbb{F}_{16}$

Dans cette sous section nous voulons construire $\mathbb{F}_{16}$. Nous considérons donc $p = 2$ et $n = 4$. Des polynôme irréductibles de degré 4 dans $\mathbb{F}_2[X]$ ne sont pas très difficiles à trouver. Par exemple $X^4 + X^3 + X^2 + X + 1$, plus généralement un polynôme contenant un nombre impair de termes non nuls dont le terme indépendant.

Les polynômes primitifs par contre doivent être trouvés parmi les diviseurs irréductibles de $X^{15} - 1$. Montrons que

$$P = X^4 + X^3 + 1 \quad (4.313)$$

est primitif. Nous posons $\omega = \bar{X} \in \mathbb{F}_2[X]/P$. L'ordre de ω dans le groupe $(\mathbb{F}_2[X]/P)^*$ doit être un diviseur de 15 et donc seulement 1, 3, 5 ou 15. Le fait que l'ordre ne soit ni 1 ni 3 est trivial parce que le degré de P est 4. Montrons que l'ordre de ω n'est pas 5 non plus :

$$\omega^5 = \omega^4 \omega = (\omega^3 + 1)\omega = \omega^4 + \omega = \omega^3 + \omega + 1 \neq 1. \quad (4.314)$$

Dans ce calcul nous avons abondamment utilisé le fait que $-1 = 1$.

À partir de maintenant nous posons $\mathbb{K} = \mathbb{F}_2[X]/P$. Les racines de P sont $\omega, \omega^2, \omega^4$ et ω^8 . En effet si β est une racine de P , alors β^2 est une racine en vertu de

$$P(\beta^2) = (\beta^2)^4 + (\beta^2)^3 + 1 = (\beta^4)^2 + (\beta^3)^2 + 1^2 = (\beta^4 + \beta^3 + 1)^2 = 0. \quad (4.315)$$

Ici nous avons implicitement utilisé le lemme 4.142. D'autre part P ne peut pas avoir plus de 4 racines.

Proposition 4.156.

L'ensemble $\{\omega, \omega^2, \omega^4, \omega^8\}$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.

Démonstration. Nous savons que $\{1, \omega, \omega^2, \omega^3\}$ est une base. En effet cet ensemble est libre (sinon ω aurait un polynôme annulateur de degré 3) et générateur parce que l'espace engendré par 4 vecteurs indépendants sur $\mathbb{F}_2$ contient $2^4 = 16$ éléments.

Nous posons $e_0 = 1, e_1 = \omega, e_2 = \omega^2, e_3 = \omega^3$ et $f_1 = \omega, f_2 = \omega^2, f_3 = \omega^4, f_4 = \omega^8$. En utilisant le calcul modulo $\omega^4 + \omega^3 + 1 = 0$ et $2 = 0$ nous trouvons

$$f_1 = \omega \quad (4.316a)$$

$$f_2 = \omega^2 \quad (4.316b)$$

$$f_3 = \omega^3 + 1 \quad (4.316c)$$

$$f_4 = \omega^3 + \omega^2 + \omega. \quad (4.316d)$$

Ensuite nous montrons que les vecteurs e_i peuvent être construits comme combinaisons linéaires des vecteurs f_j :

$$f_1 + f_2 + f_3 + f_4 = e_0 \quad (4.317a)$$

$$f_1 = e_1 \quad (4.317b)$$

$$f_2 = e_2 \quad (4.317c)$$

$$f_1 + f_2 + f_4 = e_3. \quad (4.317d)$$

Les quatre vecteurs f_j forment donc bien une base parce qu'ils sont générateurs d'un espace de dimension 4. □

Exemple 4.157

- (1) Résoudre dans $\mathbb{F}_{16}$ l'équation $x^5 = a$ en discutant éventuellement en fonction de la valeur de a .
- (2) Montrer qu'il existe quatre éléments $\gamma \in \mathbb{F}_{16}$ tels que pour chacun d'eux l'ensemble $B_\gamma = \{\gamma, \gamma^2, \gamma^4, \gamma^8\}$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ telle que le produit de deux éléments de B_γ est soit un élément de B_γ soit 1.

C'est parti !

- (1) Si $a = 0$, alors $x = 0$ est la seule solution. Si $a \neq 0$ alors a est une puissance de ω ; nous posons $a = \omega^l$. Nous cherchons x sous la forme $x = \omega^k$. L'équation à résoudre pour k est

$$\omega^{5k} = \omega^l \quad (4.318)$$

où l est donné. Cette équation revient à

$$5k = l \pmod{15}. \quad (4.319)$$

Si l n'est pas un multiple de 5, alors il n'y a pas de solutions. Il n'y a des solutions uniquement pour $l = 0, 5, 10$ et elles sont :

$$k = \begin{cases} 3, 6, 9, 12 & \text{si } l=0 \\ 1 & \text{si } l=5 \\ 2 & \text{si } l=10 \end{cases} \quad (4.320)$$

- (2) Nous cherchons γ sous la forme $\gamma = \omega^k$. Parmi les nombreuses contraintes liées à l'énoncé nous devons avoir

$$\gamma^5 = 1, \gamma, \gamma^2, \gamma^4, \gamma^8. \quad (4.321)$$

Les possibilités $\gamma^5 = \gamma, \gamma^2, \gamma^4, \gamma^8$ ne sont pas bonnes parce qu'elles impliqueraient que B_γ n'est pas une base. Reste à explorer $\gamma^5 = 1$.

Étant donné le premier point nous restons avec les possibilités

$$\gamma = 1, \omega^3, \omega^6, \omega^9, \omega^{12}. \quad (4.322)$$

Évidemment $\gamma = 1$ ne produit pas une base. Avec $\gamma = \omega^3$ nous trouvons

$$B_\gamma = \{\omega^3, \omega^6, \omega^{12}, \omega^{24}\} = \{\omega^3, \omega^6, \omega^{12}, \omega^9\} \quad (4.323)$$

où nous avons utilisé le fait que $\omega^k = \omega^{k \pmod{15}}$. En utilisant le fait que $\omega^4 = \omega^3 + 1$ nous trouvons

$$\omega^5 = \omega^3 + \omega + 1 \quad (4.324a)$$

$$\omega^6 = \omega^3 + \omega^2 + \omega + 1 \quad (4.324b)$$

$$\omega^9 = \omega^2 + 1 \quad (4.324c)$$

$$\omega^{12} = \omega + 1. \quad (4.324d)$$

L'ensemble B_γ est alors formé des éléments

$$f_1 = \omega^3 \quad (4.325a)$$

$$f_2 = \omega^3 + \omega^2 + \omega + 1 \quad (4.325b)$$

$$f_3 = \omega + 1 \quad (4.325c)$$

$$f_4 = \omega^2 + 1. \quad (4.325d)$$

Il est assez simple de vérifier que cela est une base en remarquant que $f_1 + f_2 + f_3 + f_4 = 1$. Les possibilités $\gamma = \omega^6, \omega^9, \omega^{12}$ produisent les mêmes ensemble B_γ .

△

4.6.7 Polynômes irréductibles sur $\mathbb{F}_q$

Définition 4.158.

La fonction de Möbius est la fonction $\mu: \mathbb{N}^* \rightarrow \{-1, 0, 1\}$ définie par

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par un carré différent de } 1, \\ 1 & \text{si } n \text{ est le produit d'un nombre pair de nombres premiers distincts,} \\ -1 & \text{si } n \text{ est le produit d'un nombre impair de nombres premiers distincts,} \end{cases} \quad (4.326)$$

Proposition 4.159 ([53]).

Si m et n sont strictement positifs et premiers entre eux, alors

$$\mu(mn) = \mu(m)\mu(n). \quad (4.327)$$

De plus nous avons

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases} \quad (4.328)$$

Proposition 4.160 (Formule d'inversion de Möbius[53]).

Soient $f, g: \mathbb{N} \rightarrow \mathbb{C}$ telles que pour tout $n \geq 1$,

$$g(n) = \sum_{d|n} f(d). \quad (4.329)$$

Alors

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) \quad (4.330)$$

où μ est la fonction de Möbius pour tout $n \geq 1$.

Lemme 4.161 ([54]).

Soient $P, Q \in \mathbb{K}[X]$ ayant une racine commune dans une extension $\mathbb{L}$ de $\mathbb{K}$. Si P est irréductible, alors $P \mid Q$.

Démonstration. Si P ne divise pas Q , alors P et Q sont premiers entre eux parce que dans la décomposition en irréductibles de Q , il n'y a pas de P tandis que dans celle de P , il n'y a que P . Par conséquent, il existe $a, b \in \mathbb{K} \subset \mathbb{L}$ tels que²¹ $aP + bQ = 1$. Cette dernière égalité est encore valable dans $\mathbb{L}$ et donc rend impossible l'existence d'une racine commune. $\square$

Proposition 4.162 ([54, 1]).

Soit p un nombre premier, $n \geq 1$ et $r \in \mathbb{N}^*$. Nous notons $q = p^r$, $A(n, q)$, l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_q$. Nous notons aussi $I(n, q) = \text{Card}(A(n, q))$. Alors :

(1) Le polynôme $X^{q^n} - X$ se décompose en irréductibles de la façon suivante :

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d, q)} P. \quad (4.331)$$

(2) Le nombre d'irréductibles est donné par

$$I(n, q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \quad (4.332)$$

où μ est la fonction de Möbius (définition 4.158).

(3) Nous avons l'équivalence de suite

$$I(n, q) \sim_{n \rightarrow \infty} \frac{q^n}{n}. \quad (4.333)$$

21. Théorème de Bézout, 3.105.

Démonstration. (1) Soit un diviseur d de n et $P \in A(d, q)$. Montrons que P divise $X^{q^n} - X$. Nous considérons la corps $\mathbb{K} = \mathbb{F}_q[X]/(P)$, qui est une extension de degré $\deg(P)$ de $\mathbb{F}_q$ parce qu'il s'agit des polynômes de degré au maximum $\deg(P)$ à coefficients dans $\mathbb{F}_q$. Ce corps possède donc q^d éléments et est isomorphe à $\mathbb{F}_{q^d}$ par la proposition 4.150. Par construction dans $\mathbb{K}$, l'élément $\alpha = [X]$ (la classe de X dans le quotient par P) est une racine de P . Cet élément est également une racine de $X^{q^d} - X$ parce que tout élément de $\mathbb{F}_{q^d}$ est une racine de ce polynôme. Ce dernier point est la proposition 4.123.

Nous sommes donc dans la situation où P et $X^{q^d} - X$ ont une racine commune dans l'extension $\mathbb{F}_q[X]/(P)$. Nous en déduisons que α est aussi une racine de $X^{q^n} - X$. En effet en utilisant le fait que $\alpha^{q^d} = \alpha$, nous avons

$$\alpha^{q^n} = \alpha^{q^{kd}} = \alpha^{q^d q^{(k-1)d}} = \left(\alpha^{q^d}\right)^{q^{(k-1)d}} = \alpha^{q^{(k-1)d}}, \quad (4.334)$$

donc par récurrence, on a encore $\alpha^{q^n} = \alpha$, et α est racine de $X^{q^n} - X$. Vu que P est irréductible, le lemme 4.161 nous indique que P divise $X^{q^n} - X$. Nous en déduisons que P divise $X^{q^n} - X$.

Étant donné que tous les éléments de $A(d, q)$ divisent $X^{q^n} - X$ et sont irréductibles, leur produit divise encore $X^{q^n} - X$:

$$\prod_{d|n} \prod_{P \in A(d, q)} P \mid X^{q^n} - X. \quad (4.335)$$

Nous devons à présent montrer que tous les facteurs irréductibles de $X^{q^n} - X$ sont dans un $A(d, q)$ avec $d \mid n$. Soit donc P un facteur irréductible de $X^{q^n} - X$ de degré $d \geq 1$. Nous posons encore $\mathbb{K} = \mathbb{F}_q[X]/(P)$ et nous utilisons la propriété de multiplication sur les degrés (proposition 4.45) :

$$[\mathbb{F}_{q^n} : \mathbb{K}][\mathbb{K} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n, \quad (4.336)$$

donc $[\mathbb{K} : \mathbb{F}_q]$, qui vaut $\deg(P)$ est un diviseur de n .

Étant donné que $X^{q^n} - X$ n'a que des racines simples sur $\mathbb{F}_{q^n}$ (à nouveau la proposition 4.123), dans sa décomposition en irréductibles sur $\mathbb{F}_q$, il n'a pas de facteurs carrés ; il n'a donc qu'une fois chacun des $P \in A(d, q)$ avec $d \mid n$. Autrement dit, tous les facteurs irréductibles de $X^{q^n} - X$ sont dans le produit $\prod_{d|n} \prod_{P \in A(d, q)} P$ et donc $X^{q^n} - X$ divise ce gros produit :

$$X^{q^n} - X \mid \prod_{d|n} \prod_{P \in A(d, q)} P. \quad (4.337)$$

Ayant déjà obtenu la divisibilité inverse et les polynômes étant unitaires, nous avons égalité.

(2) Nous passons au degré dans l'expression que nous venons de démontrer :

$$q^n = \sum_{d|n} d \operatorname{Card}(A(d, q)) = \sum_{d|n} dI(d, q). \quad (4.338)$$

Nous pouvons utiliser la formule d'inversion de Möbius (proposition 4.160) pour les fonctions $g(n) = q^n$ et $f(n) = dI(n, q)$. Nous écrivons alors

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d, \quad (4.339)$$

ou encore

$$I(n, q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d, \quad (4.340)$$

ce qu'il fallait.

(3) Nous posons

$$r_n = \sum_{\substack{d|n \\ d < n}} \mu\left(\frac{n}{d}\right) q^d, \quad (4.341)$$

mais sachant que les diviseurs de n , outre n lui-même, sont tous plus petit ou égal à $n/2$ et qu'en valeur absolue, la fonction de Möbius est toujours plus petite ou égale à ²² 1,

$$|r_n| \leq \sum_{d=1}^{\lfloor n/2 \rfloor} q^d = \frac{q - q^{\lfloor n/2 \rfloor + 1}}{1 - q} = q \frac{q^{\lfloor n/2 \rfloor} - 1}{q - 1} \leq \frac{q^{\lfloor n/2 \rfloor + 1}}{q - 1}. \quad (4.342)$$

D'autre part en reprenant la formule déjà prouvée,

$$I(n, q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \left(r_n + \mu\left(\frac{n}{n}\right) q^n \right) = \frac{r_n + q^n}{n}. \quad (4.343)$$

Au numérateur, le plus haut degré en n est q^n parce que r_n est en $q^{\lfloor n/2 \rfloor}$. Donc nous avons bien l'équivalence de suite pour $n \rightarrow \infty$:

$$\frac{q^n + r_n}{n} \sim_{n \rightarrow \infty} \frac{q^n}{n}. \quad (4.344)$$

□

4.7 Constructions à la règle et au compas

Définition 4.163 ([55]).

Soit E une partie de $\mathbb{R}^2$. Un point de $\mathbb{R}^2$ est *constructible* en une étape à partir de E si il est une point de E ou une intersection de deux objets parmi

- les droites passant par deux points distincts de E ;
- les cercles centrés en un point de E et dont le rayon est la distance entre deux points de E .

Nous notons $C_1(E)$ l'ensemble des points constructibles en une étape à partir de E .

Les points constructibles en n étapes à partir de E sont définis par récurrence : $C_{n+1}(E) = C_1(C_n(E))$. Enfin un point de $\mathbb{R}^2$ est **constructible** à partir de E si il appartient à

$$C(E) = \bigcup_{n=1}^{\infty} C_n(E). \quad (4.345)$$

Un réel est **constructible** si il est l'abscisse d'un point constructible.

Pour toute la suite nous allons considérer les points et réels constructibles à partir de l'ensemble $E = \{(0, 0), (0, 1)\}$.

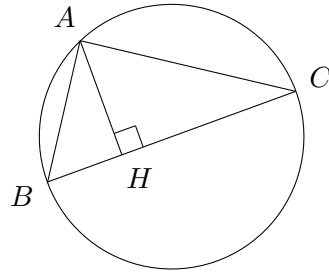
4.7.1 Quelques constructions

Proposition 4.164 ([56]).

Les nombres rationnels sont tous constructibles.

Démonstration. Si le réel r est constructible, alors kr est également constructible pour tout $k \in \mathbb{Z}$. Nous devons donc seulement pouvoir construire le nombre $1/n$ pour tout $n \in \mathbb{N}^*$.

²². Dans [1], ma dernière inégalité arrive comme une égalité.

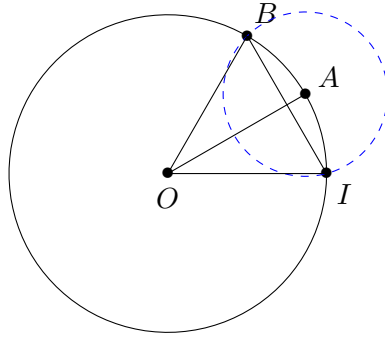


△

Exemple 4.167(Duplication d'un angle)

Si un angle α est constructible, nous allons construire les angles 2α , 3α , etc. Pour cela nous considérons un cercle de centre O et les points A et I sur le cercle tels que $\widehat{AOI} = \alpha$. Le cercle de centre A et de rayon AI intersecte le cercle de départ en les points I et B .

Le point A est à égale distance de B et I ; le point O également. Donc la droite (OA) est médiatrice du segment $[BI]$. Par conséquent elle est la hauteur du triangle isocèle OBI . L'angle $\widehat{BOA}$ est alors le même que $\widehat{AOI}$; par conséquent $\widehat{BOI} = 2\alpha$.



En traçant le cercle de centre B et de rayon BA , nous continuons et nous construisons 3α .

△

L'exemple suivant qui permet d'additionner des angles repose sur le fait que deux cordes de mêmes longueurs sous-tendent des angles égaux, et est une adaptation simple de la duplication d'angle.

Exemple 4.168(Addition d'angles)

Quitte à soustraire ou additionner un certain nombre de fois 90° , nous supposons que les deux angles donnés sont entre 0° et 90° .

Soient A, B, I sur un cercle de centre O , et nous notons $\alpha = \widehat{OAI}$, $\beta = \widehat{BOI}$. Nous traçons le cercle de centre B et de rayon AI ; il intersecte le cercle en des points K_1 et K_2 . Les angles $\widehat{K_1OB}$ et $\widehat{K_2OB}$ sont tout deux égaux à α .

Les angles $\widehat{K_1OA}$ et $\widehat{K_2OA}$ sont égaux à $\beta - \alpha$ et $\beta + \alpha$.

△

4.7.2 Nombres constructibles**Théorème 4.169** (Wantzel[57]).

Le réel a est constructible si et seulement si il existe une suite finie de corps $\mathbb{L}_i$ tels que

- (1) $\mathbb{L}_0 = \mathbb{Q}$,
- (2) $\mathbb{L}_{i+1}$ est une extension quadratique²³ de $\mathbb{L}_i$

23. C'est à dire une extension finie de degré 2.

(3) $a \in \mathbb{L}_n$.

Démonstration. Soit $\mathbb{K}$ un corps de nombres constructibles (par exemple $\mathbb{Q}$) ; nous notons $E_{\mathbb{K}}$ l'ensemble des points de $\mathbb{R}^2$ dont les coordonnées sont dans $\mathbb{K}$. Ce sont des points forcément constructibles.

Intersection de droites Si $A, B \in E_{\mathbb{K}}$ alors la droite (AB) a pour équation $ax + by + c = 0$ avec $a, b, c \in \mathbb{K}$, et le point d'intersection entre deux droites est donné par la solution du système

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0, \end{cases} \quad (4.347a)$$

$$(4.347b)$$

dont les solutions sont encore dans $\mathbb{K}$.

Intersection droite-cercle L'équation d'un cercle est de la forme

$$(x - u)^2 + (y - v)^2 = r^2 \quad (4.348)$$

où $(u, v) \in E_{\mathbb{K}}$ et r est la distance entre deux points de $E_{\mathbb{K}}$; donc $r^2 \in \mathbb{K}$. En développant et en redéfinissant u, v nous voyons que tous les cercles à considérer ont une équation de la forme

$$x^2 + y^2 + ux + vy + t = 0 \quad (4.349)$$

avec $u, v, t \in \mathbb{K}$. Il s'agit de voir où sont les solutions du système

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + ux + vy + t = 0. \end{cases} \quad (4.350a)$$

$$(4.350b)$$

Si $a \neq 0$ alors nous pouvons faire la substitution $x = -(c + by)/a$ et obtenir l'équation suivante pour y :

$$\left(\frac{-c - by}{a}\right)^2 + y^2 + u\left(\frac{-c - by}{a}\right) + vy + t = 0. \quad (4.351)$$

Cela est de la forme $P(y) = 0$ où P est un polynôme du second degré à coefficients dans $\mathbb{K}$. Si $a = 0$ nous substituons y au lieu de x et le résultat est le même.

C'est le moment de relire la proposition 4.65 qui nous assure que si le réel α est une solution de $P(y) = 0$ hors de $\mathbb{K}$, alors l'extension $\mathbb{K}(\alpha)$ est de degré 2 parce que le polynôme minimal de α est de degré 2 :

$$[\mathbb{K}[\alpha] : \mathbb{K}] = 2. \quad (4.352)$$

De plus $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

Intersection cercle-cercle Le système

$$\begin{cases} x^2 + y^2 + ux + vy + y = 0 \\ x^2 + y^2 + ax + by + c = 0 \end{cases} \quad (4.353a)$$

$$(4.353b)$$

est équivalent au système (en substituant la seconde équation par la différence entre les deux)

$$\begin{cases} x^2 + y^2 + ux + vy + y = 0 \\ (u - a)x + (v - b)y + t - c = 0 \end{cases} \quad (4.354a)$$

$$(4.354b)$$

qui est à nouveau une intersection entre un cercle et une droite.

Passons à la conclusion. Si α est un nombre constructible, alors il apparaît dans les coordonnées d'un point de $C_m(E_{\mathbb{Q}})$ pour un certain m . Nous supposons (pour la récurrence) que pour chaque réel constructible en $m - 1$ étapes possède sa pile d'extension quadratiques en partant de $\mathbb{Q}$. Le nombre α vérifie donc

$$a\alpha^2 + b\alpha + c = 0 \quad (4.355)$$

avec a, b, c trois réels constructibles en $m - 1$ étapes. L'hypothèse de récurrence donne donc des piles d'extensions

$$\begin{array}{lll} \mathbb{L}_0 = \mathbb{Q} & \mathbb{L}'_0 = \mathbb{Q} & \mathbb{L}''_0 = \mathbb{Q} \\ L_{i+1} = \mathbb{L}_i(a_i) & \mathbb{L}'_{i+1} = \mathbb{L}'_i(b_i) & \mathbb{L}''_{i+1} = \mathbb{L}''_i(c_i) \\ a \in \mathbb{L}_n & b \in \mathbb{L}'_{n'} & c \in \mathbb{L}''_{n''}. \end{array} \quad (4.356)$$

Nous considérons donc la suite d'extensions de $\mathbb{Q}$ qui consiste à étendre successivement par les nombres $a_1, \dots, a_n, b_1, \dots, b_{n'}, c_1, \dots, c_{n''}$ tout en excluant les doublons : il est possible que par exemple b_3 soit déjà dans $\mathbb{Q}(a_1, \dots, a_n)$. Cela nous fournit une suite d'extensions

$$\begin{array}{l} \mathbb{M}_0 = \mathbb{Q} \\ \mathbb{M}_{i+1} = \mathbb{M}_i(\alpha_i) \\ a, b, c \in \mathbb{M}_n. \end{array} \quad (4.357)$$

Ici le n n'est pas spécialement le même que celui plus haut. Maintenant, α est dans une extension quadratique de $\mathbb{M}_n$.

Pour la réciproque nous supposons avoir une tour d'extensions quadratiques $\mathbb{L}_0 = \mathbb{Q}$, $\mathbb{L}_i$ et $\alpha \in \mathbb{L}_n$ et nous voulons prouver que α est constructible. Nous y allons par récurrence : si $n = 0$ alors α est rationnel et il est constructible par la proposition 4.164.

Supposons que tous les points à coordonnées dans $\mathbb{L}_i$ sont constructibles. Alors nous allons prouver que les éléments de $\mathbb{L}_{i+1}$ le sont également. Vu que α est solution d'une équation de degré 2 à coefficients dans $\mathbb{L}_i$, nous avons

$$a\alpha^2 + b\alpha + c = 0 \quad (4.358)$$

pour certains $a, b, c \in \mathbb{L}_i$ et donc

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \quad (4.359)$$

Les exemples 4.165 et 4.166 montrent que les produits et les racines carrées de nombres constructibles sont constructibles. Donc α est constructible. □

4.7.3 Polygones constructibles

Définition 4.170.

Un angle α est **constructible** si le nombre $\cos(\alpha)$ est constructible.

La raison est que si qu'il suffit de prendre la perpendiculaire à l'axe horizontal

Lemme 4.171 ([1]).

Soient m et n , deux nombres premiers entre eux. L'angle $\frac{2\pi}{mn}$ est constructible si et seulement si les angles $\frac{2\pi}{m}$ et $\frac{2\pi}{n}$ sont constructibles.

Démonstration. **Sens direct** Il suffit de pouvoir multiplier un angle par un entier, ce qui est fait dans l'exemple 4.167.

Sens réciproque Le théorème de Bézout 2.24 nous donne $a, b \in \mathbb{Z}$ tels que $an + bm = 1$. Cela donne immédiatement

$$\frac{1}{mn} = \frac{a}{m} + \frac{b}{n}, \quad (4.360)$$

et donc

$$\frac{2\pi}{mn} = a \frac{2\pi}{m} + b \frac{2\pi}{n}, \quad (4.361)$$

ce qui fait que l'angle $2\pi/mn$ est une combinaison entière d'angles constructibles. Il est donc constructible par l'exemple 4.168. $\square$

Lemme 4.172.

Soit un entier $n \geq 3$ ayant

$$n = \prod_{i=1}^k p_i^{\alpha_i} \quad (4.362)$$

comme décomposition en facteurs premiers. Les polynôme régulier à n côtés est constructible si et seulement si les angles $\frac{2\pi}{p_i^{\alpha_i}}$ sont constructibles.

Démonstration. Le polygone régulier à n côtés est constructible si et seulement si l'angle $\frac{2\pi}{n}$ est constructible, c'est à dire si l'angle

$$\frac{2\pi}{\prod_{i=1}^k p_i^{\alpha_i}} \quad (4.363)$$

est constructible. Par récurrence sur le lemme 4.171, cet angle est constructible si et seulement si les angles $\frac{2\pi}{p_i^{\alpha_i}}$ sont constructibles. $\square$

Théorème 4.173 (Gauss-Wantzel[1]).

Soit $\alpha \in \mathbb{N}^*$.

- (1) L'angle $\frac{2\pi}{2^\alpha}$ est constructible.
- (2) Si p est premier $p \neq 2$ alors l'angle $\frac{2\pi}{p^\alpha}$ est constructible si et seulement si $\alpha = 1$ et p est un **nombre de Fermat**, c'est à dire de la forme $1 + 2^{(2^\beta)}$ pour $\beta \in \mathbb{N}$.
- (3) Le polygone régulier à n côtés est constructible si et seulement si n est le produit d'une puissance de 2 et d'un nombre fini de nombre de Fermat distincts.

Démonstration. Le point (1) est une construction de bissectrice, et le point (3) consistera à remettre en place différents morceaux. Le gros de la preuve est donc consacré à (2).

Sens direct Nous supposons que l'angle $\frac{2\pi}{p^\alpha}$ est constructible ; alors le nombre $\cos(2\pi/p^\alpha)$ l'est également et le théorème de Wantzel 4.169 nous indique que

$$[\mathbb{Q}(\cos(2\pi/p^\alpha)) : \mathbb{Q}] = 2^m \quad (4.364)$$

pour un certain m . Posons $q = p^\alpha$ et $\omega = e^{2i\pi/q}$. Grâce au corollaire 4.114, nous savons que le polynôme minimal de ω est le polynôme cyclotomique ϕ_q dont le degré est ²⁴

$$\varphi(q) = \varphi(p^\alpha) = p^{\alpha-1}(p-1). \quad (4.365)$$

Par conséquent

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p^{\alpha-1}(p-1). \quad (4.366)$$

Mais par ailleurs

$$\omega + \omega^{-1} = 2 \cos(2\pi/q), \quad (4.367)$$

donc $\cos(2\pi/q) \in \mathbb{Q}(\omega)$. Et en multipliant (4.367) par ω nous trouvons le polynôme annulateur suivant pour ω :

$$\omega^2 - 2 \cos\left(\frac{2\pi}{q}\right) \omega + 1 = 0. \quad (4.368)$$

Cela signifie que ω est de degré 2 dans $\mathbb{Q}(\cos(2\pi/q))$, c'est à dire

$$[\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/q))] = 2. \quad (4.369)$$

24. Voir juste en dessous de la définition 4.107.

En remettant bout à bout et en utilisant la propriété multiplicative des degrés des extensions²⁵,

$$\underbrace{[\mathbb{Q}(\omega) : \mathbb{Q}]}_{p^{\alpha-1}(p-1)} = \underbrace{[\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/p^\alpha))]}_2 \underbrace{[\mathbb{Q}(\cos(2\pi/p^\alpha)) : \mathbb{Q}]}_{2^m}, \quad (4.370)$$

donc $p^{\alpha-1}(p-1) = 2^{m+1}$, mais comme p est premier et impair, $\alpha = 1$ et $p = 2^{m+1} + 1$. Par ailleurs $m+1$ est un entier et nous nous proposons de mettre en facteur la puissance de 2 dans son développement en facteurs premiers : $m+1 = \lambda 2^\beta$ avec $\beta \in \mathbb{N}$ et un certain nombre impair $\lambda \in \mathbb{N}^*$. Nous avons :

$$p = 2^{\lambda 2^\beta} + 1 = \left(2^{2^\beta}\right)^\lambda + 1, \quad (4.371)$$

mais le lemme 3.118(1) nous indique alors que $1 + 2^{2^\beta}$ divise $1 + \left(2^{2^\beta}\right)^\lambda = p$. Mais vu que p est premier, il ne peut être divisé que par p lui-même et donc λ soit être égal à 1 et nous avons

$$p = 1 + 2^{2^\beta}, \quad (4.372)$$

ce qui signifie que p est un nombre de Fermat premier.

Sens réciproque Nous supposons que p est un nombre premier de la forme $p = 1 + 2^{2^\beta}$ et nous devons prouver que l'angle $\frac{2\pi}{p}$ est constructible. Pour cela nous posons tout de suite $n = 2^\beta$ et $\omega = e^{2i\pi/p}$. Comme dans la première partie nous nous souvenons que le polynôme minimal de ω est le polynôme cyclotomique ϕ_p de degré $p-1$; donc

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1. \quad (4.373)$$

Un groupe d'automorphismes Nous considérons le groupe $G = \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))$ des automorphismes du corps $\mathbb{Q}(\omega)$ agissant sur $\mathbb{Q}$ comme l'identité. Tous les éléments de $\mathbb{Q}(\omega)$ étant des polynômes en ω (proposition 4.65), un élément $g \in G$ est uniquement déterminé par $g(\omega)$, et de plus $g(0) = 0$ ainsi que $\phi_p(\omega) = 0$ et que ϕ_p commute avec g , donc

$$\phi_p(g(\omega)) = g(\phi_p(\omega)) = g(0) = 0, \quad (4.374)$$

ce qui signifie que $g(\omega)$ est une racine du polynôme cyclotomique ϕ_p . Par définition 4.107, les racines sont $\{\omega, \omega^2, \dots, \omega^{p-1}\}$, ce qui signifie que l'action de g consiste à élever ω à une certaine puissance entre 1 et $p-1$. Le groupe G est donc d'ordre $|G| = p-1$ et a pour éléments

$$g_k : \omega \mapsto \omega^k \quad (4.375)$$

avec $k = 1, \dots, p-1$. L'application²⁶

$$\begin{aligned} \psi : G &\rightarrow (\mathbb{Z}/p\mathbb{Z})^* \\ g_k &\mapsto [k]_p. \end{aligned} \quad (4.376)$$

est un morphisme surjectif entre deux groupes finis de même cardinal, donc c'est un isomorphisme. Le corollaire 4.122 nous donne de plus l'isomorphisme $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, ce qui fait que G a un élément d'ordre $p-1$ (parce que $\mathbb{Z}/(p-1)\mathbb{Z}$ en a un). Nous notons g_0 cet élément.

La tour d'extensions À partir de cet élément $g_0 \in G$ nous définissons avec $0 \leq i \leq n$:

$$\mathbb{K}_i = \{z \in \mathbb{Q}(\omega) \text{ tel que } g_0^{2^i}(z) = z\}. \quad (4.377)$$

Ces ensembles sont bien des corps parce que g_0 est un morphisme : $g_0(zz') = g_0(z)g_0(z')$; on en déduit immédiatement que $g_0^2(zz') = g_0^2(z)g_0^2(z')$.

25. Proposition 4.45.

26. Pour rappel, la notation $[k]_p$ est la classe de l'entier k modulo p , qui est un élément de $\mathbb{Z}/p\mathbb{Z}$.

$\mathbb{K}_n = \mathbb{Q}(\omega)$ Cela est dû au fait que g_0 est par définition d'ordre 2^n , ce qui signifie que $g_0^{2^n}(z) = z$ pour tout $z \in \mathbb{Q}(\omega)$.

$\mathbb{K}_0 = \mathbb{Q}$ Vu que les éléments de G laissent $\mathbb{Q}$ invariant nous avons forcément $\mathbb{Q} \subset \mathbb{K}_0$. Nous nous attelons maintenant à prouver l'inclusion inverse. Nous savons par la proposition 4.65(2) que $\{\omega^i\}_{i=0,\dots,p-2}$ est une base²⁷ de $\mathbb{Q}(\omega)$. Vu que $g_0: \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ est un isomorphisme, l'image d'une base est une base :

$$\{g_0(\omega)^i\}_{i=0,\dots,p-2} \quad (4.378)$$

est également une base de $\mathbb{Q}(\omega)$. Soit $z \in \mathbb{K}_0$ et décomposons-le dans cette base²⁸ :

$$z = \sum_{i=0}^{p-2} \lambda_i g_0(\omega)^i; \quad (4.379)$$

nous appliquons g_0 à cette égalité en tenant compte du fait que $g_0(z) = z$:

$$z = \sum_{i=0}^{p-2} \lambda_i g_0(\omega)^{i+1}. \quad (4.380)$$

En identifiant les coefficients (et en remarquant que le dernier terme dans (4.379) est le premier dans (4.380)) nous voyons que tous les coefficients sont égaux :

$$z = \lambda_0 g_0(\omega + \dots + \omega^{p-1}) = \lambda_0 g_0(\phi_p(\omega) - 1) = -\lambda_0 \in \mathbb{Q}. \quad (4.381)$$

Dans cette chaîne d'égalités nous avons utilisé le fait que $\phi_p(X) = 1 + X + \dots + X^{p-1}$ (corollaire 4.112) et que $\phi_p(\omega) = 0$ par définition.

$\mathbb{K}_i \subset \mathbb{K}_{i+1}$ **strictement** Nous avons une inclusion pour la simple raison que si $z \in \mathbb{K}_i$, alors $g_0^{2^i}(z) = z$. Par conséquent :

$$g_0^{2^{i+1}}(z) = g_0^{2 \times 2^i}(z) = (g_0^{2^i})^2(z) = z. \quad (4.382)$$

Afin de voir que l'inclusion est stricte nous montrons que l'élément

$$x = \sum_{k=0}^{2^{n-i-1}-1} g_0^{k2^{i+1}}(\omega) \quad (4.383)$$

est dans $\mathbb{K}_{i+1} \setminus \mathbb{K}_i$. Dans la base $\{1, \omega, \dots, \omega^{p-1}\}$ l'élément x a une composante ω avec le terme $k = 0$, mais si on lui applique $g_0^{2^i}$ nous obtenons

$$g_0^{2^i}(x) = \sum_{k=0}^{2^{n-i-1}-1} g_0^{2^i(1+2k)}(\omega). \quad (4.384)$$

Une composante ω pour cela demanderait d'avoir $2^i(1+2k) = \lambda 2^n$ avec $\lambda \in \mathbb{N}$; cela demanderait

$$k = \lambda 2^{n-i-1} - \frac{1}{2} \quad (4.385)$$

ce qui est impossible. Donc $x \notin \mathbb{K}_i$.

Nous montrons que $x \in \mathbb{K}_{i+1}$ de la même manière :

$$g_0^{2^{i+1}}(x) = \sum_{k=0}^{2^{n-i-1}-1} g_0^{2^{i+1}(k+1)}(\omega). \quad (4.386)$$

Soit k_0 entre 0 et $2^{n-i-1} - 1$; nous voulons trouver un k entre 0 et $2^{n-i-1} - 1$ tel que $k_0 2^{i+1} = 2^{i+1}(k+1)$; cela est très simple : il suffit de prendre $k = k_0 - 1$ tant que $k_0 \neq 0$. Si $k_0 = 0$ alors cela correspond au terme ω dans (4.383), et il se trouve dans (4.386) avec $k = 2^{n-i-1} - 1$. Donc $g_0^{2^{i+1}}(x) = x$ et $x \in \mathbb{K}_{i+1}$.

27. Ici [1] parle de $\mathbb{Q}(\omega)/\mathbb{Q}$. Dans ce cas il me semble qu'il faille faire partir les valeurs de i de 0 et non de 1.

28. Il s'agit d'une base en tant qu'espace vectoriel sur $\mathbb{Q}$, donc les $\lambda\beta$ sont dans $\mathbb{Q}$.

Les degrés dans la tour Par définition de n et de ω , et par la propriété multiplicative des degrés²⁹ nous avons :

$$2^n = p - 1 = [\mathbb{Q}(\omega) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\omega) : \mathbb{K}_{n-1}] \dots [\mathbb{K}_1 : \mathbb{Q}]}_{n \text{ facteurs}}. \quad (4.387)$$

Un produit de n facteurs entiers tous strictement plus grand que zéro doit valoir 2^n . Ils doivent donc tous valoir 2 et nous avons en particulier

$$[\mathbb{K}_{n-1} : \mathbb{Q}] = 2^{n-1}. \quad (4.388)$$

$\cos(2\pi/p) \in \mathbb{K}_{n-1}$ Soit $f = g_0^{2^{n-1}}$; vu que l'action de g_0 (comme de tous les éléments de G) est de décaler les puissances de ω , il existe $\lambda \in \mathbb{N}$ tel que $f(\omega) = \omega^\lambda$. Mais $f^2 = \text{Id}$ donc

$$\omega = f^2(\omega) = \omega^{2\lambda}, \quad (4.389)$$

ce qui donne $1 = \omega^{\lambda^2-1}$ ou encore que p divise $\lambda^2 - 1$ parce que ω est une racine primitive p^e de l'unité. Par conséquent $[\lambda^2 - 1]_p = 0$ ce qui donne $[\lambda]_p = \pm[1]_p$, mais comme $f \neq \text{Id}$ nous avons

$$[\lambda]_p = -[1]_p. \quad (4.390)$$

Cela fait $f(\omega) = \omega^{-1}$.

Par ailleurs $\mathbb{Q}(\omega)$ est un corps, donc il contient

$$\cos\left(\frac{2\pi}{p}\right) = \frac{1}{2}(\omega + \omega^{-1}). \quad (4.391)$$

Nous en déduisons que $\cos(2\pi/p)$ est un point fixe de $f = g_0^{2^{n-1}}$:

$$f(\cos(2\pi/p)) = \frac{1}{2}(f(\omega) + f(\omega^{-1})) = \cos(2\pi/p). \quad (4.392)$$

Être un point fixe de $g_0^{2^{n-1}}$ signifie être un élément de $\mathbb{K}_{n-1}$:

$$\cos\left(\frac{2\pi}{p}\right) \in \mathbb{K}_{n-1}. \quad (4.393)$$

Questions de degrés Nous avons alors les (non)inclusions suivantes :

$$\mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{K}_{n-1} \subsetneq \mathbb{K}_n = \mathbb{Q}(\omega), \quad (4.394)$$

ce qui fait que

$$1 < [\mathbb{Q}(\omega) : \mathbb{K}_{n-1}] \leq [\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/p))] = 2 \quad (4.395)$$

La première inégalité est le fait que $\mathbb{Q}(\omega)$ n'est pas égal à $\mathbb{K}_{n-1}$. La dernière égalité se démontre de la même manière que (4.369) (ici $\alpha = 1$). Les inégalités de (4.395) sont donc en réalité des égalités :

$$[\mathbb{Q}(\omega) : \mathbb{K}_{n-1}] = [\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/p))] = 2. \quad (4.396)$$

Cela, combiné au fait que $\mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{K}_{n-1}$ donne

$$\mathbb{K}_{n-1} = \mathbb{Q}(\cos(2\pi/p)). \quad (4.397)$$

Mais nous savons déjà que $[\mathbb{K}_{n-1} : \mathbb{Q}] = 2^{n-1}$, donc

$$[\mathbb{Q}(\cos(2\pi/p)) : \mathbb{Q}] = 2^{n-1} \quad (4.398)$$

et le nombre $\cos(2\pi/p)$ est bien sur le sommet d'une tour d'extensions quadratiques partant de $\mathbb{Q}$. Il est donc constructible par le théorème de Wantzel 4.169.

29. Proposition 4.45

Il est maintenant l'heure de conclure en prouvant le point (3). D'abord si n est un produit de nombres premiers de Fermat distincts, alors $n = p_1 \dots p_m$ et l'angle $\frac{2\pi}{n}$ est constructible si et seulement si chacun des angles $\frac{2\pi}{p_k}$ est constructible (lemme 4.172), ce qui est le cas d'après la partie (2). Si n est le produit d'une puissance de 2 avec un produit de nombres premiers de Fermat, le polygone à n côtés est tout autant constructible : il suffit de bissecter les angles.

À l'inverse si le polynôme à n avec n impair côtés est constructible alors $n = \prod_i p_i^{\alpha_i}$, dont l'angle est constructible si et seulement si $\alpha = 1$ et p_i est un nombre premier de Fermat. Et si le polygone à n côtés (n pair) est constructible, alors $n = 2^\lambda \prod_i p_i^{\alpha_i}$. Ce polygone est constructible si et seulement si le polygone à $\prod_i p_i^{\alpha_i}$ est constructible : il suffit de regrouper les côtés par deux. $\square$

Remarque 4.174.

D'après Wikipédia[58], les seuls nombres de Fermat connus pour être premiers sont

$$F_0 = 3 \quad (4.399a)$$

$$F_1 = 5 \quad (4.399b)$$

$$F_2 = 17 \quad (4.399c)$$

$$F_3 = 257 \quad (4.399d)$$

$$F_4 = 65537. \quad (4.399e)$$

Pour les autres, essentiellement on ne sait pas. Il n'est même pas sûr qu'il y en ait d'autres. Le problème des polygones constructibles n'est donc pas encore tout à fait terminé.

Remarque 4.175.

Les angles $\frac{2\pi}{p^\alpha}$ avec p premier et $\alpha > 1$ ne sont pas constructibles. Il n'est donc pas possible de trisecter l'angle $\frac{2\pi}{3}$. Voilà qui règle un des vieux problèmes de l'antiquité.

4.7.4 Matrices

Proposition 4.176.

Nous avons

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}). \quad (4.400)$$

Démonstration. Par construction il existe une bijection entre $\mathrm{GL}(n, \mathbb{F}_p)$ et l'ensemble des bases de $\mathbb{F}_p^n$. Nous devons donc seulement compter le nombre de bases. Pour le premier vecteur de base nous avons le choix entre les $p^n - 1$ éléments non nuls de $\mathbb{F}_p^n$. Pour le second nous avons le choix entre $p^n - p$ éléments, et ainsi de suite. $\square$

4.8 Minuscule morceau sur la théorie de Galois

Vous trouverez des détails et des preuves à propos de la théorie de Galois dans [59].

Définition 4.177.

Soit $\mathbb{K}$, un corps.

Le **groupe de Galois** d'une extension $\mathbb{L}$ de $\mathbb{K}$ est le groupe des automorphismes de $\mathbb{L}$ laissant $\mathbb{K}$ invariant.

Le groupe de Galois d'un polynôme sur $\mathbb{K}$ est le groupe de Galois de son corps de décomposition sur $\mathbb{K}$.

Définition 4.178.

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

$$\sum \alpha_{i_1 \dots i_n} b_1^{i_1} \dots b_n^{i_n} = 0 \quad (4.401)$$

avec $\alpha_{i_1 \dots i_n} \in \mathbb{K}$.

Nous disons que l'équation

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \quad (4.402)$$

est l'**équation générale** de degré n si les coefficients a_i sont algébriquement indépendants sur $\mathbb{K}$.

Théorème 4.179.

Le groupe de Galois d'un polynôme de degré n est isomorphe au groupe symétrique S_n .

Corollaire 4.180 ([60]).

L'équation générale de degré n est résoluble par radicaux si et seulement si $n \leq 5$.

Chapitre 5

Topologie générale

5.1 Topologie en général

5.1.1 Définitions basiques

Définition 5.1.

Soit E , un ensemble et $\mathcal{T}$, une partie de l'ensemble de ses parties qui vérifie les propriétés suivantes

- (1) les ensembles $\emptyset$ et E sont dans $\mathcal{T}$,
- (2) Une union quelconque¹ 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 E est une **topologie** sur E , et les éléments de $\mathcal{T}$ sont appelés des **ouverts**. Nous disons que un sous ensemble A de E est **fermé** si son complémentaire, A^c est ouvert.

Lemme 5.2.

Union et intersection de fermés.

- (1) Une intersection quelconque de fermés est fermée.
- (2) Une union finie de fermés est fermée.

Démonstration. Soit $\{F_i\}_{i \in I}$ est un ensemble de fermés ; nous avons

$$\left(\bigcap_{i \in I} F_i \right)^c = \bigcup_{i \in I} F_i^c. \quad (5.1)$$

L'union de droite est un ouvert (union d'ouvert), et donc le terme de gauche est le complémentaire d'un ouvert. Donc fermé.

Le complémentaire de l'union finie est une intersection finie de complémentaires et est donc ouvert. $\square$

Dans un espace topologique, nous avons une caractérisation très importante des ouverts.

Théorème 5.3.

Une partie d'un espace topologique est ouverte si et seulement si elle contient un voisinage ouvert 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 à A .

Pour le sens inverse, nous supposons que A contienne un ouvert autour de chacun de ses points. Pour chaque $x \in A$, nous considérons l'ensemble $\mathcal{O}_x \subset A$, un ouvert autour de x . Nous avons que

$$A = \bigcup_{x \in A} \mathcal{O}_x. \quad (5.2)$$

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.

En effet $A \subset \bigcup_{x \in A} \mathcal{O}_x$ parce que tous les éléments de A sont dans un des $\mathcal{O}_x$, par construction. D'autre part, $\bigcup_{x \in A} \mathcal{O}_x \subset A$ parce que chacun des $\mathcal{O}_x$ est compris dans A .

L'union du membre de droite de (5.2) est une union d'ouverts et est donc un ouvert. Cela prouve que A est un ouvert. □

Une utilisation typique de ce théorème est faite dans le lemme 5.154.

Dès que nous avons une topologie nous avons une notion de convergence.

Définition 5.4 (Convergence de suite).

Une suite (x_n) d'éléments de E **converge** vers l'élément y de E si pour tout ouvert $\mathcal{O}$ contenant y , il existe un K tel que $k > K$ implique $x_k \in \mathcal{O}$.

5.1.2 Topologie produit

Définition 5.5 (Produit d'espaces topologiques).

Soient $X_1, \dots, X_n$ des espaces topologiques. Leur **produit** est l'ensemble

$$X = \prod_{i=1}^n X_i \quad (5.3)$$

muni de la topologie suivante. L'ensemble U est ouvert si et seulement si pour tout $x \in U$ il existe des ouverts $A_i \in X_i$ tels que $x \in A_1 \times \dots \times A_n \subset U$.

5.1.3 Séparabilité

Définition 5.6 (Espace séparé).

Si deux points distincts ont toujours deux voisinages distincts, nous disons que l'espace est **séparé** ou **Hausdorff**.

La notion d'espace séparé est particulièrement importante parce qu'elle assure l'unicité de la limite d'une fonction en un point par la proposition 5.51.

Définition 5.7.

Un espace topologique est **séparable** si il possède une partie dénombrable dense.

À ne pas confondre avec :

Définition 5.8.

Un espace topologique est **séparé** ou **Hausdorff** si deux points distincts possèdent des voisinages disjoints.

Définition 5.9.

Une partie A d'un espace topologique est **compacte** si il 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 tirer un recouvrement fini.

Remarque 5.10.

Certaines sources (dont wikipédia) disent que pour être compact il faut aussi être séparé². Pour ces sources, un espace qui ne vérifie que la propriété de Borel-Lebesgue est alors dit **quasi-compact**.

Définition 5.11.

Une partie d'un espace topologique est **relativement compact** si son adhérence est compacte.

Définition 5.12.

Un espace topologique est **localement compact** si tout élément possède un voisinage compact.

2. Définition 5.8.

Définition 5.13 (Séquentiellement compact).

Nous disons qu'un espace topologique est **séquentiellement compact** si toute suite admet une sous-suite convergente.

Définition 5.14.

Un espace topologique est **dénombrable à l'infini** si il est réunion dénombrable de compacts.

Définition 5.15 (Base de topologie).

Une famille $\mathcal{B}$ d'ouverts de X est une **base de la topologie** de X si pour tout $x \in X$ et pour tout voisinage V de x , il existe $A \in \mathcal{B}$ tel que $x \in A \subset V$.

Proposition 5.16.

Si $\mathcal{B}$ est une base de la topologie de X alors tout ouvert de X est une union d'éléments de $\mathcal{B}$.

Démonstration. Soit $\mathcal{O}$ un ouvert de X ; pour chaque $x \in \mathcal{O}$ nous considérons un ouvert $U(x)$ tel que $x \in U(x) \subset \mathcal{O}$ (possible par le théorème 5.3). Nous prenons alors $B(x) \in \mathcal{B}$ tel que

$$x \in B(x) \subset U(x) \subset \mathcal{O}. \quad (5.4)$$

Alors nous avons $\mathcal{O} = \bigcup_{x \in \mathcal{O}} B(x)$. □

Notons toutefois que nous sommes loin d'avoir une union dénombrable en général.

5.1.4 Topologie métrique

Définition 5.17.

Si E est un ensemble, une **distance** sur E est une application $d: E \times E \rightarrow \mathbb{R}$ telle que pour tout $x, y \in E$,

- (1) $d(x, y) \geq 0$
- (2) $d(x, y) = 0$ si et seulement si $x = y$,
- (3) $d(x, y) = d(y, x)$
- (4) $d(x, y) \leq d(x, z) + d(z, y)$.

La dernière condition est l'**inégalité triangulaire**.

Un couple (E, d) formé d'un ensemble et d'une distance est un **espace métrique**.

Définition 5.18.

Un sous ensemble $A \subset \mathbb{R}^n$ est **borné** si il existe une boule de $\mathbb{R}^n$ contenant A .

Proposition 5.19.

Toute réunion finie d'ensembles bornés est un ensemble borné. Toute partie d'un ensemble borné est un ensemble borné.

La définition suivante donne une topologie sur les espaces métriques en partant des boules. Par construction, les boules sont une base de la topologie³ d'un espace métrique.

Montrons que cette définition donne bien une topologie.

Théorème-définition 5.20.

Soit (E, d) un espace métrique. Nous définissons les **boules ouvertes** par

$$B(x, r) = \{y \in E \text{ tel que } d(x, y) < r\}. \quad (5.5)$$

Alors en posant

$$\mathcal{T} = \{\mathcal{O} \subset E \text{ tel que } \forall x \in A, \exists r > 0 \text{ tel que } B(x, r) \subset \mathcal{O}\} \quad (5.6)$$

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.

3. Définition 5.15.

Démonstration. D'abord $\emptyset \in \mathcal{T}$ parce que tout élément de l'ensemble vide ...heu ...enfin parce que d'accord hein⁴.

Ensuite si $(A_i)_{i \in I}$ 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 $(A_i)_{i \in \{1, \dots, n\}}$ 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 $B(x, r) \subset \bigcap_{i=1}^n A_i$. $\square$

Remarque 5.21.

Deux remarques à propos de cette définition.

- (1) Cette définition est faite exprès pour respecter le théorème 5.3.
- (2) Par construction, les boules ouvertes sont une base de la topologie (définition 5.15) des espaces métriques.

Définition 5.22.

Si (X, d_X) et (Y, d_Y) sont des espaces métrique, une **isométrie** est une application bijective $f: X \rightarrow Y$ telle que pour tout $x, y \in X$ nous ayons

$$d_Y(f(x), f(y)) = d_X(x, y). \quad (5.7)$$

Remarque 5.23.

Une application vérifiant (5.7) est automatiquement injective. En pratique, il ne faut donc vérifier que la surjectivité.

Exemple 5.24 (Manque de surjectivité)

Si $X = [0, \infty[$ et $f(x) = x + 1$ alors f vérifie (5.7) pour la distance $d(x, y) = |x - y|$, mais n'est pas surjective. $\triangle$

Exemple 5.25

Si X est un ensemble, nous pouvons écrire la **métrique discrète**

$$d(x, y) = \begin{cases} 0 & \text{si } x = y \\ 1 & \text{si } x \neq y. \end{cases} \quad (5.8)$$

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. $\triangle$

Proposition 5.26.

Une isométrie est continue.

Proposition-définition 5.27 (Groupe des isométries).

Si (X, d) est un espace métrique,

- (1) l'ensemble des isométries de X , noté $\text{Isom}(X)$ est un groupe pour la composition.
- (2) Ce groupe agit fidèlement sur X .

5.1.5 Espace vectoriel normé

Définition 5.28.

Un espace vectoriel E sur le corps $\mathbb{K}$ muni d'une topologie est un **espace vectoriel topologique** si

- (1) La somme de deux vecteurs est une application continue $E \times E \rightarrow E$
- (2) La multiplication par un scalaire est une application continue $\mathbb{K} \times E \rightarrow E$.

4. Pour qui ne serait pas d'accord, allez ajouter $\emptyset$ dans la définition des ouverts et puis c'est tout.

Note : le corps⁵ lui-même doit avoir sa topologie ; typiquement c'est $\mathbb{R}$ ou $\mathbb{C}$ muni de la topologie usuelle.

Dans un espace vectoriel topologique, nous avons une notion de suite de Cauchy et donc de complétude.

Définition 5.29 (Suite de Cauchy[61]).

*Soit E un espace vectoriel topologique. Une suite (x_k) dans E est une **suite de 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 $k, l \geq N$.*

Définition 5.30 (Espace complet).

*Nous disons qu'une partie A d'un espace topologique est **complet** si toute suite de Cauchy d'éléments de A converge vers un élément de A .*

Définition 5.31.

*Soit E un espace vectoriel réel. Une **norme** est une application $N: E \rightarrow \mathbb{R}^+$ vérifiant les axiomes*

- (1) $N(0_E) = 0$, et $N(x) = 0$ implique $x = 0_E$;
- (2) $N(\lambda x) = |\lambda|N(x)$ pour tout $\lambda \in \mathbb{R}$ et $x \in E$;
- (3) $N(x + y) \leq N(x) + N(y)$ pour tout $x, y \in E$. Cette propriété est appelée **inégalité triangulaire**.

Ici et dans la suite, 0_E désigne l'élément zéro de l'espace E .

En prenant $\lambda = -1$ dans la propriété (2), nous trouvons immédiatement que $N(-x) = N(x)$.

Proposition 5.32.

Toute norme N sur l'espace vectoriel E vérifie l'inégalité

$$|N(x) - N(y)| \leq N(x - y) \quad (5.9)$$

pour tout $x, y \in E$.

Démonstration. Nous avons, en utilisant le point (3) de la définition 5.31,

$$N(x) = N(x - y + y) \leq N(x - y) + N(y), \quad (5.10a)$$

$$N(y) = N(y - x + x) \leq N(y - x) + N(x). \quad (5.10b)$$

Supposons d'abord que $N(x) \geq N(y)$. Dans ce cas, en utilisant (5.10a),

$$|N(x) - N(y)| = N(x) - N(y) \leq N(x - y) + N(y) - N(y) = N(x - y). \quad (5.11)$$

Si par contre $N(x) \leq N(y)$, alors nous utilisons (5.10b) et nous trouvons

$$|N(x) - N(y)| = N(y) - N(x) \leq N(y - x) + N(x) - N(x) = N(y - x). \quad (5.12)$$

Dans les deux cas, nous avons retrouvé l'inégalité annoncée. $\square$

Cette proposition signifie aussi que

$$-N(x - y) \leq N(x) - N(y) \leq N(x - y). \quad (5.13)$$

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 5.32 s'énoncera donc

$$|\|x\| - \|y\|| \leq \|x - y\|. \quad (5.14)$$

Définition 5.33.

*Un espace vectoriel E muni d'une norme est une **espace vectoriel normé**, et on écrit $(E, \|\cdot\|)$.*

5. Définition 1.16

Si la distance d est déduite d'une norme, alors elle est invariante par translation :

$$d(a, b) = d(a + u, b + u) \quad (5.15)$$

pour tout $a, b, u \in E$.

Lemme-définition 5.34.

Si $\|\cdot\|$ est une norme alors la formule $d(x, y) = \|x - y\|$ donne une distance. C'est la **distance induite** par la norme.

Démonstration. Le seul point délicat à vérifier de la définition 5.17 est l'inégalité triangulaire. Nous avons $\|x\| = d(x, 0)$, donc nous pouvons écrire

$$d(x, y) = \|x - y\| \quad (5.16a)$$

$$\leq \|x\| + \|y\| \quad (5.16b)$$

$$= d(x, 0) + d(y, 0) \quad (5.16c)$$

$$= d(x, z) + d(y, z) \quad (5.16d)$$

parce que la distance associée à la norme est invariante par translation (équation (5.15)). $\square$

Un espace vectoriel normé est alors immédiatement un espace vectoriel topologique

Proposition 5.35.

Soit (E, d) un espace vectoriel topologique normé.

- (1) Une suite (x_n) dans E est convergente⁶ vers x si et seulement si pour tout $\epsilon \in \mathbb{R}$ il existe N_ϵ tel que pour tout $n \geq N_\epsilon$ nous avons $d(x_n, x) \leq \epsilon$.
- (2) Une suite (x_n) dans E est de Cauchy⁷ si pour tout $\epsilon \in \mathbb{R}$, il existe un N_ϵ tel que si $p, q \geq N_\epsilon$, nous avons $d(x_p, x_q) \leq \epsilon$.

Démonstration. En ce qui concerne la convergence :

Sens direct Nous supposons que $x_k \rightarrow x$ 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 $d(x, x_k) \leq \epsilon$.

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 5.20 et en particulier la liste des ouverts est donnée par (5.6). 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 :

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 $p, q \geq N_\epsilon$ alors $x_p - x_q \in B(0, \epsilon)$. Posons $u = x_p - x_q$; en utilisant l'égalité (5.15) nous avons

$$d(u, 0) = d(x_p - x_q, 0) = d(x_p, x_q). \quad (5.17)$$

Par conséquent $d(x_p, x_q) \leq \epsilon$.

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 $d(x_p, x_q) \leq \epsilon$ dès que $p, q \geq N_\epsilon$. En utilisant encore (5.15) nous avons

$$d(x_p, x_q) = d(x_p - x_q, 0), \quad (5.18)$$

et comme cela est plus petit que ϵ , nous avons $x_p - x_q \in B(0, \epsilon) \subset \mathcal{O}$.

6. Définition 5.4.

7. Définition 5.29.

□

Proposition 5.36 ([62]).

Toute suite convergente dans un espace métrique est de Cauchy.

Démonstration. Nous utilisons les caractérisations de la proposition 5.35 des suites convergentes et de Cauchy.

Soit un espace métrique (X, d) et $x_n \rightarrow \ell$ une suite convergente. Si $\epsilon > 0$, la proposition 5.35(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

$$d(x_n, x_m) \leq d(x_n, \ell) + d(\ell, x_m) \leq 2\epsilon. \quad (5.19)$$

Cela prouve que (x_n) est de Cauchy. □

5.1.6 Topologie sur l'ensemble des réels

Nous allons à présent donner la topologie sur $\mathbb{R}$ et ainsi résoudre les questions laissées en suspend lors de la construction des réels, voir 1.26.

Lemme 5.37.

L'application

$$x \mapsto |x| \quad (5.20)$$

est une norme sur $\mathbb{R}$.

La valeur absolue est celle de la définition 1.17(2).

Démonstration. Les conditions de la définition 5.31 sont immédiatement vérifiées grâce au lemme 1.18 et à la remarque 1.19. □

5.38.

Tant sur $\mathbb{Q}$ que sur $\mathbb{R}$, nous considérons la topologie métrique correspondant à cette norme (hors cas rarissimes qui seront signalés). Nous utiliserons toujours les caractérisations de la proposition 5.35 pour parler de suites convergentes et de suites de Cauchy.

Lemme 5.39 ([11]).

Toute suite de Cauchy dans $\mathbb{Q}$ converge dans $\mathbb{R}$ vers le réel qu'elle représente.

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 $\lim_{n \rightarrow \infty} x_n = \bar{x}$. Dans cette dernière limite, chacun des x_n est vu dans $\mathbb{R}$.

Si $\epsilon \in \mathbb{Q}$ est donné, il existe N_ϵ tel que si $p, q \geq N_\epsilon$ alors $|x_p - x_q| < \epsilon$, c'est à dire

$$x_p - \epsilon < x_q < x_p + \epsilon. \quad (5.21)$$

Soit $p \geq N_\epsilon$ fixé. Pour tout $q \geq N_\epsilon$ nous avons $x_p - \epsilon < x_q < x_p + \epsilon$. Par conséquent, la suite $n \mapsto (x_p - \epsilon) - q_n$ est un élément de $\mathcal{E}^-$ et au niveau des classes nous pouvons écrire

$$\overline{n \mapsto (x_p - \epsilon) - x_n} \leq 0. \quad (5.22)$$

Vu que $x_p - \epsilon$ représente la suite constante nous avons l'inégalité suivante dans $\mathbb{R}$:

$$x_p - \epsilon - \bar{x} \leq 0 \quad (5.23)$$

ou encore : $\bar{x} \geq x_p - \epsilon$. En faisant de même avec l'autre partie de l'inégalité, $x_p - \epsilon \leq \bar{x} \leq x_p + \epsilon$, ce qui signifie que

$$x_p \in B(\bar{x}, \epsilon) \quad (5.24)$$

dès que $p \geq N_\epsilon$. Cela signifie que $x_p \rightarrow \bar{x}$ dans $\mathbb{R}$. □

Théorème 5.40 (Complétude de $\mathbb{R}$ [11]).

Nous avons :

- (1) L'espace topologique $(\mathbb{R}, d)$ est complet.
- (2) Une suite dans $\mathbb{R}$ est convergente si et seulement si elle est de Cauchy.

Démonstration. Soit (x_n) une suite de Cauchy dans $\mathbb{R}$. Pour chaque n , il existe par le lemme 5.39 un $y_n \in \mathbb{Q}$ tel que

$$x_n - \frac{1}{n} < y_n < x_n + \frac{1}{n}. \quad (5.25)$$

Nous allons prouver que (y_n) est une suite de Cauchy⁸ dans $\mathbb{Q}$. Vu que (x_n) est de Cauchy pour la topologie de $\mathbb{R}$ si $\epsilon > 0$ dans $\mathbb{R}$ est donné, il existe n_ϵ tel que si $p, q \geq n_\epsilon$, alors⁹ $|x_p - x_q| < \epsilon$.

Nous avons :

$$|y_p - y_q| \leq |y_p - x_p| + |x_p - x_q| + |x_q - y_q| < \frac{1}{p} + \epsilon + \frac{1}{q}. \quad (5.26)$$

En choisissant $N_\epsilon > \max\{n_\epsilon, \frac{1}{\epsilon}\}$ (ce qui est possible par le lemme 1.38), et en prenant $p, q > N_\epsilon$, nous avons

$$|y_p - y_q| \leq 3\epsilon, \quad (5.27)$$

ce qui prouve que (y_p) est une suite de Cauchy dans $\mathbb{Q}$ ¹⁰. Elle représente donc un réel $\bar{y}$. Nous allons prouver 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 5.39). 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

$$|\bar{y} - x_p| \leq |\bar{y} - y_p| + |y_p - x_p| \leq \epsilon + \frac{1}{p}. \quad (5.28)$$

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 complet.

En ce qui concerne l'affirmation suivante, si une suite est convergente, alors elle est de Cauchy par la proposition 1.20(1). Et si une suite est de Cauchy, alors elle est convergente par ce que nous venons de prouver à propos de la complétude de $\mathbb{R}$. $\square$

Proposition 5.41.

Les rationnels sont denses dans les réels.

Démonstration. Soit $r \in \mathbb{R}$ et $\epsilon \in \mathbb{R}^+$. Nous devons prouver l'existence d'un rationnel dans $B(x, \epsilon)$. Le lemme 1.40 dit qu'il existe un rationnel dans $]x - \epsilon/2, x + \epsilon/2[$ et donc dans $B(x, \epsilon)$. $\square$

Proposition 5.42 ([8]).

Quel que soit le réel r , il existe une suite croissante de rationnels convergente vers r .

Démonstration. Soit $x \in \mathbb{R}$ et $\delta \in \mathbb{R}$; vu que $x - \delta$ et x sont des réels, le lemme 1.40 donne un élément x_δ tel que

$$x - 2\delta < x_\delta < x. \quad (5.29)$$

8. Soit au sens de la définition 1.17(3), soit au sens de la définition 5.29 (précisée par la proposition 5.35). Dans le premier cas, il faudra prendre $\epsilon \in \mathbb{Q}$ au lieu de $\epsilon \in \mathbb{R}$, et nous prouvons que $\mathbb{R}$ est un corps complet au lieu d'un espace topologique complet. Mais ça ne change pas grand chose.

9. Grâce à la proposition 5.35.

10. Éventuellement on peut préciser «pour la notion de suite de Cauchy de $\mathbb{Q}$ », si on veut prouver que $\mathbb{R}$ est seulement un corps complet.

Il ne reste plus qu'à pêcher parmi ces x_δ pour trouver une suite croissante. Soit x_0 un rationnel plus petit que x . Nous posons $\delta_0 = x - x_0$ et ensuite :

$$\begin{cases} \delta_i = x - x_i \\ x_{i+1} = x_{\delta_i/2}. \end{cases} \quad (5.30a) \quad (5.30b)$$

Ainsi nous avons pour tout i les inégalités

$$x_i = x - \delta_i < x - \frac{\delta_i}{2} < x_{i+1} < x. \quad (5.31)$$

La suite est donc croissante et toujours plus petite que x . Mais nous avons à chaque étape $\delta_{i+1} < \frac{\delta_i}{2}$, ce qui donne $\delta_i \rightarrow 0$. Soit $\epsilon > 0$ et k tel que $\delta_k < \epsilon$. Nous avons alors

$$x_{k+1} \in B(x, \frac{\delta_k}{2}) \subset B(x, \epsilon). \quad (5.32)$$

□

5.1.7 Base de topologie

Proposition 5.43.

Un espace métrique séparable¹¹ accepte une base de topologie 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

$$\mathcal{B} = \{B(a_i, r_j)\}_{i,j \in \mathbb{N}} \quad (5.33)$$

est une base de la topologie de E .

Démonstration. Soit $x \in E$ 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 $r \in \mathbb{Q}$ (densité de $\mathbb{Q}$ dans $\mathbb{R}$, proposition 5.41).

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

$$\|y - x\| \leq \|y - a\| + \|a - x\| < \frac{2}{3}r + \frac{1}{3}r = r. \quad (5.34)$$

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 à V . Cela prouve que $\mathcal{B}$ est bien une base de la topologie de E . □

Remarque 5.44.

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 6.139).

Voir aussi le corollaire 7.180 qui donnera tout ouvert comme union de pavés presque disjoints.

Lemme 5.45.

Soient (X_1, d_1) et (X_2, d_2) des espace métriques séparables. Alors $X_1 \times X_2$ admet une base dénombrable de topologie constituée de produits de boule 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

$$\{B(y_1, r_1) \times B(y_2, r_2)\}_{\substack{y_i \in A_i \\ r_i \in \mathbb{Q}^+}} \quad (5.35)$$

est une base de topologie pour $X_1 \times X_2$.

11. Qui possède une partie dense dénombrable, définition 5.7.

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 produit¹², 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

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}). \quad (5.36)$$

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

$$d_i(z_i, x_i) \leq d(z_i, y_i) + d(y_i, x_i) \leq \frac{r_i}{2} + \frac{r_i}{2} = r_i. \quad (5.37)$$

Au final,

$$(x_1, x_2) \in B(y_1, \frac{r_1}{2}) \times B(y_2, \frac{r_2}{2}) \subset \mathcal{O}. \quad (5.38)$$

□

Lemme 5.46.

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.

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 5.16. Soient $\{A_j\}_{j \in J}$ un ensemble d'éléments de la base de topologie tel que chacun des $\mathcal{O}_i$ est une union de certains des A_j . Nous avons $\bigcup_{j \in J} A_j = \bigcup_{i \in I} \mathcal{O}_i$.

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 à (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 $K \subset \bigcup_{j \in J_0} A_j \subset \bigcup_{i \in I_0} \mathcal{O}_i$. □

5.2 Limite et continuité

Définition 5.47.

*Un **homéomorphisme** est une application bijective continue entre deux espaces topologiques dont la réciproque est continue. Deux espaces topologiques homéomorphes sont dits **isomorphes**.*

Définition 5.48 (Limite d'une fonction).

*Soient X et Y des espaces topologiques, $A \subset X$ et $a \in \bar{A}$. L'élément $y \in Y$ est une **limite** de $f: A \rightarrow Y$ en a si pour tout voisinage V de y , il existe un voisinage W de a dans X tel que*

$$f(W \cap A) \subset V. \quad (5.39)$$

*Si il y a unicité de l'élément vers lequel f peut converger, alors nous disons que cet élément est la **limite** de f et nous notons*

$$\lim_{x \rightarrow a} f(x) = y. \quad (5.40)$$

Remarque 5.49.

La proposition 5.183 nous dira que l'unicité est de mise dans le cas des espaces duaux pour la topologie *-faible. La proposition 5.51 nous dira qu'il y a unicité dès que l'espace d'arrivée est séparé.

Exemple 5.50

Oui, il y a moyen de converger vers plusieurs points distincts si l'espace n'est pas super cool. Nous pouvons par exemple[63] 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 $0'$. △

12. Définition 5.5.

Proposition 5.51 (Unicité de la limite pour un espace séparé).

Soient X un espace topologique, A une partie de X et Y un espace topologique séparé¹³. Nous considérons une fonction $f: A \rightarrow Y$. Si $a \in \bar{A}$, 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 :

$$\begin{cases} f(W \cap A) \subset V \\ f(W' \cap A) \subset V'. \end{cases} \quad \begin{matrix} (5.41a) \\ (5.41b) \end{matrix}$$

Quitte à prendre des sous-ensembles nous pouvons supposer que W et W' sont ouverts. L'ensemble $W \cap W'$ est un ouvert contenant a et intersecte donc A . L'ensemble $(W \cap W') \cap A$ est non vide et

$$\begin{cases} f(W \cap W' \cap A) \subset f(W \cap A) \subset V \\ f(W \cap W' \cap A) \subset f(W' \cap A) \subset V'. \end{cases} \quad \begin{matrix} (5.42a) \\ (5.42b) \end{matrix}$$

Donc les ensembles V et V' ont une intersection. Au final nous avons prouvé que deux voisinages de y et y' ont forcément une intersection ; étant donné que Y est séparé, nous devons avoir $y = y'$. $\square$

La définition suivante est la définition de la continuité dans tous les cas.

Définition 5.52 (Fonction continue).

Une fonction $f: X \rightarrow Y$ est **continue au point** $a \in X$ si $f(a)$ est une limite¹⁴ de f en a .

Une fonction $f: X \rightarrow Y$ est **continue** si pour tout ouvert $\mathcal{O}$ de Y , l'ensemble $f^{-1}(\mathcal{O})$ est ouvert dans X .

La proposition 5.118 donnera des détails sur ce qu'il se passe lorsque l'espace est métrique.

Théorème 5.53.

Une fonction $f: X \rightarrow Y$ est une fonction continue si et seulement si elle est continue en chacun des points de X .

Démonstration. **Sens direct** Nous supposons que f est une fonction continue. Soit $a \in X$ et V , un voisinage de $f(a)$. Nous considérons $\mathcal{O}$, un voisinage ouvert de $f(a)$ contenu dans V ; 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 V .

Sens inverse 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 5.3 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 ¹⁵ nous assure qu'il existe un voisinage W de a tel que $f(W) \subset \mathcal{O}$. En prenant un ouvert contenant a à l'intérieur de W nous avons un voisinage ouvert de a contenu dans $f^{-1}(\mathcal{O})$. $\square$

Remarque 5.54.

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 la remarque 5.49.

13. Définition 5.6.

14. Définition 5.48.

15. Définition 5.52.

5.3 Compacité

Quelques liens vers la notion de compacité.

- (1) La définition d'un ensemble compact est la définition 5.9.
- (2) Les compacts sont les fermés bornés par le théorème 5.107.

5.3.1 Quelque propriétés

Définition 5.55.

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 5.56.

Soit X un espace topologique et $K \subset X$. Les propriétés suivantes sont équivalentes :

- (1) K est compact.
- (2) Si $\{F_i\}$ est une famille de fermés telle que $K \cap_{i \in I} F_i = \emptyset$, alors il existe un sous-ensemble fini A de I tel que $K \cap_{i \in A} F_i = \emptyset$.
- (3) Si $\{F_i\}_{i \in I}$ est une famille de fermés telle que $K \cap_{i \in A} F_i \neq \emptyset$ pour tout choix de A fini dans I , alors l'intersection complète est non vide : $K \cap_{i \in I} F_i \neq \emptyset$.
- (4) Toute famille ayant 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 reformulation en français de la propriété (3).

Prouvons (1) $\Rightarrow$ (2). Soit $\{F_i\}_{i \in I}$ une famille de fermés tels que $K \cap_{i \in I} F_i = \emptyset$. Les complémentaires $\mathcal{O}_i$ de F_i dans X recouvrent K et donc on peut en extraire un sous-recouvrement fini :

$$K \subset \bigcup_{i \in A} \mathcal{O}_i \quad (5.43)$$

pour un certain sous-ensemble fini A de I . Pour ce même choix A , nous avons alors aussi

$$K \cap_{i \in A} F_i = \emptyset. \quad (5.44)$$

L'implication (2) $\Rightarrow$ (1) est la même histoire. □

Proposition 5.57 ([64]).

Tout compact d'un espace topologique séparé est fermé.

Démonstration. Soit X un espace séparé et K compact dans X . Nous considérons $x \in \mathbb{C}K$ et, par hypothèse de séparation, pour chaque $x \in K$ nous considérons un voisinage ouvert V_x de x et un voisinage ouvert W_x de y tels que $V_x \cap W_x = \emptyset$. Bien entendu les V_x forment un recouvrement ouvert de K dont nous pouvons extraire un sous-recouvrement fini : soit S fini dans K tel que

$$K \subset \bigcup_{x \in S} V_x. \quad (5.45)$$

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 . De plus W n'intersecte pas K parce que si $x \in K$ alors $x \in V_s$ pour un certain $s \in S$ par conséquent x n'est pas dans W_s et donc pas non plus dans l'intersection.

L'ouvert W prouve que y est dans l'intérieur du complémentaire de K , ce qui nous permet de conclure que le complémentaire de K est ouvert (théorème 5.3), aka que K est fermé. □

Lemme 5.58 ([65]).

Une partie fermée d'un compact est elle-même compacte.

Démonstration. Soit F fermé dans un compact K et $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de F par des ouverts. Vu que F est fermé, F^c est ouvert et $\{\mathcal{O}_i\}_{i \in I} \cup \{K \setminus F\}$ est un recouvrement de K par des ouverts. Si nous en extrayons un sous-recouvrement fini, c'est un recouvrement de F , et en supprimant éventuellement l'ouvert $K \setminus F$, ça reste un sous-recouvrement fini de F tout en étant extrait de $\{\mathcal{O}_i\}_{i \in I}$. $\square$

Proposition 5.59.

Si V est une partie de l'espace topologique X muni de la topologie induite 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 . $\square$

Théorème 5.60.

L'image d'un compact par une fonction continue est un compact

Dans le cadre des espaces vectoriels normés, ce théorème est démontré en la proposition 5.113.

Démonstration. Soit $K \subset X$, un ensemble compact, et regardons $f(K)$; en particulier, nous considérons Ω , un recouvrement de $f(K)$ par des ouverts. Nous avons que

$$f(K) \subseteq \bigcup_{\mathcal{O} \in \Omega} \mathcal{O}. \quad (5.46)$$

Par construction, nous avons aussi

$$K \subseteq \bigcup_{\mathcal{O} \in \Omega} f^{-1}(\mathcal{O}), \quad (5.47)$$

en effet, si $x \in K$, alors $f(x)$ est dans un des ouverts de Ω , disons $f(x) \in \mathcal{O}_0$, 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

$$K \subseteq \bigcup_{i=1}^n f^{-1}(\mathcal{O}_i). \quad (5.48)$$

Dans ce cas, nous avons que

$$f(K) \subseteq \bigcup_{i=1}^n \mathcal{O}_i, \quad (5.49)$$

ce qui prouve la compacité de $f(K)$. $\square$

5.4 Topologie induite

Définition 5.61.

*Soit X un espace topologique et $A \subset X$. L'ensemble A devient un espace topologique en lui-même par la **topologie induite** de X . Un ouvert de A est un ensemble de la forme $A \cap \mathcal{O}$ où $\mathcal{O}$ est un ouvert de X .*

Lemme 5.62.

Si $B \subset A$ alors la fermeture de B pour la topologie de A (induite de X) que nous noterons $\tilde{B}$ est

$$\tilde{B} = \bar{B} \cap A \quad (5.50)$$

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 . Vu que $a \in \bar{B}$, l'ensemble $\mathcal{O}$ intersecte B et donc $(\mathcal{O} \cap A) \cap B \neq \emptyset$. Donc a est bien dans l'adhérence de B au sens de la topologie de A .

Pour l'inclusion inverse, soit $a \in \tilde{B}$, et 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 $a \in \bar{B}$. $\square$

Exemple 5.63

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 des choses se passent quand même. 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 $\mathbb{R}$. $\triangle$

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 5.64

Quid de la boule ouverte $B(1, \epsilon)$ dans le compact $[0, 1]$? Par définition c'est

$$B(1, \epsilon) = \{x \in [0, 1] \text{ tel que } |x - 1| < \epsilon\} =]1 - \epsilon, 1]. \quad (5.51)$$

Oui, cela 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 à $[0, 1]$. $\triangle$

Lemme 5.65.

Soit $A \subset X$ muni de la topologie induite de X et (x_n) une suite dans A . Si $x_n \xrightarrow{A} x$, alors $x_n \xrightarrow{X} x$.

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 $n \geq N$, alors $x_n \in A \cap \mathcal{O} \subset \mathcal{O}$. $\square$

Lemme 5.66 ([8]).

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 le complémentaire de F dans S est un ouvert de (S, τ_S) : il existe un ouvert $\Omega \in \tau_X$ tel que $S \setminus F = S \cap \Omega$. Si maintenant nous considérons le complémentaire de S dans X nous avons

$$F^c = (S \setminus F) \cup (X \setminus S) = (S \cap \Omega) \cup S^c = (S \cap \Omega) \cup (S^c \cap \Omega) \cup S^c = \Omega \cup S^c. \quad (5.52)$$

Vu que 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 . $\square$

5.5 Connexité

Dès qu'un ensemble est muni d'une métrique, nous pouvons définir les boules ouvertes, les voisinages et les sous-ensembles ouverts. Dès que l'on a identifié les sous-ensemble ouverts de E , nous disons que E devient un **espace topologique**. Nous allons maintenant un pas plus loin.

Définition 5.67.

Lorsque E 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

$$A = (A \cap O_1) \cup (A \cap O_2), \quad (5.53)$$

et tels que $A \cap O_1 \neq \emptyset$, et $A \cap O_2 \neq \emptyset$. Si un sous-ensemble n'est pas non-connexe, alors on dit qu'il est connexe.

Une autre façon d'exprimer la condition (5.53) 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 .

Proposition 5.68.

Soit X un espace topologique. Les conditions suivantes sont équivalentes.

- (1) L'espace X est connexe.
- (2) Si $X = A \sqcup B$ avec A et B fermés dans X , alors $A = \emptyset$ ou $B = \emptyset$.
- (3) Si $A \subset X$ avec A ouvert et fermé en même temps, alors $A = \emptyset$ ou $A = X$.
- (4) Toute application continue $X \rightarrow \mathbb{Z}$ est constante.

Proposition 5.69.

L'image d'un ensemble connexe par une fonction continue est connexe.

Démonstration. Soit $f: X \rightarrow Y$ une application continue entre deux espaces topologiques, et E une partie connexe de X . Nous devons montrer que $f(E)$ est connexe dans Y .

Par l'absurde nous considérons A et B , deux ouverts de Y disjoints recouvrant $f(E)$. Étant donné que f est continue, les ensembles $f^{-1}(A)$ et $f^{-1}(B)$ sont ouverts dans X . De plus ces deux ensembles recouvrent E .

Si x est un élément de $f^{-1}(A) \cap f^{-1}(B)$, alors $f(x) \in A \cap B$, ce qui est impossible parce que nous avons supposé que A et B étaient disjoints. Par conséquent $f^{-1}(A)$ et $f^{-1}(B)$ sont deux ouverts disjoints recouvrant E . Contradiction avec la connexité de E . Nous concluons que $f(E)$ est connexe. $\square$

Une application de ce théorème sera le théorème de valeurs intermédiaires 11.50.

Exemple 5.70

Les espaces topologiques $\mathbb{R}$ et $\mathbb{R}^2$ ne sont pas homéomorphes. $\triangle$

Démonstration. Soit $f: \mathbb{R} \rightarrow \mathbb{R}^2$ un homéomorphisme. Nous posons $E = f(\mathbb{R} \setminus \{0\})$ et $z_0 = f(0)$. Vu que f est bijective nous avons

$$E = \mathbb{R}^2 \setminus \{z_0\}, \quad (5.54)$$

qui est connexe.

Vu que E est connexe et que f^{-1} est continue, la proposition 5.69 nous dit que $f^{-1}(E)$ est connexe. Mais par définition, $f^{-1}(E) = \mathbb{R} \setminus \{0\}$ qui n'est pas connexe. $\square$

Proposition 5.71.

Si $A \subset X$ est connexe et si $A \subset B \subset \bar{A}$, alors B est connexe.

Proposition 5.72.

Stabilité de la connexité par union.

- (1) Une union quelconque de connexes ayant une intersection non vide est connexe.
- (2) 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. (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

- (a) $C_j \subset A \cup B$,
- (b) $C_j \cap A \neq \emptyset$ parce que p est dans l'intersection,
- (c) $C_j \cap B \neq \emptyset$ 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. 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 $A_1 \cap A_2$ et A_3 ont un point d'intersection par hypothèse, et ainsi de suite.

□

5.6 Un peu de topologie réelle

Afin de pouvoir étudier la topologie des espaces métriques, il faut savoir quelques propriétés des réels parce que nous allons étudier la fonction distance qui est une fonction continue à valeurs dans les réels.

5.6.1 Suites numériques

La propriété suivante est le plus souvent donnée comme une définition lorsque seule la topologie sur $\mathbb{R}$ est considérée.

Proposition 5.73 (Limite d'une suite numérique).

La suite (x_n) est convergente si et seulement si il existe un réel ℓ tel que

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N, |x_n - \ell| < \epsilon. \quad (5.55)$$

Dans ce cas, le nombre ℓ est la limite de la suite (x_n) . Nous dirons aussi souvent que la suite **converge** vers le nombre ℓ .

Démonstration. La limite d'une suite dans un espace topologique est la définition 5.4.

Si $x_n \rightarrow \ell$ et si $\epsilon > 0$ il existe N_ϵ tel que pour tout $n \geq N$ nous avons $x_n \in B(\ell, \epsilon)$ (parce que cette boule est un ouvert contenant ℓ). Vu la définition d'une boule (définition 5.20) et de la norme sur $\mathbb{R}$ (par 5.38), cette condition est bien $|x_n - \ell| < \epsilon$.

Dans l'autre sens, soit $\mathcal{O}$ un ouvert contenant ℓ . Par définition de la topologie, il existe $\epsilon > 0$ tel que $B(\ell, \epsilon) \subset \mathcal{O}$. La condition (5.55) nous assure qu'il existe N_ϵ tel que pour tout $n \geq N_\epsilon$ nous ayons

$$x_n \in B(\ell, \epsilon) \subset \mathcal{O}, \quad (5.56)$$

ce qui assure que la suite (x_n) converge vers ℓ pour la topologie métrique de $\mathbb{R}$. □

Une façon équivalente d'exprimer le critère (5.55) est de dire que pour tout ϵ positif, il existe un rang $N \in \mathbb{N}$ tel que l'intervalle $[\ell - \epsilon, \ell + \epsilon]$ contient tous les termes x_n au-delà de N .

Il est à noter que le rang N dont il est question dans la définition de suite convergente dépend de ϵ .

Exemple 5.74

Quelques suites usuelles.

- (1) La suite $x_n = \frac{1}{n}$ converge vers 0.

(2) La suite $x_n = (-1)^n$ ne converge pas.

△

Une suite est dite **contenue** dans un ensemble A si $x_n \in A$ pour tout n . Une suite est **bornée supérieurement** si il existe un M tel que $x_n \leq M$ pour tout n . De la même manière, la suite est bornée inférieurement si il existe un m tel que $x_n \geq m$ pour tout n .

Le lemme suivant est souvent utilisé pour prouver qu'une suite est convergente.

Lemme 5.75.

Une suite croissante et bornée supérieurement converge. Une suite décroissante bornée inférieurement est convergente.

Théorème 5.76.

Toute suite réelle contenue dans un compact admet une sous-suite convergente.

Démonstration. Soit (x_n) une suite contenue dans la partie bornée $A \subset \mathbb{R}$. Nous disons qu'un élément x_k de la suite est *maximal* si il est plus grand ou égal que tous les suivants : $x_k \geq x_{k'}$ dès que $k' \geq k$.

Si la suite a un nombre infini d'éléments maximaux, alors la suite des éléments maximaux est décroissante. Si nous n'avons qu'un nombre fini de points maximaux, alors la suite de départ est croissante à partir du dernier point maximal.

Dans les deux cas nous avons trouvé une sous-suite des x_n qui est monotone (décroissante ou croissante selon le cas), et donc convergente parce que contenue dans un borné (lemme 5.75). $\square$

Lemme 5.77.

Pour tout $\alpha > 0$ et $a < 1$ nous avons la limite

$$\lim_{n \rightarrow \infty} n^\alpha a^n = 0 \quad (5.57)$$

Démonstration. Soit $k \in \mathbb{N}$ plus grand que α . Soit la suite numérique $s_n = n^k a^n$. Tous ses termes sont positifs et

$$\frac{s_n}{s_{n+1}} = \left(\frac{n}{n+1} \right)^k \frac{1}{a}. \quad (5.58)$$

Étant donné que $n/n+1 \rightarrow 1$ et que $a < 1$, il existe un certain rang à partir duquel la suite (s_n) est décroissante. Deux conclusions :

- Elle est majorée par une constante M .
- Elle est convergente par le lemme 5.75.

Soit l tel que $ka^l < 1$ et $n > l$ alors

$$s_{n+l} = (n+l)^k a^{n+l} \leq kn^k a^n a^l = ka^l s_n \leq ka^l M. \quad (5.59)$$

La majoration est due au fait que dans $(n+l)^k$ nous avons k termes tous plus petits que n^k . De la même façon,

$$s_{2n+2l} \leq ka^{2l} s_{2n} \leq ka^{2l} M. \quad (5.60)$$

En posant $\varphi(i) = in + il$ nous avons

$$s_{\varphi(i)} \leq ka^i M, \quad (5.61)$$

qui est une sous-suite convergente vers 0. Or si une suite est convergente (ce qui est le cas de (s_n)), toutes les sous-suites convergent vers la même limite. Nous en concluons que $s_n \rightarrow 0$. $\square$

Remarque 5.78.

Nous ne pouvons pas prouver cette limite en utilisant les propriétés de l'exponentielle ou du logarithme (en particulier les dérivées comme on voudrait en utiliser pour la règle de l'Hospital ou pour un développement limité) parce que les exponentielles sont définies par leur série entière et que leurs propriétés de dérivation dépendent de la proposition 16.24.

Proposition 5.79.

Une suite (x_n) dans $\mathbb{R}^m$ est convergente dans $\mathbb{R}^m$ si et seulement si les suites de chaque composantes sont convergentes dans $\mathbb{R}$. Dans ce cas nous avons

$$\lim x_n = \left(\lim(x_n)_1, \lim(x_n)_2, \dots, \lim(x_n)_m \right) \quad (5.62)$$

où $(x_n)_k$ dénote la k -ième composante de (x_n) .

Exemple 5.80

La suite $x_n = \left(\frac{1}{n}, 1 - \frac{1}{n}\right)$ converge vers $(0, 1)$ dans $\mathbb{R}^2$. En effet, en utilisant la proposition 5.79, nous devons calculer séparément les limites

$$\begin{aligned} \lim \frac{1}{n} &= 0 \\ \lim \left(1 - \frac{1}{n}\right) &= 1. \end{aligned} \quad (5.63)$$

△

Exemple 5.81

Étant donné que la suite $(-1)^n$ n'est pas convergente, la suite $x_n = ((-1)^n, \frac{1}{n})$ n'est pas convergente dans $\mathbb{R}^2$. △

5.6.2 Maximum, supremum et compagnie

Ce n'est un secret pour personne que $\mathbb{R}$ est un ensemble totalement ordonné¹⁶ : 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 $\mathbb{R}$.

Si je regarde l'intervalle $I = [0, 1]$, je peux même dire que 10 est plus grand que tous les éléments de I . Nous disons que 10 est un *majorant* de $[0, 1]$. La définition est la suivante.

Définition 5.82.

Lorsque A est un sous-ensemble de $\mathbb{R}$, on dit que s est un **majorant** de A si s est plus grand que tous les éléments de A . En d'autres termes, si

$$\forall x \in A, s \geq x.$$

Je me permet d'insister 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 évident $s + 1$, $s + 4$, $s + \pi^2$ majorent également A .

Exemple 5.83

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 majorants.

△

16. Définition 1.34.

Définition 5.84.

Le **supremum** d'un ensemble est le plus petit majorant. En d'autres termes, s est un supremum de A si tout nombre plus petit que s ne majore pas A , ou encore,

$$\forall x < s, \exists y \in A \text{ tel que } y > x.$$

Nous disons que M est un **maximum** de A si M est un supremum et $M \in A$.

Quand s est un supremum de A , ça veut dire que le moindre pas vers la gauche que l'on fait à partir de s (c'est à dire le moindre ϵ), et on tombe dans A , ou tout au moins, il existe des éléments de A qui sont plus grand que $s - \epsilon$.

5.6.2.1 ... et 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 5.85

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 :

$$10 = \max[0, 10] = \sup[0, 10] \qquad 10 = \sup[0, 10[$$

Exemple 5.86

Si on dit que 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 9,99999 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 5.87

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.

△

Lorsque vous lisez que la charge maximale d'un camion est de 2.5 tonnes, est-ce que cela veut dire que vous pouvez y mettre 2.5 tonnes, mais que si un oiseau se pose dessus, le camion s'effondre ? Ou bien est-ce que cela signifie qu'à 2.5 tonnes le camion s'écroule, mais que toute charge inférieure est valable ?

C'est à cette rude question que nous allons nous attaquer maintenant.

Définition 5.88.

Soit une partie A de $\mathbb{R}$. Nous disons qu'un nombre M est un **majorant** de A si M est plus grand ou égal que tous les éléments de A , c'est à dire si

$$\forall a \in A, M \geq a. \tag{5.64}$$

Un **minorant** de A est un nombre m tel que

$$\forall a \in A, m \leq a. \tag{5.65}$$

Définition 5.89.

Soit A une partie majorée de $\mathbb{R}$. Le **supremum** de A est le plus petit des majorants, c'est à dire le nombre M tel que

- (1) $M \geq x$ 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 $x > M - \varepsilon$.

Nous notons $\sup A$ le supremum de A .

De la même façon, l'**infimum** de A , noté $\inf A$, est le plus grand de ses minorants.

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 $\infty \notin \mathbb{R}$.

La définition est justifiée par le lemme 5.90 et la proposition 5.92. Le premier montre que si A possède un infimum, alors il est unique, tandis que le second montre que toute partie majorée de $\mathbb{R}$ accepte un supremum, et que toute partie minorée accepte un infimum.

Lemme 5.90.

Soit A une partie de $\mathbb{R}$. Supposons que m_1 et m_2 soient deux nombres qui vérifient les propriétés de l'infimum de A . Alors $m_1 = m_2$.

Démonstration. Si $m_1 \neq m_2$, nous pouvons supposer $m_2 > m_1$. Dans ce cas, étant donné que m_1 est un infimum, m_2 ne peut pas minorer A , et donc ne peut pas être un infimum. $\square$

Maintenant il est important de se rendre compte d'une chose : un ensemble ne peut avoir qu'un seul maximum et supremum. Jusqu'à présent nous avons toujours dit *un* supremum. À partir de maintenant nous pouvons dire *le* supremum. La preuve de cela est assez simple.

Proposition 5.91.

Si A est un sous-ensemble de $\mathbb{R}$ admettant un supremum, alors il n'a qu'un seul supremum ; et si il accepte un maximum, il n'en accepte un seul, et le maximum est égal au supremum.

Démonstration. Commençons par l'affirmation concernant le supremum. Supposons que x et y soient tous les deux suprema différents de A . Étant donné que $x \neq y$, nous pouvons supposer que $x < y$, et donc, par définition du fait que y est un supremum, il existe un élément de A qui est plus grand que x . Cela contredit le fait que x soit supremum. En conclusion, il ne peut pas y avoir deux suprema différents pour un même ensemble.

Étant donné qu'un maximum est un supremum, il ne peut pas y avoir deux maxima différents vu qu'il ne peut pas y avoir deux suprema différents. $\square$

Proposition 5.92.

Tout sous-ensemble de $\mathbb{R}$ borné vers le bas possède un infimum ; tout sous-ensemble de $\mathbb{R}$ borné vers le haut possède un supremum.

La preuve qui suit est proche de celle donnée par Wikipédia dans l'article Least upper bound principle.

Démonstration. 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) :

$$\begin{aligned}
 x_0 &\text{ est un élément de } A, \\
 x_1 &\text{ est un minorant de } A, \\
 a_0 &= x_0 \\
 b_0 &= x_1 \\
 b_1 &= x_1.
 \end{aligned}
 \tag{5.66}$$

Ensuite, nous faisons la récurrence suivante :

$$\begin{aligned} x_{n+1} &= \frac{a_n + b_n}{2}, \\ a_{n+1} &= \begin{cases} a_n & \text{si } x_{n+1} \text{ minore } A \\ x_{n+1} & \text{sinon,} \end{cases} \\ b_{n+1} &= \begin{cases} x_{n+1} & \text{si } x_{n+1} \text{ minore } A \\ b_n & \text{sinon.} \end{cases} \end{aligned} \quad (5.67)$$

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

$$\begin{aligned} |a_n - b_n| &= |a_{n-1} - x_n| \\ &= \left| a_{n-1} - \frac{a_{n-1} + b_{n-1}}{2} \right| \\ &= \frac{1}{2} |a_{n-1} - b_{n-1}|, \end{aligned} \quad (5.68)$$

ce qui prouve que $|a_n - b_n| \rightarrow 0$. Nous montrons maintenant que la suite (a_n) est de Cauchy. En effet nous avons

$$|a_n - a_{n-1}| = \begin{cases} 0 \\ \left| \frac{a_n - b_n}{2} \right| \end{cases} \leq \frac{1}{2n}. \quad (5.69)$$

Il en est de même pour la suite (b_n) . Ce sont deux suites de Cauchy (donc convergentes par le théorème 5.40) 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.

□

Définition 5.93.

Si le supremum d'un ensemble appartient à l'ensemble, nous l'appelons **maximum**. De la même façon si l'infimum d'un ensemble appartient à l'ensemble, nous disons que c'est le **minimum**.

Exemple 5.94

Pour les intervalles, ces notions sont simples : les bornes de l'intervalle sont les supremum et infimum, et ce sont des minima et maxima si l'intervalle est fermé. Le nombre 53 est un majorant.

- (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.

△

Il existe évidemment de nombreux exemples plus vicieux.

Exemple 5.95

Prenons $E = \{\frac{1}{n} \text{ tel que } n \in \mathbb{N}_0\}$, dont les premiers points sont indiqués sur la figure 5.1. Cet

ensemble est constitué des nombres $1, \frac{1}{2}, \frac{1}{3}, \dots$. Le plus grand d'entre eux est 1 parce que tous les nombres de la forme $\frac{1}{n}$ avec $n \geq 1$ 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. $\triangle$

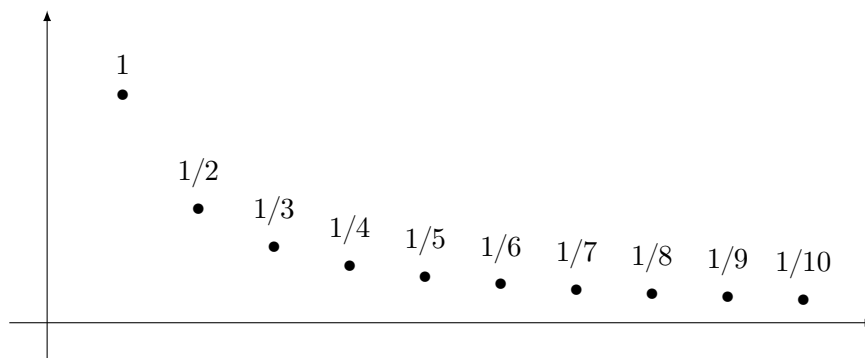


FIGURE 5.1 – Les premiers points du type $x_n = 1/n$.

L'exemple suivant est une source classique d'erreurs en ce qui concerne l'infimum. Il sera à relire après avoir vu la définition de limite (définition 5.73).

Exemple 5.96

Les premiers points de l'ensemble $F = \{\frac{(-1)^n}{n} \text{ tel que } n \in \mathbb{N}_0\}$ sont représentés à la figure 5.2. 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. $\triangle$

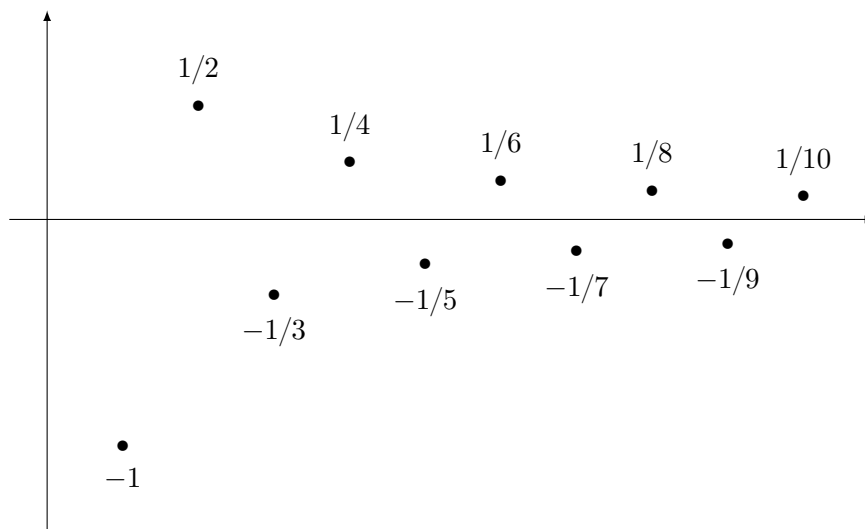


FIGURE 5.2 – Les quelques premiers points du type $(-1)^n/n$.

Lorsque $x \in E$, nous disons qu'un **voisinage** de x est n'importe quel sous-ensemble de E qui

contient une boule ouverte centrée en x . Nous disons qu'un ensemble est **ouvert** si il contient un voisinage de chacun de ses points. Par convention, nous disons que l'ensemble vide est ouvert.

Définition 5.97.

*L'ensemble des boules ouvertes d'un espace métrique forment la **topologie** de l'espace.*

Nous allons dire qu'une partie A d'un espace métrique est **bornée** si il existe une boule¹⁷ qui contient A .

Lemme 5.98.

Le supremum d'un ensemble ouvert n'est pas dans l'ensemble (et n'est donc pas un maximum).

Démonstration. Soit $\mathcal{O}$, un ensemble ouvert et s , son supremum. Si s était dans $\mathcal{O}$, on aurait un voisinage $B = B(s, r)$ de s contenu dans $\mathcal{O}$. Le point $s + r/2$ est alors à la fois dans $\mathcal{O}$ et plus grand que s , ce qui contredit le fait que s soit un supremum de $\mathcal{O}$. $\square$

Par le même genre de raisonnements, on montre que l'union et l'intersection de deux ouverts sont encore des ouverts.

Remarque 5.99.

L'intersection d'une *infinité* d'ouverts n'est pas spécialement un ouvert comme le montre l'exemple suivant :

$$\mathcal{O}_i =]1, 2 + \frac{1}{i}[.$$

Tous les ensembles $\mathcal{O}_i$ contiennent le point 2 qui est donc dans l'intersection. Mais quel que soit le $\epsilon > 0$ que l'on choisisse, le point $2 + \epsilon$ n'est pas dans $\mathcal{O}_{(1/\epsilon)+1}$. Donc aucun point au-delà de 2 n'est dans l'intersection, ce qui prouve que 2 ne possède pas de voisinages contenus dans $\bigcap_{i=1}^{\infty} \mathcal{O}_i$.

Proposition 5.100.

Prouver que, quels que soient les ensembles A et B dans $\mathbb{R}$, nous avons

$$\sup(A \cap B) \leq \sup A \leq \sup(A \cup B).$$

5.6.3 Intervalles

5.6.3.1 Connexité

Nous allons déterminer tous les sous-ensembles connexes¹⁸ de $\mathbb{R}$. Pour cela nous avons besoin d'une définition précise de ce que l'on appelle un *intervalle* dans $\mathbb{R}$.

Définition 5.101.

*Un **intervalle** est une partie de $\mathbb{R}$ telle que tout élément compris entre deux éléments de la partie soit dedans. En formule, la partie I de $\mathbb{R}$ est un intervalle si*

$$\forall a, b \in I, (a \leq x \leq b) \Rightarrow x \in I.$$

*Si I est un intervalle, les nombres $\inf(I)$ et $\sup(I)$ ¹⁹ sont les **extrémités** de I .*

Cette définition englobe tous les exemples connus d'intervalles ouverts, fermés avec ou sans infini : $[a, b]$, $[a, b[$, $] - \infty, a]$, $\dots$ L'ensemble $\mathbb{R}$ lui-même est un intervalle.

Définition 5.102.

*Étant donnés deux points a et b dans $\mathbb{R}^p$ on appelle **segment** d'extrémités a et b , et on note $[a, b]$, l'image de $[0, 1]$ par l'application $s : [0, 1] \rightarrow \mathbb{R}^p$, $s(t) = (1 - t)a + tb$. On pose $]a, b[= s(]0, 1[)$, et $]a, b] = s(]0, 1])$.*

17. À titre d'exercice, je te laisse te convaincre que l'on peut dire boule *ouverte* ou *fermée* au choix sans changer la définition.

18. Définition 5.67.

19. Qui existent par la proposition 5.92, quitte à poser $\pm\infty$ comme infimum et supremum lorsque I n'est pas borné.

Il faut observer que le segment $[a, b]$ est une courbe orientée : certes en tant que ensembles, $[a, b] = [b, a]$, mais si nous regardons la fonction de t correspondante à $[b, a]$, nous voyons qu'elle va dans le sens inverse de celle qui correspond à $[a, b]$. Nous approfondirons ces questions lorsque nous parlerons d'arcs paramétrés autour de la section 14.6.

Le segment $[b, a]$ est l'image de l'application $r: [0, 1] \rightarrow \mathbb{R}^p$ donnée par $r(t) = (1 - t)b + ta$.

Une des nombreuses propositions qui vont servir à prouver le théorème des valeurs intermédiaires 11.50 est la suivante.

Proposition 5.103.

Une partie de $\mathbb{R}$ est connexe si et seulement si c'est un intervalle.

Démonstration. La preuve est en deux parties. D'abord nous démontrons que si un sous-ensemble de $\mathbb{R}$ est connexe, alors c'est un intervalle ; et ensuite nous démontrons que tout intervalle est connexe.

Afin de prouver qu'un ensemble connexe est toujours un intervalle, nous allons prouver que si un ensemble n'est pas un intervalle, alors il n'est pas connexe. Prenons A , une partie de $\mathbb{R}$ qui n'est pas un intervalle. Il existe donc $a, b \in A$ et un x_0 entre a et b qui n'est pas dans A . Comme le but est de prouver que A n'est pas connexe, il faut couper A en deux ouverts disjoints. L'élément x_0 qui n'est pas dans A est le bon candidat pour effectuer cette coupure. Prenons M , un majorant de A et m , un minorant de A , et définissons

$$\begin{aligned}\mathcal{O}_1 &=]m, x_0[\\ \mathcal{O}_2 &=]x_0, M[.\end{aligned}$$

Si A n'a pas de minorant, nous remplaçons la définition de $\mathcal{O}_1$ par $] - \infty, x_0[$, et si A n'a pas de majorant, nous remplaçons la définition de $\mathcal{O}_2$ par $]x_0, \infty[$. Dans tous les cas, ce sont deux ensembles ouverts dont l'union recouvre tout A . En effet, $\mathcal{O}_1 \cup \mathcal{O}_2$ contient tous les nombres entre un minorant de A et un majorant sauf x_0 , mais on sait que x_0 n'est pas dans A . Cela prouve que A n'est pas connexe.

Jusqu'à présent nous avons prouvé que si un ensemble n'est pas un intervalle, alors il ne peut pas être connexe. Pour remettre les choses à l'endroit, prenons un ensemble connexe, et demandons-nous si il peut être autre chose qu'un intervalle ? La réponse est *non* parce que si il était autre chose, il ne serait pas connexe.

Prouvons à présent que tout intervalle est connexe. Pour cela, nous refaisons le coup de la contraposée. Nous allons donc prendre une partie A de $\mathbb{R}$, supposer qu'elle n'est pas connexe et puis prouver qu'elle n'est alors pas un intervalle. Nous avons deux ouverts disjoints $\mathcal{O}_1$ et $\mathcal{O}_2$ tels que $A \subset \mathcal{O}_1 \cup \mathcal{O}_2$. Prenons $a \in A_1$ et $b \in A_2$. Pour fixer les idées, on suppose que $a < b$. Maintenant, le jeu est de montrer qu'il existe un point x_0 entre a et b qui ne soit pas dans A (cela montrerait que A n'est pas un intervalle). Nous allons prouver que c'est le cas du point

$$x_0 = \sup\{x \in \mathcal{O}_1 \text{ tel que } x < b\}.$$

Étant donné que l'ensemble $\mathcal{A} = \{x \in \mathcal{O}_1 \text{ tel que } x < b\}$ est ouvert²⁰, le point x_0 n'est pas dans l'ensemble par le lemme 5.98. Nous avons donc

- soit x_0 n'est pas dans $\mathcal{O}_1$,
- soit $x_0 \leq b$,
- soit les deux en même temps.

Nous allons montrer qu'un tel x_0 ne peut pas être dans A . D'abord, remarquons que $\sup \mathcal{A} \leq \sup \mathcal{O}$ parce que $\mathcal{A}$ est une intersection de $\mathcal{O}$ avec quelque chose. Ensuite, il n'est pas possible que x_0 soit dans $\mathcal{O}_2$ parce que tout élément de $\mathcal{O}_2$ possède un voisinage contenu dans $\mathcal{O}_2$. Un point de $\mathcal{O}_2$ est donc toujours strictement plus grand que le supremum de $\mathcal{O}_1$.

Maintenant, remarque que si $x_0 \leq b$, alors $x_0 = b$, sinon b serait un majorant de $\mathcal{A}$ plus petit que x_0 , ce qui n'est pas possible vu que x_0 est le supremum de $\mathcal{A}$ et donc le plus petit majorant.

20. C'est l'intersection entre l'ouvert $\mathcal{O}_1$ et l'ouvert $\{x \text{ tel que } x < b\}$.

Oui mais si $x_0 = b$, c'est que $x_0 \in \mathcal{O}_2$, ce qu'on vient de montrer être impossible. Nous voilà déjà débarrassé des deuxièmes et troisièmes possibilités.

Si la première possibilité est vraie, alors x_0 n'est pas dans A parce qu'on a aussi prouvé que $x_0 \notin \mathcal{O}_2$. Or n'être ni dans $\mathcal{O}_1$ ni dans $\mathcal{O}_2$ implique de ne pas être dans A . Ce point $x_0 = \sup \mathcal{A}$ est donc hors de A .

Oui, mais comme $a \in \mathcal{A}$, on a obligatoirement que $x_0 \geq a$. Mais par construction, on a aussi que $x_0 \leq b$ (ici, l'inégalité est même stricte, mais ce n'est pas important). Donc

$$a \leq x_0 \leq b$$

avec $a, b \in A$, et $x_0 \notin A$. Cela finit de prouver que A n'est pas un intervalle. $\square$

Exemple 5.104

L'application

$$\begin{aligned} f:]0, 2\pi[&\rightarrow S^1 \\ x &\mapsto \begin{pmatrix} \cos(x) \\ \sin(x) \end{pmatrix} \end{aligned} \quad (5.70)$$

est un homéomorphisme. Vu que $]0, 2\pi[$ est connexe (proposition 5.103) la proposition 5.69 implique que le cercle privé d'un point est connexe. $\triangle$

5.6.3.2 Compacité

Lemme 5.105 ([66]).

Si $a < b \in \mathbb{R}$ alors le segment $[a, b]$ est compact²¹.

Démonstration. Soit $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de $[a, b]$ par des ouverts. Nous posons

$$M = \{x \in [a, b] \text{ tel que } [a, x] \text{ admet un sous-recouvrement fini extrait de } \{\mathcal{O}_i\}_{i \in I}\}. \quad (5.71)$$

Notre but est de prouver que $b \in M$.

a est dans M Le point a est naturellement dans un des $\mathcal{O}_i$. L'intervalle $[a, a]$ est donc recouvert par un seul des $\mathcal{O}_i$.

M est un intervalle Soit $m \in M$ et $m' \in [a, m[$. Le sous-recouvrement fini qui recouvre $[a, m]$ recouvre a fortiori $[a, m']$.

Les trois possibilités restantes À ce niveau de la preuve, il reste trois possibilités pour M soit il est de la forme $[a, c]$ ou $[a, c[$ avec $c < b$, soit il est de la forme $[a, b]$. Nous allons maintenant éliminer les deux premiers cas.

Ce que M n'est pas D'abord M n'est pas de la forme $[a, c[$ avec $c < b$. En effet nous commençons par considérer $\mathcal{O}_{i_0}$ un ouvert du recouvrement contenant c et $m < c$ dans $\mathcal{O}_{i_0}$. Si nous joignons $\mathcal{O}_{i_0}$ à un recouvrement fini de $[a, m]$ alors nous avons un recouvrement fini de $[a, c]$, et donc $c \in M$.

Ensuite M n'est pas de la forme $[a, c]$ avec $c < b$. En effet si on a un recouvrement fini de $[a, c]$ par des ouverts, alors un de ces ouverts contient c et donc contient des éléments de $[a, b]$ plus grands que c .

Nous déduisons que $M = [a, b]$ et qu'il est possible d'extraire un sous-recouvrement fini recouvrant $[a, b]$. $\square$

Lemme 5.106 ([8]).

Si K_1 et K_2 sont des compacts dans $\mathbb{R}$ alors $K_1 \times K_2$ est compact dans $\mathbb{R}^2$.

21. Définition 5.9

Démonstration. Soit $\{\mathcal{O}_i\}_{i \in I}$ un recouvrement de $K_1 \times K_2$ par des ouverts ; grâce au lemme 5.46 nous pouvons supposer que ce sont des carrés. Pour chaque $x \in K_1$, l'ensemble $\{x\} \times K_2$ est compact et donc recouvert par un nombre fini des $\mathcal{O}_i$. Soit R_x un ensemble fini des $\mathcal{O}_i$ recouvrant $\{x\} \times K_2$.

Vu que R_x est une collection finie de carrés nous pouvons considérer m_x , le minimum des rayons. L'ensemble K_1 est recouvert par les boules $B(x, m_x)$ et il existe donc une collection finie de $\{x_i\}_{i \in A}$ tels que $B(x_i, m_{x_i})$ recouvre K_1 .

Alors $\{R_{x_i}\}_{i \in A}$ recouvre $K_1 \times K_2$ parce que R_{x_i} recouvre l'ensemble $B(x_i, m_{x_i}) \times \{K_2\}$. $\square$

Théorème 5.107 (Théorème de Borel-Lebesgue).

Une partie d'un espace vectoriel normé réel de dimension finie est compacte si et seulement si elle est fermée et bornée.

Démonstration. Sens direct.

Compact implique borné En effet si K est non borné dans E alors K contient une suite (x_n) avec $\|x_n\| > n$. Les boules $B_i(x_i, \frac{1}{3})$ sont disjointes. On pose $\mathcal{O}_0 = \mathbb{C} \setminus \bigcup_i \overline{B(x_i, \frac{1}{5})}$, qui est ouvert comme complément d'un fermé. Pour $i \geq 1$ nous posons $\mathcal{O}_i = B(x_i, \frac{1}{4})$. Nous avons

$$K \subset \bigcup_{i \in \mathbb{N}} \mathcal{O}_i \quad (5.72)$$

mais vu que x_i est uniquement dans $\mathcal{O}_i$, nous ne pouvons pas extraire de sous-recouvrement fini.

Compact implique fermé Cela est la proposition 5.57.

Sens réciproque.

Un intervalle fermé et borné est compact dans $\mathbb{R}$ C'est le lemme 5.105.

Un produit de segments est compact Le produit de deux compacts de $\mathbb{R}$ est un compact dans $\mathbb{R}^2$ par le lemme 5.106.

Un fermé et borné et compact Soit K fermé et borné. Vu que K est borné, il est contenu dans un produit de segments. L'ensemble K est donc compact parce que fermé dans un compact, lemme 5.58.

$\square$

Exemple 5.108(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 $\{\emptyset, X\}$. Toutes les parties de cet espace sont compactes, mais les seuls fermés sont $\{\emptyset, X\}$. Toutes les autres parties sont alors compactes et non fermées. $\triangle$

Exemple 5.109(Compacité de la boule unité)

La boule unité fermée $\overline{B(0, 1)}$ d'un espace vectoriel normé de dimension finie est compacte parce que fermée et bornée. En dimension infinie, cela n'est plus le cas. Certes la boule unité est encore fermée et bornée, mais elle n'est plus compacte. En effet nous allons donner un recouvrement par des ouverts duquel il ne sera pas possible d'extraire un sous-recouvrement fini.

Autour de chacune des extrémités des vecteurs de base, nous considérons la boule $A_i = B(e_i, \frac{1}{3})$. Ensuite aussi l'ouvert

$$B(0, 1) \setminus \bigcup_i \overline{B(e_i, \frac{1}{4})}. \quad (5.73)$$

Le tout recouvre $B(0, 1)$ mais toutes les premières boules sont nécessaires. $\triangle$ Le théorème de

Bolzano-Weierstrass nous permettra de prouver plus simplement la non compacité en dimension infinie. Voir l'exemple 5.132.

5.6.4 Image d'un compact

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 (dans d'autres cours) énormément utilisé pour trouver des maxima et minima de fonctions. Le théorème exact est le suivant.

Théorème 5.110.

Une fonction à valeurs réelles continue sur un compact est bornée et atteint ses bornes.

C'est à dire qu'il existe $x_0 \in K$ tel que $f(x_0) = \inf\{f(x) \text{ tel que } x \in K\}$ ainsi que x_1 tel que $f(x_1) = \sup\{f(x) \text{ tel que } x \in K\}$.

Démonstration. Soit K un espace topologique compact et $f: K \rightarrow \mathbb{R}$ une fonction continue. Alors le théorème 5.60 indique que $f(K)$ est compact. Par conséquent $f(K)$ est un fermé borné de $\mathbb{R}$ par le théorème de Borel-Lebesgue 5.107. Vu que $f(K)$ est borné, la fonction f est bornée.

De plus $f(K)$ étant fermé, son infimum est un minimum et son supremum est un maximum : il existe $x \in K$ tel que $f(x) = \sup f(K)$ et il existe $y \in K$ tel que $f(y) = \inf f(K)$. $\square$

Théorème 5.111 (Théorème de Bolzano-Weierstrass).

Toute suite contenue dans un compact de $\mathbb{R}^m$ admet une sous-suite convergente.

Ce théorème est un cas particulier du théorème 5.131 qui donne pour tout espace métrique, l'équivalence entre la compacité et la compacité séquentielle.

Démonstration. Nous rappelons qu'une partie compacte de $\mathbb{R}^n$ est fermée et bornée par le théorème de Borel-Lebesgue 5.107.

Soit (x_n) une suite contenue dans une partie bornée de $\mathbb{R}^m$. Considérons (a_n) , la suite réelle des premières composantes des éléments de (x_n) : pour chaque $n \in \mathbb{N}$, le nombre a_n est la première composante de x_n . Étant donné que la suite (x_n) est bornée, il existe un M tel que $\|x_n\| < M$. La croissance de la fonction racine carré donne

$$|a_n| \leq \|x_n\| \leq M. \quad (5.74)$$

La suite (a_n) est donc une suite réelle bornée et donc contient une sous-suite convergente. Soit a_{I_1} une sous-suite convergente de (a_n) . Nous considérons maintenant x_{I_1} , c'est à dire la suite de départ dont on a enlevé tous les éléments qu'il faut pour qu'elle converge en ce qui concerne la première composante.

Si nous considérons la suite b_{I_1} des *secondes* composantes de x_{I_1} , nous en extrayons, de la même façon que précédemment, une sous-suite convergente, c'est à dire que nous avons un $I_2 \subset I_1$ tel que b_{I_2} est convergent. Notons que a_{I_2} est une sous-suite de la (sous) suite convergente x_{I_1} , et donc a_{I_2} est encore convergente.

En continuant ainsi, nous construisons une sous-sous-sous-suite x_{I_3} telle que la suite des *troisième* composantes est convergente. Lorsque nous avons effectué cette procédure m fois, la suite x_{I_m} est une suite dont toutes les composantes convergent, et donc est une suite convergente par la proposition 5.79.

Le tableau suivant donne un petit schéma de la façon dont nous procédons. Les $\bullet$ sont les éléments de la suite que nous gardons, et les $\times$ sont ceux que nous «jetons».

$$\begin{array}{cccccccccccc}
 x_{\mathbb{N}} & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet & \dots \\
 x_{I_1} & \times & \bullet & \bullet & \times & \bullet & \times & \times & \bullet & \bullet & \bullet & \dots \\
 x_{I_2} & \times & \bullet & \times & \times & \bullet & \times & \times & \bullet & \bullet & \times & \dots \\
 \vdots & & & & & & & & & & & \\
 x_{I_m} & \times & \times & \times & \times & \bullet & \times & \times & \times & \bullet & \times & \dots
 \end{array} \quad (5.75)$$

La première ligne, $x_{\mathbb{N}}$, est la suite de départ. $\square$

Corollaire 5.112.

Si une suite est croissante et bornée alors elle est convergente.

Démonstration. Nous nommons (x_n) la suite et nous prenons un majorant M . Toute la suite est alors contenue dans le compact $[x_0, M]$, ce qui donne une sous-suite $(x_{\alpha(n)})$ convergente par le théorème de Bolzano-Weierstrass 5.111. Si ℓ est la limite de cette sous-suite alors nous avons $\ell \geq x_n$ pour tout n .

Pour tout $\epsilon > 0$ il existe K tel que si $n > K$ alors $|\ell - x_{\alpha(n)}| < \epsilon$. Vu que ℓ majore la suite nous avons même

$$x_{\alpha(n)} + \epsilon > \ell. \quad (5.76)$$

Vu que la suite est croissante pour tout $m > \alpha(K)$ nous avons $x_m + \epsilon > \ell$, ce qui signifie $|x_m - \ell| < \epsilon$. $\square$

Nous aurons une version pour les fonctions croissantes et bornées en la proposition 11.21.

Proposition 5.113.

Soient V et W deux espaces vectoriels normés. Soit K , une partie compacte de V , et $f: K \rightarrow W$, une fonction continue. Alors l'image $f(K)$ est compacte dans W .

Ce résultat est démontré dans un cadre plus général par le théorème 5.60.

Démonstration. Nous allons prouver que $f(K)$ est fermée et bornée.

$f(K)$ 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 5.111). 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 $\lim f(x'_n) = a$ parce que f est continue. Par conséquent nous avons

$$f(a) = \lim f(x'_n) = \lim y_n. \quad (5.77)$$

Cela prouve que la limite de (y_n) est dans $f(K)$ et par conséquent que $f(K)$ est fermé.

$f(K)$ est borné Si $f(K)$ n'est pas borné, nous pouvons trouver une suite (x_n) dans K telle que

$$\|f(x_n)\|_W > n \quad (5.78)$$

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

$$|f(a)| = \lim |f(x'_n)|. \quad (5.79)$$

La suite $f(x'_n)$ est alors une suite bornée, ce qui n'est pas possible au vu de la condition (5.78) imposée à la suite de départ (x_n) . $\square$

Corollaire 5.114.

Si $f: K \rightarrow \mathbb{R}$ 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 5.113 montre que $f(K)$ est compact et donc borné. $\square$

5.6.5 Connexité par arcs

Définition 5.115.

Le sous ensemble $A \subset \mathbb{R}^n$ est **connexe par arcs** si pour tout $x, y \in A$, il existe un chemin²² contenu dans A les reliant, c'est-à-dire une application continue

$$\gamma : [0, 1] \rightarrow \mathbb{R}^n \text{ tel que } \gamma(0) = x \text{ et } \gamma(1) = y$$

avec $\gamma(t) \in A$ pour tout $t \in [0, 1]$.

La connexité d'un ensemble n'implique pas sa connexité par arc. Il suffit pour cela de prendre un ensemble constitué de deux connexes reliés par un chemin de longueur infinie (le graphe d'une fonction de type $\sin(1/x)$ par exemple).

5.7 Espaces métriques

Quelques liens internes :

- (1) Le théorème-définition 5.20 donne la topologie sur un espace métrique.
- (2) La définition de la convergence d'une suite est la définition 5.4.
- (3) Dans un espace vectoriel normé, une application est continue si et seulement si elle est bornée, proposition 6.217.

5.7.1 Espaces métrisables

Définition 5.116.

Un espace topologique est **métrisable** si il est homéomorphe à un espace métrique.

Proposition 5.117.

Si X est un espace topologique dont la topologie est donnée par une famille dénombrable de semi-normes, alors il est métrisable.

5.7.2 Fonctions continues

La propriété suivante donne des caractérisations importantes de la continuité dans le cas des espaces métriques.

Proposition 5.118 (Continuité, ouverts et voisinages et limite[67]).

Soit $f : E \rightarrow F$ 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 $W' = B(f(a), \epsilon)$, il existe une boule $V' = B(a, \delta)$ telle que $f(V') \subset W'$.
- (4) $\forall \epsilon > 0, \exists \delta > 0$ tel que $f(B(a, \delta)) \subset B(f(a), \epsilon)$.
- (5) $\lim_{x \rightarrow a} f(x) = f(a)$ où la limite est donnée par la définition 5.48,
- (6) Pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que $\|x - a\| < \delta$ implique $\|f(x) - f(a)\| < \epsilon$.

La proposition 5.179 nous montrera que ces équivalences tiennent encore lorsque l'espace a une topologie de semi-normes.

22. Attention : ici quand on dit *chemin*, on demande que l'application soit continue. Dans de nombreux cours de géométrie différentielle, on demande C^∞ . Il faut s'adapter au contexte.

Démonstration. L'équivalence (1) $\Leftrightarrow$ (2) est la définition 5.52. L'équivalence (3) $\Leftrightarrow$ (4) est une simple paraphrase.

Montrons (2) $\Rightarrow$ (3). Si $W' = B(f(a), \delta)$, nous avons un voisinage V de a tel que $f(V) \subset W$. L'ensemble V contenant une boule autour de chacun de ses points²³, il en contient un autour de a : $V' = B(a, \delta) \subset V$. A fortiori nous avons $f(V') \subset W$.

Montrons (3) $\Rightarrow$ (2). Si W est un ouvert autour de $f(a)$, il contient une boule autour de $f(a)$: $B(f(a), \epsilon) \subset W$. Il existe donc une boule $V' = B(a, \delta)$ telle que $f(V') \subset B(f(a), \epsilon) \subset W$.

L'équivalence (1) $\Leftrightarrow$ (5) est la définition 5.52 de la continuité en un point couplée à l'unicité de la limite due à la proposition 5.51 parce qu'un espace métrique est séparé.

Prouvons (5) $\Rightarrow$ (6). Soit $\epsilon > 0$ et $V = B(f(a), \epsilon)$. Étant donné que $f(a)$ est une limite de f pour $x \rightarrow a$, 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 $x \in B(a, \delta) \subset W$ et donc $f(x) \in B(f(a), \epsilon)$, c'est à dire $\|f(a) - f(x)\| < \epsilon$.

Enfin l'implication (2) $\Rightarrow$ (5) est une réécriture de la définition de la limite en un point. $\square$

Proposition 5.119.

Une isométrie entre deux espaces métriques est continue.

Démonstration. Soient $f: X \rightarrow Y$, une application isométrique et $\mathcal{O}$ un ouvert de Y . Soit $a \in f^{-1}(\mathcal{O})$; si $d(a, b) < r$, alors $d(f(a), f(b)) < r$ et donc $b \in f^{-1}(B(f(a), r))$. 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. $\square$

Théorème 5.120 (Théorème des fermés emboîtés[68]).

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. **Condition suffisante** Soit $\{F_n\}_{n \in \mathbb{N}}$ une telle suite de fermés emboîtés. 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 $N \geq n$, la queue de suite $(x_n)_{n \geq N}$ 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 à un point.

Condition nécessaire Soit une suite de Cauchy (x_n) . Nous considérons les ensembles

$$F_n = \overline{\{x_i \text{ tel que } i \geq n\}}. \quad (5.80)$$

Le fait que la suite soit de Cauchy implique que $\text{diam}(F_n) \rightarrow 0$. Par hypothèse, nous avons alors

$$\bigcap_{n \in \mathbb{N}} F_n = \{a\}. \quad (5.81)$$

Pour s'assurer que a est bien la limite de (x_n) , il suffit de remarquer que

$$d(x_n, a) \leq \text{diam } F_n \rightarrow 0. \quad (5.82)$$

$\square$

5.7.3 Caractérisations séquentielles

Définition 5.121.

*Si X est un espace topologique, une fonction $f: X \rightarrow \mathbb{R}$ est **séquentiellement continue** en un point a si pour toute suite convergente $x_n \rightarrow a$ dans X nous avons $f(x_n) \rightarrow f(a)$ dans $\mathbb{R}$.*

²³. Cela est le théorème-définition 5.20 des ouverts dans un espace métrique, à ne pas confondre avec le théorème 5.3.

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.

Proposition 5.122 (Caractérisation séquentielle de la continuité[8]).

Le lien entre continuité et continuité séquentielle.

- (1) Une application continue est séquentiellement continue (quels que soient les espaces de départ et d'arrivée).
- (2) Si X et Y sont des espaces métriques, alors une fonction $f: X \rightarrow Y$ est continue en un point si et seulement si elle est y séquentiellement continue.

Démonstration. **Sens direct** Supposons que f soit continue en a et considérons une suite $a_k \rightarrow a$. Soit V un voisinage de $f(a)$ et W un voisinage de a tel que $f(W) \subset V$ (définition 5.48 de la continuité en un point). Par la convergence $a_k \rightarrow a$, il existe N tel que pour tout $k > N$, $a_k \in W$, et donc tel que $f(a_k) \in V$, ce qui donne la continuité séquentielle de f .

Sens réciproque, espaces métriques Nous supposons maintenant que X et Y soient métriques. Si f n'est pas continue en a , il existe $\epsilon > 0$ tel que pour tout $\delta > 0$, il existe x tel que $\|x - a\| \leq \delta$ et $\|f(x) - f(a)\| > \epsilon$. Nous considérons un tel ϵ et pour chaque $n \geq 1 \in \mathbb{N}$ nous considérons un x_n correspondant à $\delta = \frac{1}{n}$. Cela nous donne une suite $x_n \rightarrow a$ dans X mais $\|f(x_n) - f(a)\|$ reste plus grand que ϵ . Cela montre que f n'est pas non plus séquentiellement continue. □

Les espaces métriques ont une propriété importante que la fermeture séquentielle est équivalente à la fermeture.

Proposition 5.123 (Caractérisation séquentielle d'un fermé).

Soit X un espace métrique et $F \subset X$. L'ensemble F est fermé si et seulement si toute suite contenue dans F et convergant dans X converge vers un élément de F .

Démonstration. Si F est fermé alors $X \setminus F$ est ouvert. Soit une suite $x_n \xrightarrow{X} x$ contenue dans F . Si A est un ouvert autour de x contenu dans $X \setminus F$ (existence par le théorème 5.3), alors la suite ne peut pas entrer dans A et ne peut donc pas converger vers x .

Dans l'autre sens maintenant. Supposons que $X \setminus F$ ne soit pas ouvert. Alors il existe $x \in X \setminus F$ pour lequel tout voisinage intersecte F . En prenant $x_k \in B(x, \frac{1}{k})$, nous construisons une suite contenue dans F qui converge vers x . □

Proposition 5.124.

Soit E et Y , deux espaces métriques. Soit $f: E \rightarrow Y$ une application séquentiellement continue. Alors f est continue.

Démonstration. Soit $\mathcal{O}$ un ouvert de Y ; nous allons voir que le complémentaire de $f^{-1}(\mathcal{O})$ est fermé dans E . Pour cela nous considérons une suite convergente $x_k \xrightarrow{E} x$ avec $x_k \in \mathbb{C}f^{-1}(\mathcal{O})$ pour tout k . Nous allons montrer que $x \in \mathbb{C}f^{-1}(\mathcal{O})$ et la caractérisation séquentielle²⁴ de la fermeture conclura que $\mathbb{C}f^{-1}(\mathcal{O})$ est fermé.

Pour tout k , nous avons $f(x_k) \in \mathbb{C}\mathcal{O}$, mais $\mathcal{O}$ est ouvert et $f(x_k) \xrightarrow{Y} f(x)$ parce que f est séquentiellement continue. Par conséquent $f(x) \in \mathbb{C}\mathcal{O}$ et $x \in \mathbb{C}f^{-1}(\mathcal{O})$. □

Proposition 5.125.

Une fonction séquentiellement continue sur un espace métrisable et à valeurs dans un espace métrique est continue.

24. Proposition 5.123.

Démonstration. Soit E un espace métrique et un homéomorphisme $\phi: X \rightarrow (E, d)$. Nous supposons que $f: X \rightarrow Y$ est séquentiellement continue. Nous considérons l'application $\tilde{f} = f \circ \phi^{-1}$, c'est à dire

$$\begin{aligned}\tilde{f}: E &\rightarrow Y \\ a &\mapsto f(\phi^{-1}(a)).\end{aligned}\tag{5.83}$$

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

$$\tilde{f}(a_k) = f(\phi^{-1}(a_k)),\tag{5.84}$$

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

$$\lim_{k \rightarrow \infty} \tilde{f}(a_k) = \lim_{k \rightarrow \infty} f(\phi^{-1}(a_k)) = f(\phi^{-1}(a)) = \tilde{f}(a).\tag{5.85}$$

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 5.124. L'application $f = \tilde{f} \circ \phi$ est donc continue en tant que composée d'applications continues. $\square$

Proposition 5.126.

Si X et Y sont deux espaces métriques et $f, g: X \rightarrow Y$ sont deux fonctions continues égales sur une partie dense de X alors $f = g$.

Démonstration. Les fonctions f et g sont séquentiellement continues (proposition 5.122(2)). Soit 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 $a_n \rightarrow x$. La séquentielle continuité de f et g donnent

$$f(a_n) \rightarrow f(x)\tag{5.86a}$$

$$g(a_n) \rightarrow g(x),\tag{5.86b}$$

mais pour tout n , $f(a_n) = g(a_n)$. Par unicité de la limite²⁵ dans Y , $f(x) = g(x)$. $\square$

5.7.4 Distance entre un point et un ensemble

Définition 5.127.

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

$$d(x, A) = \inf_{a \in A} d(x, a).\tag{5.87}$$

Proposition 5.128.

Soit (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 $d(x_\epsilon, x) \leq \epsilon$. 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 $\lim_{k \rightarrow \infty} x_k = x$ par la proposition 5.35(1).

Par la caractérisation séquentielle des fermés (un fermé contient les limites de toutes ses suites, proposition 5.123), la suite (x_k) étant dans F , la limite est dans F . Donc $x \in F$. $\square$

²⁵. Proposition 5.51.

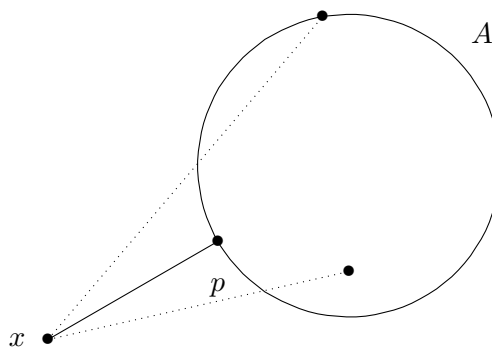


FIGURE 5.3 – La distance entre x et A est donnée par la distance entre x et p . Les distances entre x et les autres points de A sont plus grandes que $d(x, p)$.

5.7.5 Compacité

Lemme 5.129 (de Lebesgue[69]).

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 . Ce des x_n nous extrayons une sous-suite convergente (que nous nommons encore (x_n)) et nous posons $x_n \rightarrow x$. 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 . $\square$

Lemme 5.130 ([69]).

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 d'ensemble finis autour des points duquel les boules de taille ϵ recouvrent X .

Nous construisons par récurrence une suite ne possédant pas de sous-suites convergente. Le premier terme, x_0 est pris arbitrairement dans X . Ensuite si nous en avons N termes, nous savons que les boules de rayon ϵ et centrées en 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. $\square$

Théorème 5.131 (Bolzano-Weierstrass[69]).

Un espace métrique est compact si et seulement si toute suite admet une sous-suite qui converge à l'intérieur de l'espace.

Une version dédiée à $\mathbb{R}^n$ sera démontrée dans le théorème 5.111.

Démonstration. Soit X un espace métrique compact et (x_n) une suite dans X . Nous considérons la suite de fermés emboîtés

$$X_n = \overline{\{x_k \text{ tel que } k > n\}}. \quad (5.88)$$

Ce sont des fermés ayant la propriété d'intersection finie non vide, et donc la proposition 5.56 nous dit qu'ils ont une intersection non vide. Un élément de cette intersection est automatiquement un point d'accumulation de la suite.

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 5.129, 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 5.130, 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 . $\square$

Exemple 5.132 (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-suites convergentes. $\triangle$

Le théorème de Bolzano-Weierstrass 5.131 a l'importante conséquence suivante.

Théorème 5.133 (Weierstrass).

Une fonction continue à valeurs réelles définie sur un compact est bornée et atteint ses bornes.

Démonstration. Soit K un compact et $f: K \rightarrow \mathbb{R}$ une fonction continue. Nous désignons par A l'ensemble des valeurs prises par f sur K :

$$A = f(K) = \{f(x) \text{ tel que } x \in K\}. \quad (5.89)$$

Nous considérons le supremum $M = \sup A = \sup_{x \in K} f(x)$ avec la convention comme quoi si A n'est pas borné supérieurement, nous posons $M = \infty$ (voir définition 5.89).

Nous allons maintenant construire une suite (x_n) de deux façons différentes suivant que $M = \infty$ ou non.

- (1) Si $M = \infty$, nous choisissons, pour chaque $n \in \mathbb{N}$, un $x_n \in K$ tel que $f(x_n) > n$. Cela est certainement possible parce que si A n'est pas borné, nous pouvons y trouver des nombres aussi grands que nous voulons.
- (2) Si $M < \infty$, 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 5.131. Afin d'alléger la notation, nous allons noter (x_n) la sous-suite convergente. Nous avons donc

$$x_n \rightarrow x \in K. \quad (5.90)$$

Par la proposition 5.122, nous avons que f prend en x la valeur

$$f(x) = \lim_{n \rightarrow \infty} f(x_n). \quad (5.91)$$

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 $\lim_{n \rightarrow \infty} f(x_n) < \infty$. Nous en concluons que $M < \infty$, et donc que f est bornée sur K .

Afin de prouver que f atteint sa borne, c'est à dire que $M \in A$, nous considérons les inégalités

$$M - \frac{1}{n} < f(x_n) \leq M. \quad (5.92)$$

En passant à la limite $n \rightarrow \infty$, ces inégalités deviennent

$$M \leq f(x) \leq M, \quad (5.93)$$

et donc $f(x) = M$, ce qui prouve que f atteint sa borne M au point $x \in K$. $\square$

Lemme 5.134.

Soit A_n une suite décroissante de fermés dans un espace métrique²⁶ compact K . Alors

$$C = \bigcap_{n \in \mathbb{N}} A_n \quad (5.94)$$

est non vide.

²⁶. L'hypothèse métrique provient de l'utilisation de Bolzano-Weierstrass, lequel est vrai pour les espaces séquentiellement compacts, dont les espaces métriques.

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 5.58), 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 5.131. Une queue de la suite y_n est dans A_2 et nous considérons donc une sous suite convergente dans A_2 donnée par

$$z_n = y_{\sigma_2(n)} = x_{\sigma_1\sigma_2(n)}. \quad (5.95)$$

En continuant ainsi nous construisons une suite convergente dans A_k . Nous considérons enfin la suite

$$y_n = x_{\sigma_1 \dots \sigma_n(n)}. \quad (5.96)$$

Pour tout k , une queue de cette suite est une sous suite de $x_{\sigma_1 \dots \sigma_k(n)}$ et par conséquent cette suite converge dans A_k . La limite de cette suite est donc dans l'intersection demandée. $\square$

Remarque 5.135.

Cette propriété est fausse pour les ouverts. Par exemple

$$\bigcap_{n \geq 1}]0, \frac{1}{n}[= \emptyset. \quad (5.97)$$

Lemme 5.136.

Si K est un compact dans un espace métrique et F un fermé disjoint de K , alors $d(K, F) > 0$.

Démonstration. Le fonction

$$\begin{aligned} K &\rightarrow \mathbb{R} \\ x &\mapsto d(x, F) \end{aligned} \quad (5.98)$$

est une fonction continue sur K , et donc atteint son minimum par le théorème de Weierstrass 5.133. 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. $\square$

Proposition 5.137 ([69]).

Une isométrie d'un espace métrique compact sur lui-même est une bijection.

Démonstration. Soit X un espace métrique compact et $f: X \rightarrow X$ 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 5.136 appliqué au fermé $\{x\}$ et au compact $f(K)$ donne un $r > 0$ tel que

$$d(x, f(K)) > r. \quad (5.99)$$

Soit la suite $u_n = f^n(x)$; c'est une suite dans K et possède donc une sous-suite convergente (Bolzano-Weierstrass 5.131) que l'on nomme (y_n) . Vu que f est une isométrie,

$$d(y_n, y_{n+1}) = d(x, y_m) > r \quad (5.100)$$

pour un certain $m \leq n + 1$. Ce la 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. $\square$

Proposition 5.138.

Soit (X, d) un espace métrique compact et (u_n) une suite de X telle que

$$\lim_{n \rightarrow \infty} d(u_n, u_{n+1}) = 0. \quad (5.101)$$

Alors l'ensemble des points d'accumulation de (u_n) est connexe.

Démonstration. Nous notons Γ l'ensemble des points d'accumulation de la suite.

Γ est compact Nous notons $A_p = \{u_n \text{ tel que } n \geq p\}$ et nous avons

$$\Gamma = \bigcap_{p \in \mathbb{N}} \overline{A_p} \quad (5.102)$$

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 5.2). En tant que fermé dans un compact, Γ est compact (lemme 5.58).

Recouvrement par deux compacts Supposons que Γ ne soit ²⁷ pas connexe. Nous pouvons alors considérer S et O , deux ouverts disjoints recouvrant Γ et intersectant tout deux Γ . Nous posons alors

$$A = S \cap \Gamma \quad (5.103a)$$

$$B = O \cap \Gamma, \quad (5.103b)$$

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.

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 5.136. Nous notons

$$A' = \{x \in X \text{ tel que } d(x, A) < \frac{\alpha}{3}\} \quad (5.104a)$$

$$B' = \{x \in X \text{ tel que } d(x, B) < \frac{\alpha}{3}\} \quad (5.104b)$$

Nous avons $A' = \bigcup_{x \in A} B(x, \frac{\alpha}{3})$ et donc en tant qu'union d'ouverts, A' est ouvert (définition de la topologie). Même chose pour B' .

Enfin nous notons

$$K = X \setminus (A' \cup B') \quad (5.105)$$

qui est fermé en tant que complémentaire d'ouvert, et donc compact. Étant donné que $A \subset A'$ et $B \subset B'$, nous avons $K \cap \Gamma = \emptyset$.

L'idée est maintenant de montrer que K contient un point d'accumulation de (u_n) .

Sous-suites de (u_n) L'hypothèse sur la suite (u_n) nous indique qu'il existe un N_0 tel que $\forall n \geq N_0$,

$$d(u_n, u_{n+1}) < \frac{\alpha}{3}. \quad (5.106)$$

Soit $N > N_0$ 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 $B' \cap A' = \emptyset$, mais n_0 n'est pas n_2 lui-même parce que $d(A', B') \geq \frac{\alpha}{3}$ 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 (5.106) est important. Nous avons donc $N_0 < n_1 < n_0 < n_2$.

27. est-ce qu'il faut vraiment un subjonctif ici ?

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

$$\begin{aligned} d(u_{n_0}, B) &\geq d(u_{n_0-1}, B) - d(u_{n_0-1}, u_{n_0}) \\ &\geq d(A, B) - d(u_{n_0-1}, A) - d(u_{n_0-1}, u_{n_0}) \\ &\geq \alpha - \frac{\alpha}{3} - \frac{\alpha}{3} \\ &= \frac{\alpha}{3}. \end{aligned} \tag{5.107}$$

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 $N \geq N_0$, il existe un $n_0 \geq N$ 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 5.139.

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 5.140.

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 à $\text{Int}(K_n)$ pour un certain n .

Définition 5.141.

*Une suite de compacts telle que décrite dans le lemme 5.140 est une **suite exhaustive** de compacts pour Ω .*

Démonstration. Nous considérons les ensembles

$$V_n = \{z \in E \text{ tel que } |z| \} \cup \bigcup_{a \notin \Omega} B(a, \frac{1}{n}), \tag{5.108}$$

et nous définissons $K_n = \mathbb{C}V_n$. Vérifions que ces ensembles vérifient tout ce qu'il faut.

- (1) Si $a \notin \Omega$ alors a est dans tous les V_n et donc dans aucun des K_n ; nous avons donc bien $K_n \subset \Omega$.

- (2) Si $z \in \Omega$ alors nous prenons $n_1 > |z|$ puis n_2 tel que $B(z, \frac{1}{n_2}) \subset \Omega$. Alors $z \in K_n$ avec $n > \max(n_1, n_2)$.
- (3) Une chose à comprendre est que si $z \in K_n$, alors $d(z, \mathbb{C}\Omega) \geq \frac{1}{n}$. Du coup si nous prenons δ tel que

$$\frac{1}{n+1} < \delta < \frac{1}{n} \quad (5.109)$$

alors $B(z, \delta) \subset K_{n+1}$.

- (4) 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 $K_n \rightarrow \mathbb{R}$ donnée par $z \mapsto d(z, \mathbb{C}K_{n+1})$. 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

$$\Omega = \bigcup_{n=0}^{\infty} K_n \subset \bigcup_{n=0}^{\infty} \text{Int}(K_{n+1}) \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \quad (5.110)$$

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

$$K \subset \bigcup_{n=0}^{\infty} \text{Int}(K_n). \quad (5.111)$$

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

$$\frac{1}{n+1} < \delta_n < \frac{1}{n}. \quad (5.112)$$

Théorème 5.142 (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 5.147.

5.7.6 Ensembles enchaînés

Soit (x, d) un espace métrique.

Définition 5.143.

Une ϵ -chaîne 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 $0 \leq i \leq n-1$ nous avons $d(u_i, u_{i+1}) \leq \epsilon$.

*Une partie A de X est **bien enchaînée** si pour tout $\epsilon > 0$ et pour tout $a, b \in A$, il existe une ϵ -chaîne joignant a et b dans A .*

Les rationnels dans $\mathbb{R}$ sont bien enchaînés.

Proposition 5.144.

Un espace connexe est bien enchaîné.

Proposition 5.145.

La fermeture d'un ensemble bien enchaîné dans un espace métrique compact (X, d) est connexe.

Démonstration. Soit $A \subset X$ un ensemble bien enchaîné, 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 $\frac{1}{n}$ -chaîne $\{v_i^{(n)}\}_{i \in I_n}$ 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 $\lim_{k \rightarrow \infty} d(u_k, u_{k+1}) = 0$. Par conséquent la proposition 5.138 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

$$\bigcup_{x \in \bar{A}} C_{a,x} = \bar{A}. \quad (5.113)$$

Vu que le membre de gauche est une union de connexes, c'est un connexe par la proposition 5.72. $\square$

En particulier, un espace métrique compact est connexe si et seulement si il est bien enchaîné.

5.7.7 Produit fini d'espaces métriques**Définition 5.146.**

Si $(E_1, d_1), \dots, (E_n, d_n)$ sont des espaces métriques nous mettons la distance suivante sur le produit cartésien $E = E_1 \times \dots \times E_n$:

$$d(x, y) = \max_{i=1, \dots, n} d_i(x_i, y_i). \quad (5.114)$$

Théorème 5.147 ([8]).

Un produit fini d'espaces métriques non vides est compact si et seulement si chacun de ses facteurs est compact.

Démonstration. Soient $K_1, \dots, K_n$ des compacts et $K = K_1 \times \dots \times K_n$ le produit muni de sa métrique usuelle de la définition (5.146) (attention : chacun des K_i peut être de dimension infinie) :

$$d(\alpha, \beta) = \max\{d_i(\alpha_i, \beta_i)\} \quad (5.115)$$

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 5.131). 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. Nous nommons ℓ_k les limites correspondantes. Soit $\epsilon > 0$ pour chaque $k = 1, \dots, n$, il existe $N_k > 0$ tel que si $p > N_k$ alors

$$d((\alpha_p)_k - \ell_p) \leq \epsilon. \quad (5.116)$$

Ici $\alpha_p \in K$ est le p^{e} élément de la suite α et $(\alpha_p)_i \in K_i$ est la i^{e} composante de α_p . En prenant $N = \max_k N_k$ et $n > N$ nous avons

$$d(\alpha_n, (\ell_1, \dots, \ell_n)) \leq \epsilon. \quad (5.117)$$

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

$$\mathcal{P}_i = \mathcal{O}_i \times K_2 \times \dots \times K_n, \quad (5.118)$$

qui est un recouvrement de K par des ouverts (de K) d'où aucun sous-recouvrement fini ne peut être extrait. $\square$

Pour la culture générale, il y a bien entendu moyen de faire des produits dénombrables et pire d'espaces métriques.

Définition 5.148 ([64]).

Soient (E_n, d_n) des espaces métriques. Sur l'ensemble produit $E = \prod_{i=1}^{\infty} E_i$ nous définissons la métrique

$$d(x, y) = \sum_{k=1}^{\infty} \frac{1}{2^k} d'_k(x_i, y_i) \quad (5.119)$$

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 5.149 (Tykhonov dénombrable[64]).

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 5.142.

5.8 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 en tout cas métriques. Voir aussi la section 5.12 sur les espaces de Baire.

Définition 5.150.

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).

Théorème 5.151 (Baire[70]).

Une réunion dénombrable d'ensembles nulle part denses est d'intérieur vide.

Démonstration. Soit $a \in S$ 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

$$B(x_1, r_1) \cap A_1 = \emptyset. \quad (5.120)$$

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 $B(x_2, r_2) \cap A_2 = \emptyset$. Notons que $B(x_2, r_2) \cap A_1 = \emptyset$ aussi, par construction.

Par récurrence nous construisons une suite d'éléments x_n et de rayons $r_n < \epsilon/2^n$ tels que

- (1) $B(x_n, r_n) \cap A_j = \emptyset$ pour tout $j \leq n$,
- (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 converge²⁸ 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 . $\square$

28. Par le théorème 5.40

5.9 Encore de la topologie réelle

Dans cette section, nous travaillons dans l'espace $\mathbb{R}^n$ pour un certain naturel n . Nous y définissons la notion d'ouvert et de fermé, qui sont la base de la topologie générale. Notons que ces définitions n'ont de sens que relativement à l'espace ambiant, aussi un ouvert de $\mathbb{R}$ ne sera en général pas un ouvert de $\mathbb{R}^2$: d'une part, il n'y a pas d'inclusion canonique de $\mathbb{R}$ dans $\mathbb{R}^2$ (les ouverts du second ne sont même pas des sous-ensembles du premier) et, d'autre part, les définitions se basent sur la notion de boule de $\mathbb{R}^n$ qui dépend évidemment de la valeur de n (une boule dans $\mathbb{R}$ est un intervalle, dans $\mathbb{R}^2$ c'est un disque, etc.)

5.9.1 Ouverts et fermés

Définition 5.152.

La **boule ouverte** de centre $x_0 \in \mathbb{R}^n$ et de rayon $r \in \mathbb{R}^+$ est définie par

$$B(x_0, r) = \{x \in \mathbb{R}^n \text{ tel que } \|x - x_0\| < r\}, \quad (5.121)$$

tandis que la **boule fermée** de centre x_0 et de rayon r est

$$\bar{B}(x_0, r) = \{x \in \mathbb{R}^n \text{ tel que } \|x - x_0\| \leq r\}; \quad (5.122)$$

la différence est que l'inégalité dans la première est stricte.

Définition 5.153.

Une partie A de $\mathbb{R}^n$ est **ouverte** si pour tout $a \in A$ il existe $r > 0$ tel que $B(a, r) \subset A$. Une partie est donc ouverte lorsqu'elle contient une boule autour de chacun de ses éléments.

Cette définition est évidemment à mettre en rapport avec le théorème 5.3.

Le lemme suivant justifie le vocabulaire des définitions 5.152.

Lemme 5.154.

Pour tout $x \in \mathbb{R}^n$ et tout $r > 0$ la boule $B(x, r)$ 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 $B(p, r - d(p, x))$ est contenue dans $B(x, r)$. Pour cela, nous prenons $p' \in B(p, r - d(p, x))$, et nous essayons de prouver que $p' \in B(x, r)$. En effet, en utilisant l'inégalité triangulaire,

$$d(x, p') \leq d(x, p) + d(p, p') \leq d(x, p) + r - d(p, x) = r. \quad (5.123)$$

□

5.9.2 Intérieur, adhérence et frontière

Définition 5.155.

Soit $A \subset \mathbb{R}^n$ et $x \in \mathbb{R}^n$. Le point x est **intérieur** à A si il existe une boule autour de x complètement contenue dans A . L'ensemble des points intérieurs à A est noté $\text{Int } A$ ou $\overset{\circ}{A}$, de sorte qu'on a précisément

$$x \in \text{Int } A \stackrel{\text{def}}{\iff} \exists \epsilon > 0 \text{ tel que } B(x, \epsilon) \subset A.$$

Définition 5.156.

Le point x est dans l'**adhérence** de A si toute boule autour de x intersecte A . L'ensemble de ces points est noté $\text{Adh } A$ ou $\bar{A}$, et on a donc de manière plus précise

$$x \in \text{Adh } A \stackrel{\text{def}}{\iff} \forall \epsilon > 0, B(x, \epsilon) \cap A \neq \emptyset \quad (5.124)$$

Proposition 5.157.

Pour $A \subset \mathbb{R}^n$, nous avons

$$\text{Int } A \subseteq A \subseteq \text{Adh } A$$

Définition 5.158.

La **frontière** ou le **bord** de A est défini par $\partial A = \text{Adh } A \setminus \text{Int } A$. L'ensemble A est un **ouvert** si $A = \text{Int } A$, et c'est un **fermé** si $A = \text{Adh } A$.

Lemme 5.159 (Caractérisation équivalente de la frontière).

Soit un espace topologique X et une partie $S \subset X$. Un point $x \in X$ est dans ∂S si et seulement si tout voisinage de x contient un point de S et un point de S^c .

Démonstration. Supposons que tout voisinage de x contienne un point de S et un point de S^c . Alors $x \in \text{Adh}(S)$ (définition 5.156), 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 . $\square$

Corollaire 5.160.

Un ensemble et son complémentaire ont même frontière.

Démonstration. Conséquence du lemme 5.159. Les points de $\partial(S^c)$ sont caractérisés par le fait que tout voisinage contient un point de S^c et un point de $(S^c)^c = S$. $\square$

Exemple 5.161

Soit $X = [0, 1]$ muni de la topologie de la distance $|x - y|$ (définition 5.20). 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

$$B(1, r) = \{x \in X \text{ tel que } |x - 1| < r\} =]1 - r, 1] \quad (5.125)$$

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 $\mathbb{R}$. $\triangle$

Lemme 5.162 (Passage de douane[71, 72]).

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 $X \setminus \bar{A}$ ne peuvent pas recouvrir γ parce que ce sont deux ouverts disjoints alors que γ est connexe (voir la définition 5.67 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 . $\square$

On vérifiera que les notations et les dénominations sont cohérentes en prouvant la proposition suivante.

Proposition 5.163.

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 5.164.

Si $A \subset \mathbb{R}^n$ et $A^c = \mathbb{R}^n \setminus A$, nous avons

- (1) $(\text{Int } A)^c = \text{Adh}(A^c)$ et $(\text{Adh } A)^c = \text{Int}(A^c)$,
- (2) A est ouvert si et seulement si A^c est fermé,
- (3) $\text{Int } A$ est le plus grand ouvert contenu dans A ,
- (4) $\text{Adh } A$ est le plus petit fermé contenant A ,

Exemple 5.165

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, $A \cap B = \emptyset$ alors que $\bar{A} \cap \bar{B} = \{1\}$. $\triangle$

5.9.3 Point d'accumulation, point isolé

Soit $D \subset \mathbb{R}$. Un point $a \in D$ est **isolé** dans D (relativement à $\mathbb{R}$) si il existe $\varepsilon > 0$ tel que

$$[a - \varepsilon, a + \varepsilon] \cap D = \{a\}. \quad (5.126)$$

Autrement dit, il existe un intervalle autour de a dans lequel a est le seul élément de D .

Un point $a \in \mathbb{R}$ est un **point d'accumulation** de D si pour tout $\varepsilon > 0$,

$$([a - \varepsilon, a + \varepsilon] \setminus \{a\}) \cap D \neq \emptyset. \quad (5.127)$$

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 5.166

Prenons $D = [0, 1[\cup]2, 3]$. Cet ensemble n'a pas de points isolés, 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 . $\triangle$

Exemple 5.167

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. $\triangle$

[73]

5.9.4 Limite de suite

Définition 5.168 (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

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall n \geq N, \|x_n - \ell\| < \varepsilon. \quad (5.128)$$

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 $x_n \rightarrow \ell$.

Notez aussi la similarité avec la définition 5.73.

Remarque 5.169.

Nous n'écrivons pas « $\lim_{n \rightarrow \infty} x_n$ » 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 $\lim_{n \rightarrow 4} x_n$ parce que cela vaudrait x_4 et rien d'autre.

Ceci est une différence importante avec les limites de fonctions.

Lemme 5.170 (Unicité de la limite).

Il ne peut pas y avoir deux nombres différents qui satisfont à la condition (5.128). 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

$$\|x_n - \ell\| < \varepsilon \quad (5.129)$$

pour tout $n \geq N$, et $N' > 0$ tel que

$$\|x_n - \ell'\| < \varepsilon \quad (5.130)$$

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

$$\|\ell - \ell'\| = \|\ell - x_n + x_n - \ell'\| \leq \|\ell - x_n\| + \|x_n - \ell'\| < 2\varepsilon. \quad (5.131)$$

Cela prouve que $\|\ell - \ell'\| = 0$. $\square$

Le théorème de Bolzano-Weierstrass 5.131 dit que dans le cas métrique, la compacité séquentielle est équivalente à la compacité.

5.10 Application réciproque

Définition 5.171 (injection, surjection, bijection).

Soient des ensembles A et B ainsi qu'une application $f: A \rightarrow B$.

- (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 domaines sur laquelle nous la considérons.

Définition 5.172.

Soit une bijection $f: A \rightarrow B$. L'**application réciproque** de f est la fonction

$$\begin{aligned} f^{-1}: B &\rightarrow A \\ y &\mapsto \text{le } x \in A \text{ tel que } f(x) = y. \end{aligned} \quad (5.132)$$

Plus généralement si $f: X \rightarrow Y$ est une application quelconque et si $S \subset Y$ nous notons

$$f^{-1}(S) = \{x \in X \text{ tel que } f(x) \in S\}, \quad (5.133)$$

et dans le cas où S est réduit à un unique élément y , nous notons $f^{-1}(y)$ au lieu de $f^{-1}(\{y\})$. Si de plus $f^{-1}(S)$ est un singleton x , nous noterons $f^{-1}(S) = x$ et non $f^{-1}(S) = \{x\}$.

Les plus acharnés parmi les lecteurs se rendront compte de la différence ontologique fondamentale entre x et $\{x\}$.

Proposition 5.173.

Soit $f: A \subset \mathbb{R}^n \rightarrow B \subset \mathbb{R}^m$ une bijection continue. Si A est compact, alors $f^{-1}: B \rightarrow A$ est continue.

Proposition 5.174.

Soient I un intervalle dans $\mathbb{R}$ et $f: I \rightarrow \mathbb{R}$ une fonction continue strictement monotone. Alors la fonction réciproque $f^{-1}: f(I) \rightarrow \mathbb{R}$ est continue sur l'intervalle $f(I)$.

5.11 Topologie des semi-normes

Définition 5.175.

Si E est un espace vectoriel, une **semi-norme** sur E est une application $p: E \rightarrow \mathbb{R}$ telle que

- (1) $p(x) \geq 0$,
- (2) $p(\lambda x) = |\lambda|p(x)$
- (3) $p(x + y) \leq p(x) + p(y)$.

Lemme 5.176 ([74]).

Si p est une semi-norme nous avons

$$|p(x) - p(y)| \leq p(x - y). \quad (5.134)$$

Démonstration. Nous avons d'une part $p(x + h) \leq p(x) + p(h)$ et d'autre part $p(x) \leq p(x + h) + p(-h) = p(x + h) + p(h)$. En isolant $p(x + h) - p(x)$ dans chacune de ces deux inégalités,

$$-p(h) \leq p(x + h) - p(x) \leq p(h) \quad (5.135)$$

ou encore

$$|p(x + h) - p(x)| \leq p(h) \quad (5.136)$$

qui donne le résultat demandé en posant $h = y - x$. $\square$

Soit une famille $(p_i)_{i \in I}$ de semi-normes sur E . Nous construisons alors une topologie sur E de la façon suivante.

Définition 5.177 (Topologie et semi-normes [75, 76]).

Pour tout J fini dans I nous définissons les **boules ouvertes**

$$B_J(x, r) = \{y \in E \text{ tel que } p_j(y - x) < r \forall j \in J\}. \quad (5.137)$$

La **topologie** sur E donnée par la famille de semi-norme 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 $\mathcal{O}$.

Proposition 5.178.

Une suite (x_n) dans E converge vers x au sens de la topologie des semi-normes si et seulement si pour tout $i \in I$,

$$p_i(x - x_n) \rightarrow 0. \quad (5.138)$$

Démonstration. Si la suite (x_n) converge²⁹ vers x , alors pour tout ouvert $\mathcal{O}$ autour de x , il existe un N tel que si $n \geq N$, alors $x_n \in \mathcal{O}$. En particulier pour tout j et pour tout $\epsilon > 0$, il doit exister un $n \geq N_j$ 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 $n \geq N_i$ implique $p_i(x - x_n) \leq \epsilon$. 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 $p_j(x - x_n) \leq \epsilon$ pour tout j et donc $x_n \in B_J(x, r)$. $\square$

La proposition suivante est un vulgaire plagiat de la proposition 5.118.

Proposition 5.179.

Soit une application $f: \mathbb{R} \rightarrow (E, p_i)_{i \in I}$. 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 $f(V) \subset W$,

29. Définition 5.4.

(3) pour tout $i \in I$ et $\epsilon > 0$ il existe $\delta > 0$ tel que

$$f(B(t_0, \delta)) \subset B_i(f(t_0), \epsilon). \quad (5.139)$$

Démonstration. L'équivalence (1) $\Leftrightarrow$ (2) est la définition 5.52.

Prouvons (2) $\Rightarrow$ (3). Soit $i \in I$ et $\epsilon > 0$ et considérons la boule $B_i(f(t_0), \epsilon)$, qui est un ouvert de E contenant $f(t_0)$. Il existe donc un ouvert V autour de t_0 tel que $f(V) \subset B_i(f(t_0), \epsilon)$. En particulier V contient une boule $B(t_0, \delta)$ et nous avons

$$f(B(t_0, \delta)) \subset f(V) \subset B_i(f(t_0), \epsilon). \quad (5.140)$$

Prouvons (3) $\Rightarrow$ (2). Soit W un ouvert autour de $f(t_0)$. Il existe un $i \in I$ et $\epsilon > 0$ tel que $B_i(f(t_0), \epsilon) \subset W$. Nous avons alors un $\delta > 0$ tel que

$$f(B(t_0, \delta)) \subset B_i(f(t_0), \epsilon) \subset W. \quad (5.141)$$

□

Lorsqu'on a un espace E muni d'une quantité dénombrable de semi-normes $\{p_k\}_{k \in I}$ nous définissons l'écart³⁰

$$d(x, y) = \sup_{k \geq 1} \min \left\{ \frac{1}{k}, p_k(x - y) \right\}. \quad (5.142)$$

Notons que cette écart est invariant par translation au sens où pour tout x, y, h dans E nous avons

$$d(x + h, y + h) = \sup_{k \geq 1} \min \left\{ \frac{1}{k}, p_k(x - y) \right\} = d(x, y). \quad (5.143)$$

Proposition 5.180 ([74]).

La topologie donnée par les boules

$$B(a, r) = \{x \in E \text{ tel que } \forall k \leq \frac{1}{r}, p_k(x - a) < r\} \quad (5.144)$$

est la même que celle «usuelle» donnée par les semi-normes. 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 (5.144) et par P celle des semi-normes : P -continue, d -ouvert, etc.

D'abord nous avons

$$B(a, r) = \bigcap_{k \leq \frac{1}{r}} B_k(a, r). \quad (5.145)$$

Si $\mathcal{O}$ est un d -ouvert, il contient une d -boule autour de chacun de ses points. Or d'après la formule (5.145), 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 semi-normes p_k sont d -continues. En effet soient $k \in \mathbb{N}$, $\epsilon \leq \frac{1}{k}$ et $x, y \in E$ tels que $d(x, y) \leq \epsilon$; nous avons

$$|p_k(y) - p_k(x)| \leq p_k(x - y) \quad (5.146a)$$

$$= \min \left\{ \frac{1}{k}, p_k(x - y) \right\} \quad (5.146b)$$

$$\leq d(x, y) \quad (5.146c)$$

$$\leq \epsilon. \quad (5.146d)$$

30. Dans le cas de $E = \mathcal{D}(K)$, la première semi-norme est numérotée à zéro, donc il faudra poser $d(\varphi_1, \varphi_2)$ avec p_{k-1} au lieu de p_k .

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 $x \in B_k(a, r)$ et montrons que si ϵ est suffisamment petit, la d -boule $B(x, \epsilon)$ est incluse à $B_k(a, r)$. Pour cela prenons $y \in B(x, \epsilon)$; nous avons

$$|p_k(a - x) - p_k(a - y)| \leq d(x, y) \leq \epsilon. \quad (5.147)$$

Par conséquent le nombre $p_k(a - y)$ est dans l'intervalle

$$p_k(a - x) \pm \epsilon \quad (5.148)$$

et il suffit de prendre $\epsilon < \frac{r - p_k(a - x)}{2}$. □

5.11.1 Espace dual

Définition 5.181.

Soit F , un espace métrique et E un espace topologique vectoriel. Une topologie possible³¹ sur l'espace des applications linéaires $\mathcal{L}(E, F)$ est la **topologie *-faible** qui est la topologie des semi-normes

$$p_v(T) = \|T(v)\|_F. \quad (5.149)$$

C'est une famille de semi-normes 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 $E \rightarrow \mathbb{R}$.

La proposition suivante indique qu'elle est un peu la topologie de la convergence ponctuelle.

Proposition 5.182.

Soit E un espace muni de la topologie des semi-normes $\{p_i\}_{i \in I}$ et F un espace métrique. Soit 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 :

$$T_n \xrightarrow{*} T \quad (5.150a)$$

$$p_v(T_n - T) \rightarrow 0 \forall v \in E \quad \text{proposition 5.178} \quad (5.150b)$$

$$\|T_n(v) - T(v)\|_E \rightarrow 0 \forall v \in E \quad (5.150c)$$

$$T_n(v) \xrightarrow{E} T(v). \quad (5.150d)$$

□

5.11.2 Espace $C^k(\mathbb{R}, E')$

Nous revenons à nos histoires de limites de la définition 5.4.

Proposition 5.183 (Unicité de la limite dans un dual topologique).

Soit E un espace métrique et E' son dual topologique muni de sa topologie de la définition 5.181. Il y a unicité de l'élément de E' vers lequel une fonction $u: \mathbb{R} \rightarrow E'$ peut converger.

Démonstration. Soit T un élément vers lequel u_t converge lorsque $t \rightarrow t_0$. Soit $\epsilon > 0$ 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 $|t - t_0| \leq \delta$. Nous avons donc, pour tout $x \in E$, la limite (dans $\mathbb{R}$) :

$$\lim_{t \rightarrow t_0} u_t(x) = T(x). \quad (5.151)$$

31. C'est, dans l'idée, celle qui sera choisie pour les espaces de distributions, voir la définition 22.10.

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

$$\lim_{t \rightarrow t_0} u_t(x) = T'(x). \quad (5.152)$$

Par unicité de la limite dans $\mathbb{R}$ nous devons alors avoir $T(x) = T'(x)$ pour tout x , c'est à dire $T = T'$. $\square$

Proposition 5.184.

Soit une fonction continue $u: \mathbb{R} \rightarrow E'$. 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 $\mathbb{R}$

$$\lim_{y \rightarrow t_0} u_t(x) = u_{t_0}(x), \quad (5.153)$$

- (3) nous avons la limite dans E'

$$\lim_{t \rightarrow t_0} u_t = u_{t_0}. \quad (5.154)$$

Démonstration. Soient $x \in E$ et $\epsilon > 0$. Par la proposition 5.179 la continuité de u donne un $\delta > 0$ tel que

$$u_{B(t_0, \delta)} \subset B_x(u_{t_0}, \epsilon). \quad (5.155)$$

C'est à dire que si $|t - t_0| \leq \delta$ nous avons

$$|u_{t_0}(x) - u_t(x)| < \epsilon, \quad (5.156)$$

ce qui signifie bien que la fonction $t \mapsto u_t(x)$ est continue en tant que fonction $\mathbb{R} \rightarrow \mathbb{R}$. Cela est le point (1). Le théorème de limite et continuité dans $\mathbb{R}$ nous donne immédiatement la limite (5.153).

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

$$u_{B(t_0, \delta)} \subset B_i(u_{t_0}, \epsilon) \subset \mathcal{O}. \quad (5.157)$$

Cela signifie bien que

$$|t - t_0| \leq \delta \Rightarrow u_t \in \mathcal{O}, \quad (5.158)$$

c'est à dire que nous avons la limite $\lim_{t \rightarrow t_0} u_t = u_{t_0}$ dans E' . Pour dire cela nous avons utilisé la définition 5.48 de la limite et le résultat d'unicité 5.183. $\square$

Définition 5.185.

Si nous avons une application $u: \mathbb{R} \rightarrow E'$ nous considérons sa **dérivée** donnée par la limite

$$u'_{t_0} = \lim_{t \rightarrow t_0} \frac{u_t - u_{t_0}}{t - t_0}. \quad (5.159)$$

Cela est un nouvel élément de E' (pour peu que la limite existe). La fonction $u': \mathbb{R} \rightarrow E'$ 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 utilisation que nous ferons de ces espaces seront les espaces de fonctions à valeurs dans les distributions tempérées dont nous parlerons dans la section 22.4.

5.12 Espaces de Baire

Définition 5.186.

Un **espace de Baire** est un espace topologique dans lequel toute intersection dénombrable d'ouverts denses est dense.

Théorème 5.187 (Théorème de Baire[77]).

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. **Espaces topologiques localement compact**

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 emboîtés B_n telle que

$$\bigcap_{n \in \mathbb{N}} U_n \cap V \tag{5.160}$$

contient l'intersection des B_n . Par le théorème 5.120 des fermés emboîtés (que nous utilisons parce que E est métrique et complet), cette intersection est non vide.

Ouvert d'un espace de Baire

□

Une des application du théorème de Baire est le théorème de Banach-Steinhaus 18.8.

Chapitre 6

Espaces vectoriels

6.1 Parties libres, génératrices, bases et dimension

Définition 6.1.

Un sous-ensemble $B = \{v_1, \dots, v_q\}$ de $\mathbb{R}^m$ est une **base** de $\mathbb{R}^m$ s'il satisfait les conditions suivantes

— B est **libre**, c'est à dire

$$\sum_{i=1}^q a_i v_i = 0_m \quad \Leftrightarrow \quad a_i = 0, \forall i = 1, \dots, q.$$

— B est **générateur**, c'est à dire que pour tout x dans $\mathbb{R}^m$ il existe un ensemble de coefficients $\{a_i \in \mathbb{R}, i = 1, \dots, n\}$ tel que

$$\sum_{i=1}^q a_i v_i = x.$$

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.

La base de $\mathbb{R}^m$ qu'on dit **canonique** (c.à.d. celle qu'on utilise tout le temps) est $\mathcal{B} = \{e_1, \dots, e_m\}$, où le vecteur e_j est

$$e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow j\text{-ème} \quad .$$

La composante numéro j de e_i est 1 si $i = j$ et 0 si $i \neq j$. Cela s'écrit $(e_i)_j = \delta_{ij}$ où δ est le **symbole de Kronecker** défini par

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases} \quad (6.1)$$

Les éléments de la base canonique de $\mathbb{R}^m$ peuvent donc être écrits $e_i = \sum_{k=1}^m \delta_{ik} e_k$.

Définition 6.2.

Si E est un espace vectoriel, une partie finie $(u_i)_{1 \leq i \leq n}$ de E est **libre** si l'égalité

$$a_1 u_1 + \dots + a_n u_n = 0 \quad (6.2)$$

implique $a_i = 0$ pour tout i .

Une partie infinie est libre si toute ses parties finies le sont.

La définition de liberté dans le cas des parties infinies a son importance lorsqu'on parle d'espaces vectoriels de dimension infinies (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.

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 6.3.

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 – qui n'est pas exactement la dimension d'un espace vectoriel fixé. Pour $n = 1$, nous avons $E = \langle e \rangle$ et donc si $v_1, v_2 \in E$ nous avons $v_1 = \lambda_1 e$, $v_2 = \lambda_2 e$ et donc $\lambda_2 v_1 - \lambda_1 v_2 = 0$. Cela prouve le résultat dans le cas de la dimension 1.

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 λ_{ij} par

$$v_i = \sum_{k=1}^n \lambda_{ik} e_k \quad (6.3)$$

Vu que

$$v_{n+1} = \sum_{k=1}^n \lambda_{n+1,k} e_k \neq 0, \quad (6.4)$$

quitte à changer la numérotation des e_i nous pouvons supposer que $\lambda_{n+1,n} \neq 0$. Nous considérons les vecteurs

$$w_i = \lambda_{n+1,n} v_i - \lambda_{i,n} v_{n+1}. \quad (6.5)$$

En calculant un peu,

$$w_i = \lambda_{n+1,n} \sum_k \lambda_{i,k} e_k - \lambda_{i,n} \sum_k \lambda_{n+1,k} e_k \quad (6.6a)$$

$$= \sum_{k=1}^{n-1} (\lambda_{n+1,n} \lambda_{i,k} - \lambda_{i,n} \lambda_{n+1,k}) e_k \quad (6.6b)$$

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

$$0 = \sum_{i=1}^n \alpha_i w_i = \sum_{i=1}^n \alpha_i \lambda_{n+1,n} v_i - \left(\sum_{i=1}^n \alpha_i \lambda_{i,n} \right) v_{n+1}. \quad (6.7)$$

Vu que $\lambda_{n+1,n} \neq 0$ et que parmi les α_i au moins un est non nul, nous avons au moins un des produits $\alpha_i \lambda_{n+1,n}$ qui est non nul. Par conséquent (6.7) est une combinaison linéaire nulle non triviale des vecteurs de $\{v_1, \dots, v_{n+1}\}$. Cette partie est donc liée. $\square$

Lemme 6.4.

Soit L une partie libre et G une partie génératrice. Soit B une partie maximale parmi les parties libres L' telles que $L \subset L' \subset G$. Alors B est une base.

Qu'entend-on par «maximale»? La partie B doit être libre, contenir L , être contenue dans G et de plus avoir la propriété que $\forall x \in G \setminus B$, la partie $B \cup \{x\}$ est liée.

Démonstration. D'abord si G est une base, alors toutes les parties de G sont libres et le maximum est $B = G$. Dans ce cas le résultat est évident. Nous supposons donc que G est liée.

La partie $B = \{b_1, \dots, b_l\}$ est libre parce qu'on l'a prise parmi les libres. Montrons que B est génératrice. Soit $x \in G \setminus B$; par hypothèse de maximalité, $B \cup \{x\}$ est liée, c'est à dire qu'il existe des nombres λ_i, λ_x non tous nuls tels que

$$\sum_{i=1}^l \lambda_i b_i + \lambda_x x = 0. \quad (6.8)$$

Si $\lambda_x = 0$ alors un de λ_i doit être non nul et l'équation (6.8) 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

$$x = \frac{1}{\lambda_x} \sum_{i=1}^l \lambda_i b_i. \quad (6.9)$$

Donc tous les éléments de $G \setminus B$ sont des combinaisons linéaires des éléments de B , et par conséquent, G étant génératrice, tous les éléments de E sont combinaisons linéaires d'éléments de B . $\square$

Théorème 6.5 (Théorème de la base incomplète).

Soit E un espace vectoriel de type fini sur le corps $\mathbb{K}$.

- (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.

Démonstration. Point par point.

- (1) Vu que E est de type fini, il admet une partie génératrice G de cardinal fini n . Donc une partie libre est de cardinal au plus n par le lemme 6.3. Soit L , une partie libre contenue dans G (ça existe : par exemple $L = \emptyset$). La partie B maximale libre contenue dans G et contenant L est une base par le lemme 6.4.
- (2) Notons que puisque E lui-même est générateur, le point (1) implique que toute partie libre peut être étendue en une base.
- (3) Soient B et B' , deux bases. En particulier B est génératrice et B' est libre, donc le lemme 6.3 indique que $\text{Card}(B') \leq \text{Card}(B)$. Par symétrie on a l'inégalité inverse. Donc $\text{Card}(B) = \text{Card}(B')$.

$\square$

Remarque 6.6.

Le théorème de la base incomplète 6.5(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 6.7.

La **dimension** d'un espace vectoriel de type fini est la cardinal d'une de ses bases.

Le théorème suivant est essentiellement une reformulation du théorème 6.5.

Théorème 6.8.

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.

(3) Si E est un espace vectoriel de dimension n , alors toute partie libre contenant n éléments est une base.

Démonstration. Nous ne prouvons que le troisième point. Une partie libre contenant n éléments peut être étendue en une base ; si ladite extension est non triviale (c'est à dire qu'on ajoute vraiment au moins un élément) une telle base contiendra une partie de $n + 1$ éléments qui serait liée par le lemme 6.3. $\square$

Soit F un sous-espace vectoriel de l'espace vectoriel E . La **codimension** de F dans E est

$$\text{codim}_E(F) = \dim(E/F). \quad (6.10)$$

6.2 Applications linéaires

6.2.1 Définition

Définition 6.9.

Une application $T : \mathbb{R}^m \rightarrow \mathbb{R}^n$ est dite **linéaire** si

- $T(x + y) = T(x) + T(y)$ pour tout x et y dans $\mathbb{R}^m$,
- $T(\lambda x) = \lambda T(x)$ pour tout λ dans $\mathbb{R}^m$ et λ dans $\mathbb{R}$.

Si V et W sont deux espaces vectoriels réels, nous définissons de la même manière une application linéaire de V dans W comme étant une application $T : V \rightarrow W$ telle que $T(v_1 + v_2) = T(v_1) + T(v_2)$ et $T(\lambda v) = \lambda T(v)$ pour tout v, v_1, v_2 dans V et pour tout réel λ .

L'ensemble des applications linéaires de $\mathbb{R}^m$ vers $\mathbb{R}^n$ est noté $\mathcal{L}(\mathbb{R}^m, \mathbb{R}^n)$, et plus généralement nous notons $\mathcal{L}(V, W)$ l'ensemble des applications linéaires de V dans W .

Exemple 6.10

Soit $m = n = 1$. 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 $\mathbb{N}$. $\triangle$

Définition 6.11.

Si E est un espace vectoriel, une application linéaire $E \rightarrow E$ est un **endomorphisme** de E . L'ensemble des endomorphismes de E est noté $\text{End}(E)$. Une application linéaire bijective $E \rightarrow E$ est un **automorphisme** de E . L'ensemble des automorphismes de E est noté $\text{Aut}(E)$.

6.2.2 Rang

Définition 6.12.

Si $T : V \rightarrow W$ est une application linéaire, son **rang** est la dimension de son image.

Le théorème suivant est valable également en dimension infinie ; ce sera une des rares incursions en dimension infinie de ce chapitre.

Théorème 6.13 (Théorème du rang).

Soient E et F deux espaces vectoriels (de dimensions finies ou non) et soit $f : E \rightarrow F$ une application linéaire. Alors le rang¹ de f est égal à la codimension du noyau, c'est à dire

$$\text{rang}(f) + \dim \ker f = \dim E. \quad (6.11)$$

1. Définition 6.12.

Dans le cas de dimension infinie afin d'éviter les problèmes d'arithmétique avec l'infini nous énonçons le théorème en disant que si $(u_s)_{s \in S}$ est une base de $\ker(f)$ et si $(f(v_t))_{t \in T}$ est une base de $\text{Image}(f)$ alors $(u_s)_{s \in S} \cup (v_t)_{t \in T}$ est une base de E .

Démonstration. Nous devons montrer que

$$(u_s)_{s \in S} \cup (v_t)_{t \in T} \quad (6.12)$$

est libre et générateur.

Soit $x \in E$. Nous définissons les nombres x_t par la décomposition de $f(x)$ dans la base $(f(v_t))$:

$$f(x) = \sum_{t \in T} x_t f(v_t). \quad (6.13)$$

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) :

$$x - \sum_t x_t v_t = \sum_s x_s u_s. \quad (6.14)$$

Par conséquent

$$x = \sum_s x_s u_s + \sum_t x_t v_t. \quad (6.15)$$

En ce qui concerne la liberté nous écrivons

$$\sum_t x_t v_t + \sum_s x_s u_s = 0. \quad (6.16)$$

En appliquant f nous trouvons que

$$\sum_t x_t f(v_t) = 0 \quad (6.17)$$

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 $x_s = 0$. $\square$

Un exemple d'utilisation de ce théorème en dimension infinie sera donné dans le cadre du théorème de Fréchet-Riesz, théorème 17.19.

Définition 6.14.

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 $A = PBP^{-1}$.

Lemme 6.15.

Une matrice de rang r dans $\mathbb{M}(n, \mathbb{K})$ est équivalente à la matrice par blocs

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \quad (6.18)$$

Démonstration. Nous devons prouver que pour toute matrice $A \in \mathbb{M}(n, \mathbb{K})$ de rang r , il existe $P, Q \in \text{GL}(n, \mathbb{K})$ 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 $i > r$.

Nous considérons la matrice inversible P telle que $Pe_i = f_i$. Elle vérifie

$$APe_i = Af_i = \begin{cases} 0 & \text{si } i > r \\ \neq 0 & \text{sinon.} \end{cases} \quad (6.19)$$

La matrice AP se présente donc sous la forme

$$AP = \begin{pmatrix} M & 0 \\ * & 0 \end{pmatrix} \quad (6.20)$$

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

$$QAPe_i = \begin{cases} e_i & \text{si } i < r \\ 0 & \text{sinon.} \end{cases} \quad (6.21)$$

Cela signifie que QAP est la matrice J_r . □

Corollaire 6.16 (Équivalence et rang).

Deux matrices sont équivalentes² si et seulement si elles ont même rang.

Démonstration. D'abord il y a des implicites dans l'énoncé. Vu que nous voulons soit pas 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 carré représentant des applications linéaires de l'espace vectoriel $E = \mathbb{K}^n$ vers lui-même.

Par le lemme 6.15, 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 : $A = PBQ^{-1}$ avec P et B inversibles. Alors

$$\text{Image}(PBQ^{-1}) = \{PBQ^{-1}v \text{ tel que } v \in E\} \quad (6.22a)$$

$$= PB \underbrace{\{Q^{-1}v \text{ tel que } v \in E\}}_{=E} \quad (6.22b)$$

$$= P(B(E)). \quad (6.22c)$$

L'ensemble $B(E)$ est un sous-espace vectoriel de E . Vu que le rang de P est maximum, la dimension de $P(B(E))$ est la même que celle de $B(E)$. Par conséquent

$$\dim(\text{Image}(PBQ^{-1})) = \dim(B(E)) = \text{rang}(B). \quad (6.23)$$

Le membre de gauche de cela n'est autre que $\text{rang}(A) = \dim(\text{Image}(PBQ^{-1}))$. □

6.3 Matrice d'une application linéaire

6.3.1 Écriture dans une base

Exemple 6.17

Soit $m = n$. 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, parce que

$$U_\lambda(ax) = \lambda(ax) + v \neq \lambda(bx + v) = aU_\lambda(x).$$

△

Exemple 6.18

Soit A une matrice fixée de $\mathcal{M}_{n \times m}$. La fonction $T_A: \mathbb{R}^m \rightarrow \mathbb{R}^n$ définie par $T_A(x) = Ax$ est une application linéaire. En effet,

$$— T_A(x + y) = A(x + y) = Ax + Ay = T_A(x) + T_A(y),$$

2. Définition 6.14(1).

$$— T_A(ax) = A(ax) = a(Ax) = aT_A(x).$$

△

On peut observer que, si on identifie $\mathcal{M}_{1 \times 1}$ et $\mathbb{R}$, on obtient le premier exemple comme cas particulier.

Proposition 6.19.

Toute application linéaire T de $\mathbb{R}^m$ dans $\mathbb{R}^n$ s'écrit de manière unique par rapport aux bases canoniques de $\mathbb{R}^m$ et $\mathbb{R}^n$ sous la forme

$$T(x) = Ax,$$

avec A dans $\mathcal{M}_{n \times m}$.

Démonstration. Soit x un vecteur dans $\mathbb{R}^m$. On peut écrire x sous la forme $x = \sum_{i=1}^m x_i e_i$. Comme T est une application linéaire on a

$$T(x) = \sum_{i=1}^m x_i T(e_i).$$

Les images de la base de $\mathbb{R}^m$, $T(e_j)$, $j = 1, \dots, m$, sont des éléments de $\mathbb{R}^n$, donc on peut les écrire sous la forme de vecteurs

$$T(e_i) = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}.$$

On obtient alors

$$T(x) = \sum_{i=1}^m x_i T(e_i) = \sum_{i=1}^m x_i \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = Ax.$$

□

Définition 6.20.

Une application $S : \mathbb{R}^m \rightarrow \mathbb{R}^n$ est dite **affine** si elle est la somme d'une application linéaire et d'une application constante. Autrement dit, S est affine s'il existe $T : \mathbb{R}^m \rightarrow \mathbb{R}^n$, linéaire, telle que $S(x) - T(x)$ soit un vecteur constant dans $\mathbb{R}^n$.

Exemple 6.21

Les exemples les plus courants d'applications affines sont les droites et les plans ne passant pas par l'origine.

Les droites Une droite dans $\mathbb{R}^2$ (ou $\mathbb{R}^3$) qui ne passe pas par l'origine est le graphe d'une fonction de la forme $s(x) = ax + b$ (ou $s(t) = ux + v$, avec u et v dans $\mathbb{R}^2$). On reconnaît ici la fonction de l'exemple 6.17.

Les plans De la même façon nous savons que tout plan qui ne passe pas par l'origine dans $\mathbb{R}^3$ est le graphe d'une application affine, $P(x, y) = (a, b)^T \cdot (x, y)^T + (c, d)^T$.

△

Lemme 6.22 ([78]).

Soit une application linéaire $f : E \rightarrow F$.

- (1) L'application f est injective si et seulement si il existe $g : F \rightarrow E$ telle que $g \circ f = \text{Id}|_E$.
- (2) L'application f est surjective si et seulement si il existe $g : F \rightarrow E$ telle que $f \circ g = \text{Id}|_F$.

Démonstration. Nous démontrons séparément les deux affirmations.

- (1) Si f est injective, alors $f: E \rightarrow \text{Image}(f)$ est un isomorphisme. Si V est un supplémentaire de $\text{Image}(f)$ dans F (c'est à dire $F = \text{Image}(f) \oplus V$) alors nous pouvons poser $g(x + v) = f^{-1}(x)$ où $x + v$ est la décomposition (unique) d'un élément de F en $x \in \text{Image}(f)$ et $v \in V$. Avec cela nous avons bien $g \circ f = \text{Id}$.
Inversement, si il existe $g: F \rightarrow E$ telle que $g \circ f = \text{Id}$ alors $f: E \rightarrow E$ 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

$$\begin{aligned} g: F &\rightarrow E \\ \sum_k a_k f(x_k) &\mapsto \sum_k x_k. \end{aligned} \quad (6.24)$$

Cela donne $f \circ g = \text{Id}|_F$ parce que si $v \in F$ alors $v = \sum_k v_k f(x_k)$ avec $v_k \in \mathbb{K}$, et nous avons

$$(f \circ g)(v) = \sum_k v_k (f \circ g)f(x_k) = f\left(\sum_k v_k x_k\right) = \sum_k f(x_k) = v. \quad (6.25)$$

Inversement, si il existe $g: F \rightarrow E$ tel que $f \circ g = \text{Id}$ alors f soit être surjective parce que

$$F = \text{Image}(f \circ g) = f(\text{Image}(g)) \subset \text{Image}(f). \quad (6.26)$$

□

6.3.2 Changement de base : vecteurs de base

Soit un espace vectoriel V muni d'une base $\{e_i\}$ et une application linéaire inversible $Q: V \rightarrow V$ dont nous notons (Q_{ij}) les coordonnées dans la base $\{e_i\}$. Nous considérons aussi la base $e'_i = Qe_i$.

Nous exprimons les vecteurs e'_i en termes des vecteurs e_i et inversement de la façon suivante. D'abord

$$e'_i = Qe_i = \sum_{kl} Q_{kl}(e_i)_k e_l = \sum_l Q_{il} e_l \quad (6.27)$$

donc

$$e'_i = \sum_k Q_{ik} e_k. \quad (6.28)$$

6.23.

Afin de ne pas se tromper dans les indices, il est bon d'utiliser systématiquement les noms " $ijk \dots$ " pour les indices de la base $\{e_i\}$ et les noms " $\alpha\beta\gamma \dots$ " pour les indices de la base $\{e'_\alpha\}$. Nous écrivons donc

$$e'_\alpha = \sum_i Q_{i\alpha} e_i. \quad (6.29)$$

Pour trouver la transformation inverse, nous multiplions par $(Q^{-1})_{\alpha j}$ et nous sommes sur α :

$$\sum_\alpha (Q^{-1})_{\alpha j} e'_\alpha = \sum_{i\alpha} Q_{i\alpha} Q_{\alpha j}^{-1} e_i = e_j \quad (6.30)$$

donc

$$e_j = \sum_\alpha (Q^{-1})_{\alpha j} e'_\alpha. \quad (6.31)$$

Quelque remarques :

- (1) Notons que nous ne pouvons pas écrire formellement quelque chose comme $f = Qe$.
- (2) La matrice Q vient toujours avec les indices de type $Q_{i\alpha}$ (latin en premier et grec en second) tandis que la matrice de l'application inverse Q^{-1} vient toujours avec les indices de type $(Q^{-1})_{\alpha i}$.

Ceci est un puissant outil pour ne pas se tromper lors des manipulations d'indices et en particulier lorsque nous renommons des indices.

6.3.3 Changement de base : coordonnées

Un vecteur x peut s'écrire des façons suivantes dans les deux bases considérées :

$$x = \sum_i x_i e_i = \sum_\alpha x'_\alpha e'_\alpha. \quad (6.32)$$

En remplaçant e_i par sa valeur (6.31) nous obtenons l'égalité

$$\sum_{k\alpha} x_k (Q^{-1})_{\alpha k} e'_\alpha = \sum_\alpha x'_\alpha e'_\alpha \quad (6.33)$$

et par unicité de la décomposition d'un vecteur dans une base nous déduisons

$$x'_\alpha = \sum_k (Q^{-1})_{\alpha k} x_k. \quad (6.34)$$

De même en remplaçant e'_α par sa valeur (6.29) nous trouvons

$$x_i = \sum_\alpha Q_{i\alpha} x'_\alpha. \quad (6.35)$$

Attention : il n'est pas question d'écrire quelque chose comme $x = Qx'$ parce qu'il n'y a pas de vecteur x' .

6.3.4 Changement de base : matrice d'une application linéaire

Soit une application linéaire $f: V \rightarrow V$ de matrice A dans la base $\{e_i\}$ et de matrice A' dans la base $\{e'_\alpha\}$. Notre but est maintenant d'exprimer A' en termes de A et de Q .

Nous avons l'égalité

$$f(x) = \sum_{kl} A_{kl} x_l e_k = \sum_{\alpha\beta} A'_{\alpha\beta} x'_\beta e'_\alpha. \quad (6.36)$$

Il suffit d'y substituer les valeurs (6.35) et (6.31) :

$$f(x) = \sum_{kl} A_{kl} \sum_\beta Q_{l\beta} x'_\beta \sum_\alpha (Q^{-1})_{\alpha k} e'_\alpha = \sum_{\alpha\beta} (Q^{-1} A Q)_{\alpha\beta} x'_\beta e'_\alpha. \quad (6.37)$$

Cela est égal à $\sum_{\alpha\beta} A'_{\alpha\beta} x'_\beta e'_\alpha$ pour tout x . En tenant encore compte de l'unicité de la décomposition du vecteur $f(x)$ dans la base $\{e'_\alpha\}$ nous déduisons

$$A' = Q^{-1} A Q. \quad (6.38)$$

Remarque 6.24.

L'égalité (6.38) est une égalité de matrices, et non une égalité d'applications linéaire. Il n'est pas question d'écrire quelque chose comme $f' = Q^{-1} \circ f \circ Q$.

6.3.5 Changement de base : matrice d'une forme bilinéaire

Soit une forme bilinéaire $q: V \times V \rightarrow \mathbb{R}$ de matrice (q_{ij}) dans la base $\{e_i\}$ et de matrice $q'_{\alpha\beta}$ dans la base $\{e'_\alpha\}$. Nous notons le changement de variables $e'_\alpha = \sum_i Q_{i\alpha} e_i$. Nous avons l'égalité

$$q(x, y) = \sum_{ij} q_{ij} x_i y_j = \sum_{\alpha\beta} q'_{\alpha\beta} x'_\alpha y'_\beta. \quad (6.39)$$

En remplaçant x_i et y_j par leurs valeurs en termes des x'_α et y'_β nous trouvons

$$q(x, y) = \sum_{ij\alpha\beta} q_{ij} Q_{i\alpha} x'_\alpha Q_{j\beta} y'_\beta, \quad (6.40)$$

c'est à dire

$$q' = Q^t q Q. \quad (6.41)$$

Encore une fois, cette égalité est une égalité de matrices, et non de formes bilinéaires, et encore moins d'applications linéaires.

Remarque 6.25.

La «loi de transformation» (6.41) n'est pas la même que la loi de transformation (6.38).

6.4 Dualité

Proposition 6.26.

Si A est la matrice d'une application linéaire, alors le rang de cette application linéaire est égal à la taille de la plus grande matrice carré de déterminant non nul contenue dans A .

Définition 6.27.

Si E est un espace vectoriel sur $\mathbb{K}$, le **dual** de E est l'ensemble des formes linéaires sur E . Le **dual topologique** est l'ensemble des formes linéaires continues de E vers $\mathbb{K}$.

En dimension infinie, ces deux notions ne coïncident pas, voir la proposition 6.217 et la remarque 6.218.

6.4.1 Orthogonal

Soit E , un espace vectoriel, et F une sous-espace de E . L'**orthogonal** de F est la partie $F^\perp \subset E^*$ donnée par

$$F^\perp = \{\alpha \in E^* \text{ tel que } \forall x \in F, \alpha(x) = 0\}. \quad (6.42)$$

Cette définition d'orthogonal via le dual n'est pas du pur snobisme. En effet, la définition «usuelle» qui ne parle pas de dual,

$$F^\perp = \{y \in E \text{ tel que } \forall x \in F, y \cdot x = 0\}, \quad (6.43)$$

demande la donnée d'un produit scalaire. Évidemment dans le cas de $\mathbb{R}^n$ munie 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.

Si $B \subset E^*$, on note B° son orthogonal :

$$B^\circ = \{x \in E \text{ tel que } \omega(x) = 0 \forall \omega \in B\}. \quad (6.44)$$

Notons qu'on le note B° 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.

La définition (6.42) est intrinsèque : elle ne dépend que de la structure d'espace vectoriel.

Proposition 6.28.

Soit E un espace vectoriel, et F un sous-espace vectoriel. Alors nous avons

$$\dim F + \dim F^\perp = \dim E. \quad (6.45)$$

Démonstration. Soit $\{e_1, \dots, e_p\}$ une base de F que nous complétons en une base $\{e_1, \dots, e_n\}$ de E par le théorème 6.5. Soit $\{e_1^*, \dots, e_n^*\}$ la base duale. Alors nous prouvons que $\{e_{p+1}^*, \dots, e_n^*\}$ est une base de $F^\perp$.

Déjà c'est une partie libre en tant que partie d'une base.

Ensuite ce sont des éléments de F^{perp} parce que si $i \leq p$ et si $k \geq 1$ nous avons $e_{p+k}^*(e_i^*) = 0$; donc oui, $e_{p+k}^* \in F^\perp$.

Enfin $F^\perp \subset \text{Span}\{e_{p+1}^*, e_n^*\}$ 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 $i \leq p$. Donc $\omega = \sum_{i=p+1}^n \omega_k e_k^*$. $\square$

6.4.2 Transposée

Définition 6.29.

Si $f: E \rightarrow F$ est une application linéaire entre deux espaces vectoriels, la **transposée** est l'application $f^t: F^* \rightarrow E^*$ donnée par

$$f^t(\omega)(x) = \omega(f(x)). \quad (6.46)$$

pour tout $\omega \in F^*$ et $x \in E$.

Lemme 6.30.

Soit E muni de la base $\{e_i\}$ et F muni de la base $\{g_i\}$ et une application $f: E \rightarrow F$. 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^* .

Démonstration. Nous allons montrer que les formes $f^t(g_i^*)$ et $\sum_k (A^t)_{ik} g_k^*$ sont égales en les appliquant à un vecteur.

Par définition de la matrice d'une application linéaire dans une base,

$$f^t(g_i^*) = \sum_j (f^t)_{ij} e^{*j}, \quad (6.47)$$

et

$$f(e_k) = \sum_l A_{kl} g_l. \quad (6.48)$$

Du coup, si $x = \sum_k x_k e_k$, nous avons

$$f^t(g_i^*)x = \sum_{kl} x_k g_i^* A_{kl} g_l = \sum_{kl} x_k A_{kl} \delta_{il} = \sum_k x_k A_{ki} = \sum_k (A^t)_{ik} x_k. \quad (6.49)$$

D'autre part,

$$\sum_k (A^t)_{ik} g_k^* x = \sum_{kl} (A^t)_{ik} g_k^* x_l e_l = \sum_k (A^t)_{ik} x_k. \quad (6.50)$$

Le fait que (6.49) et (6.50) donnent le même résultat prouve le lemme. $\square$

En corollaire, les rangs de f et de f^t sont égaux parce que le rang est donné par la plus grande matrice carré de déterminant non nul. Nous prouvons cependant ce résultat de façon plus intrinsèque.

Lemme 6.31 (Gilles Dubois).

Si $f: E \rightarrow F$ est une application linéaire, alors

$$\text{rang}(f) = \text{rang}(f^t). \quad (6.51)$$

Démonstration. Nous posons $\dim \ker(f) = p$ et donc $\text{rang}(f) = n - p$. 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

$$g_i = f(e_{p+i}) \quad (6.52)$$

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

$$\sum_{k=1}^{n-p} a_k f(e_{p+k}) = 0, \quad (6.53)$$

alors $f(\sum_k a_k e_{p+k}) = 0$, ce qui signifierait que $\sum_k a_k e_{p+k}$ se trouve dans le noyau de f , ce qui est impossible par construction de la base $\{e_i\}_{i=1, \dots, n}$. Étant donné que les vecteurs $g_1, \dots, g_{n-p}$ sont libres, nous les complétons en une base

$$\underbrace{\{g_1, \dots, g_{n-p}\}}_{\text{images}} \underbrace{\{g_{n-p+1}, \dots, g_r\}}_{\text{complétion}} \quad (6.54)$$

de F .

Nous prouvons maintenant que $\text{rang}(f^t) \geq n - p$ en montrant que les formes $\{g_i^*\}_{i=1, \dots, n-p}$ est 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

$$f^t(g_i^*)e_k = g_i^*(f e_k), \quad (6.55)$$

Si $k = 1, \dots, p$, alors $fe_k = 0$ et donc $g_i^*(fe_k) = 0$; si $k = p + l$ alors

$$f^t(g_i^*)e_k = g_i^*(fe_{k+l}) = g_i^*(g_l) = \delta_{i,l} = \delta_{i,k-p} = \delta_{k,i+p}. \quad (6.56)$$

Donc $f^t(g_i^*) = e_{i+p}^*$. Cela prouve que les formes $f^t(g_i^*)$ sont libres et donc que

$$\text{rang}(f^t) \geq n - p = \text{rang}(f). \quad (6.57)$$

En appliquant le même raisonnement à f^t au lieu de f , nous trouvons

$$\text{rang}((f^t)^t) \geq \text{rang}(f^t) \quad (6.58)$$

et donc, vu que $(f^t)^t = f$, nous obtenons $\text{rang}(f) = \text{rang}(f^t)$. □

Proposition 6.32 ([79]).

Si f est une application linéaire entre les espaces vectoriels E et F , alors nous avons

$$\text{Image}(f^t) = \ker(f)^\perp. \quad (6.59)$$

Démonstration. Soient donc l'application $f: E \rightarrow F$ et sa transposée $f^t: F^* \rightarrow E^*$. 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

$$\dim(\text{Image}(f^t)) = \text{rang}(f^t) \quad (6.60a)$$

$$= \text{rang}(f) \quad \text{lemme 6.31} \quad (6.60b)$$

$$= \dim(E) - \dim \ker(f) \quad \text{théorème 6.13} \quad (6.60c)$$

$$= \dim((\ker f)^\perp) \quad \text{proposition 6.28.} \quad (6.60d)$$

□

Lemme 6.33 ([78]).

Soit $\mathbb{K}$ un corps, E et F deux $\mathbb{K}$ -espaces vectoriels de dimension finie et une application linéaire $f: E \rightarrow F$. L'application f est injective si et seulement si sa transposée³ f^t est surjective.

Démonstration. Supposons que f soit injective. Alors par le lemme 6.22, il existe $g: F \rightarrow E$ 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 $f^t: F^* \rightarrow E^*$ est surjective. Alors en nous souvenant que E et F sont de dimension finie et en faisons jouer les identifications $(f^t)^t = f$ et $(E^*)^* = E$ nous pouvons savoir qu'il existe $s: E^* \rightarrow F^*$ tel que $f^t \circ s = \text{Id}|_{E^*}$. En passant à la transposée,

$$s^t \circ f = \text{Id}|_E, \quad (6.61)$$

qui implique que f est injective. □

3. Définition 6.29.

6.4.3 Transposée : sans le dual

Problèmes et choses à faire

J'aimerais une confirmation de ce qui est écrit dans ici à propos du fait que si f est une application linéaire, f^t n'est pas bien définie.

Il est légitime, si $f: V \rightarrow V$ est une application linéaire, de dir que sa transposée soit l'application linéaire $f^t: V \rightarrow V$ dont la matrice est la matrice transposée de celle de f . Lorsque nous travaillons sur $\mathbb{R}^n$ muni de la base canonique, cela ne pose pas de problèmes et nous pouvons écrire des égalités du type $\langle x, Ay \rangle = \langle A^t x, y \rangle$.

Hélas nous allons voir que cette façon de définir une transposée est mauvaise. Nous reprenons les notations de 6.23. Nous avons

$$f(x) = \sum_{kl} A_{kl} x_l e_k = \sum_{\alpha\beta} A'_{\alpha\beta} x'_\beta e'_\alpha. \quad (6.62)$$

Nous écrivons l'application transposée par rapport à la première base :

$$f^{t_1}(x) = \sum_{kl} A_{lk} x_l e_k \quad (6.63)$$

et par rapport à la seconde base :

$$f^{t_2}(x) = \sum_{\alpha\beta} A'_{\beta\alpha} x'_\beta e'_\alpha. \quad (6.64)$$

En remplaçant dans $f^{(t_1)}$ les nombres x_l et les vecteurs e_k par les valeurs en termes des x'_β et e'_α nous obtenons

$$f^{t_1}(x) = \sum_{\alpha\beta} (Q^{-1} A^t Q)_{\alpha\beta} x'_\beta e'_\alpha. \quad (6.65)$$

Nous avons égalité avec (6.64) seulement lorsque $A'_{\beta\alpha} = (Q^{-1} A^t Q)_{\alpha\beta}$, mais sachant que $A' = Q^{-1} A Q$ nous avons besoin que

$$Q^{-1} = Q^t \quad (6.66)$$

(cela étant une égalité de matrice).

6.34.

Autrement dit, la façon «usuelle» de voir la transposée d'une application linéaire ne fonctionne dans les livres pour enfant uniquement parce qu'on n'y considère toujours $\mathbb{R}^n$ muni de la base canonique ou de bases orthonormées.

6.4.4 Polynômes de Lagrange

Soit $E = \mathbb{R}_n[X]$ l'ensemble des polynômes à coefficients réels de degré au plus n . Soient les $n+1$ réels distincts $a_0, \dots, a_n$. Nous considérons les formes linéaires associées $f_i \in E^*$,

$$f_i(P) = P(a_i). \quad (6.67)$$

Lemme 6.35.

Ces formes forment une base de E^* .

Démonstration. Nous prouvons que l'orthogonal est réduit au nul :

$$\text{Span}\{f_0, \dots, f_n\}^\perp = \{0\} \quad (6.68)$$

pour que la proposition 6.28 conclue. 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. $\square$

Les **polynômes de Lagrange** sont les polynômes de la base (pré)duale de la base $\{f_i\}$.

Proposition 6.36.

Les polynômes de Lagrange sont donnés par

$$P_i = \prod_{k \neq i} \frac{X - a_k}{a_i - a_k}. \quad (6.69)$$

Démonstration. Il suffit de vérifier que $f_j(P_i) = \delta_{ij}$. Nous avons

$$f_j(P_i) = P_i(a_j) = \prod_{k \neq i} \frac{a_j - a_k}{a_i - a_k}. \quad (6.70)$$

Si $j \neq i$ alors un des termes est nul. Si au contraire $i = j$, tous les termes valent 1. $\square$

6.4.5 Dual de $\mathbb{M}(n, \mathbb{K})$ **Proposition 6.37** ([1]).

Soit $\mathbb{K}$, un corps. Les formes linéaires sur $\mathbb{M}(n, \mathbb{K})$ sont les applications de la forme

$$\begin{aligned} f_A: \mathbb{M}_n(\mathbb{K}) &\rightarrow \mathbb{K} \\ M &\mapsto \text{Tr}(AM). \end{aligned} \quad (6.71)$$

Démonstration. Nous considérons l'application

$$\begin{aligned} f: \mathbb{M}(n, \mathbb{K}) &\rightarrow \mathbb{M}(n, \mathbb{K})' \\ A &\mapsto f_A \end{aligned} \quad (6.72)$$

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 $(E_{ij})_{kl} = \delta_{ik}\delta_{jl}$:

$$0 = f_A(E_{ij}) = \sum_k (AE_{ij})_{kk} = \sum_{kl} A_{kl}\delta_{il}\delta_{jk} = A_{ij}. \quad (6.73)$$

Donc $A = 0$. $\square$

Corollaire 6.38 ([1]).

Soit $\mathbb{K}$ un corps et $\phi \in \mathbb{M}(n, \mathbb{K})^*$ telle que pour tout $X, Y \in \mathbb{M}(n, \mathbb{K})$ on ait

$$\phi(XY) = \phi(YX). \quad (6.74)$$

Alors il existe $\lambda \in \mathbb{K}$ tel que $\phi = \lambda \text{Tr}$.

Démonstration. La proposition 6.37 nous donne une matrice $A \in \mathbb{M}(n, \mathbb{K})$ telle que $\phi = f_A$. L'hypothèse nous dit que $f_A(XY) = f_A(YX)$, c'est à dire

$$\text{Tr}(AXY) = \text{Tr}(AYX) \quad (6.75)$$

pour toute matrices $X, Y \in \mathbb{M}(n, \mathbb{K})$. L'invariance cyclique de la trace nous dit que $\text{Tr}(AXY) = \text{Tr}(XAY)$, ce qui signifie que

$$\text{Tr}((AX - XA)Y) = 0 \quad (6.76)$$

ou encore que $f_{AX-XA} = 0$ pour tout X . La fonction f étant injective nous en déduisons que la matrice A doit satisfaire

$$AX = XA \quad (6.77)$$

pour tout $X \in \mathbb{M}$. En particulier en prenant la fameuse matrice E_{ij} et en calculant un peu,

$$A_{li}\delta_{jm} = \delta_{il}A_{jm} \quad (6.78)$$

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,

$$\phi(X) = f_{\lambda \mathbb{1}}(X) = \lambda \operatorname{Tr}(X). \quad (6.79)$$

□

Corollaire 6.39 ([1]).

Soit $\mathbb{K}$ un corps. Tout hyperplan de $\mathbb{M}(n, \mathbb{K})$ coupe $\operatorname{GL}(n, \mathbb{K})$.

Démonstration. Soit $\mathcal{H}$ un hyperplan de $\mathbb{M}$. Il existe une forme linéaire ϕ sur $\mathbb{M}(n, \mathbb{K})$ telle que $\mathcal{H} = \ker(\phi)$. Encore une fois la proposition 6.37 nous donne $A \in \mathbb{M}$ telle que $\phi = f_A$; nous notons r le rang de A . Par le lemme 6.15 nous avons $A = PJ_rQ$ avec $P, Q \in \operatorname{GL}(n, \mathbb{K})$ et

$$J_r = \begin{pmatrix} \mathbb{1}_r & 0 \\ 0 & 0 \end{pmatrix}. \quad (6.80)$$

Pour tout $X \in \mathbb{M}$ nous avons

$$\phi(X) = \operatorname{Tr}(AX) = \operatorname{Tr}(PJ_rQX) = \operatorname{Tr}(J_rQXP). \quad (6.81)$$

Ce que nous cherchons est $X \in \operatorname{GL}(n, \mathbb{K})$ telle que $\phi(X) = 0$. Nous commençons par trouver $Y \in \operatorname{GL}(n, \mathbb{K})$ telle que $\operatorname{Tr}(J_rY) = 0$. Celle-là est facile : c'est

$$Y = \begin{pmatrix} 0 & 1 \\ \mathbb{1}_{n-1} & 0 \end{pmatrix}. \quad (6.82)$$

Les éléments diagonaux de J_rY sont tous nuls. Par conséquent en posant $X = Q^{-1}YP^{-1}$ nous avons notre matrice inversible dans le noyau de ϕ . □

6.5 Déterminants

6.5.1 Formes multilinéaires alternées

Définition 6.40.

Soit E , un $\mathbb{K}$ -espace vectoriel. Une forme linéaire **alternée** sur E est une application linéaire $f: E \rightarrow \mathbb{K}$ telle que $f(v_1, \dots, v_k) = 0$ dès que $v_i = v_j$ pour certains $i \neq j$.

Lemme 6.41.

Une forme linéaire alternée est antisymétrique. Si $\mathbb{K}$ est de caractéristique différente de 2, alors une forme antisymétrique est alternée.

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

$$0 = f(x + y, x + y) = f(x, x) + f(x, y) + f(y, x) + f(y, y) = f(x, y) + f(y, x). \quad (6.83)$$

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 6.42 ([80]).

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. Soit $\{e_i\}$, une base de E et $f: E \rightarrow \mathbb{K}$ une n -forme linéaire alternée, puis $(v_1, \dots, v_n)$ des vecteurs de E . Nous pouvons les écrire dans la base

$$v_j = \sum_{i=1}^n \alpha_{ij} e_i \quad (6.84)$$

et alors exprimer f par

$$f(v_1, \dots, v_n) = f\left(\sum_{i_1=1}^n \alpha_{1i_1} e_{i_1}, \dots, \sum_{i_n=1}^n \alpha_{ni_n} e_{i_n}\right) \quad (6.85a)$$

$$= \sum_{i,j} \alpha_{1i_1} \dots \alpha_{ni_n} f(e_{i_1}, \dots, e_{i_n}). \quad (6.85b)$$

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

$$f(v_1, \dots, v_n) = \sum_{\sigma \in S_n} \alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}). \quad (6.86)$$

En utilisant encore une fois le fait que la forme f soit alternée, $f = f(e_1, \dots, e_n)\Pi$ où

$$\Pi(v_1, \dots, v_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n}. \quad (6.87)$$

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 6.41, il suffit de prouver que cette forme est antisymétrique⁴.

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 $\alpha_{i1} = \alpha_{i2}$:

$$\Pi(v, v, v_3, \dots, v_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \alpha_{\sigma(2)2} \alpha_{\sigma(3)3} \dots \alpha_{\sigma(n)n} \quad (6.88a)$$

$$= \sum_{\sigma \in S_n} \epsilon(\sigma\tau) \alpha_{\sigma\tau(1)1} \alpha_{\sigma\tau(2)2} \alpha_{\sigma\tau(3)3} \dots \alpha_{\sigma\tau(n)n} \quad \text{où } \tau = (12) \quad (6.88b)$$

$$= - \sum_{\sigma \in S_n} \epsilon(\sigma) \alpha_{\sigma(1)1} \alpha_{\sigma(2)2} \alpha_{\sigma(3)3} \dots \alpha_{\sigma(n)n} \quad (6.88c)$$

$$= -\Pi(v, v, v_3, \dots, v_n). \quad (6.88d)$$

□

Lemme 6.43.

Soit $\mathbb{K}$ un corps fini autre que $\mathbb{F}_2$ ⁵, soit un groupe abélien M et un morphisme $\varphi: \text{GL}(n, \mathbb{K}) \rightarrow M$. Alors il existe un unique morphisme $\delta: \mathbb{K}^* \rightarrow M$ tel que $\varphi = \delta \circ \det$.

Démonstration. D'abord le groupe dérivé de $\text{GL}(n, \mathbb{K})$ est $\text{SL}(n, \mathbb{K})$ parce que les éléments de $D(\text{GL}(n, \mathbb{K}))$ sont de la forme $ghg^{-1}h^{-1}$ dont le déterminant est 1.

De plus le groupe $\text{SL}(n, \mathbb{K})$ est normal dans $\text{GL}(n, \mathbb{K})$. Par conséquent $\text{GL}(n, \mathbb{K})/\text{SL}(n, \mathbb{K})$ est un groupe et nous pouvons définir l'application relevée

$$\tilde{\varphi}: \frac{\text{GL}(n, \mathbb{K})}{\text{SL}(n, \mathbb{K})} \rightarrow M \quad (6.89)$$

4. C'est ici que joue l'hypothèse sur la caractéristique de $\mathbb{K}$.

5. Je ne comprends pas très bien à quel moment joue cette hypothèse.

vérifiant $\varphi = \tilde{\varphi} \circ \pi$ où π est la projection.

Nous pouvons faire la même chose avec l'application

$$\det: \mathrm{GL}(n, \mathbb{K}) \rightarrow \mathbb{K}^* \quad (6.90)$$

qui est un morphisme de groupes dont le noyau est $\mathrm{SL}(n, \mathbb{K})$. Cela nous donne une application

$$\tilde{\det}: \frac{\mathrm{GL}(n, \mathbb{K})}{\mathrm{SL}(n, \mathbb{K})} \rightarrow \mathbb{K}^* \quad (6.91)$$

telle que $\det = \tilde{\det} \circ \pi$. Cette application $\tilde{\det}$ est un isomorphisme. En effet elle est surjective parce que le déterminant l'est et elle est injective parce que son noyau est précisément ce par quoi on prend le quotient. Par conséquent $\tilde{\det}$ possède un inverse et nous pouvons écrire

$$\varphi = \tilde{\varphi} \circ \tilde{\det}^{-1} \circ \tilde{\det} \circ \pi. \quad (6.92)$$

État donné que $\tilde{\det} \circ \pi = \det$, nous avons alors $\varphi = \delta \circ \det$ avec $\delta = \tilde{\varphi} \circ \tilde{\det}^{-1}$. Ceci conclut la partie existence de la preuve.

En ce qui concerne l'unicité, nous considérons $\delta': \mathbb{K}^* \rightarrow M$ telle que $\varphi = \delta' \circ \det$. Pour tout $u \in \mathrm{GL}(n, \mathbb{K})$ nous avons $\delta'(\det(u)) = \varphi(u) = \delta(\det(u))$. L'application $\det$ étant surjective depuis $\mathrm{GL}(n, \mathbb{K})$ vers $\mathbb{K}^*$, nous avons $\delta' = \delta$. $\square$

Théorème 6.44.

Soit $p \geq 3$ un nombre premier et V , un $\mathbb{F}_p$ -espace vectoriel de dimension finie n . Pour tout $u \in \mathrm{GL}(V)$ nous avons

$$\epsilon(u) = \left(\frac{\det(u)}{p} \right). \quad (6.93)$$

Ici ϵ est la signature de u vue comme une permutation des éléments de $\mathbb{F}_p$.

Démonstration. Commençons par prouver que

$$\epsilon: \mathrm{GL}(V) \rightarrow \{-1, 1\}. \quad (6.94)$$

est un morphisme. Si nous notons $\bar{u} \in S(V)$ l'élément du groupe symétrique correspondant à la matrice $u \in \mathrm{GL}(V)$, alors nous avons $\overline{uv} = \bar{u} \circ \bar{v}$, et la signature étant un homomorphisme (proposition 2.78),

$$\epsilon(uv) = \epsilon(\bar{u} \circ \bar{v}) = \epsilon(\bar{u})\epsilon(\bar{v}). \quad (6.95)$$

Par ailleurs $\{-1, 1\}$ est abélien, donc le lemme 6.43 s'applique et nous pouvons considérer un morphisme $\delta: \mathbb{F}_p^* \rightarrow \{-1, 1\}$ tel que $\epsilon = \delta \circ \det$.

Nous allons utiliser le lemme 4.131 pour montrer que δ est le symbole de Legendre. Pour cela il nous faudrait trouver un $x \in \mathbb{F}_p^*$ tel que $\delta(x) = -1$. Étant donné que $\det$ est surjective, nous cherchons ce x sous la forme $x = \det(u)$. Par conséquent nous aurions

$$\delta(x) = (\delta \circ \det)(u) = \epsilon(u), \quad (6.96)$$

et notre problème revient à trouver une matrice $u \in \mathrm{GL}(V)$ dont la permutation associée soit de signature -1 .

Soit $n = \dim V$; en conséquence de la proposition 4.151(3), l'espace $\mathbb{F}_q = \mathbb{F}_{p^n}$ est un $\mathbb{F}_p$ -espace vectoriel de dimension n et est donc isomorphe en tant qu'espace vectoriel à V . Étant donné que $\mathbb{F}_q$ est un corps fini, nous savons que $\mathbb{F}_q^*$ est un groupe cyclique à $q - 1$ éléments. Soit y , un générateur de $\mathbb{F}_q^*$ et l'application

$$\begin{aligned} \beta: \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ x &\mapsto yx. \end{aligned} \quad (6.97)$$

Cela est manifestement $\mathbb{F}_p$ -linéaire (ici y et x sont des classes de polynômes et $\mathbb{F}_p$ est le corps des coefficients). L'application β fixe zéro et à part zéro, agit comme le cycle

$$(1, y, y^2, \dots, y^{q-2}). \quad (6.98)$$

Nous savons qu'un cycle de longueur n est de signature $(-1)^{n+1}$. Ici le cycle est de longueur $q - 1$ qui est pair (parce que $p \geq 3$) et par conséquent, l'application β est de signature -1 . $\square$

6.5.2 Déterminant d'une famille de vecteurs

Nous considérons un corps $\mathbb{K}$ et l'espace vectoriel E de dimension n sur $\mathbb{K}$.

Définition 6.45 (Déterminant d'une famille de vecteurs[29]).

Le **déterminant** $(v_1, \dots, v_n)$ dans la base B est l'élément de $\mathbb{K}$

$$\sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n e_{\sigma(i)}^*(v_i) \quad (6.99)$$

où la somme porte sur le groupe symétrique, $\epsilon(\sigma)$ est la signature de la permutation σ et e_k^* est le dual de e_k .

Nous le notons $\det_{(e_1, \dots, e_n)}(v_1, \dots, v_n)$.

Lemme 6.46 ([29]).

Les propriétés du déterminant. Soit B une base de E .

- (1) L'application $\det_B: E^n \rightarrow \mathbb{K}$ est n -linéaire et alternée.
- (2) Pour toute base, $\det_B(B) = 1$.
- (3) Le déterminant ne change pas si on remplace un vecteur par une combinaison linéaire des autres :

$$\det_B(v_1, \dots, v_n) = \det_B\left(v_1 + \sum_{s=2}^n a_s v_s, v_2, \dots, v_n\right). \quad (6.100)$$

- (4) Si on permute les vecteurs,

$$\det_B(v_1, \dots, v_n) = \epsilon(\sigma) \det_B(v_{\sigma(1)}, \dots, v_{\sigma(n)}). \quad (6.101)$$

- (5) Si B' est une autre base :

$$\det_B = \det_B(B') \det_{B'} \quad (6.102)$$

- (6) Nous avons aussi la formule $\det_B(B') \det_{B'}(B) = 1$.

- (7) 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.

- (1) En posant $v_1 = x_1 + \lambda x_2$ nous avons

$$\det_B(x_1 + \lambda x_2, v_2, \dots, v_n) = \sum_{\sigma} \epsilon(\sigma) \prod_{i=1}^n e_{\sigma(i)}^*(v_i) \quad (6.103a)$$

$$= \sum_{\sigma} \epsilon(\sigma) \left(e_{\sigma(1)}^*(x_1 + \lambda x_2) \right) \prod_{i=2}^n e_{\sigma(i)}^*(v_i). \quad (6.103b)$$

À partir de là, la linéarité de $e_{\sigma(1)}^*$ montre que $\det_B$ est linéaire en son premier argument. Pour les autres argument, le même calcul tient.

En ce qui concerne le fait d'être alternée, permuter v_k et v_l revient à calculer $\det_B(v_{\sigma_{kl}(1)}, \dots, v_{\sigma_{kl}(n)})$, c'est à dire changer la somme $\sum_{\sigma}$ en $\sum_{\sigma \circ \sigma_{kl}}$. Cela ajoute 1 à $\epsilon(\sigma)$ vu que l'on ajoute une permutation.

- (2) Nous avons

$$\det_B(B) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n \underbrace{e_{\sigma(i)}^*(e_i)}_{=\delta_{\sigma(i), i}}. \quad (6.104)$$

Si σ n'est pas l'identité, le produit contient forcément un facteur nul. Il ne reste de la somme que $\sigma = \text{Id}$ et le résultat est 1.

(3) Vu que $\det_B$ est linéaire en tous ses arguments,

$$\det_B \left(v_1 + \sum_{s=2}^n a_s v_s, v_2, \dots, v_n \right) = \det_B(v_1, \dots, v_n) + \sum_{s=2}^n a_s \det_B(v_s, v_2, \dots, v_n). \quad (6.105)$$

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.

(4) 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 :

$$\det_B(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \sum_{\sigma'} \epsilon(\sigma') \prod_{i=1}^n e_{\sigma'(i)}^*(w_i) \quad (6.106a)$$

$$= \sum_{\sigma'} \epsilon(\sigma') \prod_{i=1}^n e_{\sigma'(i)}^*(v_{\sigma(i)}) \quad (6.106b)$$

$$= \sum_{\sigma'} \epsilon(\sigma') \prod_{i=1}^n e_{\sigma^{-1}\sigma'(i)}^*(v_i) \quad (6.106c)$$

$$= \sum_{\sigma'} \epsilon(\sigma\sigma') \prod_{i=1}^n e_{\sigma'(i)}^*(v_i) \quad (6.106d)$$

$$= \epsilon(\sigma) \det_B(v_1, \dots, v_n). \quad (6.106e)$$

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 $\epsilon: S_n \rightarrow \{0, 1\}$ était un morphisme de groupe (proposition 2.78).

(5) 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' :

$$\det_B(B') = \lambda \det_{B'}(B'), \quad (6.107)$$

donc $\lambda = \det_B(B')$.

(6) Il suffit d'appliquer l'égalité précédente à B en nous souvenant que $\det_B(B) = 1$.

(7) 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 le théorème 6.8(3). Il y a donc moyen de remplacer un des vecteurs par une combinaison linéaire des autres. Le déterminant s'annule alors.

□

D'après la proposition 6.42, il existe une unique forme n -linéaire alternée égale à 1 sur B , et c'est $\det_B: E^n \rightarrow \mathbb{K}$.

6.5.3 Déterminant d'un endomorphisme

L'interprétation géométrique du déterminant en termes d'aires et de volumes est donnée après la proposition 13.85.

Lemme 6.47.

Si $f: E \rightarrow E$ est un endomorphisme, si B et B' sont deux bases, alors $\det_B(f(B)) = \det_{B'}(f(B'))$.

Démonstration. L'application

$$\begin{aligned} \varphi: E^n &\rightarrow \mathbb{K} \\ v_1, \dots, v_n &\mapsto \det_B(f(v_1), \dots, f(v_n)) \end{aligned} \quad (6.108)$$

est n -linéaire et alternée ; il existe donc $\lambda \in \mathbb{K}$ tel que $\varphi = \lambda \det_B$. En appliquant cela à B :

$$\det_B (f(B)) = \lambda \det_B(B) = \lambda. \quad (6.109)$$

Nous avons donc déjà prouvé que $\lambda = \det_B (f(B))$, c'est à dire

$$\det_B (f(v)) = \det_B (f(B)) \det_B(v). \quad (6.110)$$

Nous allons maintenant introduire B' là où il y a du v en utilisant les formules (6.102) :

$$\det_B (f(v)) = \det_B(B') \det_{B'} (f(v)) \quad (6.111a)$$

$$\det_B(v) = \det_B(B') \det_{B'}(v). \quad (6.111b)$$

Nous obtenons

$$\det_{B'} (f(v)) = \det_B (f(B)) \det_{B'}(v). \quad (6.112)$$

Et on applique cela à $v = B'$:

$$\det_{B'} (f(B')) = \det_B (f(B)) \underbrace{\det_{B'}(B')}_{=1}. \quad (6.113)$$

□

Cette proposition nous permet de définir le déterminant d'un endomorphisme de la façon suivante sans préciser la base.

Définition 6.48 ([29]).

Si $f: E \rightarrow E$ est un endomorphisme, le **déterminant** de f est

$$\det(f) = \det_B (f(B)) \quad (6.114)$$

Proposition 6.49.

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 automorphisme⁶ si et seulement si $\det(f) \neq 0$.
- (3) Si $\det(f) \neq 0$ alors $\det(f^{-1}) = \det(f)^{-1}$.
- (4) L'application $\det: \text{GL}(E) \rightarrow \mathbb{K} \setminus \{0\}$ est un morphisme de groupe.

Démonstration. Point par point.

- (1) Nous considérons l'application

$$\begin{aligned} \varphi: E^n &\rightarrow \mathbb{K} \\ v &\mapsto \det_B (f(v)). \end{aligned} \quad (6.115)$$

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 $\det_B (f(B)) = \lambda$. Autrement dit :

$$\lambda = \det(f). \quad (6.116)$$

Calculons à présent $\varphi(g(B))$: d'une part,

$$\varphi(g(B)) = \det_B ((f \circ g)(B)) \quad (6.117)$$

et d'autre part,

$$\varphi(g(B)) = \lambda \det_B (g(B)) = \lambda \det(g) \quad (6.118)$$

En égalisant et en reprenant la la valeur déjà trouvée de λ ,

$$\det (f \circ g)(B) = \det(f) \det(g), \quad (6.119)$$

ce qu'il fallait.

6. Endomorphisme inversible, définition 6.11.

- (2) Supposons que f soit un automorphisme. Alors si B est une base, $f(B)$ est une base. Par conséquent $\det(f) = \det_B(f(B)) \neq 0$ parce que $f(B)$ est une base (lemme 6.46(7)).
Réciproquement, supposons que $\det(f) \neq 0$. Alors si B est une base quelconque nous avons $\det_B(f(B)) \neq 0$, 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, $1 = \det(f \circ f^{-1}) = \det(f) \det(f^{-1})$.

□

6.5.4 Déterminant de Vandermonde

Liens internes sur l'utilisation du déterminant de Vandermonde :

- (1) Pour prouver que $\text{Tr}(u^p) = 0$ pour tout p si et seulement si u est nilpotente (lemme 6.347).
(2) Pour prouver qu'un endomorphisme possédant $\dim(E)$ valeurs propres distinctes est cyclique (proposition 6.340).

Proposition 6.50 ([35]).

Le **déterminant de Vandermonde** est le polynôme en n variables donné par

$$V(T_1, \dots, T_n) = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ T_1 & T_2 & \dots & T_n \\ \vdots & \ddots & \ddots & \vdots \\ T_1^{n-1} & T_2^{n-1} & \dots & T_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (T_j - T_i). \quad (6.120)$$

Notez que l'inégalité du milieu est stricte (sinon d'ailleurs l'expression serait nulle).

Démonstration. Nous considérons le polynôme

$$f(X) = V(T_1, \dots, T_{n-1}, X) \in (\mathbb{K}[T_1, \dots, T_{n-1}])[X]. \quad (6.121)$$

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 il existe $\alpha \in \mathbb{K}[T_1, \dots, T_{n-1}]$ tel que

$$f = \alpha(X - T_{n-1}) \dots (X - T_1). \quad (6.122)$$

Nous trouvons α en écrivant $f(0)$. D'une part la formule (6.122) nous donne

$$f(0) = \alpha(-1)^{n-1} T_1 \dots T_{n-1}. \quad (6.123)$$

D'autre par la définition donne

$$f(0) = \det \begin{pmatrix} 1 & \dots & 1 & 1 \\ T_1 & & T_{n-1} & 0 \\ \vdots & & \vdots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} & 0 \end{pmatrix} \quad (6.124a)$$

$$= (-1)^{n-1} \det \begin{pmatrix} T_1 & \dots & T_{n-1} \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} \end{pmatrix} \quad (6.124b)$$

$$= (-1)^{n-1} T_1 \dots T_{n-1} \det \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ T_1^{n-1} & \dots & T_{n-1}^{n-1} \end{pmatrix} \quad (6.124c)$$

$$= (-1)^{n-1} T_1 \dots T_{n-1} V(T_1, \dots, T_{n-1}) \quad (6.124d)$$

En égalisant avec (6.123), nous trouvons $\alpha = V(T_1, \dots, T_{n-1})$, et donc

$$f = V(T_1, \dots, T_{n-1}) \prod_{j \leq n-1} (X - T_j) \quad (6.125)$$

Enfin, une récurrence montre que

$$V(T_1, \dots, T_n) = f(T_n) \quad (6.126a)$$

$$= V(T_1, \dots, T_{n-1}) \prod_{j \leq n-1} (T_n - T_j) \quad (6.126b)$$

$$= \prod_{k \leq n} \prod_{j \leq k-1} (T_k - T_j) \quad (6.126c)$$

$$= \prod_{1 \leq j < k \leq n} (T_k - T_j). \quad (6.126d)$$

□

Exemple 6.51

Le déterminant de Vandermonde (proposition 6.50) 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. $\triangle$

Proposition 6.52.

Un polynôme semi-symétrique $f \in \mathbb{K}[T_1, \dots, T_n]$ se décompose de façon unique en

$$f = P + VQ \quad (6.127)$$

où P et Q sont deux polynômes symétriques.

Démonstration. Nous commençons par prouver l'unicité en montrant que si $f = PVQ$ 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 $\{1, \dots, n\}$, alors $\sigma_1 \cdot f = \sigma_2 \cdot f$ parce que l'élément $\sigma_2^{-1}\sigma_1$ est pair (proposition 2.78), 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

$$g = \tau \cdot f = P - VQ. \quad (6.128)$$

Donc $f + g = 2P$ et $f - g = 2VQ$. Cela donne P et Q en terme 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,

$$\sigma \cdot (f + g) = \sigma \cdot f + \sigma\tau \cdot f = g + f \quad (6.129)$$

parce que $\sigma\tau$ est pair. De la même façon,

$$\sigma \cdot (f - g) = g - f = \epsilon(\sigma)(f - g). \quad (6.130)$$

Dans les deux cas nous concluons en utilisant le fait que toute permutation est un produit de transpositions (proposition 2.77) et que ϵ est un homomorphisme.

Soient maintenant deux entiers $h < k$ dans $\{1, \dots, n\}$ et l'anneau

$$(\mathbb{K}[T_1, \dots, \hat{T}_k, \dots, T_n])[T_k]. \quad (6.131)$$

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 $T_k - T_h$:

$$f - g = (T_k - T_h)q + r \quad (6.132)$$

où $\deg_{T_k} r < 1$, c'est à dire que r ne dépend pas de T_k . Nous revoyons maintenant l'égalité (6.132) 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

$$-(f - g) = -(T_k - T_h)\tau_{kh} \cdot q + \tau_{kh} \cdot r \quad (6.133)$$

où $\tau_{kh} \cdot r$ ne dépend pas de T_h . Nous appliquons à (6.133) l'application

$$\begin{aligned} t\alpha: \mathbb{K}[T_1, \dots, T_n] &\rightarrow \mathbb{K}[T_1, \dots, \hat{T}_k, \dots, T_n] \\ \alpha(PT_1, \dots, \hat{T}_k, \dots, T_n) &= P(T_1, \dots, T_h, \dots, T_n). \end{aligned} \quad (6.134)$$

Cette application vérifie $\alpha(\tau_{kh} \cdot r) = \alpha(r)$ et nous avons

$$-\alpha(f - g) = \alpha(r). \quad (6.135)$$

Puis en appliquant α à la relation $f - g = (T_k - T_h)q + r$, nous trouvons

$$\alpha(f - g) = \alpha(r), \quad (6.136)$$

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

$$f - g = 2Q \prod_{h < k} \prod_{k \leq n} (T_k - T_h) = 2Q(T_1, \dots, T_n)V(T_1, \dots, T_n), \quad (6.137)$$

où nous avons utilisé la formule du déterminant de Vandermonde de la proposition 6.50.

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

$$\sigma \cdot (f - g) = \epsilon(\sigma)(f - g) = \epsilon(\sigma)2QV, \quad (6.138)$$

Mais en appliquant σ à l'équation (6.137),

$$\sigma \cdot (f - g) = 2(\sigma \cdot V)(T_1, \dots, T_n)(\sigma \cdot Q)(T_1, \dots, T_n) \quad (6.139a)$$

$$= 2\epsilon(\sigma)V(T_1, \dots, T_n)(\sigma \cdot Q)(T_1, \dots, T_n). \quad (6.139b)$$

En égalisant avec (6.138) et en se souvenant que l'anneau $\mathbb{K}[T_1, \dots, T_n]$ était intègre (théorème 3.90), nous simplifions par $2\epsilon(\sigma)V$ pour obtenir

$$Q = \sigma \cdot Q, \quad (6.140)$$

c'est à dire que Q est symétrique.

Au final nous avons $f + g = 2P$ et $f - g = 2VQ$ avec P et Q symétriques. En faisant la somme,

$$f = P + VQ. \quad (6.141)$$

□

6.5.5 Déterminant de Gram

Si $x_1, \dots, x_r$ sont des vecteurs d'un espace vectoriel, alors le **déterminant de Gram** est le déterminant

$$G(x_1, \dots, x_r) = \det(\langle x_i, x_j \rangle). \quad (6.142)$$

Notons que la matrice est une matrice symétrique.

Proposition 6.53.

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

$$d(x, F)^2 = \frac{G(x, x_1, \dots, x_n)}{G(x_1, \dots, x_n)}. \quad (6.143)$$

6.5.6 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

$$D_n = \det \left(\frac{1}{a_i + b_j} \right). \quad (6.144)$$

Proposition 6.54 ([81]).

Le déterminant de Cauchy est donné par la formule

$$D_n = \frac{\prod_{i < j} (a_j - a_i) \prod_{i < j} (b_j - b_i)}{\prod_{i,j} (a_i + b_j)}. \quad (6.145)$$

6.5.7 Matrice de Sylvester

La définition est pompée de wikipédia. Soient P et Q deux polynômes non nuls, de degrés respectifs m et n :

$$P(x) = p_0 + p_1x + \dots + p_nx^n \quad (6.146a)$$

$$Q(x) = q_0 + q_1x + \dots + q_mx^m. \quad (6.146b)$$

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 :

$$(p_n \ p_{n-1} \ \dots \ p_1 \ p_0 \ 0 \ \dots \ 0); \quad (6.147)$$

- (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 :

$$(q_m \ q_{m-1} \ \dots \ q_1 \ q_0 \ 0 \ \dots \ 0); \quad (6.148)$$

- (5) les $(m - 1)$ lignes suivantes sont formées par des permutations circulaires.

Ainsi dans le cas $n = 4$ et $m = 3$, la matrice obtenue est

$$S_{p,q} = \begin{pmatrix} p_4 & p_3 & p_2 & p_1 & p_0 & 0 & 0 \\ 0 & p_4 & p_3 & p_2 & p_1 & p_0 & 0 \\ 0 & 0 & p_4 & p_3 & p_2 & p_1 & p_0 \\ q_3 & q_2 & q_1 & q_0 & 0 & 0 & 0 \\ 0 & q_3 & q_2 & q_1 & q_0 & 0 & 0 \\ 0 & 0 & q_3 & q_2 & q_1 & q_0 & 0 \\ 0 & 0 & 0 & q_3 & q_2 & q_1 & q_0 \end{pmatrix}. \quad (6.149)$$

Le déterminant de la matrice de Sylvester associée à P et Q est appelé le **résultant** de P et Q et noté $\text{res}(P, Q)$.

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 6.55 ([82]).

Si P et Q sont deux polynômes de degrés n et m à coefficients dans l'anneau $\mathbb{A}$, alors pour tout $\lambda \in \mathbb{A}$,

$$\text{res}(\lambda P, Q) = \lambda^m \text{res}(P, Q) \quad (6.150a)$$

$$\text{res}(P, \lambda Q) = \lambda^n \text{res}(P, Q). \quad (6.150b)$$

Démonstration. Cela est simplement un comptage de 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 . $\square$

L'équation de Bézout (3.129) peut être traitée avec une matrice de Sylvester. Soient P et Q , deux polynômes donnés et à résoudre l'équation

$$xP + yQ = 0 \quad (6.151)$$

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 (6.151) sous la forme

$$S_{PQ}^t \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix} = 0. \quad (6.152)$$

Pour s'en convaincre, écrivons pour les polynômes de l'exemple (6.149) :

$$\begin{pmatrix} p_4 & 0 & 0 & q_3 & 0 & 0 & 0 \\ p_3 & p_4 & 0 & q_2 & q_3 & 0 & 0 \\ p_2 & p_3 & p_4 & q_1 & q_2 & q_3 & 0 \\ p_1 & p_2 & p_3 & q_0 & q_1 & q_2 & q_3 \\ p_0 & p_1 & p_2 & 0 & q_0 & q_1 & q_2 \\ 0 & p_0 & p_1 & 0 & 0 & q_0 & q_1 \\ 0 & 0 & p_0 & 0 & 0 & 0 & q_0 \end{pmatrix} \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} = \begin{pmatrix} x_2 p_4 + y_2 q_3 \\ p_3 x_2 + p_4 x_1 + q_2 y_3 + q_3 y_2 \\ \vdots \end{pmatrix} \quad (6.153)$$

Nous voyons que sur la ligne numéro k (en partant du bas et en numérotant de à partir de zéro) nous avons les produits $p_i x_j$ et $q_i y_j$ avec $i + j = k$. La colonne de droite représente donc bien les coefficients du polynôme $xP + yQ$.

Proposition 6.56.

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 13.205 sur l'intégration de fractions rationnelles.

Exemple 6.57

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

$$S_{P,P'} = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}. \quad (6.154)$$

Le résultant est alors

$$\text{res}(P, P') = -a(b^2 - 4ac). \quad (6.155)$$

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. $\triangle$

La matrice de Sylvester permet aussi de récrire l'équation de Bézout pour les polynômes ; voir le théorème 3.105 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 6.58.

Si

$$P(X) = a_p \prod_{i=1}^p (X - \alpha_i) \quad (6.156a)$$

$$Q(X) = b_q \prod_{j=1}^q (X - \beta_j) \quad (6.156b)$$

alors nous avons les expressions suivantes pour le résultant :

$$\text{res}(P, Q) = a_p^q b_q^p \prod_{i=1}^p \prod_{j=1}^q (\beta_j - \alpha_i) = b_q^p \prod_{j=1}^q P(\beta_j) = (-1)^{pq} a_p^q \prod_{i=1}^p Q(\alpha_i). \quad (6.157)$$

Démonstration. Si P et Q ne sont pas premiers entre eux, d'une part la proposition 6.56 nous dit que $\text{res}(P, Q) = 0$ 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 (6.157) 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

$$\mathbb{A} = \mathbb{Z}[\alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_q]. \quad (6.158)$$

Dans cet anneau, l'élément $\beta_j - \alpha_i$ est irréductible (tout comme $X - Y$ est irréductible dans $\mathbb{Z}[X, Y]$). Le résultant $R = \text{res}(P, Q)$ 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

$$R = \lambda(\alpha_1, \dots, \beta_q) \prod_{i=1}^p \prod_{j=1}^q (\beta_j - \alpha_i). \quad (6.159)$$

Comptons les degrés. Pour donner une idée de ce calcul de degré, voici comment se présente, au niveau des dimensions, le déterminant :

$$\begin{array}{ccccccc}
 & \xleftarrow{p+1} & & \xleftarrow{q-1} & & & \\
 & & & & & & \\
 a_p & \cdots & a_{p-1} & \cdots & a_0 & \cdots & 0 \cdots 0 \\
 & \searrow & & & \searrow & & \\
 0 & \cdots & 0 & & a_p & \cdots & a_1 \cdots a_0
 \end{array}
 \begin{array}{c}
 \uparrow q \\
 \downarrow q
 \end{array}
 \quad (6.160)$$

$\xleftarrow{p+q}$

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 (6.160). Le même raisonnement montre que R est de degré p en les β_j . Par ailleurs le polynôme $\prod_{i=1}^p \prod_{j=1}^q (\beta_j - \alpha_i)$ 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 6.55 nous permet de conclure. $\square$

6.5.8 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

$$P = X^n + \sum_{k=0}^{n-1} a_k X^k. \quad (6.161)$$

Théorème 6.59 (Kronecker[1]).

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 $R = X^n + \sum_{k=0}^{n-1} b_k X^k$ un élément de K_n dont nous notons $\beta_1, \dots, \beta_n$ les racines dans $\mathbb{C}$. Les relations coefficients-racines stipulent que

$$b_k = \sum_{1 \leq i_1 < \dots < i_{n-k} \leq n} \prod_{j=1}^{n-k} \beta_{i_j}. \quad (6.162)$$

En prenant le module et en se souvenant que $|\beta_l| \leq 1$ pour tout l , nous trouvons que

$$|b_k| \leq \binom{n}{n-k}. \quad (6.163)$$

Mais comme $b_k \in \mathbb{Z}$, nous avons

$$b_k \in \left\{ -\binom{n}{n-k}, -\binom{n}{n-k} + 1, \dots, 0, \dots, \binom{n}{n-k} \right\} \quad (6.164)$$

qui est de cardinal $\binom{n}{n-k} + 1$. Nous avons donc

$$\text{Card}(K_n) \leq \prod_{k=0}^{n-1} \left(1 + \binom{n}{n-k} \right) < \infty. \quad (6.165)$$

La conclusion jusqu'ici est que K_n est un ensemble fini.

Pour chaque $k \in \mathbb{N}^*$ nous considérons les polynômes

$$P_k = \prod_{i=1}^n (X - \alpha_i^k) \quad (6.166a)$$

$$Q_k = X^k - Y \in \mathbb{Z}[X, Y], \quad (6.166b)$$

et puis nous considérons le résultant $R_k = \text{res}_X(P, Q_k) \in \mathbb{Z}[Y]$:

$$R_k = \text{res}_X(P, Q_k) = \begin{pmatrix} 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & & & \\ 0 & \cdots & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 & a_{n-1} & \cdots & a_0 \\ 1 & 0 & \cdots & 0 & -Y & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & -Y & 0 & \cdots & 0 \\ & & \ddots & & & \ddots & \ddots & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & -Y \end{pmatrix} \quad (6.167)$$

Cela est un polynôme en Y dont le terme de plus haut degré est $(-1)^n Y^n$. Les petites formules de la proposition 6.58 nous permettent d'exprimer $R_k(Y)$ en termes des racines de P :

$$R_k(Y) = \prod_{i=1}^n Q_k(\alpha_i) = \prod_{i=1}^n (\alpha_i^k - Y) = (-1)^n \prod_{i=1}^n (Y - \alpha_i^k) = (-1)^n P_k(Y). \quad (6.168)$$

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)⁷. 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

$$\alpha^{2^l/2^k} = \alpha^{2^{l-k}} \quad (6.169)$$

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 (6.169) est racine de P_{2^l} , il est aussi racine de P_{2^k} . Donc

$$(\alpha^{2^{l-k}})^{2^{l-k}} = \alpha^{2^{2(l-k)}} \quad (6.170)$$

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

$$\alpha^{2^{n(l-k)}} = \alpha^{2^{m(l-k)}} \quad (6.171)$$

pour certains entiers $m > n$, alors

$$\alpha^{2^{n(l-k)} - 2^{m(l-k)}} = 1, \quad (6.172)$$

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. $\square$

6.6 Directions conservées

6.6.1 Généralités

Nous savons qu'une application *linéaire* $A: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ est complètement définie par la donnée de son action sur les trois vecteurs de base, c'est à dire par la donnée de

$$Ae_1, \quad Ae_2 \quad \text{et} \quad Ae_3. \quad (6.173)$$

7. Ici dans [1], il déduit qu'on a un k tel que $P_k = P_1 = P$. Mais 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.

Nous allons former la matrice de A en mettant simplement les vecteurs Ae_1 , Ae_2 et Ae_3 en colonne. Donc la matrice

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad (6.174)$$

signifie que l'application linéaire A envoie le vecteur e_1 sur $\begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}$, le vecteur e_2 sur $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ 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 $\times$ matrice :

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x + 2y + 3z \\ 4x + 5y + 6z \\ 7x + 8y + 9z \end{pmatrix}. \quad (6.175)$$

Une chose intéressante est de savoir quelles sont les directions invariantes de la transformation linéaire. Par exemple, on peut lire sur la matrice (6.174) 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

$$(A - \lambda \mathbb{1}) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \quad (6.176)$$

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.

6.6.2 Matrice orthogonale

Définition 6.60.

Une matrice U est **orthogonale** si $UU^t = \mathbb{1}$. Le **groupe orthogonal** noté $O(n)$ est l'ensemble des matrices orthogonales $n \times n$.

Proposition 6.61.

À propos de matrices orthogonales.

- (1) L'ensemble des matrices réelles orthogonales forme un groupe noté $O(n, \mathbb{R})$.
- (2) Si A est une matrice orthogonale, alors $\det(A) = \pm 1$.
- (3) Le groupe $O(n)$ est le groupe des isométries de $\mathbb{R}^n$.

Démonstration. Si A et B sont orthogonales, alors

$$(AB)(AB)^t = ABB^tA^t = A\mathbb{1}A^t = \mathbb{1}. \quad (6.177)$$

Vu que $\mathbb{1}$ est orthogonale, nous avons bien un groupe.

En ce qui concerne le déterminant, $AA^t = \mathbb{1}$ donne $\det(A)\det(A^t) = 1$ ou encore $\det(A)^2 = 1$. 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,

$$\langle A^t Ax, y \rangle = \langle x, y \rangle \quad (6.178)$$

pour tout $x, y \in \mathbb{R}^n$. En prenant $y = e_i$ nous trouvons

$$(A^t Ax)_i = x_i, \quad (6.179)$$

ce qui signifie que pour tout x , $A^t Ax = x$, ce qui signifie que $A^t A$ est l'identité.

Réciproquement si $A^t A$ est l'identité nous avons

$$\langle a, y \rangle = \langle A^t Ax, y \rangle = \langle Ax, Ay \rangle, \quad (6.180)$$

ce qui prouve que A est une isométrie. $\square$

Le sous-groupe des matrices orthogonales de déterminant 1 est le groupe **spécial orthogonal** noté $SO(n)$.

6.6.3 Comment trouver la matrice d'une symétrie donnée ?

6.6.3.1 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,
- (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

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \quad (6.181)$$

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 plan⁸, 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

$$f_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}. \quad (6.182)$$

Nous avons

$$\begin{aligned} Af_1 &= f_1 \\ Af_2 &= f_2. \end{aligned} \quad (6.183)$$

8. Pour le trouver, penser au produit vectoriel.

Afin de trouver un vecteur perpendiculaire au plan, calculons le produit vectoriel :

$$f_3 = f_1 \times f_2 = \begin{vmatrix} e_1 & e_2 & e_3 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{vmatrix} = -e_1 - e_3 = \begin{pmatrix} -1 \\ 0 \\ -1 \end{pmatrix}. \quad (6.184)$$

Nous avons

$$Af_3 = -f_3. \quad (6.185)$$

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 équation (6.182) dit que

$$f_1 = e_2. \quad (6.186)$$

Ensuite, nous avons

$$\begin{aligned} f_2 &= e_1 - e_3 \\ f_3 &= -e_1 - e_3. \end{aligned} \quad (6.187)$$

La somme de ces deux équations donne $-2e_3 = f_2 + f_3$, c'est à dire

$$e_3 = -\frac{f_2 + f_3}{2} \quad (6.188)$$

Et enfin, nous avons

$$e_1 = \frac{f_2 - f_3}{2}. \quad (6.189)$$

Maintenant nous pouvons calculer les images de e_1 , e_2 et e_3 en faisant

$$\begin{aligned} Ae_1 &= \frac{Af_2 - Af_3}{2} = \frac{1}{2} \begin{pmatrix} 0 \\ 0 \\ -2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}, \\ Ae_2 &= Af_1 = f_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \\ Ae_3 &= -\frac{f_2 - f_3}{2} = -\frac{1}{2} \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}. \end{aligned} \quad (6.190)$$

La matrice A s'écrit maintenant en mettant les trois images trouvées en colonnes :

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}. \quad (6.191)$$

6.6.3.2 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

$$f_2 = \begin{pmatrix} 1 \\ 0 \\ x \end{pmatrix}, \quad (6.192)$$

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 .

6.6.3.3 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.

6.7 Normes et distances

6.7.1 Introduction : valeur absolue et norme

La valeur absolue est essentielle pour introduire les notions de limite et de continuité pour les fonctions d'une variable. En fait nous disons que la fonction $f: \mathbb{R} \rightarrow \mathbb{R}$ est continue au point a lorsque pour tout ε , il existe un δ tel que

$$|x - a| \leq \delta \Rightarrow |f(x) - f(a)| \leq \varepsilon. \quad (6.193)$$

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 éloigné 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) $|x + y| \leq |x| + |y|$

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 notion 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 :

$$\text{taille de } (a, b) = \sqrt{a^2 + b^2}. \quad (6.194)$$

Nous pouvons introduire une la notion de distance entre les éléments de $\mathbb{R}^2$ de façon similaire :

$$d((a_x, a_y), (b_x, b_y)) = \sqrt{(a_x - b_x)^2 + (a_y - b_y)^2}. \quad (6.195)$$

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 définitions possibles de «taille» et distance en $\mathbb{R}^2$?

6.7.2 Norme

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.

La définition d'une norme a déjà été donné à la définition 5.31.

Il est possible de définir de nombreuses normes sur $\mathbb{R}^n$. Citons en quelque unes.

Les normes $\|\cdot\|_{L^p}$ ($p \in \mathbb{N}$) sont définies de la façon suivante :

$$\|x\|_{L^p} = \left(\sum_{i=1}^n |x_i|^p \right)^{1/p}, \quad (6.196)$$

pour tout $x = (x_1, \dots, x_n) \in \mathbb{R}^n$. Parmi ces normes, celles qui seront le plus souvent utilisées dans ces notes sont

$$\begin{aligned} \|x\|_{L^1} &= \sum_{i=1}^n |x_i|, \\ \|x\|_{L^2} &= \left(\sum_{i=1}^n |x_i|^2 \right)^{1/2}. \end{aligned} \quad (6.197)$$

La norme L^2 est la **norme euclidienne**. Nous définissons également la **norme supremum** par

$$\|x\|_{\infty} = \sup_{1 \leq i \leq n} |x_i|. \quad (6.198)$$

Nous admettons sans démonstration que les fonctions $\|\cdot\|_{L^p} : \mathbb{R}^n \rightarrow \mathbb{R}^+$ sont bien des normes.

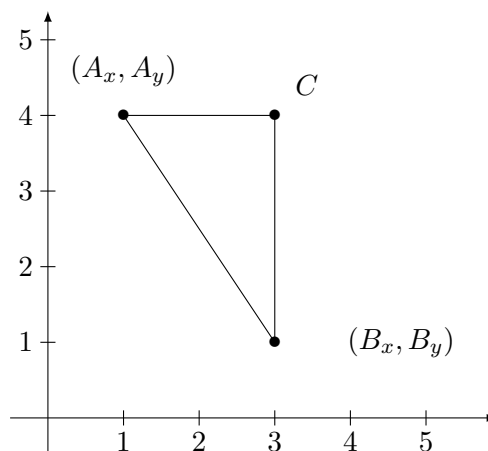


FIGURE 6.1 – La *norme* euclidienne induit la *distance* euclidienne. D'où son nom. Le point C est construit aux coordonnées (A_x, B_y) .

Soient $A = (A_x, A_y)$ et $B = (B_x, B_y)$ deux éléments de $\mathbb{R}^2$. La distance⁹ euclidienne entre A et B est donnée par $\|A - B\|_2$. En effet, sur la figure 6.1, la distance entre les points A et B est donnée par

$$|AB|^2 = |AC|^2 + |CB|^2 = |A_x - B_x|^2 + |A_y - B_y|^2, \quad (6.199)$$

par conséquent,

$$|AB| = \sqrt{|A_x - B_x|^2 + |A_y - B_y|^2} = \|A - B\|_2. \quad (6.200)$$

Remarque 6.62.

Si A , B et C sont trois points dans le plan $\mathbb{R}^2$, alors l'inégalité triangulaire $|AB| \leq |AC| + |CB|$ est précisément la propriété (3) de la norme (définition 5.31). En effet l'inégalité triangulaire s'exprime de la façon suivante en terme de la norme $\|\cdot\|_2$:

$$\|A - B\|_2 \leq \|A - C\|_2 + \|C - B\|_2. \quad (6.201)$$

En notant $u = A - C$ et $v = C - B$, l'équation (6.201) devient exactement la propriété de définition de la norme :

$$\|u + v\|_2 \leq \|u\|_2 + \|v\|_2. \quad (6.202)$$

Ceci explique pourquoi cette propriété des norme est appelée «inégalité triangulaire».

Les distances que nous avons vues jusqu'à présent sont des distances définies à partir d'une norme. La définition générale d'une distance est la définition 5.17.

9. Ne pas confondre «distance» et «norme».

6.8 Produit scalaire

Définition 6.63.

Une **forme bilinéaire** sur un espace vectoriel E est une application $b: E \times E \rightarrow \mathbb{K}$ telle que

- (1) $b(u, v) = b(v, u)$,
- (2) $b(u + v, w) = b(u, w) + b(v, w)$,
- (3) $b(\lambda u, v) = \lambda b(u, v)$

pour tout $u, v, w \in E$ et $\lambda \in \mathbb{K}$ où $\mathbb{K}$ est un corps commutatif.

Définition 6.64.

Si g est une application bilinéaire sur un espace vectoriel E nous disons qu'elle est

- (1) **définie positive** si $g(u, u) \geq 0$ pour tout $u \in E$ et $g(u, u) = 0$ si et seulement si $u = 0$.
- (2) **semi-définie positive** si $g(u, u) \geq 0$ pour tout $u \in E$. Nous dirons aussi parfois qu'elle est simplement «positive».

Cela est évidemment à lier à la définition 6.294 et la proposition 6.366 : une application bilinéaire est définie positive si et seulement si sa matrice symétrique associée l'est.

Définition 6.65.

Un **produit scalaire** sur un espace vectoriel E est une forme bilinéaire¹⁰ symétrique strictement définie positive¹¹.

Étant donné que l'inégalité de Cauchy-Schwarz sera surtout utilisée dans le cas où un produit scalaire est bel et bien donné, nous l'énonçons et le démontrons avec des notations adaptée à l'usage. Le produit scalaire sera noté $X \cdot Y$ pour $b(X, Y)$ si b est la forme.

Théorème 6.66 (Inégalité de Cauchy-Schwarz).

Si X et Y sont des vecteurs, alors

$$|X \cdot Y| \leq \|X\| \|Y\|. \quad (6.203)$$

Nous avons une égalité si et seulement si X et Y sont multiples l'un de l'autre.

Démonstration. Étant donné que les deux membres de l'inéquation sont positifs, nous allons travailler en passant au carré afin d'éviter les racines carrées dans le second membre.

Nous considérons le polynôme

$$P(t) = \|X + tY\|^2 = (X + tY) \cdot (X + tY) = X \cdot X + tX \cdot Y + tY \cdot X + t^2Y \cdot Y. \quad (6.204)$$

En ordonnant les termes selon les puissances de t ,

$$P(t) = \|Y\|^2 t^2 + 2(X \cdot Y)t + \|X\|^2. \quad (6.205)$$

Cela est un polynôme du second degré en t . Par conséquent le discriminant¹² doit être négatif. Nous avons donc

$$\Delta = 4(X \cdot Y)^2 - 4\|X\|^2\|Y\|^2 \leq 0, \quad (6.206)$$

ce qui donne immédiatement

$$(X \cdot Y)^2 \leq \|X\|^2\|Y\|^2. \quad (6.207)$$

En ce qui concerne le cas d'égalité, si nous avons $X \cdot Y = \|X\| \|Y\|$, alors le discriminant Δ ci-dessus est nul et le polynôme P admet une racine double t_0 . Pour cette valeur nous avons

$$P(t_0) = \|X + t_0Y\|^2 = 0, \quad (6.208)$$

ce qui implique $X + t_0Y = 0$ et donc que X et Y sont liés. □

10. Définition 6.63.

11. Définition 6.64.

12. Le fameux $b^2 - 4ac$.

Vu que nous allons voir un pâté d'espaces avec des produits scalaires, nous leur donnons un nom.

Définition 6.67.

Un espace vectoriel **euclidien** est un espace vectoriel de dimension finie muni d'un produit scalaire.

Proposition 6.68.

Si $x, y \mapsto x \cdot y$ est un produit scalaire sur un espace vectoriel E , alors $N(x) = \sqrt{x \cdot x}$ est une norme vérifiant l'identité du parallélogramme :

$$\|x - y\|^2 + \|x + y\|^2 = 2\|x\|^2 + 2\|y\|^2. \quad (6.209)$$

Démonstration. Prouvons l'inégalité triangulaire. Si $x, y \in E$ nous avons

$$\|x + y\| = \sqrt{\|x\|^2 + \|y\|^2 + 2x \cdot y}. \quad (6.210)$$

Par l'inégalité de Cauchy-Schwartz, théorème 6.66 nous avons aussi

$$\|x\|^2 + \|y\|^2 + 2x \cdot y \leq \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| = (\|x\| + \|y\|)^2, \quad (6.211)$$

donc

$$\|x + y\| \leq \sqrt{(\|x\| + \|y\|)^2} = \|x\| + \|y\|. \quad (6.212)$$

La seconde assertion est seulement un calcul :

$$\begin{aligned} \|x - y\|^2 + \|x + y\|^2 &= (x - y) \cdot (x - y) + (x + y) \cdot (x + y) \\ &= x \cdot x - x \cdot y - y \cdot x + y \cdot y \\ &\quad + x \cdot x + x \cdot y + y \cdot x + y \cdot y \\ &= 2x \cdot x + 2y \cdot y \\ &= 2\|x\|^2 + 2\|y\|^2. \end{aligned} \quad (6.213)$$

□

Le produit scalaire permet de donner une norme via la formule suivante :

$$\|x\|^2 = x \cdot x. \quad (6.214)$$

Lemme 6.69 ([1]).

Soit V un espace vectoriel muni d'un produit scalaire et de la norme associée. Si $x, y \in V$ satisfont à $\|x + y\| = \|x\| + \|y\|$, alors il existe $\lambda \geq 0$ tel que $x = \lambda y$.

Démonstration. Quitte à raisonner avec $x/\|x\|$ et $y/\|y\|$, nous supposons que $\|x\| = \|y\| = 1$. Dans ce cas l'hypothèse signifie que $\|x + y\|^2 = 4$. D'autre part en écrivant la norme en terme de produit scalaire,

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x, y \rangle, \quad (6.215)$$

ce qui nous mène à affirmer que $\langle x, y \rangle = 1 = \|x\|\|y\|$. Nous sommes donc dans le cas d'égalité de l'inégalité de Cauchy-Schwarz¹³, ce qui nous donne un λ tel que $x = \lambda y$. Étant donné que $\|x\| = \|y\| = 1$ nous avons obligatoirement $\lambda = \pm 1$, mais si $\lambda = -1$ alors $\langle x, y \rangle = -1$, ce qui est le contraire de ce qu'on a prétendu plus haut. Par soucis de cohérence, nous allons donc croire que $\lambda = 1$. □

13. Théorème 6.66.

6.8.1 Projection et angles

Proposition 6.70 (Propriétés du produit scalaire).

Si X et Y sont des vecteurs de $\mathbb{R}^3$, alors

Symétrie $X \cdot Y = Y \cdot X$;

Linéarité $(\lambda X + \mu X') \cdot Y = \lambda(X \cdot Y) + \mu(X' \cdot Y)$ pour tout λ et μ dans $\mathbb{R}$;

Défini positif $X \cdot X \geq 0$ et $X \cdot X = 0$ si et seulement si $X = 0$.

Note : lorsque nous écrivons $X = 0$, nous voulons dire $X = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$.

Définition 6.71.

La **norme** du vecteur X , notée $\|X\|$, est définie par

$$\|X\| = \sqrt{X \cdot X} = \sqrt{x^2 + y^2 + z^2} \quad (6.216)$$

si $X = (x, y, z)$. Cette norme sera parfois nommée «norme euclidienne».

Cette définition est motivée par le théorème de Pythagore. Le nombre $X \cdot X$ est bien la longueur de la «flèche» X . Plus intrigante est la définition suivante :

Définition 6.72.

Deux vecteurs X et Y sont **orthogonaux** si $X \cdot Y = 0$.

Cette définition de l'orthogonalité est motivée par la proposition suivante.

Proposition 6.73.

Si nous écrivons proj_Y l'opération de projection sur la droite qui sous-tend Y , alors nous avons

$$\|\text{proj}_Y X\| = \frac{X \cdot Y}{\|Y\|}. \quad (6.217)$$

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

$$X = \begin{pmatrix} x \\ y \\ 0 \end{pmatrix}, \quad Y = \begin{pmatrix} l \\ 0 \\ 0 \end{pmatrix} \quad (6.218)$$

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 $\|\text{proj}_Y X\| = x$. Par conséquent,

$$\|\text{proj}_Y X\| = \frac{X \cdot Y}{l} = \frac{X \cdot Y}{\|Y\|}. \quad (6.219)$$

□

Corollaire 6.74.

Si la norme de Y est 1, alors le nombre $X \cdot Y$ est la longueur de la projection de X sur Y .

Démonstration. Poser $\|Y\| = 1$ dans la proposition 6.73. □

Nous sommes maintenant en mesure de déterminer, pour deux vecteurs quelconques u et v , la projection orthogonale de u sur v . Ce sera le vecteur $\bar{u}$ parallèle à v tel que $u - \bar{u}$ est orthogonal à v . Nous avons donc

$$\bar{u} = \lambda v \quad (6.220)$$

et

$$(u - \lambda v) \cdot v = 0. \quad (6.221)$$

La seconde équation donne $u \cdot v - \lambda v \cdot v = 0$, ce qui fournit λ en fonction de u et v :

$$\lambda = \frac{u \cdot v}{\|v\|^2}. \quad (6.222)$$

Nous avons par conséquent

$$\bar{u} = \frac{u \cdot v}{\|v\|^2} v. \quad (6.223)$$

Armés de cette interprétation graphique du produit scalaire, nous comprenons pourquoi nous disons que deux vecteurs sont orthogonaux lorsque leur produit scalaire est nul.

Nous pouvons maintenant savoir quel est le coefficient directeur d'une droite orthogonale à une droite donnée. En effet, supposons que la première droite soit parallèle au vecteur X et la seconde au vecteur Y . Les droites seront perpendiculaires si $X \cdot Y = 0$, c'est à dire si

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 0. \quad (6.224)$$

Cette équation se développe en

$$x_1 y_1 = -x_2 y_2. \quad (6.225)$$

Le coefficient directeur de la première droite est $\frac{x_2}{x_1}$. Isolons cette quantité dans l'équation (6.225) :

$$\frac{x_2}{x_1} = -\frac{y_1}{y_2}. \quad (6.226)$$

Donc le coefficient directeur de la première est l'inverse et l'opposé du coefficient directeur de la seconde.

Exemple 6.75

Soit la droite $d \equiv y = 2x + 3$. Le coefficient directeur de cette droite est 2. Donc le coefficient directeur d'une droite perpendiculaires doit être $-\frac{1}{2}$. $\triangle$

Preuve alternative. La preuve peut également être donnée en ne faisant pas référence au produit scalaire. Il suffit d'écrire toutes les quantités en termes des coordonnées de X et Y . Si nous posons

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, \quad (6.227)$$

l'inégalité à prouver devient

$$(x_1 y_1 + x_2 y_2 + x_3 y_3)^2 \leq (x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2). \quad (6.228)$$

Nous considérons la fonction

$$\varphi(t) = (x_1 + t y_1)^2 + (x_2 + t y_2)^2 + (x_3 + t y_3)^2 \quad (6.229)$$

En tant que norme, cette fonction est évidemment positive pour tout t . En regroupant les termes de chaque puissance de t , nous avons

$$\varphi(t) = (y_1^2 + y_2^2 + y_3^2)t^2 + 2(x_1 y_1 + x_2 y_2 + x_3 y_3)t + (x_1^2 + x_2^2 + x_3^2). \quad (6.230)$$

Cela est un polynôme du second degré en t . Par conséquent le discriminant doit être négatif. Nous avons donc

$$4(x_1 y_1 + x_2 y_2 + x_3 y_3)^2 - (x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) \leq 0. \quad (6.231)$$

La thèse en découle aussitôt. $\square$

Proposition 6.76.

La norme euclidienne a les propriétés suivantes :

- (1) Pour tout vecteur X et réel λ , $\|\lambda X\| = |\lambda|\|X\|$. Attention à ne pas oublier la valeur absolue !
 (2) Pour tout vecteurs X et Y , $\|X + Y\| \leq \|X\| + \|Y\|$.

Démonstration. Nous ne prouvons pas le premier point. Pour le second, nous avons les inégalités suivantes :

$$\|X + Y\|^2 = \|X\|^2 + \|Y\|^2 + 2X \cdot Y \quad (6.232a)$$

$$\leq \|X\|^2 + \|Y\|^2 + 2|X \cdot Y| \quad (6.232b)$$

$$\leq \|X\|^2 + \|Y\|^2 + 2\|X\|\|Y\| \quad (6.232c)$$

$$= (\|X\| + \|Y\|)^2 \quad (6.232d)$$

Nous avons utilisé d'abord la majoration $|x| \geq x$ qui est évident pour tout nombre x ; et ensuite l'inégalité de Cauchy-Schwarz. $\square$

6.8.2 Angle entre deux vecteurs

Si a et b sont des réels, l'inégalité $|a| \leq b$ peut se développer en une double inégalité

$$-b \leq a \leq b. \quad (6.233)$$

L'inégalité de Cauchy-Schwarz devient alors

$$-\|X\|\|Y\| \leq X \cdot Y \leq \|X\|\|Y\|. \quad (6.234)$$

Si $X \neq 0$ et $Y \neq 0$, nous avons alors

$$-1 \leq \frac{X \cdot Y}{\|X\|\|Y\|} \leq 1. \quad (6.235)$$

Il existe donc un angle $\theta \in [0, \pi]$ tel que

$$\cos(\theta) = \frac{X \cdot Y}{\|X\|\|Y\|}. \quad (6.236)$$

L'angle ainsi défini est l'**angle** entre X et Y . La définition (6.236) est souvent utilisée sous la forme

$$X \cdot Y = \|X\|\|Y\| \cos(\theta). \quad (6.237)$$

Notez que les angles sont toujours des angles plus petits ou égaux à 180° .

6.8.3 Procédé de Gram-Schmidt**Proposition 6.77** (Procédé de Gram-Schmidt).

Un espace euclidien possède une base orthonormée.

Démonstration. Soit E un espace euclidien et $\{v_1, \dots, v_n\}$, une base quelconque de E . Nous posons d'abord

$$f_1 = v_1, \quad e_1 = \frac{f_1}{\|f_1\|}. \quad (6.238)$$

Ensuite

$$f_2 = v_2 - \langle v_2, e_1 \rangle e_1, \quad e_2 = \frac{f_2}{\|f_2\|}. \quad (6.239)$$

Notons que $\{e_1, e_2\}$ est une base de $\text{Span}\{v_1, v_2\}$. De plus elle est orthogonale :

$$\langle e_1, f_2 \rangle = \langle e_1, v_2 \rangle - \underbrace{\langle v_2, e_1 \rangle \langle e_1, e_1 \rangle}_{=1} = 0. \quad (6.240)$$

Le fait que $\|e_1\| = \|e_2\| = 1$ est par construction. Nous avons donc donné une base orthonormée de $\text{Span}\{v_1, v_2\}$.

Nous continuons par récurrence en posant

$$f_k = v_k - \sum_{i=1}^{k-1} \langle v_k, e_i \rangle e_i, \quad e_k = \frac{f_k}{\|f_k\|}. \quad (6.241)$$

Pour tout $j < k$ nous avons

$$\langle e_j, f_k \rangle = \langle e_j, v_k \rangle - \sum_{i=1}^{k-1} \langle v_k, e_i \rangle \underbrace{\langle e_i, e_j \rangle}_{=\delta_{ij}} = 0 \quad (6.242)$$

□

Cet algorithme de Gram-Schmidt nous donne non seulement l'existence de bases orthonormées pour tout espace euclidien, mais aussi le moyen d'en construire à partir de n'importe quelle base.

6.9 Norme opérateur

Nous définissons ici la norme opérateur, et donnons des résultats généraux. D'autres résultats sur la norme opérateur :

(1) Le lemme à propos d'exponentielle de matrice 16.81 donne :

$$\|e^{tA}\| \leq P(|t|) \sum_{i=1}^r e^{t \operatorname{Re}(\lambda_i)}. \quad (6.243)$$

Définition 6.78 ([83]).

Soit E un espace vectoriel (pas spécialement de dimension finie). Une **norme** sur E est une application $\|\cdot\|: E \rightarrow \mathbb{R}$ telle que

- (1) $\|v\| = 0$ seulement si $A = 0$,
- (2) $\|\lambda v\| = |\lambda| \cdot \|v\|$,
- (3) $\|v + w\| \leq \|v\| + \|w\|$

pour tout $v, w \in E$ et pour tout $\lambda \in \mathbb{R}$.

Définition 6.79.

Si V et W sont des espaces vectoriels nous munissons $\mathcal{L}(V, W)$ d'une structure d'espace vectoriel en définissant la somme et le produit par un scalaire de la façon suivante. Si T et U sont des éléments de $\mathcal{L}(V, W)$ et si λ est un réel, nous définissons les éléments $T + U$ et λT par

- (1) $(T + U)(x) = T(x) + U(x)$;
- (2) $(\lambda T)(x) = \lambda T(x)$

pour tout $x \in V$.

La proposition suivante donne une norme (au sens de la définition 5.31) sur $\mathcal{L}(V, W)$ afin d'obtenir un espace vectoriel normé.

Proposition 6.80.

Soit le nombre

$$\|T\|_{\mathcal{L}} = \sup_{x \in V} \frac{\|T(x)\|_W}{\|x\|_V}. \quad (6.244)$$

- (1) Si V est de dimension finie, alors $\|T\|_{\mathcal{L}} < \infty$.
- (2) L'application $T \mapsto \|T\|_{\mathcal{L}}$ est une norme sur l'espace vectoriel des applications linéaires $V \rightarrow W$.

(3) Nous avons la formule

$$\|T\|_{\mathcal{L}} = \sup_{x \in V} \frac{\|T(x)\|_W}{\|x\|_V} = \sup_{\|x\|_V=1} \|T(x)\|_W \quad (6.245)$$

Démonstration. Si V est de dimension finie alors l'ensemble $\{\|x\| = 1\}$ est compact par le théorème de Borel-Lebesgue 5.107. Alors la fonction

$$x \mapsto \frac{\|T(x)\|}{\|x\|} \quad (6.246)$$

est une fonction continue sur un compact. Le corollaire 5.114 nous dit alors qu'elle est bornée. Le supremum est donc un nombre réel fini.

Nous vérifions que l'application $\|\cdot\|$ de $\mathcal{L}(V, W)$ dans $\mathbb{R}$ ainsi définie est effectivement une norme.

- (1) $\|T\|_{\mathcal{L}} = 0$ signifie que $\|T(x)\| = 0$ pour tout x dans V . Comme $\|\cdot\|_W$ est une norme nous concluons que $T(x) = 0_n$ pour tout x dans V , donc T est l'application nulle.
- (2) Pour tout a dans $\mathbb{R}$ et tout T dans $\mathcal{L}(V, W)$ nous avons

$$\|aT\|_{\mathcal{L}} = \sup_{\|x\|_V \leq 1} \|aT(x)\|_W = |a| \sup_{\|x\|_V \leq 1} \|T(x)\|_W = |a| \|T\|_{\mathcal{L}}. \quad (6.247)$$

- (3) Pour tous T_1 et T_2 dans $\mathcal{L}(V, W)$ nous avons

$$\begin{aligned} \|T_1 + T_2\|_{\mathcal{L}} &= \sup_{\|x\| \leq 1} \|T_1(x) + T_2(x)\| \leq \\ &\leq \sup_{\|x\| \leq 1} \|T_1(x)\| + \sup_{\|x\| \leq 1} \|T_2(x)\| \\ &= \|T_1\| + \|T_2\|. \end{aligned}$$

Enfin nous prouvons la formule alternative (6.245). Nous allons montrer que les ensembles sur lesquels on prend le supremum sont en réalité les mêmes :

$$\underbrace{\left\{ \frac{\|Ax\|}{\|x\|} \right\}_{x \neq 0}}_A = \underbrace{\{ \|Ax\| \text{ tel que } \|x\| = 1 \}}_B. \quad (6.248)$$

Attention : ce sont des sous-ensembles de réels ; pas de sous-ensembles de $\mathbb{M}(\mathbb{R})$ ou des sous-ensembles de $\mathbb{R}^n$.

Pour la première inclusion, prenons un élément de A , et prouvons qu'il est dans B . C'est à dire que nous prenons $x \in V$ et nous considérons le nombre $\|Ax\|/\|x\|$. Le vecteur $y = x/\|x\|$ est un vecteur de norme 1, donc la norme de Ay est un élément de B , mais

$$\|Ay\| = \frac{\|Ax\|}{\|x\|}. \quad (6.249)$$

Nous avons donc $A \subset B$.

L'inclusion $B \subset A$ est immédiate. □

Définition 6.81 (Norme opérateur, thème 17).

Le nombre

$$\|T\|_{\mathcal{L}} = \sup_{x \in V} \frac{\|T(x)\|_W}{\|x\|_V} = \sup_{\|x\|_V=1} \|T(x)\|_W \quad (6.250)$$

est la **norme opérateur** de T .

La norme opérateur est liée à la continuité par la proposition 6.217.

Lorsque nous considérons un espace vectoriel d'applications linéaires, nous considérons toujours¹⁴ dessus la topologie liée à cette norme.

14. Sauf lorsque les événements nous forceront à trahir.

6.9.1 Norme algébrique

Définition 6.82 (Norme d'algèbre).

Si A est une algèbre¹⁵, une **norme d'algèbre** sur A est une norme telle que pour toute $u, v \in A$,

$$\|uv\| \leq \|u\|\|v\|. \quad (6.251)$$

L'intérêt d'une norme d'algèbre est entre autres de mieux se comporter pour les séries, voir par exemple 16.4.7.

Définition 6.83.

Le **rayon spectral** d'une matrice carrée A , noté $\rho(A)$, est défini de la manière suivante :

$$\rho(A) = \max_i |\lambda_i| \quad (6.252)$$

où les λ_i sont les valeurs propres de A .

Remarque 6.84.

Une matrice de taille $n \times n$ a toujours n valeurs propres (pas toujours distinctes) dans $\mathbb{C}$. Donc le maximum dont on parle dans le

<++>

Proposition 6.85.

Pour tout norme algébrique, le rayon spectral d'une matrice sur $\mathbb{C}$ est toujours plus petit que sa norme. C'est à dire que nous avons toujours $\rho(A) \leq \|A\|$ pour toute norme algébrique $\|\cdot\|$.

Définition 6.86 (Norme opérateur).

Pour chaque norme sur $\mathbb{R}^n$, nous pouvons définir une norme correspondante sur $M_n(\mathbb{R})$, appelée **norme opérateur**. Si $\|\cdot\|$ est une norme sur $\mathbb{R}^n$, nous définissons $\|A\|$ par

$$\|A\| = \sup_{\|x\| \neq 0} \frac{\|Ax\|}{\|x\|} \quad (6.253)$$

En particulier, cela donne lieu à toutes les normes $\|A\|_p$ qui correspondent aux normes $\|\cdot\|_p$ sur $\mathbb{R}^n$. Cette norme est la norme **subordonnée** à celle sur $\mathbb{R}^n$.

La norme opérateur est souvent écrite $\|A\|_\infty$ parce que cette norme donne lieu à la **topologie forte** sur l'espace des opérateurs. La topologie forte n'est pas la seule possible. Il existe aussi par exemple la **topologie faible** donnée par la notion de convergence $A_i \rightarrow A$ si et seulement si $A_i x \rightarrow Ax$ pour tout $x \in E$.

Il faut noter que la topologie faible n'est pas une topologie métrique. Cela même si la condition $A_i x \rightarrow Ax$, elle, est métrique vu qu'elle est écrite dans E . et que dans le cas où E est de dimension infinie, elle est réellement différente de la topologie forte. Nous verrons à la sous-section 17.3.5 que dans le cas des projections sur un espaces de Hilbert, l'égalité

$$\sum_{i=1}^{\infty} \text{proj}_{u_i} = \text{Id} \quad (6.254)$$

est vraie pour la topologie faible, mais pas pour la topologie forte.

Définition 6.87.

Si E et F sont deux espaces vectoriels normés nous notons $\text{GL}(E, F)$ le sous-espace de $\mathcal{L}(E, F)$ des isométries linéaires de E vers F . Un élément de $\text{GL}(E, F)$ est donc linéaire, continue et bijective.

Proposition 6.88.

Inégalités sur la norme opérateur.

15. Définition 4.3.

(1) Si E et F sont des espaces vectoriels normés alors la norme opérateur est une norme d'algèbre¹⁶ sur $\text{GL}(E, F)$:

$$\|AB\| \leq \|A\|\|B\| \quad (6.255)$$

pour tout $A, B \in \text{GL}(E)$.

(2) Pour tout $A \in \mathcal{L}(E, F)$, et pour tout $u \in E$ nous avons la majoration

$$\|Au\| \leq \|A\|\|u\| \quad (6.256)$$

où la norme sur A est la norme opérateur subordonnée à la norme sur u .

Démonstration. Nous avons

$$\|AB\| = \sup_{x \in E} \frac{\|ABx\|}{\|x\|} \frac{\|Bx\|}{\|Bx\|} \quad (6.257a)$$

$$= \sup_{x \in E} \frac{\|A(Bx)\|}{\|Bx\|} \frac{\|Bx\|}{\|x\|} \quad (6.257b)$$

$$\leq \sup_{x \in E} \frac{\|A(Bx)\|}{\|Bx\|} \sup_{x \in E} \frac{\|Bx\|}{\|x\|}. \quad (6.257c)$$

Le premier facteur est égal à $\|A\|$ parce que B est surjective. Le second est $\|B\|$ par définition.

Si $u \in E$ alors, étant donné que le supremum d'un ensemble est plus grand ou égal à tous les éléments qui le compose,

$$\|A\| = \sup_{x \in E} \frac{\|Ax\|}{\|x\|} \geq \frac{\|Au\|}{\|u\|}, \quad (6.258)$$

donc le résultat annoncé : $\|Au\| \leq \|A\|\|u\|$. $\square$

Notons qu'en réalité nous n'avons utilisé seulement le fait que B était surjective

Lemme 6.89.

Soit F un espace de Banach et deux suites $A_k \rightarrow A$ et $B_k \rightarrow B$ dans $\mathcal{L}(F, F)$. Alors $A_k \circ B_k \rightarrow A \circ B$ dans $\mathcal{L}(F, F)$, c'est à dire

$$\lim_{n \rightarrow \infty} (A_k B_k) = \left(\lim_{n \rightarrow \infty} A_k \right) \left(\lim_{n \rightarrow \infty} B_k \right). \quad (6.259)$$

Démonstration. Il suffit d'écrire

$$\|A_k B_k - AB\| \leq \|A_k B_k - A_k B\| + \|A_k B - AB\|. \quad (6.260)$$

Le premier terme tend vers zéro pour $k \rightarrow \infty$ parce que

$$\|A_k B_k - A_k B\| = \|A_k(B_k - B)\| \quad (6.261a)$$

$$\leq \|A_k\| \|B_k - B\| \rightarrow \|A\| \cdot 0 \quad (6.261b)$$

$$= 0 \quad (6.261c)$$

où nous avons utilisé la propriété fondamentale de la norme opérateur : la proposition 6.88. Le second terme tend également vers zéro pour la même raison. $\square$

Proposition 6.90 (Distributivité de la somme infinie).

Soient E un espace normé, une suite (u_k) dans $\text{GL}(E)$ ainsi que $a \in \text{GL}(E)$. Pourvu que la série $\sum_{n=0}^{\infty} u_k$ converge nous avons

$$\left(\sum_{k=0}^{\infty} u_k \right) a = \sum_{k=0}^{\infty} (u_k a). \quad (6.262)$$

¹⁶. Définition 6.82.

Démonstration. Par définition de la somme infinie,

$$\spadesuit = \left(\sum_{k=0}^{\infty} u_k \right) a = \left(\lim_{n \rightarrow \infty} \sum_{k=0}^n u_k \right) a. \quad (6.263)$$

Le lemme 6.89 appliqué à $n \mapsto \sum_{k=0}^n u_k$ et à la suite constante a nous donne

$$\spadesuit = \lim_{n \rightarrow \infty} \left(\sum_{k=0}^n u_k a \right), \quad (6.264)$$

ce que nous voulions par distributivité de la somme finie : dans (6.264), le a est dans ou hors de la somme, au choix. L'important est qu'il soit dans la limite. $\square$

6.9.2 Normes de matrices et d'applications linéaires

Théorème 6.91 (Norme matricielle et rayon spectral[84]).

La norme 2 d'une matrice est liée au rayon spectral de la façon suivante :

$$\|A\|_2 = \sqrt{\rho(A^t A)} \quad (6.265)$$

ou plus généralement par $\|A\|_2 = \sqrt{\rho(A^* A)}$.

Proposition 6.92.

La fonction

$$\begin{aligned} f: \mathbb{M}(n, \mathbb{R}) \times \mathbb{M}(n, \mathbb{R}) &\rightarrow \mathbb{R} \\ (X, Y) &\mapsto \text{Tr}(X^t Y) \end{aligned} \quad (6.266)$$

est un produit scalaire sur $\mathbb{M}(n, \mathbb{R})$.

Démonstration. Il faut vérifier la définition 6.65.

- La bilinéarité est la linéarité de la trace.
- La symétrie de f est le fait que $\text{Tr}(A^t) = \text{Tr}(A)$.
- L'application f est définie positive parce que si $X \in \mathbb{M}$, alors $X^t X$ est symétrique définie positive, donc diagonalisable avec des nombres positifs sur la diagonale. La trace étant un invariant de similitude, nous avons $f(X, X) = \text{Tr}(X^t X) \geq 0$. De plus si $\text{Tr}(X^t X) = 0$, alors $X^t X = 0$ (pour la même raison de diagonalisation). Mais alors $\|Xu\| = 0$ pour tout $u \in E$, ce qui signifie que $X = 0$.

$\square$

Exemple 6.93

Soit $m = n$, un point λ dans $\mathbb{R}$ et T_λ l'application linéaire définie par $T_\lambda(x) = \lambda x$. La norme de T_λ est alors

$$\|T_\lambda\|_{\mathcal{L}} = \sup_{\|x\|_{\mathbb{R}^m} \leq 1} \|\lambda x\|_{\mathbb{R}^n} = |\lambda|.$$

Notez que T_λ n'est rien d'autre que l'homothétie de rapport λ dans $\mathbb{R}^m$. $\triangle$

Exemple 6.94

Considérons la rotation T_α d'angle α dans $\mathbb{R}^2$. Elle est donnée par l'équation matricielle

$$T_\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos(\alpha)x + \sin(\alpha)y \\ -\sin(\alpha)x + \cos(\alpha)y \end{pmatrix} \quad (6.267)$$

Étant donné que cela est une rotation, c'est une isométrie : $\|T_\alpha x\| = \|x\|$. En ce qui concerne la norme de T_α nous avons

$$\|T_\alpha\| = \sup_{x \in \mathbb{R}^2} \frac{\|T_\alpha(x)\|}{\|x\|} = \sup_{x \in \mathbb{R}^2} \frac{\|x\|}{\|x\|} = 1. \quad (6.268)$$

Toutes les rotations dans le plan ont donc une norme 1. La même preuve tient pour toutes les rotations en dimension quelconque. $\triangle$

Exemple 6.95

Soit $m = n$, un point b dans $\mathbb{R}^m$ et T_b l'application linéaire définie par $T_b(x) = b \cdot x$ (petit exercice : vérifiez qu'il s'agit vraiment d'une application linéaire). La norme de T_b satisfait les inégalités suivantes

$$\|T_b\|_{\mathcal{L}} = \sup_{\|x\|_{\mathbb{R}^m} \leq 1} \|b \cdot x\|_{\mathbb{R}^n} \leq \sup_{\|x\|_{\mathbb{R}^m} \leq 1} \|b\|_{\mathbb{R}^n} \|x\|_{\mathbb{R}^n} \leq \|b\|_{\mathbb{R}^n},$$

$$\|T_b\|_{\mathcal{L}} = \sup_{\|x\|_{\mathbb{R}^m} \leq 1} \|b \cdot x\|_{\mathbb{R}^n} \geq \left\| b \cdot \frac{b}{\|b\|_{\mathbb{R}^n}} \right\|_{\mathbb{R}^n} = \|b\|_{\mathbb{R}^n},$$

donc $\|T_b\|_{\mathcal{L}} = \|b\|_{\mathbb{R}^n}$. $\triangle$

Proposition 6.96.

Une application linéaire de $\mathbb{R}^m$ dans $\mathbb{R}^n$ est continue.

Démonstration. Soit x un point dans $\mathbb{R}^m$. Nous devons vérifier l'égalité

$$\lim_{h \rightarrow 0_m} T(x + h) = T(x). \quad (6.269)$$

Cela revient à prouver que $\lim_{h \rightarrow 0_m} T(h) = 0$, parce que $T(x + h) = T(x) + T(h)$. Nous pouvons toujours majorer $\|T(h)\|_n$ par $\|T\|_{\mathcal{L}(\mathbb{R}^m, \mathbb{R}^n)} \|h\|_{\mathbb{R}^m}$ (proposition 6.88(2)). Quand h s'approche de 0_m sa norme $\|h\|_m$ tend vers 0, ce que nous permet de conclure parce que nous savons que de toutes façons, $\|T\|_{\mathcal{L}}$ est fini. $\square$

Note : dans un espace de dimension infinie, la linéarité ne suffit pas pour avoir la continuité : il faut de plus être borné (ce que sont toutes les applications linéaires $\mathbb{R}^m \rightarrow \mathbb{R}^n$). Voir la proposition 6.217.

6.10 Produit vectoriel

Définition 6.97.

Soient u et v , deux vecteurs de $\mathbb{R}^3$. Le **produit vectoriel** de u et v est le vecteur $u \times v$ défini par

$$u \times v = \begin{vmatrix} e_1 & e_2 & e_3 \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} \quad (6.270)$$

$$= (u_2 v_3 - u_3 v_2) e_1 + (u_3 v_1 - u_1 v_3) e_2 + (u_1 v_2 - u_2 v_1) e_3$$

où les vecteurs e_1 , e_2 et e_3 sont les vecteurs de la base canonique de $\mathbb{R}^3$.

La notion de produit vectoriel est propre à $\mathbb{R}^3$; il n'y a pas de généralisation simple aux espaces $\mathbb{R}^m$.

Nous n'allons pas nous attarder sur les nombreuses propriétés du produit vectoriel. Les principales sont résumées dans la proposition suivante.

Proposition 6.98.

Si u et v sont des vecteurs de $\mathbb{R}^3$, alors le vecteur $u \times v$ est l'unique vecteur qui est perpendiculaire à u et v en même temps, de norme égal à la surface du parallélogramme construit sur u et v et tel que les vecteurs u , v , $u \times v$ forment une base dextrogyre.

La chose importante à retenir est que le produit vectoriel permet de construire un vecteur simultanément perpendiculaire à deux vecteurs donnés. Le vecteur $u \times v$ est donc linéairement indépendant de u et v . En pratique, si u et v sont déjà linéairement indépendants, alors le produit vectoriel permet de compléter une base de $\mathbb{R}^3$.

À l'aide du produit vectoriel et du produit scalaire, nous construisons le **produit mixte** de trois vecteurs de $\mathbb{R}^3$ par la formule

$$(u \times v) \cdot w = \begin{vmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{vmatrix}. \quad (6.271)$$

Pourquoi nous ne considérons pas la combinaison $(u \cdot v) \times w$?

Proposition 6.99.

Les applications produit scalaire, vectoriel et mixte sont multilinéaires. Spécifiquement, nous avons les propriétés suivantes.

- (1) *Les applications produit scalaire et vectoriel sont bilinéaires. Le produit mixte est trilinéaire.*
- (2) *Le produit vectoriel est antisymétrique, c'est à dire $u \times v = -v \times u$.*
- (3) *Nous avons $u \times v = 0$ si et seulement si u et v sont colinéaires, c'est à dire si et seulement si l'équation $\alpha u + \beta v = 0$ a une solution différente de la solution triviale $(\alpha, \beta) = (0, 0)$.*
- (4) *Pour tout u et v dans $\mathbb{R}^3$, nous avons*

$$\langle u, v \rangle^2 + \|u \times v\|^2 = \|u\|^2 \|v\|^2 \quad (6.272)$$

- (5) *Par rapport à la dérivation, le produit scalaire et vectoriel vérifient une règle de Leibnitz. Soit I un intervalle de $\mathbb{R}$, et si u et v sont dans $C^1(I, \mathbb{R}^3)$, alors*

$$\begin{aligned} \frac{d}{dt}(u(t) \cdot v(t)) &= (u'(t) \cdot v(t)) + (u(t) \cdot v'(t)) \\ \frac{d}{dt}(u(t) \times v(t)) &= (u'(t) \times v(t)) + (u(t) \times v'(t)). \end{aligned} \quad (6.273)$$

Les deux formules suivantes, qui mêlent le produit scalaire et le produit vectoriel, sont souvent utiles en analyse vectorielle :

$$\begin{aligned} (u \times v) \cdot w &= u \cdot (v \times w) \\ (u \times v) \times w &= -(v \cdot w)u + (u \cdot w)v \end{aligned} \quad (6.274)$$

pour tout vecteurs u, v et w dans $\mathbb{R}^3$. Nous les admettons sans démonstration. La seconde formule est parfois appelée **formule d'expulsion**.

6.11 Topologie

6.11.1 Boules et sphères

Définition 6.100.

Soit $(V, \|\cdot\|)$, un espace vectoriel normé, $a \in V$ et $r > 0$. Nous allons abondamment nous servir des ensembles suivants :

- (1) *la **boule ouverte** $B(a, r) = \{x \in V \text{ tel que } \|x - a\| < r\}$;*
- (2) *la **boule fermée** $\bar{B}(a, r) = \{x \in V \text{ tel que } \|x - a\| \leq r\}$;*
- (3) *la **sphère** $S(a, r) = \{x \in V \text{ tel que } \|x - a\| = r\}$.*

Les différences entre ces trois ensembles 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. Nous avons

$$\bar{B}(a, r) = B(a, r) \cup S(a, r). \quad (6.275)$$

Définition 6.101.

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 6.102

Dans $\mathbb{R}$, les boules sont les intervalles ouverts et fermés tandis que la sphère est donnée par les points extrêmes des intervalles :

$$\begin{aligned} B(a, r) &=]a - r, a + r[, \\ \bar{B}(a, r) &= [a - r, a + r], \\ S(a, r) &= \{a - r, a + r\}. \end{aligned} \tag{6.276}$$

△

Exemple 6.103

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 $\|\cdot\|_1$, $\|\cdot\|_2$ et $\|\cdot\|_\infty$.

Pour la norme $\|\cdot\|_1$, la sphère de rayon r est donnée par l'équation

$$|x| + |y| = r. \tag{6.277}$$

Pour la norme $\|\cdot\|_2$, l'équation de la sphère de rayon r est

$$\sqrt{x^2 + y^2} = r, \tag{6.278}$$

et pour la norme supremum, la sphère de rayon r a pour équation

$$\max\{|x|, |y|\} = r. \tag{6.279}$$

Elles sont dessinées sur la figure 6.2

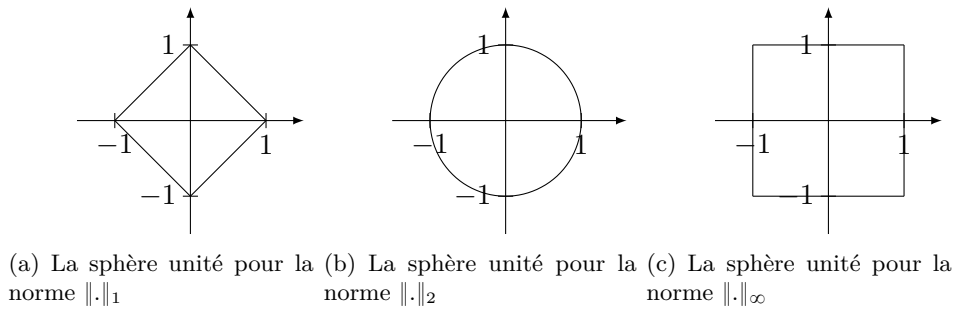


FIGURE 6.2 – Les sphères de rayon 1 pour les trois normes classiques.

△

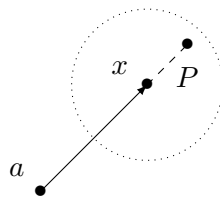


FIGURE 6.3 – Le point P est un peu plus loin que x , en suivant la même droite.

Proposition 6.104.

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 $d(Q, a) < r$.

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» (voir figure 6.3). Plus précisément, nous considérons le point

$$P = x + \frac{v}{N} \quad (6.280)$$

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

$$d(P, x) = \|P - x\| = \frac{\|v\|}{N} \quad (6.281)$$

peut être rendu aussi petit que l'on veut par un choix approprié de N . Montrons maintenant que $d(a, P) > d(a, x)$:

$$\begin{aligned} d(a, P) &= \|a - x - \frac{v}{N}\| \\ &= \|a - x + \frac{a}{N} - \frac{x}{N}\| \\ &= \|(1 + \frac{1}{N})(a - x)\| \\ &> \|a - x\| = d(a, x). \end{aligned} \quad (6.282)$$

Nous laissons en exercice le soin de trouver un point Q tel que $d(Q, a) < r$ et $d(Q, x) < \delta$. $\square$

6.11.2 Ouverts, fermés, intérieur et adhérence**Définition 6.105.**

Soit $(V, \|\cdot\|)$ 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 $\text{Int}(A)$ l'intérieur de A .

Notons que $\text{Int}(A) \subset A$ parce que si $a \in \text{Int}(A)$, nous avons $B(a, r) \subset A$ pour un certain r et en particulier $a \in A$.

Exemple 6.106

Trouver l'intérieur d'un intervalle dans $\mathbb{R}$ consiste à «ouvrir là où c'est fermé».

- (1) $\text{Int}([0, 1]) =]0, 1[$.

Prouvons d'abord que $]0, 1[\subset \text{Int}([0, 1])$. 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 6.4). Cela prouve que a est dans l'intérieur de $[0, 1]$.

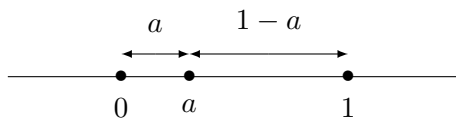


FIGURE 6.4 – Trouver le rayon d'une boule autour de a . Une boule qui serait centrée en a avec un rayon strictement plus petit à la fois de a et de $1 - a$ est entièrement contenue dans le segment $]0, 1[$.

Prouvons maintenant que $\text{Int}([0, 1]) \subset]0, 1[$. Vu que l'intérieur d'un ensemble est inclus à l'ensemble, nous savons déjà que $\text{Int}([0, 1]) \subset [0, 1]$. 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) $\text{Int}([0, \infty[) =]0, \infty[.$
 (3) $\text{Int}(]2, 3[) =]2, 3[.$

△

Exemple 6.107

Les intérieurs des boules et sphères sont importantes à savoir.

- (1) $\text{Int}(B(a, r)) = B(a, r)$. Si $x \in B(a, r)$, nous avons $d(a, x) < r$. Alors la boule $B(x, r - d(x, a))$ est incluse à $B(a, r)$, et donc x est dans l'intérieur de $B(a, r)$. Conseil : faire un dessin.
 (2) $\text{Int}(\bar{B}(a, r)) = B(a, r)$. 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 6.104.
 (3) $\text{Int}(S(a, r)) = \emptyset$. 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 6.108.

Une partie A de l'espace vectoriel normé $(V, \|\cdot\|)$ est dite **ouverte** si chacun de ses points est intérieur. La partie A est donc ouverte si $A \subset \text{Int}(A)$. Par convention, nous disons que l'ensemble vide $\emptyset$ est ouvert.

Une partie est dite **fermée** si son complémentaire est ouvert. La partie A est donc fermée si $V \setminus A$ est ouvert.

Remarque : un ensemble A est ouvert si et seulement si $\text{Int}(A) = A$.

Définition 6.109.

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 6.110

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 6.111.

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 incluses à V . Le vide est alors fermé (parce que son complémentaire est V).
- (2) Soit une famille $(\mathcal{O}_i)_{i \in I}$ d'ouverts¹⁷, et l'union

$$\mathcal{O} = \bigcup_{i \in I} \mathcal{O}_i. \quad (6.283)$$

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

$$\mathcal{O} = \bigcap_{k=1}^n \mathcal{O}_k. \quad (6.284)$$

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 incluse dans toutes les autres (parce que $B(a, r) \subset B(a, r')$ lorsque $r \leq r'$), par conséquent

$$B(a, r) \subset \bigcap_{k=1}^n B(a, r_k) \subset \bigcap_{k=1}^n \mathcal{O}_k = \mathcal{O}, \quad (6.285)$$

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 :

$$\bigcap_{i=1}^{\infty} \left] -\frac{1}{n}, \frac{1}{n} \right[= \{0\}. \quad (6.286)$$

Chacun des ensembles $\left] -\frac{1}{n}, \frac{1}{n} \right[$ est ouvert, mais le singleton $\{0\}$ est fermé (pourquoi?).

Nous reportons à la proposition 5.92 la preuve du fait que tout ensemble borné de $\mathbb{R}$ possède un infimum et un supremum.

Définition 6.112.

L'ensemble des ouverts de V est la **topologie** de V . La topologie dont nous parlons ici est dite **induite** par la norme $\|\cdot\|$ 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.

¹⁷. L'ensemble I avec lequel nous «numérotions» 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.

Exemple 6.113

Les ensemble 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 $\mathbb{R}$:

- $]1, 3[$;
- $]1, 3]$;
- $[0, 5[\setminus \{3\}$.

△

Proposition 6.114.

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 :

$$\bigcup_{n=1}^{\infty} \left[-1 + \frac{1}{n}, 1 - \frac{1}{n}\right] =]-1, 1[. \quad (6.287)$$

Chacun des intervalles dont on prend l'union est fermé tandis que l'union est ouverte.

Définition 6.115.

Soit A , une partie de l'espace vectoriel normé V . Un point $a \in V$ est dit **adhérent** à A dans V si pour tout $\varepsilon > 0$,

$$B(a, \varepsilon) \cap A \neq \emptyset. \quad (6.288)$$

Nous notons $\bar{A}$ l'ensemble des points adhérents à A et nous disons que $\bar{A}$ est l'adhérence de A . L'ensemble $\bar{A}$ sera aussi souvent nommé **fermeture** de l'ensemble A .

Un point peut être adhérent à A sans faire partie de A , et nous avons toujours $A \subset \bar{A}$.

Exemple 6.116

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 $\bar{A} \subset B$. Nous acceptons cela sans preuve.
- (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 6.110.

△

Exemple 6.117

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 $B(M, \varepsilon) \cap A \neq \emptyset$.

Le même raisonnement montre que l'infimum est également dans l'adhérence de A .

△

Exemple 6.118

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 6.119.

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. $\square$

Exemple 6.120

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) $\overline{]3, \infty[} = [3, \infty[$.

△

Proposition 6.121.

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 6.122.

Pour toute partie A d'un espace vectoriel normé nous avons

- (1) $V \setminus \bar{A} = \text{Int}(V \setminus A)$,
- (2) $V \setminus \text{Int}(A) = \overline{V \setminus A}$.

En utilisant les notations du complémentaire (1.1.2), les deux points de la proposition se récrivent

- (1) $\complement \bar{A} = \text{Int}(\complement A)$,
- (2) $\complement \text{Int}(A) = \overline{\complement A}$.

Démonstration. Nous avons $a \in V \setminus \bar{A}$ 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 $B(a, \varepsilon) \subset V \setminus A$. Or cela est exactement la définition du fait que a est à l'intérieur de $V \setminus A$. Nous avons donc montré que $a \in V \setminus \bar{A}$ si et seulement si $a \in \text{Int}(V \setminus A)$. Cela prouve la première affirmation.

Pour prouver la seconde affirmation, nous appliquons la première au complémentaire de A : $\complement(\bar{A}) = \text{Int}(\complement A)$. En prenant le complémentaire des deux membres nous trouvons successivement

$$\begin{aligned} \complement(\complement \bar{A}) &= \complement \text{Int}(\complement A), \\ \bar{A} &= \complement \text{Int}(A), \end{aligned} \tag{6.289}$$

ce qu'il fallait démontrer. $\square$

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 6.123.

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, $\overline{A \cup B} = \bar{A} \cup \bar{B}$ 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

$$\begin{aligned} B(a, \varepsilon_1) \cap A &= \emptyset, \\ B(a, \varepsilon_2) \cap B &= \emptyset. \end{aligned} \tag{6.290}$$

En prenant $r = \min\{\varepsilon_1, \varepsilon_2\}$, la boule $B(a, r)$ est incluse 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 $\mathbb{C}A$ et $\mathbb{C}B$, nous trouvons

$$\overline{\mathbb{C}A \cup \mathbb{C}B} = \overline{\mathbb{C}A} \cup \overline{\mathbb{C}B}. \tag{6.291}$$

En utilisant les propriétés du lemme 1.7, le membre de gauche devient

$$\overline{\mathbb{C}A \cup \mathbb{C}B} = \overline{\mathbb{C}(A \cap B)} = \mathbb{C} \text{Int}(A \cap B), \tag{6.292}$$

tandis que le membre de droite devient

$$\overline{\mathbb{C}A} \cup \overline{\mathbb{C}B} = \mathbb{C} \text{Int}(A) \cup \mathbb{C} \text{Int}(B) = \mathbb{C}(\text{Int}(A) \cup \text{Int}(B)). \tag{6.293}$$

En égalisant le membre de droite de (6.292) avec celui de (6.293) et en passant au complémentaire nous trouvons

$$\text{Int}(A \cap B) = \text{Int}(A) \cap \text{Int}(B), \tag{6.294}$$

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 6.124.

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 $A \cap B = \emptyset$ et donc $\overline{A \cap B} = \emptyset$. Par contre nous avons $\bar{A} \cap \bar{B} = \{1\}$.

Définition 6.125.

La **frontière** d'un sous-ensemble A de l'espace vectoriel normé V est l'ensemble des points $a \in V$ tels que

$$\begin{aligned} B(a, r) \cap A &\neq \emptyset, \\ B(a, r) \cap \mathbb{C}A &\neq \emptyset, \end{aligned} \tag{6.295}$$

pour tout rayon r . En d'autres termes, toute boule autour de a contient des points de A et des points de $\mathbb{C}A$. La frontière de A se note ∂A .

Proposition 6.126.

La frontière d'une partie A d'un espace vectoriel normé V s'exprime sous la forme

$$\partial A = \bar{A} \setminus \text{Int}(A). \tag{6.296}$$

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 $\text{Int}(A)$ signifie que toute boule centrée en a intersecte $\complement A$. $\square$

La description de la frontière donnée par la proposition 6.126 est celle qu'en pratique nous utilisons le plus souvent. Dans certains textes, elle est prise comme définition de la frontière.

Lemme 6.127.

La frontière de A peut également s'exprimer des façons suivantes :

$$\partial A = \bar{A} \cap \complement \text{Int}(A) = \bar{A} \cap \overline{\complement A}, \quad (6.297)$$

Démonstration. En partant de $\partial A = \bar{A} \setminus \text{Int}(A)$, la première égalité est une application de la propriété (4) du lemme 1.7. La seconde égalité est alors la proposition 6.122. $\square$

Exemple 6.128

Dans $\mathbb{R}$, la frontière d'un intervalle est la paire constituée des points extrêmes. En effet

$$\partial[a, b[= \overline{[a, b[} \setminus \text{Int}([a, b[) = [a, b[\setminus]a, b[= \{a, b\}. \quad (6.298)$$

Toujours dans $\mathbb{R}$ nous avons

$$\partial\mathbb{R} = \bar{\mathbb{R}} \setminus \text{Int}(\mathbb{R}) = \mathbb{R} \setminus \mathbb{R} = \emptyset, \quad (6.299)$$

et

$$\partial\mathbb{Q} = \bar{\mathbb{Q}} \setminus \text{Int}(\mathbb{Q}) = \mathbb{R} \setminus \emptyset = \mathbb{R}. \quad (6.300)$$

$\triangle$

Exemple 6.129

Dans $\mathbb{R}^n$, nous avons

$$\partial B(a, r) = \partial \bar{B}(a, r) = S(a, r). \quad (6.301)$$

Cela est un boulot pour la proposition 6.104. 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 $d(a, x) \leq r$. 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 $d(a, x) \geq r$. Les deux ensemble implique que $d(a, x) = r$. $\triangle$

Remarque 6.130.

Il serait toutefois faux de croire que $\partial A = \partial \bar{A}$ pour toute partie A de $\mathbb{R}^n$. En effet si $A = \mathbb{R} \setminus \{0\}$ nous avons $\partial A = \{0\}$ et $\bar{A} = \mathbb{R}$, donc $\partial \bar{A} = \emptyset$.

6.11.3 Point isolé, point d'accumulation

Définition 6.131.

Soit D , une partie de V .

(1) *Un point $a \in D$ est dit **isolé** dans D relativement à V si il existe un $\varepsilon > 0$ tel que*

$$B(a, \varepsilon) \cap D = \{a\}. \quad (6.302)$$

(2) *Un point $a \in V$ est un **point d'accumulation** de D si pour tout $\varepsilon > 0$,*

$$(B(a, \varepsilon) \setminus \{a\}) \cap D \neq \emptyset. \quad (6.303)$$

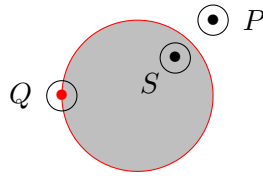


FIGURE 6.5 – L'ensemble décrit par l'équation (6.304). Le point P est un point isolé de D , tandis que les points S et Q sont des points d'accumulation.

Exemple 6.132

Considérons la partie suivante de $\mathbb{R}^2$:

$$D = \{(x, y) \text{ tel que } x^2 + y^2 < 1\} \cup \{(1, 1)\}. \quad (6.304)$$

Comme on peut le voir sur la figure 6.5, 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. $\triangle$

Remarque 6.133.

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 6.134

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. $\triangle$

Remarque 6.135.

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 .

Lemme 6.136 (Continuité des projections).

Soient deux espaces vectoriels V et W ainsi qu'une fonction continue $f: V \times W \rightarrow \mathbb{R}$. Alors pour tout $v_0 \in V$ la fonction

$$\begin{aligned} f_{v_0}: W &\rightarrow \mathbb{R} \\ w &\mapsto f(v_0, w) \end{aligned} \quad (6.305)$$

est continue.

6.12 Équivalence des normes

Au premier coup d'œil, les notions dont nous parlons dans ce chapitre ont l'air très générales. Nous prenons en effet n'importe quel espace vectoriel V de dimension finie, et nous le munissons de n'importe quelle norme (rien que dans $\mathbb{R}^m$ nous en avons défini une infinité par l'équation (6.196)). À partir de ces données, nous définissons les boules, la topologie, l'adhérence, etc.

6.12.1 En dimension finie

Dans $\mathbb{R}^n$, les normes $\|\cdot\|_{L^1}$, $\|\cdot\|_{L^2}$ et $\|\cdot\|_\infty$ ne sont pas égales. Cependant elles ne sont pas complètement indépendante au sens où l'on sent bien que si un vecteur sera grand pour une norme, il sera également grand pour les autres normes; les normes «vont dans le même sens». Cette notion est précisée par le concept de norme équivalente.

Définition 6.137.

Deux normes N_1 et N_2 sur $\mathbb{R}^m$ sont **équivalentes** si il existe deux nombres réels strictement positifs k_1 et k_2 tels que

$$k_1 N_1(x) \leq N_2(x) \leq k_2 N_1(x), \quad (6.306)$$

pour tout x dans $\mathbb{R}^m$. Dans ce cas nous écrivons que $N_1 \sim N_2$.

Il est possible de démontrer que cette notion est une relation d'équivalence (définition 1.10) sur l'ensemble des normes existantes sur $\mathbb{R}^m$.

Proposition 6.138.

Pour $\mathbb{R}^N$, nous avons les équivalences de normes $\|\cdot\|_{L^1} \sim \|\cdot\|_{L^2}$, $\|\cdot\|_{L^1} \sim \|\cdot\|_\infty$ et $\|\cdot\|_{L^2} \sim \|\cdot\|_\infty$. Plus précisément nous avons les inégalités

- (1) $\|x\|_2 \leq \|x\|_1 \leq \sqrt{n}\|x\|_2$
- (2) $\|x\|_\infty \leq \|x\|_1 \leq n\|x\|_\infty$
- (3) $\|x\|_\infty \leq \|x\|_2 \leq \sqrt{n}\|x\|_\infty$

Démonstration. En mettant au carré la première inégalité nous voyons que nous devons vérifier l'inégalité

$$|x_1|^2 + \dots + |x_n|^2 \leq (|x_1| + \dots + |x_n|)^2 \quad (6.307)$$

qui est vraie parce que le membre de droite est égal au carré de chaque terme plus les double produits. La seconde inégalité provient de l'inégalité de Cauchy-Schwarz (théorème 6.66) sur les vecteurs

$$v = \begin{pmatrix} 1/n \\ \vdots \\ 1/n \end{pmatrix}, \quad w = \begin{pmatrix} |x_1| \\ \vdots \\ |x_n| \end{pmatrix}. \quad (6.308)$$

Nous trouvons

$$\frac{1}{n} \sum_i |x_i| \leq \sqrt{b \cdot \frac{1}{n}} \sqrt{\sum_i |x_i|^2}, \quad (6.309)$$

et par conséquent

$$\sum_i |x_i| \leq \sqrt{n}\|x\|_2. \quad (6.310)$$

La première inégalité de (3) se démontre en remarquant que si a et b sont positifs, $a \leq \sqrt{a^2 + b}$. En appliquant cela à $a = \max_i |x_i|$, nous avons

$$\max_i |x_i| \leq \sqrt{|x_1|^2 + \dots + |x_n|^2} \quad (6.311)$$

parce que $\max_i |x_i|$ est évidemment un des termes de la somme. Pour la seconde inégalité de (3), nous avons

$$\sqrt{\sum_k |x_k|^2} \leq \left(\sum_k \max_i |x_i|^2 \right)^{1/2} = \sqrt{n}\|x\|_\infty. \quad (6.312)$$

Pour obtenir cette inégalité, nous avons remplacé tous les termes $|x_k|$ par le maximum. $\square$

En réalité, toutes les normes $\|\cdot\|_{L^p}$ et $\|\cdot\|_\infty$ sont équivalentes et, plus généralement, nous avons le résultat suivant, très étonnant à première vue, et en réalité assez difficile à prouver :

Théorème 6.139 ([85]).

Sur un espace vectoriel de dimension finie, toutes les normes (pas seulement les normes L^p que nous avons définies sur $\mathbb{R}^m$) sont équivalentes.

Corollaire 6.140.

Soit V un espace vectoriel de dimension finie et $\|\cdot\|_1, \|\cdot\|_2$ deux normes sur V . Alors l'identité $\text{Id}: V \rightarrow V$ est un isomorphisme d'espace topologique $(V, \|\cdot\|_1) \rightarrow (V, \|\cdot\|_2)$.

De plus les ouverts sont les mêmes : une partie de V est ouverte dans $(V, \|\cdot\|_1)$ si et seulement si elle est ouverte dans $(V, \|\cdot\|_2)$.

Le théorème d'équivalence de norme sera utilisé pour montrer que l'ensemble des formes quadratiques non dégénérées de signature (p, q) est ouvert dans l'ensemble des formes quadratiques, proposition 16.155. Plus généralement il est utilisé à chaque fois que l'on fait de la topologie sur les espaces de matrices en identifiant $\mathbb{M}(n, \mathbb{R})$ à $\mathbb{R}^{n^2}$, pour se rassurer en se disant que ce qu'on fait ne dépend pas de la norme choisie.

6.12.2 Contre-exemple en dimension infinie

Lorsque nous considérons des espaces vectoriels de dimension infinie, les choses ne sont plus aussi simples. Nous voyons ici sur l'exemple de l'espace des polynômes que le théorème 6.139 n'est plus valable si on enlève l'hypothèse de dimension finie.

On considère l'ensemble des fonctions polynômiales à coefficients réels sur l'intervalle $[0, 1]$.

$$\mathcal{P}_{\mathbb{R}}([0, 1]) = \{p : [0, 1] \rightarrow \mathbb{R} \mid p : x \mapsto a_0 + a_1x + a_2x^2 + \dots, a_i \in \mathbb{R}, \forall i \in \mathbb{N}\}. \quad (6.313)$$

Cet ensemble, muni des opérations usuelles de somme entre polynômes et multiplications par les scalaires, est un espace vectoriel.

Sur $\mathcal{P}(\mathbb{R})$ on définit les normes suivantes

$$\begin{aligned} \|p\|_{\infty} &= \sup_{x \in [0, 1]} \{p(x)\}, \\ \|p\|_1 &= \int_0^1 |p(x)| dx, \\ \|p\|_2 &= \left(\int_0^1 |p(x)|^2 dx \right)^{1/2}. \end{aligned} \quad (6.314)$$

Les inégalités suivantes sont immédiates

$$\begin{aligned} \|p\|_1 &= \int_0^1 |p(x)| dx \leq \|p\|_{\infty}, \\ \|p\|_2 &= \left(\int_0^1 |p(x)|^2 dx \right)^{1/2} \leq \|p\|_{\infty}, \end{aligned} \quad (6.315)$$

mais la norme $\|\cdot\|_{\infty}$ n'est équivalente ni à $\|\cdot\|_1$, ni à $\|\cdot\|_2$. Soit $p_k(x) = x^k$. Alors

$$\begin{aligned} \|p_k\|_{\infty} &= 1, \\ \|p_k\|_1 &= \int_0^1 x^k dx = \frac{1}{k+1}, \\ \|p_k\|_2 &= \left(\int_0^1 x^{2k} dx \right)^{1/2} = \sqrt{\frac{1}{2k+1}}. \end{aligned} \quad (6.316)$$

Pour $k \rightarrow \infty$ les normes $\|p_k\|_1, \|p_k\|_2$ tendent vers zéro, alors que la norme $\|p_k\|_{\infty}$ est constante, donc les normes ne sont pas équivalentes parce que il n'existe pas un nombre positif m tel que

$$\begin{aligned} m\|p_k\|_{\infty} &\leq \|p_k\|_1, \\ m\|p_k\|_{\infty} &\leq \|p_k\|_2, \end{aligned} \quad (6.317)$$

uniformément pour tout k dans $\mathbb{N}$.

6.13 Suites

6.13.1 Limites, convergence

Nous disons qu'une suite réelle (x_n) converge¹⁸ vers ℓ lorsque pour tout ε , il existe un M tel que

$$n > N \Rightarrow |x_n - \ell| \leq \varepsilon. \quad (6.318)$$

Le concept fondamental de cette définition est la notion de valeur absolue qui permet de donner la «distance» entre deux réels. Dans un espace vectoriel normé quelconque, cette notion est généralisée par la distance associée à la norme (définition 5.33). Nous pouvons donc facilement définir le concept de convergence d'une suite dans un espace vectoriel normé.

Définition 6.141.

Soit une suite (x_n) dans un espace vectoriel normé V . Nous disons qu'elle est **convergente** si il existe un élément $\ell \in V$ tel que

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ tel que } n \geq N \Rightarrow \|x_n - \ell\| < \varepsilon. \quad (6.319)$$

Dans ce cas, ℓ est appelé la **limite** de la suite (x_n) .

Lemme 6.142.

Soit (x_n) une suite convergente contenue dans un ensemble $A \subset V$. Alors la limite x_n appartient à $\bar{A}$.

Démonstration. Supposons que nous ayons une partie A de V , et une suite (x_n) dont la limite ℓ se trouve hors de $\bar{A}$. Dans ce cas, il existe un $r > 0$ tel que¹⁹ $B(\ell, r) \cap A = \emptyset$. Si tous les éléments x_n de la suite sont dans A , il n'y en a donc aucun tel que $d(x_n, \ell) = \|x_n - \ell\| < r$. Cela contredit la notion de convergence $x_n \rightarrow \ell$. $\square$

Nous avons déjà mentionné dans l'exemple 6.118 que zéro était un point adhérent à l'ensemble $F = \{(-1)^n/n \text{ tel que } n \in \mathbb{N}_0\}$. Nous savons maintenant que 0 étant la limite de la suite, il est automatiquement adhérent à l'ensemble des éléments de la suite.

Corollaire 6.143.

Soit a un point de l'adhérence d'une partie A de V . Alors il existe une suite d'éléments dans A qui converge vers a .

Démonstration. Si $a \in A$, alors nous pouvons prendre la suite constante $x_n = a$. Si a n'est pas dans A , alors a est dans ∂A , et pour tout n , il existe un point de A dans la boule $B(a, \frac{1}{n})$. Si nous nommons x_n ce point, la suite ainsi construite est une suite contenue dans A et qui converge vers a (ce dernier point est laissé à la sagacité du lecteur ou de la lectrice). $\square$

En termes savants, ce corollaire signifie que la fermeture $\bar{A}$ est composé de A plus de toutes les limites de toutes les suites contenues dans A .

6.13.2 Critère de Cauchy

Définition 6.144.

Une suite (a_k) dans l'espace vectoriel normé V est **de Cauchy** si pour tout ϵ , il existe N tel que si $n, m \geq N$ alors $\|a_n - a_m\| \leq \epsilon$.

Lemme 6.145.

Une suite de Cauchy dans un espace vectoriel normé admettant une sous-suite convergente est elle-même convergente vers la même limite.

18. Voir la définition 5.73 pour plus de détail.

19. Une autre manière de dire la même chose : si $\ell \notin \bar{A}$, alors $d(\ell, A) > 0$.

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 $m, p \geq N$. Nous allons montrer que si $k > N$ alors $\|a_k - \ell\| < 2\epsilon$. Pour cela nous considérons un $n > N$ tel que $\|a_n - \ell\| \leq \epsilon$ et nous calculons

$$\|a_k - \ell\| \leq \|a_k - a_n\| + \|a_n - \ell\| \leq 2\epsilon. \quad (6.320)$$

□

Théorème 6.146 (Critère de Cauchy).

Une suite réelle est convergente si et seulement si elle est de Cauchy. En particulier $\mathbb{R}$ est un espace complet.

Démonstration. Soit (a_n) une suite de Cauchy dans $\mathbb{R}$.

□

Définition 6.147.

*Nous disons que deux suites (u_n) et (v_n) sont **équivalentes** si il existe une fonction $\alpha: \mathbb{N} \rightarrow \mathbb{R}$ telle que*

$$(1) \text{ pour tout } n \text{ à partir d'un certain rang, } u_n = v_n \alpha(n)$$

$$(2) \alpha(n) \rightarrow 1.$$

Lemme 6.148.

Si les suites (u_n) et (v_n) sont équivalentes et si (v_n) admet une limite l différente de 1, alors les suites $(\ln u_n)$ et $(\ln v_n)$ sont équivalentes.

Démonstration. En effet si $u_n = v_n \alpha(n)$ alors

$$\ln(u_n) = \ln(v_n) + \ln(\alpha(n)) = \ln(v_n) \left(1 + \frac{\ln(\alpha(n))}{\ln(v_n)}\right), \quad (6.321)$$

et comme $\alpha(n) \rightarrow 1$, la parenthèse tend vers 1.

□

Lemme 6.149 (formule de Stirling[86]).

Nous avons l'équivalence de suites

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}. \quad (6.322)$$

6.14 Séries

Définition 6.150.

*Soit (a_k) une suite dans un espace vectoriel normé $(V, \|\cdot\|)$. La **série** associée, notée $\sum_{k=0}^{\infty} a_k$ est la limite des **sommes partielles**, c'est à dire la limite de la suite*

$$s_k = \sum_{i=0}^k a_i \quad (6.323)$$

si elle existe dans V .

*Si une telle limite existe nous disons que $\sum_{k=0}^{\infty} a_k$ **converge** dans V . Si la limite de la suite des sommes partielles n'existe pas nous disons que la série **diverge**.*

Remarque 6.151.

Si la limite de la suite des sommes partielles n'existe pas dans V , alors elle peut parfois exister dans des extensions de V . Par exemple une série de rationnels convergeant vers $\sqrt{2}$ dans $\mathbb{R}$ ne converge pas dans $\mathbb{Q}$. Autre exemple : avec une bonne topologie sur $\bar{\mathbb{R}}$, une série peut ne pas converger dans $\mathbb{R}$ mais converger vers $\pm\infty$ dans $\bar{\mathbb{R}}$.

Dans le cas des espaces de fonctions, nous avons une norme importante : la norme uniforme définie par $\|f\|_{\infty} = \sup\{f(x)\}$ où le supremum est pris sur l'ensemble de définition de f .

Définition 6.152 (Convergence absolue).

Nous disons que la série $\sum_{n=0}^{\infty} a_n$ dans l'espace vectoriel normé V **converge absolument** si la série $\sum_{n=0}^{\infty} \|a_n\|$ converge dans $\mathbb{R}$.

Dans le cas de l'espace des fonctions muni de la norme uniforme, nous parlons de convergence normale.

Définition 6.153 (Convergence normale).

Une série de fonctions $\sum_{n \in \mathbb{N}} u_n$ converge **normalement** si la série de nombres $\sum_n \|u_n\|_{\infty}$ converge. C'est à dire si la série converge absolument pour la norme $\|f\|_{\infty}$.

Cela n'est rien d'autre que la convergence absolue dans l'espace des fonctions muni de la norme uniforme.

La convergence normale est à ne pas confondre avec la convergence uniforme. La somme $\sum_n f_n$ **converge uniformément** vers la fonction F si la suite des sommes partielles converge uniformément, c'est à dire si

$$\lim_{N \rightarrow \infty} \left\| \sum_{n=1}^N f_n - F \right\|_{\infty} = 0. \quad (6.324)$$

Proposition 6.154.

Une série convergeant absolument dans un espace de Banach²⁰ y converge au sens usuel.

Démonstration. Soit (a_k) une suite dans un espace vectoriel normé complet dont la série converge absolument. Nous allons montrer que la suite des sommes partielles est de Cauchy. Cela suffira à montrer sa convergence par hypothèse de complétude.

Nous avons

$$\|s_p - s_l\| = \left\| \sum_{k=l+1}^p a_k \right\| \leq \sum_{k=l+1}^p \|a_k\| = \bar{s}_p - \bar{s}_l \quad (6.325)$$

où $\bar{s}_n = \sum_{k=0}^n \|a_k\|$ est la suite des sommes partielles de la série des normes (qui converge). Vu que la suite $(\bar{s}_n)$ converge dans $\mathbb{R}$, elle y est de Cauchy par le théorème 6.146. Donc il existe un N tel que $p, l > N$ implique

$$\|s_p - s_l\| = \bar{s}_p - \bar{s}_l \leq \epsilon. \quad (6.326)$$

Cela signifie que (s_n) est une suite de Cauchy et donc convergente. $\square$

Remarque 6.155.

Nous savons que sur les espaces vectoriels de dimension finie toutes les normes sont équivalentes (théorème 6.137). La notion de convergence de série ne dépend alors pas du choix de la norme. Il n'en est pas de même sur les espaces de dimension infinie. Une série peut converger pour une norme mais pas pour une autre.

Lorsque nous verrons la convergence de séries, nous verrons que la convergence normale est la convergence absolue pour la norme uniforme.

Lemme 6.156.

Si E et F sont des espaces de Banach²¹, l'espace $\mathcal{L}(E, F)$ est également de Banach.

Démonstration. Soit (u_n) une suite de Cauchy dans $\mathcal{L}(E, F)$; si $x \in E$ il existe N tel que si $l, m > N$ alors $\|u_l - u_m\| < \epsilon$, c'est à dire que pour tout $\|x\| = 1$ on a $\|u_l(x) - u_m(x)\| < \epsilon$. Cela signifie que $u_n(x)$ est une suite de Cauchy dans l'espace complet F . Cette suite converge et nous pouvons définir l'application $u: E \rightarrow F$ par

$$u(x) = \lim_{n \rightarrow \infty} u_n(x). \quad (6.327)$$

20. Un espace vectoriel normé complet. Typiquement $\mathbb{R}$.

21. Je crois qu'il ne faut pas que E soit complet.

Il suffit maintenant de prouver que u est linéaire, ce qui est une conséquence directe de la linéarité de la limite :

$$u(\alpha x + \beta y) = \lim_{n \rightarrow \infty} (\alpha u_n(x) + \beta u_n(y)). \quad (6.328)$$

□

Le lemme 16.40 donne une version plus simple de la proposition suivante.

Proposition 6.157.

Soit E un espace de Banach (espace vectoriel normé complet). Si $A \in \mathcal{L}(E, E)$ avec $\|A\| < 1$ pour la norme opérateur, alors $(\mathbb{1} - A)$ est inversible et son inverse est donné par

$$(\mathbb{1} - A)^{-1} = \sum_{k=0}^{\infty} A^k. \quad (6.329)$$

Le résultat tient aussi si A est nilpotente, même si sa norme n'est pas majorée par 1.

Démonstration. Étant donné que la norme opérateur est une norme algébrique (proposition 6.88), nous avons $\|A^k\| \leq \|A\|^k$. Par conséquent la série $\|A^k\|$ est majorée par la série géométrique qui converge. Par conséquent $\sum_k A^k$ est une série absolument convergente et donc convergente par la proposition 6.154 et le fait que $\mathcal{L}(E)$ est complet (proposition 6.156).

Montrons à présent que la somme est l'inverse de $\mathbb{1} - A$ en utilisant le produit terme à terme autorisé par la proposition 6.90 :

$$\sum_{k=0}^n A^k (\mathbb{1} - A) = \sum_{k=0}^n (A^k - A^{k+1}) = \mathbb{1} - A^{n+1}. \quad (6.330)$$

Par conséquent

$$\|\mathbb{1} - \sum_{k=0}^n A^k (\mathbb{1} - A)\| = \|A^{n+1}\| \leq \|A\|^{n+1} \rightarrow 0. \quad (6.331)$$

Si A est nilpotente, la convergence de $\sum_{k=0}^{\infty} A^k$ ne pose pas de problèmes parce que la somme est finie. Le fait que cette somme soit $(\mathbb{1} - A)^{-1}$ s'obtient de la même façon, mais il ne faut pas faire la dernière majoration : si A est nilpotente, il tombe sous le sens que $\|A^{n+1}\| \rightarrow 0$, mais il n'est cependant pas vrai que $\|A\|^{n+1}$ tende vers zéro. □

Proposition 6.158.

Les principales propriétés de la somme définie par la limite (6.150) sont

- (1) Si une série converge absolument, alors elle converge simplement.
- (2) Si la série est à termes positifs – c'est-à-dire pour tout indice k , $a_k \in \mathbb{R}$ et $a_k \geq 0$ – il n'y a aucune différence entre convergence absolue et convergence simple.
- (3) Si une série converge, son terme général doit tendre vers 0.
- (4) Si la série converge alors la somme est associative
- (5) Si la série converge absolument, alors la somme est commutative.

Démonstration. (1)

(2)

(3)

(4)

- (5) Associativité. Supposons que $\sum_k a_k$ et $\sum_k b_k$ convergent tous deux. Alors nous avons pour tout N :

$$\sum_{k=0}^N (a_k + b_k) = \sum_{k=0}^N a_k + \sum_{k=0}^N b_k. \quad (6.332)$$

Mais si deux limites existent alors la somme commute avec la limite. C'est le cas pour la limite $N \rightarrow \infty$, donc

$$\lim_{N \rightarrow \infty} \sum_{k=1}^{\infty} (a_k + b_k) = \lim_{N \rightarrow \infty} \sum_{k=0}^{\infty} a_k + \lim_{N \rightarrow \infty} \sum_{k=0}^{\infty} b_k. \quad (6.333)$$

(6)

□

6.15 Série réelle

La notion de série formalise le concept de somme infinie. L'absence de certaines propriétés de ces objets (problèmes de commutativité et même d'associativité) incitent à la prudence et montrent à quel point une définition précise est importante.

6.15.1 Rappels et définitions

Nous avons déjà vu de nombreuses choses sur les séries.

- (1) La définition de la somme d'une infinité de termes est donnée par la définition 6.150.
- (2) La définition de la convergence absolue est la définition 6.152.
- (3) Les propriétés générales de la proposition 6.158.

Remarque 6.159.

Vue comme somme infinie, l'associativité et la commutativité dans une série sont perdues. Néanmoins, il subsiste que

- (1) si la série converge, on peut regrouper ses termes sans modifier la convergence ni la somme (associativité),
- (2) si la série converge absolument, on peut modifier l'ordre des termes sans modifier la convergence ni la somme (commutativité).

6.15.2 Critères de convergence absolue

Étant donné le terme général d'une série, il est souvent –dans les cas qui nous intéressent– difficile de déterminer la somme de la série. L'exemple de la série géométrique est particulier, puisqu'on connaît une formule pour chaque somme partielle, mais pour l'exemple des séries de Riemann il n'y a aucune formule simple pour un α général. D'où l'intérêt d'avoir des critères de convergence ne nécessitant aucune connaissance de l'éventuelle limite de la série.

Lemme 6.160 (Critère de comparaison).

Soient $\sum_i a_i$ et $\sum_j b_j$ deux séries à termes positifs vérifiant

$$0 \leq a_i \leq b_i$$

alors

- (1) si $\sum_i a_i$ diverge, alors $\sum_j b_j$ diverge,
- (2) si $\sum_j b_j$ converge, alors $\sum_i a_i$ converge (absolument).

Proposition 6.161 (Critère d'équivalence[85]).

Soient $\sum_i a_i$ et $\sum_j b_j$ deux séries à termes positifs. Supposons l'existence de la limite (éventuellement infinie) suivante

$$\lim_{i \rightarrow \infty} \frac{a_i}{b_i} = \alpha \in \mathbb{R} \text{ ou } \alpha = \infty. \quad (6.334)$$

Dans ce cas, nous avons

(1) si $\alpha \neq 0$ et $\alpha \neq \infty$, alors

$$\sum_i a_i \text{ converge} \iff \sum_j b_j \text{ converge}, \quad (6.335)$$

(2) si $\alpha = 0$ et $\sum_j b_j$ converge, alors $\sum_i a_i$ converge (absolument),

(3) si $\alpha = +\infty$ et $\sum_j b_j$ diverge, alors $\sum_i a_i$ diverge.

Démonstration. (1) Le fait que la suite a_n/b_n converge vers α signifie que tant sa limite supérieure que sa limite inférieure convergent vers α . En particulier la suite $\frac{a_n}{b_n}$ est bornée vers le haut et vers le bas. À partir d'un certain rang N , il existe M tel que

$$\frac{a_n}{b_n} < M \quad (6.336)$$

et il existe m tel que

$$\frac{a_n}{b_n} > m. \quad (6.337)$$

Nous avons donc $a_n < Mb_n$ et $a_n > mb_n$. La série de (a_n) converge donc si et seulement si la série de (b_n) converge.

(2) Si $\alpha = 0$, cela signifie que pour tout ϵ , il existe un rang tel que $\frac{a_n}{b_n} < \epsilon$, et donc tel que $a_n < \epsilon b_n$. La suite de (a_i) converge donc dès que la suite de (b_i) converge.

(3) Pour tout M , il existe un rang dans la suite à partir duquel on a $\frac{a_i}{b_i} > M$, et donc $a_k > Mb_k$. Si la série de (b_k) diverge, la série de (a_k) doit également diverger. $\square$

Proposition 6.162 (Critère du quotient[87]).

Soit $\sum_i a_i$ une série. Supposons l'existence de la limite (éventuellement infinie) suivante

$$\lim_{i \rightarrow \infty} \left| \frac{a_{i+1}}{a_i} \right| = L \in \mathbb{R} \text{ ou } L = \infty. \quad (6.338)$$

Alors

(1) si $L < 1$, la série converge absolument,

(2) si $L > 1$, la série diverge,

(3) si $L = 1$ le critère échoue : il existe des exemples de convergence et des exemples de divergence.

Démonstration. (1) Soit b tel que $L < b < 1$. À partir d'un certain rang K , on a $\left| \frac{a_{i+1}}{a_i} \right| < b$. En particulier,

$$|a_{K+1}| < b|a_K|, \quad (6.339)$$

et pour a_{K+2} nous avons

$$|a_{K+2}| < b|a_{K+1}| < b^2|a_K|. \quad (6.340)$$

Au final,

$$|a_{K+n}| < b^n|a_K|. \quad (6.341)$$

Étant donné que la série $\sum_{n \geq K} b^n$ converge (parce que $b < 1$), la queue de suite $\sum_{i \geq K} a_i$ converge, et par conséquent la suite au complet converge.

(2) Si $L > 1$, on a

$$|a_K| < |a_{K+1}| < |a_{K+2}| < \dots \quad (6.342)$$

Il est donc impossible que la suite (a_i) converge vers zéro. La série ne peut donc pas converger.

- (3) Par exemple la suite harmonique $a_n = \frac{1}{n}$ vérifie $L = 1$, mais la série ne converge pas. Par contre, la suite $a_n = \frac{1}{n^2}$ vérifie aussi le critère avec $L = 1$ tandis que la série $\sum_n \frac{1}{n^2}$ converge. $\square$

Proposition 6.163 (Critère de la racine[85]).

Soit $\sum_i a_i$ une série, et considérons

$$\limsup_{i \rightarrow \infty} \sqrt[i]{|a_i|} = L \in \mathbb{R} \text{ ou } L = \infty.$$

Alors

- (1) si $L < 1$, la série converge absolument,
- (2) si $L > 1$, la série diverge,
- (3) si $L = 1$ le critère échoue.

Démonstration. (1) Si $L < 1$, il existe un $r \in]0, 1[$ tel que $|a_n|^{1/n} < r$ pour les grands n . Dans ce cas, $|a_n| < r^n$, et la série converge absolument parce que la série $\sum_n r^n$ converge du fait que $r < 1$.

- (2) Si $L > 1$, il existe un $r > 1$ tel que $|a_n|^{1/n} > r > 1$. Cela fait que $|a_n|$ prend des valeurs plus grandes que n pour une infinité de termes. Le terme général a_n ne peut donc pas être une suite convergente. Par conséquent la suite diverge au sens où elle ne converge pas. $\square$

6.15.3 Critères de convergence simple

Les critères de comparaison, d'équivalence, du quotient et de la racine sont des critères de convergence absolue. Pour conclure à une convergence simple qui n'est pas une convergence absolue, le critère d'Abel sera notre outil principal.

6.15.3.1 Critère d'Abel

Proposition 6.164 (Critère d'Abel).

Soit la série $\sum_i c_i z_i$ avec

- (1) (c_i) est une suite réelle décroissante qui tend vers zéro,
- (2) (z_i) est une suite dans $\mathbb{C}$ dont la suite des sommes partielles est bornée dans $\mathbb{C}$, c'est à dire qu'il existe un $M > 0$ tel que pour tout n ,

$$\left| \sum_{i=1}^n z_i \right| \leq M. \quad (6.343)$$

Alors la série $\sum_i c_i z_i$ est convergente.

Remarquons que ce critère ne donne pas de convergence absolue.

Corollaire 6.165 (Critère des séries alternées).

Si (a_n) est une suite décroissante à limite nulle, alors la série

$$\sum_{n=0}^{\infty} (-1)^n a_n \quad (6.344)$$

converge simplement.

6.15.4 Quelques séries usuelles

Exemple 6.166(Série harmonique)

La **série harmonique** est

$$\sum_{i=1}^{\infty} \frac{1}{i} \quad (6.345)$$

et diverge (possède une limite $+\infty$). $\triangle$

Exemple 6.167(Série géométrique)

La **série géométrique** de raison $q \in \mathbb{C}$ est

$$\sum_{i=0}^{\infty} q^i. \quad (6.346)$$

Étudions la somme partielle $S_N = 1 + q + q^2 + \dots + q^N$. Nous avons évidemment $S_N - qS_N = 1 - q^{N+1}$ et donc

$$S_N = \sum_{n=0}^N q^n = \frac{1 - q^{N+1}}{1 - q}. \quad (6.347)$$

La limite $\lim_{N \rightarrow \infty} S_N$ existe si et seulement si $|q| \leq 1$ et dans ce cas nous avons

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1 - q}. \quad (6.348)$$

La convergence est absolue.

Si la somme commence en $n = 1$ au lieu de $n = 0$ alors

$$\sum_{n=1}^{\infty} q^n = \frac{1}{1 - q} - 1 = \frac{q}{1 - q}. \quad (6.349)$$

$\triangle$

Un cas particulier de la formule (6.347) est le calcul de $\sum_{j=1}^N q^{-j}$ bien utile lorsque l'on joue avec des nombres binaires (voir l'exemple 25.12). Nous avons

$$\sum_{j=1}^N q^{-j} = \sum_{j=0}^N q^{-j} - 1 = \frac{1 - q^{-N}}{q - 1}. \quad (6.350)$$

Exemple 6.168(Série de Riemann)

Pour $\alpha \in \mathbb{R}$, la **série de Riemann**

$$\sum_{i=1}^{\infty} \frac{1}{i^\alpha} \quad (6.351)$$

converge (absolument, puisque réelle et positive) si et seulement si $\alpha > 1$, et diverge sinon. $\triangle$

Exemple 6.169(Série exponentielle)

La série exponentielle est la série (pour $t \in \mathbb{R}$)

$$\exp(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!}. \quad (6.352)$$

Nous montrons qu'elle converge pour tout $t \in \mathbb{R}$. Si $a_k = t^k/k!$ alors $\frac{a_{k+1}}{a_k} = \frac{t}{k+1}$ dont la limite $k \rightarrow \infty$ est zéro (quel que soit t). En vertu du critère du quotient 6.162 la série exponentielle converge (absolument) pour tout $t \in \mathbb{R}$.

Toutes les propriétés de la fonction de t ainsi définie sont dans le théorème 16.49. $\triangle$

Exemple 6.170(Série arithmético-géométrique[88])

La **suite arithmético-géométrique** est une suite de la forme $u_{n+1} = au_n + b$ avec a et b non nuls. Si elle possède une limite, cette dernière doit résoudre $l = al + b$, et donc être égale à

$$r = \frac{b}{1-a}. \quad (6.353)$$

Il n'est pas très compliqué de trouver le terme général de la suite en fonction de a et de b . Il suffit de considérer la suite $v_n = u_n - r$, et de remarquer que cette suite est géométrique :

$$v_{n+1} = av_n. \quad (6.354)$$

Par conséquent $v_n = a^n v_0$, ce qui donne pour la suite (u_n) la formule

$$u_n = a^n(u_0 - r) + r. \quad (6.355)$$

$\triangle$

6.15.5 Moyenne de Cesaro

Si $(a_n)_{n \in \mathbb{N}}$ est une suite dans $\mathbb{R}$ ou $\mathbb{C}$, alors sa **moyenne de Cesaro** est la limite (si elle existe) de la suite

$$c_n = \frac{1}{n} \sum_{k=1}^n a_k. \quad (6.356)$$

En un mot, c'est la limite des moyennes partielles.

Lemme 6.171.

Si la suite (a_n) converge vers la limite ℓ alors la suite admet une moyenne de Cesaro qui vaudra ℓ .

Démonstration. Soit $\epsilon > 0$ et $N \in \mathbb{N}$ tel que $|a_n - \ell| < \epsilon$ pour tout $n > N$. En remarquant que

$$\frac{1}{n} \sum_{k=1}^n a_k - \ell = \frac{1}{n} \sum_{k=1}^n (a_k - \ell), \quad (6.357)$$

nous avons

$$\left| \frac{1}{n} \sum_{k=1}^n a_k - \ell \right| \leq \left| \frac{1}{n} \sum_{k=1}^N (a_k - \ell) \right| + \left| \frac{1}{n} \sum_{k=N+1}^n \underbrace{(a_k - \ell)}_{\leq \epsilon} \right| \quad (6.358a)$$

$$\leq \epsilon + \frac{n - N - 1}{n} \epsilon \quad (6.358b)$$

$$\leq 2\epsilon. \quad (6.358c)$$

Dans ce calcul nous avons redéfini N de telle sorte que le premier terme soit inférieur à ϵ . $\square$

6.15.6 Écriture décimale d'un nombre

Soit $b \geq 2$ un entier qui sera la base dans laquelle nous allons écrire les nombres. Nous considérons l'ensemble $\mathbb{D}_b$ des suites dans $\{0, 1, \dots, b-1\}$ qui n'ont pas une queue de suite uniquement formée de $b-1$. Autrement dit une suite (c_n) est dans $\mathbb{D}_b$ lorsque pour tout N , il existe $k > N$ tel que $c_k \neq b-1$. Associé à cet ensemble nous considérons la fonction

$$\begin{aligned} \varphi_b: \mathbb{D}_b &\rightarrow [0, 1[\\ c &\mapsto \sum_{n=1}^{\infty} \frac{c_n}{b^n}. \end{aligned} \quad (6.359)$$

Lemme 6.172.

La fonction φ_b est bien définie au sens où elle converge et prend ses valeurs dans $[0, 1[$.

Démonstration. Tout se base sur la somme de la série géométrique (6.348) sous la forme

$$\sum_{k=0}^{\infty} \frac{1}{b^k} = \frac{b}{b-1}. \quad (6.360)$$

La somme (6.359) est donc majorée par $\sum_n \frac{b-1}{b^n}$ qui converge.

Pour prouver que l'image de φ_b est bien $[0, 1[$, nous savons qu'au moins un des c_n (en fait une infinité) est plus petit que $b-1$, donc nous avons la majoration stricte²²

$$\varphi_b(c) < \sum_{n=1}^{\infty} \frac{b-1}{b^n} = (b-1) \left(\sum_{n=1}^{\infty} \frac{1}{b^n} - 1 \right) = 1 \quad (6.361)$$

□

Le fait d'introduire l'ensemble $\mathbb{D}$ au lieu de l'ensemble de toutes les suites est justifié par la proposition suivante. Elle explique pourquoi un nombre possède au maximum deux écritures décimales distinctes et que ces deux sont obligatoirement de la forme, par exemple en base 10 :

$$0.34599999999 \dots = 0.34600000 \dots \quad (6.362)$$

mais qu'un nombre commençant par 0.347 ne peut pas être égal. C'est pour cela que dans la définition de $\mathbb{D}_b$ nous avons exclu les suites qui terminent par tout des $b-1$.

Proposition 6.173.

Soit la fonction

$$\begin{aligned} \varphi: \{0, \dots, b-1\}^{\mathbb{N}} &\rightarrow [0, 1[\\ x &\mapsto \sum_{n=1}^{\infty} \frac{x_n}{b^n}. \end{aligned} \quad (6.363)$$

Si $\varphi(x) = \varphi(y)$ et si n_0 est le plus petit entier tel que $x_{n_0} \neq y_{n_0}$ alors soit

$$x_{n_0} - y_{n_0} = 1 \quad (6.364)$$

et $x_n = 0, y_n = b-1$ pour tout $n > n_0$, soit le contraire : $y_{n_0} - x_{n_0} = 1$ avec $y_n = 0$ et $x_n = b-1$ pour tout $n > n_0$.

Démonstration. Nous nous basons sur la formule (facilement dérivable depuis (6.360)) suivante :

$$\sum_{k=n_0+1}^{\infty} \frac{1}{b^k} = \frac{1}{b^{n_0+1}} \frac{b}{b-1}. \quad (6.365)$$

Nous avons

$$0 = \varphi(x) - \varphi(y) = \frac{x_{n_0} - y_{n_0}}{b^{n_0}} + \sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n} \geq \frac{x_{n_0} - y_{n_0}}{b^{n_0}} - \sum_{n=n_0+1}^{\infty} \frac{b-1}{b^n} = \frac{x_{n_0} - y_{n_0} - 1}{b^{n_0}}. \quad (6.366)$$

Le dernier terme étant manifestement positif²³, il est nul et nous avons $x_{n_0} - y_{n_0} = 1$.

Nous avons donc maintenant

$$0 = \varphi(x) - \varphi(y) = \frac{1}{b^{n_0}} + \sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n}. \quad (6.367)$$

22. Notez que la somme (6.359) commence à un tandis que la série géométrique (6.360) commence à zéro.

23. C'est ici qu'intervient la subdivision entre le cas $x_{n_0} - y_{n_0} = 1$ ou le contraire. En effet si «ce dernier terme était manifestement négatif», il aurait fallu majorer avec de $1-b$ au lieu de $1-1$.

Nous majorons la dernière somme de la façon suivante, en supposant que $|x_n - y_n| \neq b - 1$ pour un certain $n > n_0$:

$$\left| \sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n} \right| \leq \sum_{n=n_0+1}^{\infty} \frac{|x_n - y_n|}{b^n} < \sum_{n=n_0+1}^{\infty} \frac{b-1}{b^n} = \frac{1}{b^{n_0}}. \quad (6.368)$$

Étant donné cette inégalité stricte, l'équation (6.367) ne peut pas être correcte (valoir zéro). Nous avons donc $|x_n - b_n| = b - 1$ pour tout $n > n_0$. Donc pour chaque $n > n_0$ nous avons soit $x_n = 0$ et $y_n = b - 1$, soit $a_n = b - 1$ et $b_n = 0$. Pour conclure il faut encore prouver que le choix doit être le même pour tout n .

Nous nous mettons dans le cas $x_{n_0} - y_{n_0} = 1$; dans ce cas nous avons bien l'égalité (6.367) sans petites nuances de signes. Nous écrivons

$$\sum_{n=n_0+1}^{\infty} \frac{x_n - y_n}{b^n} = (b-1) \sum_{n=n_0+1}^{\infty} \frac{(-1)^{s_n}}{b^n} \quad (6.369)$$

où s_n est pair ou impair suivant que $x_n = 0$, $y_n = b - 1$ ou le contraire. Si un des $(-1)^{s_n}$ est pas -1 alors nous avons l'inégalité stricte

$$(b-1) \sum_{n=n_0+1}^{\infty} \frac{(-1)^{s_n}}{b^n} > (b-1) \sum_{n=n_0+1}^{\infty} \frac{-1}{b^n} = -\frac{1}{b^{n_0}}. \quad (6.370)$$

Dans ce cas il est impossible d'avoir $\varphi(x) - \varphi(y) = 0$. Nous en concluons que $(-1)^{s_n}$ est toujours -1 , c'est à dire $x_n - y_n = 1 - b$, ce qui laisse comme seule possibilité $x_n = 0$ et $y_n = b - 1$. $\square$

Théorème 6.174.

L'application $\varphi_b: \mathbb{D}_b \rightarrow [0, 1[$ est bijective.

Démonstration. En ce qui concerne l'injection, nous savons de la proposition 6.173 que si $\varphi_b(x) = \varphi_b(y)$ pour $x, y \in \{0, \dots, b-1\}^{\mathbb{N}}$, alors soit x soit y a une queue de suite composée uniquement de $b-1$, ce qui est exclu dans $\mathbb{D}_b$. Nous en déduisons que φ_b est bien injective en prenant $\mathbb{D}_b$ comme ensemble départ.

La partie lourde est la surjectivité. Nous prenons $x \in [0, 1[$ et nous allons construire par récurrence une suite $a \in \mathbb{D}_b$ telle que $\varphi_b(a) = x$. Si il existe $a_1 \in \{0, \dots, b-1\}$ tel que $x = a_1/b$ alors nous prenons la suite $(a_1, 0, \dots)$ et nous avons évidemment $\varphi(a) = x$. Sinon il existe $a_1 \in \{0, \dots, b-1\}$ tel que

$$\frac{a_1}{b} < x < \frac{a_1 + 1}{b} \quad (6.371)$$

parce que les autres possibilités pour x sont dans l'ensemble $[0, 1[\setminus \{\frac{k}{b}\}_{k=0, \dots, b-1}$ que nous subdivisons en

$$]0, \frac{1}{b}[\cup]\frac{1}{b}, \frac{2}{b}[\cup \dots \cup]\frac{b-1}{b}, 1[. \quad (6.372)$$

Pour la récurrence nous supposons avoir trouvé $a_1, \dots, a_n$ tels que

$$\sum_{k=1}^n \frac{a_k}{b^k} < x < \sum_{k=1}^{n-1} \frac{a_k}{b^k} + \frac{a_n + 1}{b^n}. \quad (6.373)$$

Encore une fois si il existe $a_{n+1} \in \{0, \dots, b-1\}$ tel que $\sum_{k=1}^{n+1} \frac{a_k}{b^k} = x$ alors nous prenons ce a_{n+1} et nous complétons la suite avec des zéros pour avoir $\varphi(a) = x$. Sinon, pour simplifier les notations nous notons $x' = x - \sum_{k=1}^n \frac{a_k}{b^k}$ et nous avons

$$0 < x' < \frac{a_n + 1}{b^n}. \quad (6.374)$$

Le nombre x' est forcément dans un des intervalles

$$]\frac{s}{b^{n+1}}, \frac{s+1}{b^{n+1}}[\quad (6.375)$$

avec $s \in \{0, \dots, b-1\}$. Nous prenons le s correspondant à x' comme a_{n+1} . Dans ce cas nous avons

$$\sum_{k=1}^{n+1} \frac{a_k}{b^k} < x < \sum_{k=1}^{n+1} \frac{a_k}{b^k} + \frac{1}{b^{n+1}}. \quad (6.376)$$

Note : les deux inégalités sont strictes. La première parce que si il y avait égalité, nous nous serions déjà arrêté en complétant avec des zéros. La seconde parce que

$$\sum_{k=n+2}^{\infty} \frac{a_k}{b^k} \leq \sum_{k=n+2}^{\infty} \frac{b-1}{b^k} = \frac{1}{b^{n+1}} \quad (6.377)$$

où l'égalité n'est possible que si $a_k = b-1$ pour tout $k \geq n+2$. Dans ce cas nous aurions eu

$$x = \sum_{k=1}^n \frac{a_k}{b^k} + \frac{a_{n+1} + 1}{b^{n+1}} \quad (6.378)$$

et nous aurions choisit le nombre a_{n+1} autrement et complété la suite par des zéros à partir de là. Notons que cela prouve au passage que la suite que nous sommes en train de construire est bien dans $\mathbb{D}_b$ parce qu'elle ne contiendra pas de queue de suite composée de $b-1$.

Ceci termine la construction par récurrence de la suite $a \in \mathbb{D}_b$. Par construction nous avons pour tout $N \geq 1$,

$$\sum_{k=1}^N \frac{a_k}{b^k} \leq x \leq \sum_{k=1}^N \frac{a_k}{b^k} + \frac{1}{b^{N+1}}, \quad (6.379)$$

autrement dit : $\varphi_b(a_1, \dots, a_N) \in B(x, \frac{1}{b^{N+1}})$. Nous avons donc bien convergence

$$\lim_{N \rightarrow \infty} \varphi_b(a_1, \dots, a_N) = x \quad (6.380)$$

et l'application φ_b est surjective. □

L'application $\varphi_b^{-1}: [0, 1[\rightarrow \mathbb{D}_b$ est la **décomposition décimale** en base b des nombres de $[0, 1[$.

Tout cela nous permet de montrer entre autres que $\mathbb{R}$ n'est pas dénombrable. Vu qu'il y a une bijection entre $[0, 1[$ et $\mathbb{D}_b$, il suffit de prouver que $\mathbb{D}_b$ est non dénombrable. De plus il suffit de démontrer que $\mathbb{D}_b$ est non dénombrable pour un entier $b \geq 2$ donné.

Proposition 6.175 ([10]).

Il n'existe pas de surjection $\mathbb{N} \rightarrow \mathbb{D}_b$. Autrement dit $\mathbb{D}_b$ est non dénombrable.

Démonstration. Nous prenons $b \neq 2$ pour des raisons qui seront claires plus tard. Soit $f: \mathbb{N} \rightarrow \mathbb{D}_b$. Pour $i \in \mathbb{N}$ nous notons

$$f(n) = (c_i^{(n)})_{i \geq 1}, \quad (6.381)$$

et nous définissons la suite

$$c_k = \begin{cases} 0 & \text{si } c_k^{(k)} \neq 0 \\ 1 & \text{si } c_k^{(k)} = 0. \end{cases} \quad (6.382)$$

Cela est une suite dans $\mathbb{D}_b$ parce que $b \neq 2$ et que la suite ne contient que des 0 et des 1. Mais nous n'avons $f(n) = c$ pour aucun $n \in \mathbb{N}$ parce que nous avons $c_n \neq f(n)_n$.

Si $b = 2$ alors nous savons que $\mathbb{D}_2 \sim [0, 1[\sim \mathbb{D}_3$. Donc $\mathbb{D}_2 \sim \mathbb{D}_3$ et $\mathbb{D}_2$ ne peut pas plus être mis en bijection avec $\mathbb{N}$ que $\mathbb{D}_3$. □

Remarque 6.176.

La preuve ne fonctionne pas en base $b = 2$ parce que rien n'empêche d'avoir une queue de 1. Il y a alors toutefois moyen de se débrouiller en construisant la suite c de façon plus subtile. Si $b = 2$ et $n \in \mathbb{N}$ alors $f(n)$ est une suite de 0 et 1 contenant une infinité de 0 (parce qu'il n'y a pas de queue de suite ne contenant que des 1). Nous construisons alors c de la façon suivante : d'abord

nous recopions $f(0)$ jusqu'à son *deuxième* zéro que nous changeons en 1 ; nommons n_0 le rang de ce deuxième zéro. Ensuite nous recopions les éléments de $f(1)$ à partir du rang $n_0 + 1$ jusqu'au second zéro que nous changeons en 1, etc.

Le fait de prendre le deuxième zéro nous garanti que la suite c n'aura pas de queue de suite ne contenant que des 1.

Notons que cette construction s'adapte à tout b ; il suffit de prendre le second terme qui n'est pas $b - 1$ et le remplacer par $b - 1$.

Corollaire 6.177.

L'ensemble $[0, 1[$ n'est pas dénombrable.

Démonstration. L'ensemble $[0, 1[$ est en bijection avec $\mathbb{D}_b$ que nous venons de prouver n'être pas dénombrable. $\square$

6.16 Exponentielle de matrice

(1) En ce qui concerne la continuité, nous aurons évidemment besoin de théorie à propos de l'inversion de limites et de sommes. Nous en parlerons donc en 16.4.8.

(2) Les séries entières de matrices seront traitées plus en détail autour de la proposition 16.75.

Proposition 6.178.

Soit V un espace vectoriel de dimension finie et $A \in \text{End}(V)$. La série

$$\exp(A) = \mathbb{1} + A + \frac{A^2}{2} + \frac{A^3}{3} + \dots = \sum_{k=1}^{\infty} \frac{A^k}{k!}. \quad (6.383)$$

converge normalement dans $(\text{End}(V), \|\cdot\|_{op})$. L'exponentielle de la matrice A est cette matrice.

Démonstration. Vu que la norme opérateur est une norme d'algèbre par la proposition 6.88, nous avons pour tout k la majoration $\|A^k\| \leq \|A\|^k$. Nous avons donc

$$\sum_{k=0}^{\infty} \frac{\|A^k\|}{k!} \leq \sum_k \frac{\|A\|^k}{k!}. \quad (6.384)$$

La dernière somme converge en vertu de la convergence de la série exponentielle donnée en exemple 6.169. $\square$

Étant donné que c'est une limite, il y a une question de convergence et donc de topologie. C'est pour cela que nous ne pouvions pas introduire l'exponentielle de matrice avant d'avoir introduit la norme des matrices. La convergence de la série pour toute matrice sera prouvée au passage dans la proposition 6.179.

La fonction exponentielle $x \mapsto e^x$ n'est pas un polynôme en x , mais nous avons les résultat marrant suivant.

Proposition 6.179.

Si u est un endomorphisme, alors $\exp(u)$ est un polynôme en u ²⁴.

Démonstration. Nous considérons l'application

$$\begin{aligned} \varphi_u: \mathbb{K}[X] &\rightarrow \text{End}(E) \\ P &\mapsto P(u) \end{aligned} \quad (6.385)$$

Étant donné que l'image de φ_u est un fermé dans $\text{End}(E)$, il suffit de montrer que la série

$$\sum_{k=0}^{\infty} \frac{\varphi_u(X)^k}{k!} \quad (6.386)$$

24. Nan, mais j'te jure : $\exp$ n'est pas un polynôme, mais $\exp(u)$ est un polynôme de u .

converge dans $\text{End}(E)$ pour qu'elle converge dans $\text{Image}(\varphi_u)$. Pour ce faire nous nous rappelons de la norme opérateur²⁵ et de la propriété fondamentale $\|A^k\| \leq \|A\|^k$. En notant $A = \varphi_u(X)$,

$$\left\| \sum_{k=n}^m \frac{A^k}{k!} \right\| \leq \sum_{k=n}^m \frac{\|A^k\|}{k!} \leq \sum_{k=n}^m \frac{\|A\|^k}{k!}, \quad (6.387)$$

ce qui est un morceau du développement de $e^{\|A\|}$. La limite $n \rightarrow \infty$ est donc zéro par la convergence de l'exponentielle réelle. La suite des sommes partielles de e^A est donc de Cauchy. La série converge donc parce que nous sommes dans un espace vectoriel réel de dimension finie ($\text{End}(E)$). $\square$

Remarque 6.180.

Pourquoi $\exp(u)$ est-il un polynôme d'endomorphisme alors que $\exp$ n'est pas un polynôme ? Lorsque nous disons que la fonction $x \mapsto \exp(x)$ n'est pas un polynôme, nous sommes en train de localiser la fonction $\exp$ à l'intérieur de l'espace de toutes les fonctions $\mathbb{R} \rightarrow \mathbb{R}$, c'est à dire à l'intérieur d'un espace de dimension infinie. Au contraire lorsqu'on parle de $\exp(u)$ et qu'on le compare aux endomorphismes $P(u)$, nous sommes en train de repérer $\exp(u)$ à l'intérieur de l'espace des matrices qui est de dimension finie. Il n'est donc pas étonnant que l'on parvienne moins à faire la distinction.

Si par contre nous considérons $\exp$ en tant qu'application $\exp: \text{End}(E) \rightarrow \text{End}(E)$, ce n'est pas un polynôme.

Si u et v sont des endomorphismes, nous aurons des polynômes P et Q tels que $e^u = P(u)$ et $e^v = Q(v)$; mais nous n'aurons en général évidemment pas $P = Q$. En cela, $\exp$ n'est pas un polynôme.

6.17 Sommes de familles infinies

6.17.1 Convergence commutative

Définition 6.181.

Soit x_k une suite dans un espace vectoriel normé E . Nous disons que la suite **converge commutativement** vers $x \in E$ si $\lim_{n \rightarrow \infty} \|x_n - x\| = 0$ et si pour toute bijection $\tau: \mathbb{N} \rightarrow \mathbb{N}$ nous avons aussi

$$\lim_{n \rightarrow \infty} \|x_{\tau(k)} - x\| = 0. \quad (6.388)$$

La notion de convergence commutative est surtout intéressante pour les séries. La somme

$$\sum_{k=0}^{\infty} x_k \quad (6.389)$$

converge commutativement vers x si $\lim_{N \rightarrow \infty} \|x - \sum_{k=0}^N x_k\| = 0$ et si pour toute bijection $\tau: \mathbb{N} \rightarrow \mathbb{N}$ nous avons

$$\lim_{N \rightarrow \infty} \|x - \sum_{k=0}^N x_{\tau(k)}\| = 0. \quad (6.390)$$

Nous démontrons maintenant qu'une série converge commutativement si et seulement si elle converge absolument.

Pour le sens inverse, nous avons la proposition suivante.

Proposition 6.182.

Soit $\sum_{k=0}^{\infty} a_k$ une série réelle qui converge mais qui ne converge pas absolument. Alors pour tout $b \in \mathbb{R}$, il existe une bijection $\tau: \mathbb{N} \rightarrow \mathbb{N}$ telle que $\sum_{i=0}^{\infty} a_{\tau(i)} = b$.

Pour une preuve, voir chez Gilles Dubois.

25. Définition 6.86.

Proposition 6.183.

Soit $(a_i)_{i \in \mathbb{N}}$ une suite dans $\mathbb{C}$ convergent absolument. Alors elle converge commutativement.

Démonstration. Soit $\epsilon > 0$. Nous posons $\sum_{i=0}^{\infty} a_i = a$ et nous considérons N tel que

$$\left| \sum_{i=0}^N a_i - a \right| < \epsilon. \quad (6.391)$$

Étant donné que la série des $|a_i|$ converge, il existe N_1 tel que pour tout $p, q > N_1$ nous ayons $\sum_{i=p}^q |a_i| < \epsilon$. Nous considérons maintenant une bijection $\tau: \mathbb{N} \rightarrow \mathbb{N}$. Prouvons que la série $\sum_{i=0}^{\infty} |a_{\tau(i)}|$ converge. Nous choisissons M de telle sorte que pour tout $n > M$, $\tau(n) > N_1$; alors si $p, q > M$ nous avons

$$\sum_{i=p}^q |a_{\tau(i)}| < \epsilon. \quad (6.392)$$

Par conséquent la somme de la suite $(a_{\tau(i)})$ converge. Nous devons montrer à présent qu'elle converge vers la même limite que la somme « usuelle » $\lim_{N \rightarrow \infty} \sum_{i=0}^N a_i$.

Soit $n > \max\{M, N\}$. Alors

$$\sum_{k=0}^n a_{\tau(k)} - \sum_{k=0}^n a_k = \sum_{k=0}^M a_{\tau(k)} - \sum_{k=0}^N a_k + \underbrace{\sum_{k=M+1}^n a_{\tau(k)}}_{< \epsilon} - \underbrace{\sum_{k=N+1}^n a_k}_{< \epsilon}. \quad (6.393)$$

Par construction les deux derniers termes sont plus petits que ϵ parce que M et N sont les constantes de Cauchy pour les séries $\sum a_{\tau(i)}$ et $\sum a_i$. Afin de traiter les deux premiers termes, quitte à redéfinir M , nous supposons que $\{1, \dots, N\} \subset \tau\{1, \dots, M\}$; par conséquent tous les a_i avec $i < N$ sont atteints par les $a_{\tau(i)}$ avec $i < M$. Dans ce cas, les termes qui restent dans la différence

$$\sum_{k=0}^M a_{\tau(k)} - \sum_{k=0}^N a_k \quad (6.394)$$

sont des a_k avec $k > N$. Cette différence est donc en valeur absolue plus petite que ϵ , et nous avons en fin de compte que

$$\left| \sum_{k=0}^n a_{\tau(k)} - \sum_{k=0}^n a_k \right| < \epsilon. \quad (6.395)$$

□

Proposition 6.184.

Soit $\sum_{i=0}^{\infty} a_i$ une série qui converge mais qui ne converge pas absolument. Pour tout $b \in \mathbb{R}$, il existe une bijection $\tau: \mathbb{N} \rightarrow \mathbb{N}$ telle que $\sum_{i=0}^{\infty} a_{\tau(i)} = b$.

Les propositions 6.183 et 6.184 disent entre autres qu'une série dans $\mathbb{C}$ est commutativement sommable si et seulement si elle est absolument sommable.

Soit $(a_i)_{i \in I}$ une famille de nombres complexes indexée par un ensemble I quelconque. Nous allons nous intéresser à la somme $\sum_{i \in I} a_i$.

Soit $\{a_i\}_{i \in I}$ des nombres positifs. Nous définissons la somme

$$\sum_{i \in I} a_i = \sup_{J \text{ fini}} \sum_{j \in J} a_j. \quad (6.396)$$

Notons que cela est une définition qui ne fonctionne bien que pour les sommes de nombres positifs. Si $a_i = (-1)^i$, alors selon la définition nous aurions $\sum_i (-1)^i = \infty$. Nous ne voulons évidemment pas un tel résultat.

Dans le cas de familles de nombres réels positifs, nous avons une première définition de la somme.

Définition 6.185.

Soit $(a_i)_{i \in I}$ une famille de nombres réels positifs indexés par un ensemble quelconque I . Nous définissons

$$\sum_{i \in I} a_i = \sup_{J \text{ fini dans } I} \sum_{j \in J} a_j. \quad (6.397)$$

Définition 6.186.

Si $\{v_i\}_{i \in I}$ est une famille de vecteurs dans un espace vectoriel normé indexée par un ensemble quelconque I . Nous disons que cette famille est **sommable** de somme v si pour tout $\epsilon > 0$, il existe un J_0 fini dans I tel que pour tout ensemble fini K tel que $J_0 \subset K$ nous avons

$$\left\| \sum_{j \in K} v_j - v \right\| < \epsilon. \quad (6.398)$$

Notons que cette définition implique la convergence commutative.

Exemple 6.187

La suite $a_i = (-1)^i$ n'est pas sommable parce que quel que soit J_0 fini dans $\mathbb{N}$, nous pouvons trouver J fini contenant J_0 tel que $\sum_{j \in J} (-1)^j > 10$. Pour cela il suffit d'ajouter à J_0 suffisamment de termes pairs. De la même façon en ajoutant des termes impairs, on peut obtenir $\sum_{j \in J'} (-1)^j < -10$. $\triangle$

Exemple 6.188

De temps en temps, la somme peut sortir d'un espace. Si nous considérons l'espace des polynômes $[0, 1] \rightarrow \mathbb{R}$ muni de la norme uniforme, la somme de l'ensemble

$$\left\{ 1, -1, \pm \frac{x^n}{n!} \right\}_{n \in \mathbb{N}} \quad (6.399)$$

est zéro.

Par contre la somme de l'ensemble $\{1, \frac{x^n}{n!}\}_{n \in \mathbb{N}}$ est l'exponentielle qui n'est pas un polynôme.

$\triangle$

Exemple 6.189

Au sens de la définition 6.186 la famille

$$\frac{(-1)^n}{n} \quad (6.400)$$

n'est pas sommable. En effet la somme des termes pairs est ∞ alors que la somme des termes impairs est $-\infty$. Quel que soit $J_0 \in \mathbb{N}$, nous pouvons concocter, en ajoutant des termes pairs, un J avec $J_0 \subset J$ tel que $\sum_{j \in J} (-1)^j/j$ soit arbitrairement grand. En ajoutant des termes négatifs, nous pouvons également rendre $\sum_{j \in J} (-1)^j/j$ arbitrairement petit. $\triangle$

Proposition 6.190.

Si (a_{ij}) est une famille de nombres positifs indexés par $\mathbb{N} \times \mathbb{N}$ alors

$$\sum_{(i,j) \in \mathbb{N}^2} a_{ij} = \sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right) \quad (6.401)$$

où la somme de gauche est celle de la définition 6.185.

Démonstration. Nous considérons $J_{m,n} = \{0, \dots, m\} \times \{0, \dots, n\}$ et nous avons pour tout m et n :

$$\sum_{(i,j) \in \mathbb{N}^2} a_{ij} \geq \sum_{(i,j) \in J_{m,n}} a_{ij} = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} \right). \quad (6.402)$$

Si nous fixons m et que nous prenons la limite $n \rightarrow \infty$ (qui commute avec la somme finie sur i) nous trouvons

$$\sum_{(i,j) \in \mathbb{N}^2} a_{ij} \geq \sum_{i=1}^m \left(\sum_{j=1}^{\infty} a_{ij} \right). \quad (6.403)$$

Cela étant valable pour tout m , c'est encore valable à la limite $m \rightarrow \infty$ et donc

$$\sum_{(i,j) \in \mathbb{N}^2} a_{ij} \geq \sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right). \quad (6.404)$$

Pour l'inégalité inverse, il faut remarquer que si J est fini dans $\mathbb{N}^2$, il est forcément contenu dans $J_{m,n}$ pour m et n assez grand. Alors

$$\sum_{(i,j) \in J} a_{ij} \leq \sum_{(i,j) \in J_{m,n}} a_{ij} = \sum_{i=1}^m \sum_{j=1}^n a_{ij} \leq \sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right). \quad (6.405)$$

Cette inégalité étant valable pour tout ensemble fini $J \subset \mathbb{N}^2$, elle reste valable pour le supremum. $\square$

La définition générale de la somme 6.186 est compatible avec la définition usuelle dans les cas où cette dernière s'applique.

Proposition 6.191 (commutative sommabilité).

Soit I un ensemble dénombrable et une bijection $\tau: \mathbb{N} \rightarrow I$. Soit $(a_i)_{i \in I}$ une famille dans un espace vectoriel normé. Alors

$$\sum_{k=0}^{\infty} a_{\tau(k)} = \sum_{i \in I} a_i \quad (6.406)$$

dès que le membre de droite existe. Le membre de gauche est défini par la limite usuelle.

Démonstration. Nous posons $a = \sum_{i \in I} a_i$. Soit $\epsilon > 0$ et J_0 comme dans la définition. Nous choisissons

$$N > \max_{j \in J_0} \{\tau^{-1}(j)\}. \quad (6.407)$$

En tant que sommes sur des ensembles finis, nous avons l'égalité

$$\sum_{k=0}^N a_{\tau(k)} = \sum_{j \in J_0} a_j \quad (6.408)$$

où J est un sous-ensemble de I contenant J_0 . Soit J fini dans I tel que $J_0 \subset J$. Nous avons alors

$$\left\| \sum_{k=0}^N a_{\tau(k)} - a \right\| = \left\| \sum_{j \in J} a_j - a \right\| < \epsilon. \quad (6.409)$$

Nous avons prouvé que pour tout ϵ , il existe N tel que $n > N$ implique $\left\| \sum_{k=0}^n a_{\tau(k)} - a \right\| < \epsilon$. $\square$

Corollaire 6.192.

Nous pouvons permuter une somme dénombrable et une fonction continue. C'est à dire que si f est une fonction continue sur l'espace vectoriel normé E et $(a_i)_{i \in I}$ une famille sommable dans E alors

$$f \left(\sum_{i \in I} a_i \right) = \sum_{i \in I} f(a_i). \quad (6.410)$$

Démonstration. En utilisant une bijection τ entre I et $\mathbb{N}$ avec la proposition 6.191 ainsi que le résultat connu à propos des sommes sur $\mathbb{N}$, nous avons

$$f \left(\sum_{i \in I} a_i \right) = f \left(\sum_{k=0}^{\infty} a_{\tau(k)} \right) = \sum_{k=0}^{\infty} f(a_{\tau(k)}) = \sum_{i \in I} f(a_i). \quad (6.411)$$

$\square$

La proposition suivante nous enseigne que les sommes infinies peuvent être manipulées de façon usuelle.

Proposition 6.193.

Soit I un ensemble dénombrable. Soient $(a_i)_{i \in I}$ et $(b_i)_{i \in I}$, deux familles de réels positifs telles que $a_i < b_i$ et telles que (b_i) est sommable. Alors (a_i) est sommable.

Si $(a_i)_{i \in I}$ est une famille de complexes telle que $(|a_i|)$ est sommable, alors (a_i) est sommable.

6.18 Mini introduction aux nombres p-adiques

6.18.1 La flèche d'Achille

C'est un grand classique que je donne ici juste comme introduction pour montrer que des séries infinies peuvent donner des nombres finis de manière tout à fait intuitive.

Achille tire une flèche vers un arbre situé à 10 m de lui. Disons que la flèche avance à une vitesse constante de 1 m/s. Il est clair que la flèche mettra 10 s pour toucher l'arbre. En 5 s, elle aura parcouru la moitié de son chemin. On le note :

$$\text{temps} = 5s + \dots$$

Reste 5 m à faire. En 2.5 s, elle aura fait la moitié de ce chemin, soit $2.5m = \frac{10}{4}m$. On le note :

$$\text{temps} = \frac{10}{2}s + \frac{10}{4}s +$$

Reste $2.5m$ à faire. La moitié de ce trajet, soit $\frac{10}{8}m$, est parcouru en $\frac{10}{8}s$; on le note encore, mais c'est la dernière fois !

$$\text{temps} = \frac{10}{2}s + \frac{10}{4}s + \frac{10}{8}s +$$

En continuant ainsi à regarder la flèche qui parcourt des demi-trajets puis des demi de demi-trajets et encore des demi de demi de demi-trajets, et en sachant que le temps total est 10 s, on trouve :

$$10 \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots \right) = 10.$$

On doit donc croire que la somme jusqu'à l'infini des inverse des puissances de deux vaut 1 :

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = 1.$$

Cela peut être démontré à la loyale.

6.18.2 La tortue et Achille

Maintenant qu'on est convaincu que des sommes infinies peuvent représenter des nombres tout à fait normaux, passons à un truc plus marrant.

Achille, qui marche peinard à 10 m/h, part avec 1 m d'avance sur une tortue qui avance à 1 m/h. Le temps que la tortue arrive au point de départ d'Achille, Achille aura parcouru 10 m, et le temps que la tortue mettra pour arriver à ce point, eh bien, Achille ne sera déjà plus là : il sera à 100 m. Si la tortue tient bon pendant un temps infini, et si l'on est confiant en le genre de raisonnements faits à la section 6.18.1, elle rattrapera Achille dans

$$1m + 10m + 100m + 1000m + \dots$$

Autant dire que ça ne risque pas d'arriver. Et pourtant, mettons en équations :

$$\begin{cases} x_{\text{Achille}}(t) = 1 + 10t & (6.412a) \\ x_{\text{tortue}}(t) = t. & (6.412b) \end{cases}$$

La tortue rejoint Achille au temps t tel que $x_{\text{Achille}(t)} = x_{\text{tortue}}(t)$. Un mini calcul donne $t = -1/9$. Physiquement, c'est une situation logique. Peut-on en déduire une égalité mathématique du style de

$$1 + 10 + 100 + 1000 + \dots = -\frac{1}{9} ???$$

Là où les choses deviennent jolies, c'est quand on cherche à voir ce que peut bien être la valeur d'un hypothétique $x = 1 + 10 + 100 + 1000 + \dots$. En effet, logiquement on devrait avoir

$$\begin{aligned} \frac{x}{10} &= \frac{1}{10} + 1 + 10 + 100 + \dots \\ &= \frac{1}{10} + x. \end{aligned}$$

Reste à résoudre l'équation du premier degré : $\frac{x}{10} = x + \frac{1}{10}$. Ai-je besoin de donner la solution ?

6.18.3 Dans les nombres p-adiques, c'est vrai

Nous nous proposons d'apprendre sur les nombres p -adiques juste ce qu'il faut pour montrer que l'égalité

$$\sum_{k=0}^{\infty} 10^k = -\frac{1}{9} \quad (6.413)$$

est vraie dans les nombres 5-adiques. Tout ce qu'il faut est sur wikipedia.

Soit $a \in \mathbb{N}$ et p , un nombre premier. La **valuation** p -adique de a est l'exposant de p dans la décomposition de a en nombres premiers. On la note $v_p(a)$. Pour un rationnel on définit

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) \quad (6.414)$$

La **valeur absolue** p -adique de $r \in \mathbb{Q}$ est

$$|r|_p = p^{-v_p(r)}. \quad (6.415)$$

Nous posons $|0|_p = 0$. De là nous considérons la distance

$$d_p(x, y) = |x - y|_p. \quad (6.416)$$

Lemme 6.194.

L'espace $(\mathbb{Q}, d_p)$ est un espace métrique²⁶.

Nous considérons maintenant $p = 5$. Étant donné que $a = 5 \cdot 2$ nous avons $v_5(10) = 1$ et

$$v_5\left(\frac{1}{9}\right) = v_5(1) - v_5(9) = 0. \quad (6.417)$$

Nous avons

$$\sum_{k=0}^N 10^k + \frac{1}{9} = \frac{10^{N+1}}{9} \quad (6.418)$$

mais

$$v_p\left(\frac{10^{N+1}}{9}\right) = v_5(10^{N+1}) - v_5(9) = N + 1. \quad (6.419)$$

Par conséquent

$$d_5\left(\sum_{k=0}^N 10^k, -\frac{1}{9}\right) = \left|\frac{10^{N+1}}{9}\right|_p = p^{-(N+1)}. \quad (6.420)$$

26. Définition 5.17

En passant à la limite,

$$\lim_{N \rightarrow \infty} d_5\left(\sum_{k=0}^N 10^k, -\frac{1}{9}\right) = 0, \quad (6.421)$$

ce qui signifie que²⁷

$$\sum_{k=0}^{\infty} 10^k = -\frac{1}{9}. \quad (6.422)$$

6.19 Fonctions

Soient $(V, \|\cdot\|_V)$ et $(W, \|\cdot\|_W)$ deux espaces vectoriels normés, et une fonction f de V dans W . 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 $\mathbb{R}$ en changeant simplement les valeurs absolues par les normes sur V et W .

La caractérisation suivante est un recopiage de la définition 5.52 lorsque la topologie est donnée par des boules.

Proposition 6.195.

Soit $f: V \rightarrow W$ une fonction de domaine $\text{Dom}(f) \subset V$ et soit a un point d'accumulation de $\text{Dom}(f)$. La fonction f en a si et seulement si il existe un élément $\ell \in W$ tel que pour tout $\varepsilon > 0$, il existe un $\delta > 0$ tel que pour tout $x \in \text{Dom}(f)$,

$$0 < \|x - a\|_V < \delta \Rightarrow \|f(x) - \ell\|_W < \varepsilon. \quad (6.423)$$

Dans ce cas, nous écrivons $\lim_{x \rightarrow a} f(x) = \ell$ et nous disons que ℓ est la **limite** de f lorsque x tend vers a .

Remarque 6.196.

Le fait que nous limitons la formule (6.423) aux x dans le domaine de f n'est pas anodin. Considérons la fonction $f(x) = \sqrt{x^2 - 4}$, de domaine $|x| \geq 2$. Nous avons

$$\lim_{x \rightarrow 2} \sqrt{x^2 - 4} = 0. \quad (6.424)$$

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 donc 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 $[2, \infty[$.

6.20 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.

6.20.1 Norme

La définition de la norme sur un produit d'espaces vectoriels normés découle immédiatement de la définition de la distance 5.146 :

Définition 6.197.

Soient V et W deux espaces vectoriels normés. On appelle **espace produit** de V et W le produit cartésien $V \times W$

$$V \times W = \{(v, w) \mid v \in V, w \in W\}, \quad (6.425)$$

muni de la norme $\|\cdot\|_{V \times W}$

$$\|(v, w)\|_{V \times W} = \max\{\|v\|_V, \|w\|_W\}. \quad (6.426)$$

27. Voir la définition 6.150 de la convergence d'une série dans un espace métrique.

Il est presque immédiat de vérifier que le produit cartésien $V \times W$ est un espace vectoriel pour les opérations de somme et multiplication par les scalaires définies composante par composante. C'est à dire, si $(v_1, w_1), (v_2, w_2)$ sont dans $V \times W$ et a, b sont des scalaires, alors

$$a(v_1, w_1) + b(v_2, w_2) = (av_1, aw_1) + (bv_2, bw_2) = (av_1 + bv_2, aw_1 + bw_2). \quad (6.427)$$

Lemme 6.198.

L'opération $\|\cdot\|_{V \times W} : V \times W \rightarrow \mathbb{R}$ est une norme.

Démonstration. On doit vérifier les trois conditions de la définition 5.31.

- 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 $\|a(v, w)\|_{V \times W}$ est donnée par $\max\{\|av\|_V, \|aw\|_W\}$. On peut factoriser $\|av\|_V = |a|\|v\|_V$ et $\|aw\|_W = |a|\|w\|_W$ et donc $\|a(v, w)\|_{V \times W} = |a| \max\{\|v\|_V, \|w\|_W\} = |a|\|(v, w)\|_{V \times W}$.
- Soient (v_1, w_1) et (v_2, w_2) dans $V \times W$.

$$\begin{aligned} \|(v_1, w_1) + (v_2, w_2)\|_{V \times W} &= \max\{\|v_1 + v_2\|_V, \|w_1 + w_2\|_W\} \\ &\leq \max\{\|v_1\|_V + \|v_2\|_V, \|w_1\|_W + \|w_2\|_W\} \\ &\leq \max\{\|v_1\|_V, \|w_1\|_W\} + \max\{\|v_2\|_V, \|w_2\|_W\} \\ &= \|(v_1, w_1)\|_{V \times W} + \|(v_2, w_2)\|_{V \times W}. \end{aligned} \quad (6.428)$$

□

Toutes ces définitions se généralisent à un produit fini d'espaces vectoriels normés. Si les espaces V_i sont des espaces vectoriels normés, nous pouvons mettre sur le produit une topologie et une norme :

- La topologie produit donnée en 5.5
- La norme maximum $\|v_1, \dots, v_n\|_{\max} = \max\{\|v_1\|, \dots, \|v_n\|\}$. Dans le membre de droites, toutes les normes sont différentes.

Une question qui vient est la compatibilité entre ces deux constructions. Est-ce que la topologie associée à la norme maximum est la topologie produit ? Oui.

Lemme 6.199 ([89]).

La topologie de la norme maximum est la topologie produit²⁸.

Proposition 6.200 ([90]).

Soient des espaces vectoriels normés V et W ainsi qu'une forme sesquilinéaire $p : V \times W \rightarrow \mathbb{C}$. Il y a équivalence des faits suivants.

- (1) ϕ est continue.
- (2) ϕ est continue en $(0, 0)$
- (3) ϕ est bornée
- (4) Il existe $C \geq 0$ telle que $|\phi(x, y)| \leq C\|x\|\|y\|$ pour tout $(x, y) \in V \times W$.

De plus la norme de ϕ est alors donnée par

$$\|\phi\| = \min\{C \geq 0 \text{ tel que } |\phi(x, y)| \leq C\|x\|\|y\| \forall (x, y) \in V \times W\}. \quad (6.429)$$

On remarque tout de suite que la norme $\|\cdot\|_\infty$ 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

$$\|(x_1, x_2, x_3, x_4)\|_{\infty, 2} = \max\{\|(x_1, x_2)\|_\infty, \|(x_3, x_4)\|_2\}.$$

²⁸. Définition 5.5.

Les applications de projection de l'espace produit $V \times W$ vers les espaces «facteurs», V et W sont notées proj_V et proj_W et sont définies par

$$\begin{aligned} \text{proj}_V: V \times W &\rightarrow V \\ (v, w) &\mapsto v \end{aligned} \quad (6.430)$$

et

$$\begin{aligned} \text{proj}_W: V \times W &\rightarrow W \\ (v, w) &\mapsto w. \end{aligned} \quad (6.431)$$

Les inégalités suivantes sont évidentes

$$\begin{aligned} \|\text{proj}_V(v, w)\|_V &\leq \|(v, w)\|_{V \times W} \\ \|\text{proj}_W(v, w)\|_W &\leq \|(v, w)\|_{V \times W}. \end{aligned} \quad (6.432)$$

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 proj_V (respectivement 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 6.203.

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 6.201

Si V et W sont deux espaces vectoriels, nous pouvons considérer le produit $E = V \times W$. Les projections proj_V et proj_W , définies dans la section 6.20, sont des applications linéaires.

En effet, la projection $\text{proj}_V: V \times W \rightarrow V$ est donnée par $\text{proj}_V(v, w) = v$. Alors,

$$\begin{aligned} \text{proj}_V((v, w) + (v', w')) &= \text{proj}_V((v + v'), (w + w')) \\ &= v + v' \\ &= \text{proj}_V(v, w) + \text{proj}_V(v', w'), \end{aligned} \quad (6.433)$$

et

$$\text{proj}_V(\lambda(v, w)) = \text{proj}_V((\lambda v, \lambda w)) = \lambda v = \lambda \text{proj}_V(v, w). \quad (6.434)$$

Nous laissons en exercice le soin d'adapter ces calculs pour montrer que proj_W est également une projection. $\triangle$

Proposition 6.202.

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. Vu que $\mathcal{O}$ est un voisinage, il contient un ouvert et donc une boule

$$B((a, b), r) = \{(v, w) \in V \times W \text{ tel que } \max\{\|v - a\|, \|w - b\|\} < r\}. \quad (6.435)$$

Évidemment l'ensemble $B(a, r) \times B(b, r)$ est dedans. $\square$

6.20.2 Suites

Nous allons maintenant parler de suites dans $V \times W$. Nous noterons (v_n, w_n) la suite dans $V \times W$ dont l'élément numéro n est le couple (v_n, w_n) avec $v_n \in V$ et $w_n \in W$. La notions de convergence de suite découle de la définition de la norme via la définition usuelle 6.141. Il se fait que dans le cas des produits d'espaces, la convergence d'une suite est équivalente à la convergence des composantes. Plus précisément, nous avons le lemme suivant.

Lemme 6.203.

La suite (v_n, w_n) converge vers (v, w) dans $V \times W$ si et seulement les suites (v_n) et (w_n) convergent séparément vers v et w respectivement dans V et W .

Démonstration. Pour le sens direct, nous devons étudier le comportement de la norme de $(v_n, w_n) - (v, w)$ lorsque n devient grand. En vertu de la définition de la norme dans $V \times W$ nous avons

$$\|(v_n, w_n) - (v, w)\|_{V \times W} = \max\{\|v_n - v\|_V, \|w_n - w\|_W\}. \quad (6.436)$$

Soit $\varepsilon > 0$. Par définition de la convergence de la suite (v_n, w_n) , il existe un $N \in \mathbb{N}$ tel que $n > N$ implique

$$\max\{\|v_n - v\|_V, \|w_n - w\|_W\} < \varepsilon, \quad (6.437)$$

et donc en particulier les deux inéquations

$$\|v_n - v\| < \varepsilon \quad (6.438a)$$

$$\|w_n - w\| < \varepsilon. \quad (6.438b)$$

De la première, il ressort que $(v_n) \rightarrow v$, et de la seconde que $(w_n) \rightarrow w$.

Pour le sens inverse, nous avons pour tout ε un N_1 tel que $\|v_n - v\|_V \leq \varepsilon$ pour tout $n > N_1$ et un N_2 tel que $\|w_n - w\|_W \leq \varepsilon$ pour tout $n > N_2$. Si nous posons $N = \max\{N_1, N_2\}$ nous avons les deux inégalités simultanément, et donc

$$\max\{\|v_n - v\|_V, \|w_n - w\|_W\} < \varepsilon, \quad (6.439)$$

ce qui signifie que la suite (v_n, w_n) converge vers (v, w) dans $V \times W$. □

Remarque 6.204.

Il faut remarquer que la norme (6.426) est une norme *par défaut*. C'est la norme qu'on met quand on ne sait pas quoi mettre. Or il y a au moins un cas d'espace produit dans lequel on sait très bien quelle norme prendre : les espaces $\mathbb{R}^m$. La norme qu'on met sur $\mathbb{R}^2$ est

$$\|(x, y)\| = \sqrt{x^2 + y^2}, \quad (6.440)$$

et non la norme «par défaut» de $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ qui serait

$$\|(x, y)\| = \max\{|x|, |y|\}. \quad (6.441)$$

Les théorèmes que nous avons donc démontré à propos de $V \times W$ ne sont donc pas immédiatement applicables au cas de $\mathbb{R}^2$.

Cette remarque est valable pour tous les espaces $\mathbb{R}^m$. À moins de mention contraire explicite, nous ne considérons jamais la norme par défaut (6.426) sur un espace $\mathbb{R}^m$.

Étant donné la remarque 6.204, nous ne savons pas comment calculer par exemple la fermeture du produit d'intervalle $]0, 1[\times]4, 5[$. Il se fait que, dans $\mathbb{R}^m$, les fermetures de produits sont quand même les produits de fermetures.

Proposition 6.205.

Soit $A \subset \mathbb{R}^m$ et $B \subset \mathbb{R}^n$. Alors dans $\mathbb{R}^{m+n}$ nous avons $\overline{A \times B} = \bar{A} \times \bar{B}$.

La démonstration risque d'être longue ; nous ne la faisons pas ici.

6.21 Applications multilinéaires

Définition 6.206 (Application multilinéaire).

Une application $T : \mathbb{R}^{m_1} \times \dots \times \mathbb{R}^{m_k} \rightarrow \mathbb{R}^p$ est dite ***k*-linéaire** si pour tout $X = (x_1, \dots, x_k)$ dans $\mathbb{R}^{m_1} \times \dots \times \mathbb{R}^{m_k}$ les applications $x_i \mapsto T(x_1, \dots, x_i, \dots, x_k)$ sont linéaires pour tout i dans $\{1, \dots, k\}$, c'est à dire

$$\begin{aligned} T(\cdot, x_2, \dots, x_i, \dots, x_k) &\in \mathcal{L}(\mathbb{R}^{m_1}, \mathbb{R}^p), \\ T(x_1, \cdot, \dots, x_i, \dots, x_k) &\in \mathcal{L}(\mathbb{R}^{m_2}, \mathbb{R}^p), \\ &\vdots \\ T(x_1, \dots, x_i, \dots, x_{k-1}, \cdot) &\in \mathcal{L}(\mathbb{R}^{m_k}, \mathbb{R}^p). \end{aligned} \quad (6.442)$$

En particulier lorsque $k = 2$, nous parlons d'applications **bilinéaires**. Vous pouvez deviner ce que sont les applications trilinéaire ou quadrilinéaire.

L'ensemble des applications k -linéaires de $\mathbb{R}^{m_1} \times \dots \times \mathbb{R}^{m_k}$ dans $\mathbb{R}^p$ est noté $\mathcal{L}(\mathbb{R}^{m_1} \times \dots \times \mathbb{R}^{m_k}, \mathbb{R}^p)$ ou $\mathcal{L}(\mathbb{R}^{m_1}, \dots, \mathbb{R}^{m_k}; \mathbb{R}^p)$.

Exemple 6.207

Soit A une matrice avec m lignes et n colonnes. L'application bilinéaire de $\mathbb{R}^m \times \mathbb{R}^n$ dans $\mathbb{R}$ associée à A est définie par

$$T_A(x, y) = x^T A y = \sum_{i,j} a_{i,j} x_i y_j, \quad \forall x \in \mathbb{R}^m, y \in \mathbb{R}^n.$$

△

Nous énonçons la proposition suivante dans le cas d'espaces vectoriels normés²⁹ parce que nous allons l'utiliser dans ce cas, mais le cas particulier $E_i = \mathbb{R}^{m_i}$ et $F = \mathbb{R}^p$ est important.

Proposition 6.208.

Soient des espaces vectoriels normés E_i et F . Une application n -linéaire

$$T : E_1 \times \dots \times E_n \rightarrow F \quad (6.443)$$

est continue si et seulement s'il existe un réel $L \geq 0$ tel que

$$\|T(x_1, \dots, x_n)\|_F \leq L \|x_1\|_{F_1} \cdots \|x_n\|_{F_n}, \quad \forall x_i \in E_i. \quad (6.444)$$

Démonstration. Pour simplifier l'exposition nous nous limitons au cas $n = 2$ et nous notons $T(x, y) = x * y$

Supposons que l'inégalité (6.444) soit satisfaite.

$$\begin{aligned} \|x * y - x_0 * y_0\| &= \|(x - x_0) * y - x_0 * (y - y_0)\| \\ &\leq \|(x - x_0) * y\| + \|x_0 * (y - y_0)\| \\ &\leq L \|x - x_0\| \|y\| + L \|x_0\| \|y - y_0\|. \end{aligned} \quad (6.445)$$

Si $x \rightarrow x_0$ et $y \rightarrow y_0$ on voit que T est continue en passant à la limite aux deux côtes de l'inégalité (6.445).

Soit T continue en $(0, 0)$. Évidemment³⁰ $0 * 0 = 0$, donc il existe $\delta > 0$ tel que si $x \in B_{E_1}(0, \delta)$ et $y \in B_{E_2}(0, \delta)$ alors $\|x * y\| \leq 1$. En particulier si $(x, y) \in B_{E_1 \times E_2}(0, \delta)$ nous sommes dans ce cas. Soient maintenant $x \in E_1 \setminus \{0\}$ et $y \in E_2 \setminus \{0\}$

$$x * y = \left(\frac{\|x\|}{\delta} \frac{\delta x}{\|x\|} \right) * \left(\frac{\|y\|}{\delta} \frac{\delta y}{\|y\|} \right) = \frac{\|x\| \|y\|}{\delta^2} \left(\frac{\delta x}{\|x\|} \right) * \left(\frac{\delta y}{\|y\|} \right). \quad (6.446)$$

²⁹. Sans hypothèses sur la dimension.

³⁰. Dans la formule suivante, les trois zéros sont les zéros de trois espaces différents.

On remarque que $\delta x/\|x\|_m$ est dans la boule de rayon δ centrée en 0_m et que $\delta y/\|y\|_n$ est dans la boule de rayon δ centrée en 0_n . On conclut

$$x * y \leq \frac{\|x\|_m \|y\|_n}{\delta^2}.$$

Il faut prendre $L = 1/\delta^2$. □

La norme de T est alors définie comme la plus petite constante L qui fait fonctionner la proposition 6.208.

Définition 6.209.

La norme sur l'espace $\mathcal{L}(E_1 \times \dots \times E_n, F)$ des applications k -linéaires et continues est

$$\|T\|_{E_1 \times \dots \times E_n} = \sup\{\|T(u_1, \dots, u_k)\|_F \mid \|u_i\|_{E_i} \leq 1, i = 1, \dots, k\}. \quad (6.447)$$

Nous avons donc automatiquement

$$\|T(u, v)\| \leq \|T\| \|u\| \|v\|. \quad (6.448)$$

Et nous notons que cette norme est uniquement définie pour les applications linéaires continues. Ce n'est pas très grave parce qu'alors nous définissons $\|T\| = \infty$ si T n'est pas continue. Cela pour retrouver le principe selon lequel on est continue si et seulement si on est borné.

Proposition 6.210.

On définit les fonctions

$$\begin{aligned} \omega_g : \mathcal{L}(\mathbb{R}^m \times \mathbb{R}^n, \mathbb{R}^p) &\rightarrow \mathcal{L}(\mathbb{R}^m, \mathcal{L}(\mathbb{R}^n, \mathbb{R}^p)), \\ \omega_d : \mathcal{L}(\mathbb{R}^m \times \mathbb{R}^n, \mathbb{R}^p) &\rightarrow \mathcal{L}(\mathbb{R}^n, \mathcal{L}(\mathbb{R}^m, \mathbb{R}^p)), \end{aligned} \quad (6.449)$$

par

$$\omega_g(T)(x) = T(x, \cdot), \quad \forall x \in \mathbb{R}^m,$$

et

$$\omega_d(T)(y) = T(\cdot, y), \quad \forall y \in \mathbb{R}^n.$$

Les fonctions ω_g et ω_d sont des isomorphismes qui préservent les normes.

6.22 Méthode de Gauss pour résoudre des systèmes d'équations linéaires

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 :

- (a) Remplacer une ligne par elle-même + un multiple d'une autre ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 2 & 3 & 5 \\ 1 & 2 & 4 \end{array} \right) \xrightarrow{L_1 - 2L_2 \mapsto L'_1} \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array} \right)$$

- (b) Remplacer une ligne par un multiple d'elle-même ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array} \right) \xrightarrow{-L_1 \mapsto L'_1} \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 2 & 4 \end{array} \right)$$

(c) Permuter des lignes.

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 0 & -2 \end{array} \right) \xrightarrow{L_1 \leftrightarrow L_2 \text{ et } L_2 \leftrightarrow L_1} \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array} \right)$$

(3) Retransformer la matrice obtenue en système d'équations.

$$\text{p.ex. } \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array} \right) \Leftrightarrow \begin{cases} x = -2 \\ y = 3 \end{cases}$$

Remarques :

— 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 :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 3 & 4 & -2 & 2 \\ 4 & -1 & 3 & 0 \\ 0 & 0 & 0 & 7 \end{array} \right) \Leftrightarrow \begin{cases} \dots \\ \dots \\ 0x + 0y + 0z = 7 \end{cases} \Rightarrow \textbf{Impossible}$$

— Si on a moins d'équations que d'inconnues, alors il y a une infinité de solutions qui dépendent d'un ou plusieurs paramètres :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 1 & 0 & -2 & 2 \\ 0 & 1 & 3 & 0 \end{array} \right) \Leftrightarrow \begin{cases} x - 2z = 2 \\ y + 3z = 0 \end{cases} \Leftrightarrow \begin{cases} x = 2 + 2\lambda \\ y = -3\lambda \\ z = \lambda \end{cases}$$

6.23 Orthogonalité

Proposition 6.211.

si $v_1, \dots, v_k$ sont des vecteurs non nuls, orthogonaux deux à deux, alors ces vecteurs forment une famille libre.

6.24 Calcul différentiel dans un espace vectoriel normé

Nous développons dans cette section le concept de différentielle de fonction de et vers des espaces vectoriels normés au lieu de $\mathbb{R}^n$.

6.24.1 Différentielle

Définition 6.212.

Soit une application $f: E \rightarrow F$ entre deux espaces de Banach. Nous disons que f est **différentiable** en $a \in E$ si il existe une application linéaire continue³¹ $T: E \rightarrow F$ telle que

$$\lim_{h \rightarrow 0} \frac{f(a+h) - f(a) - T(h)}{\|h\|} = 0. \quad (6.450)$$

31. Nous demandons bien que le candidat différentielle soit continue; en dimension infinie ce n'est pas le cas de toutes les fonctions linéaires, comme le montre l'exemple 6.215.

L'application $a \mapsto T$ est la **différentielle** de f au point a et est notée df_a . L'application différentielle

$$\begin{aligned} df: E &\rightarrow \mathcal{L}(E, F) \\ a &\mapsto df_a \end{aligned} \quad (6.451)$$

est également très importante.

Définition 6.213.

Une application $f: E \rightarrow F$ est de **classe** C^1 lorsque l'application différentielle $df: E \rightarrow \mathcal{L}(E, F)$ est continue. Voir aussi les définitions 11.196 pour les applications de classe C^k .

Remarque 6.214.

L'application norme étant continue, le critère du théorème 5.133 est en réalité assez général. Par exemple à partir d'une application différentiable³² $f: X \rightarrow Y$ nous pouvons considérer la fonction réelle

$$a \mapsto \|df_a\| \quad (6.452)$$

où la norme est la norme opérateur³³. Si f est de classe C^1 alors cette application est continue et donc bornée sur un compact K de X .

6.24.2 (non ?) Différentiabilité des applications linéaires

Si E et F sont deux espaces vectoriels nous notons $\mathcal{L}(E, F)$ l'ensemble des applications linéaires de E vers F et $L(E, F)$ l'ensemble des applications linéaires continues de E vers F . Ces espaces seront bien entendu, sauf mention du contraire, toujours munis de la norme opérateur de la définition 6.86.

Exemple 6.215(Une application linéaire non continue)

Soit V l'espace vectoriel normé des suites *finies* de réels muni de la norme usuelle $\|c\| = \sqrt{\sum_{i=0}^{\infty} |c_i|^2}$ où la somme est finie. Nous nommons $\{e_k\}_{k \in \mathbb{N}}$ la base usuelle de cet espace, et nous considérons l'opérateur $f: V \rightarrow V$ donnée par $f(e_k) = ke_k$. C'est évidemment linéaire, mais ce n'est pas continu en zéro. En effet la suite $u_k = e_k/k$ converge vers 0 alors que $f(u_k) = e_k$ ne converge pas. $\triangle$

Cet exemple aurait pu également être donnée dans un espace de Hilbert, mais il aurait fallu parler de domaine.

Exemple 6.216(Une autre application linéaire non continue[91])

En dimension infinie, une application linéaire n'est pas toujours continue. Soit E l'espace des polynômes à coefficients réels sur $[0, 1]$ muni de la norme uniforme. L'application de dérivation $\varphi: E \rightarrow E$, $\varphi(P) = P'$ n'est pas continue.

Pour la voir nous considérons la suite $P_n = \frac{1}{n}X^n$. D'une part nous avons $P_n \rightarrow 0$ dans E parce que $P_n(x) = \frac{x^n}{n}$ avec $x \in [0, 1]$. Mais en même temps nous avons $\varphi(P_n) = X^{n-1}$ et donc $\|\varphi(P_n)\| = 1$.

Nous n'avons donc pas $\lim_{n \rightarrow \infty} \varphi(P_n) = \varphi(\lim_{n \rightarrow \infty} P_n)$ et l'application φ n'est pas continue en 0. Elle n'est donc continue nulle part par linéarité.

Nous avons utilisé le critère séquentiel de la continuité, voir la définition 5.121 et la proposition 5.122. $\triangle$

Nous avons cependant le résultat suivant.

Proposition 6.217 ([92] Continue si et seulement si bornée).

Soient E et F des espaces vectoriels normés, et $u: E \rightarrow F$ une application linéaire. Alors u est bornée³⁴ si et seulement si elle est continue.

32. Définition 6.212.

33. Définition 6.81.

34. Au sens où $\|u\| < \infty$ pour la norme opérateur.

Démonstration. Nous commençons par supposer que u est bornée. Pour tout $x, y \in E$ nous avons

$$\|u(x) - u(y)\| = \|u(x - y)\| \leq \|u\| \|x - y\|. \quad (6.453)$$

En particulier si $x_n \xrightarrow{E} x$ alors

$$0 \leq \|u(x_n) - u(x)\| \leq \|u\| \|x - x_n\| \rightarrow 0 \quad (6.454)$$

et u est continue en vertu de la caractérisation séquentielle de la continuité, proposition 5.122.

Supposons maintenant que $\|u\|$ ne soit pas borné, c'est à dire que l'ensemble $\{\|u(x)\| \mid \|x\| = 1\}$ ne soit pas borné. Alors pour tout $k \geq 1$ il existe $x_k \in B(0, 1)$ tel que $\|u(x_k)\| > k$. La suite x_k/k tend vers zéro parce que $\|x_k\| = 1$, mais $\|u(x_k)\| \geq 1$ pour tout k . Cela montre que u n'est pas continue. $\square$

Remarque 6.218.

Cette proposition permet de retrouver l'exemple 6.215 plus simplement. Si $\{e_k\}_{k \in \mathbb{N}}$ est une base d'un espace vectoriel normé formée de vecteurs de norme 1, alors l'opérateur linéaire donné par $u(e_k) = ke_k$ n'est pas borné et donc pas continu.

C'est également ce résultat qui montre que le produit scalaire est continu sur un espace de Hilbert par exemple.

Lemme 6.219.

Si f est linéaire et différentiable alors $df_a(u) = f(u)$.

Démonstration. En effet la linéarité de f donne

$$f(a + h) - f(a) - f(h) = 0 \quad (6.455)$$

pour tout h . Donc la limite (6.450) est nulle. Les applications linéaires non continues ne sont donc pas différentiables. $\square$

Lemme 6.220.

Une application linéaire continue est de classe C^∞ .

Démonstration. Soit $a \in E$. Étant donné que f est linéaire et continue, elle est différentiable et

$$\begin{aligned} df: E &\rightarrow L(E, F) \\ a &\mapsto f \end{aligned} \quad (6.456)$$

est une fonction constante et en particulier continue ; nous avons donc $f \in C^1$. Pour la différentielle seconde nous avons $d(df)_a = 0$ parce que $df(a + h) - df(a) = f - f = 0$. Toutes les différentielles suivantes sont nulles. $\square$

6.24.3 Dérivation en chaine et formule de Leibnitz

Proposition 6.221.

Soient $f_i: U \rightarrow F_i$, des fonctions de classe C^r où U est ouvert dans l'espace vectoriel normé E et les F_i sont des espaces vectoriels normés. Alors l'application

$$\begin{aligned} f &= f_1 \times \cdots \times f_n: U \rightarrow F_1 \times \cdots \times F_n \\ x &\mapsto (f_1(x), \dots, f_n(x)) \end{aligned} \quad (6.457)$$

est de classe C^r et

$$d^r f = d^r f_1 \times \cdots \times d^r f_n. \quad (6.458)$$

Démonstration. Soit $x \in U$ et $h \in E$. La différentiabilité des fonctions f_i donne

$$f_i(x+h) = f_i(x) + (df_i)_x(h) + \alpha_i(h) \quad (6.459)$$

avec $\lim_{h \rightarrow 0} \alpha_i(h)/\|h\| = 0$. Par conséquent

$$f(x+h) = (\dots, f_i(x) + (df_i)_x(h) + \alpha_i(h), \dots) = (\dots, f_i(x), \dots) + (\dots, (df_i)_x(h), \dots) + (\dots, \alpha_i(h), \dots). \quad (6.460)$$

Mais la définition 6.197 de la norme dans un espace produit donne

$$\lim_{h \rightarrow 0} \frac{\|(\alpha_1(h), \dots, \alpha_n(h))\|}{\|h\|} = 0, \quad (6.461)$$

ce qui nous permet de noter $\alpha(h) = (\alpha_1(h), \dots, \alpha_n(h))$ et avoir $\lim_{h \rightarrow 0} \alpha(h)/\|h\| = 0$. Avec tout ça nous avons bien

$$f(x+h) = f(x) + ((df_1)_x(h) + \dots + (df_n)_x(h)) + \alpha(h), \quad (6.462)$$

ce qui signifie que f est différentiable et

$$df_x = (df_1, \dots, df_n). \quad (6.463)$$

□

Théorème 6.222 (Différentielle de fonctions composées[5]).

Soient E, F et G des espaces vectoriels normés, U ouvert dans E et V ouvert dans F . Soient des applications de classe C^r ($r \geq 1$)

$$f: U \rightarrow V \quad (6.464a)$$

$$g: V \rightarrow G. \quad (6.464b)$$

Alors l'application $g \circ f: V \rightarrow G$ est de classe C^r et

$$d(g \circ f)_x = dg_{f(x)} \circ df_x. \quad (6.465)$$

Démonstration. Nous nous fixons $x \in U$. La fonction f est différentiable en $x \in U$ et g en $f(x)$, donc nous pouvons écrire

$$f(x+h) = f(x) + df_x(h) + \alpha(h) \quad (6.466)$$

et

$$g(f(x) + u) = g(f(x)) + dg_{f(x)}(u) + \beta(u) \quad (6.467)$$

où la fonction α a la propriété que

$$\lim_{h \rightarrow 0} \frac{\|\alpha(h)\|}{\|h\|} = 0; \quad (6.468)$$

et la même chose pour β . La fonction composée en $x+h$ s'écrit donc

$$(g \circ f)(x+h) = g(f(x) + df_x(h) + \alpha(h)) = g(f(x)) + dg_{f(x)}(df_x(h) + \alpha(h)) + \beta(df_x(h) + \alpha(h)). \quad (6.469)$$

Nous montrons que tous les «petits» termes de cette formule peuvent être groupés. D'abord si h est proche de 0, nous avons

$$\frac{\|df_x(h) + \alpha(h)\|}{\|h\|} \leq \frac{\|df_x\| \|h\|}{\|h\|} + \frac{\|\alpha(h)\|}{\|h\|}. \quad (6.470)$$

Si h est petit, le second terme est arbitrairement petit, donc en prenant n'importe que $M > \|df_x\|$ nous avons

$$\frac{\|df_x(h) + \alpha(h)\|}{\|h\|} \leq M. \quad (6.471)$$

Par ailleurs, nous avons

$$\frac{\|\beta(df_x(h) + \alpha(h))\|}{\|h\|} = \frac{\|\beta(df_x(h) + \alpha(h))\|}{\|df_x(h) + \alpha(h)\|} \frac{\|df_x(h) + \alpha(h)\|}{\|h\|} \leq M \frac{\|\beta(df_x(h) + \alpha(h))\|}{\|df_x(h) + \alpha(h)\|}. \quad (6.472)$$

Vu que la fraction est du type $\frac{\beta(f(h))}{f(h)}$ avec $\lim_{h \rightarrow 0} f(h) = 0$, la fraction tend vers zéro lorsque $h \rightarrow 0$. En posant

$$\gamma_1(h) = \beta(df_x(h) + \alpha(h)) \quad (6.473)$$

nous avons $\lim_{h \rightarrow 0} \gamma_1(h)/\|h\| = 0$.

L'autre candidat à être un petit terme dans (6.469) est traité en utilisant la proposition 6.88 :

$$\|dg_{f(x)}(\alpha(h))\| \leq \|dg_{f(x)}\| \|\alpha(h)\|. \quad (6.474)$$

Donc

$$\frac{\|dg_{f(x)}(\alpha(h))\|}{\|h\|} \leq \|dg_{f(x)}\| \frac{\|\alpha(h)\|}{\|h\|}, \quad (6.475)$$

ce qui nous permet de poser

$$\gamma_2(h) = dg_{f(x)}(\alpha(h)) \quad (6.476)$$

avec γ_2 qui a la même propriété que γ_1 . Avec tout cela, en posant $\gamma = \gamma_1 + \gamma_2$ nous récrivons

$$(g \circ f)(x + h) = g(f(x)) + dg_{f(x)}(df_x(h)) + \gamma(h) \quad (6.477)$$

avec $\lim_{h \rightarrow 0} \frac{\gamma(h)}{\|h\|} = 0$. Tout cela pour dire que

$$\lim_{h \rightarrow 0} \frac{(g \circ f)(x + h) - (g \circ f)(x) - (dg_{f(x)} \circ df_x)(h)}{\|h\|} = 0, \quad (6.478)$$

ce qui signifie que

$$d(g \circ f)_x = dg_{f(x)} \circ df_x. \quad (6.479)$$

Nous avons donc montré que si f et g sont différentiables, alors $g \circ f$ est différentiable avec différentielle donnée par (6.465).

Nous passons à la régularité. Nous supposons maintenant que f et g sont de classe C^r et nous considérons l'application

$$\begin{aligned} \varphi: L(F, G) \times L(E, F) &\rightarrow L(E, G) \\ (A, B) &\mapsto A \circ B. \end{aligned} \quad (6.480)$$

Montrons que l'application φ est continue en montrant qu'elle est bornée³⁵. Pour cela nous écrivons la norme opérateur

$$\|\varphi\| = \sup_{\|(A,B)\|=1} \|\varphi(A, B)\| = \sup_{\|(A,B)\|=1} \|A \circ B\| \leq \sup_{\|(A,B)\|=1} \|A\| \|B\| \leq 1. \quad (6.481)$$

Pour ce calcul nous avons utilisé le fait que la norme opérateur soit une norme algébrique (proposition 6.88) ainsi que la définition 6.197 de la norme sur un espace produit pour la dernière majoration. L'application φ est donc continue et donc C^∞ par le lemme 6.220. Nous considérons également l'application

$$\begin{aligned} \psi: U &\rightarrow L(F, G) \times L(E, F) \\ x &\mapsto (dg_{f(x)}, df_x). \end{aligned} \quad (6.482)$$

Vu que f et g sont C^1 , l'application ψ est continue. Ces deux applications φ et ψ sont choisies pour avoir

$$(\varphi \circ \psi)(x) = \varphi(dg_{f(x)}, df_x) = dg_{f(x)} \circ df_x, \quad (6.483)$$

c'est à dire $\varphi \circ \psi = d(g \circ f)$. Les applications φ et ψ étant continues, l'application $d(g \circ f)$ est continue, ce qui prouve que $g \circ f$ est C^1 .

35. Proposition 6.217.

Si f et g sont C^r alors $dg \in C^{r-1}$ et $dg \circ f \in C^{r-1}$ où il ne faut pas se tromper : $dg: F \rightarrow L(F, G)$ et $f: U \rightarrow F$; la composée est $dg \circ f: x \mapsto dg_{f(x)} \in L(F, G)$.

Pour la récurrence nous supposons que $f, g \in C^{r-1}$ implique $g \circ f \in C^{r-1}$ pour un certain $r \geq 2$ (parce que nous venons de prouver cela avec $r = 1$ et $r = 2$). Soient $f, g \in C^r$ et montrons que $g \circ f \in C^r$. Par la proposition 6.221 nous avons

$$\psi = dg \circ f \times df \in C^{r-1}, \quad (6.484)$$

et donc $d(g \circ f) = \varphi \circ \psi \in C^{r-1}$, ce qui signifie que $g \circ f \in C^r$. $\square$

On fixe maintenant une définition largement utilisée dans la suite.

Définition 6.223.

Soient U et V , deux ouverts d'un espace vectoriel normé. Une application f de U dans V est un **difféomorphisme** si elle est bijective, différentiable et dont l'inverse $f^{-1}: V \rightarrow U$ est aussi différentiable.

Remarque 6.224.

Il n'est pas possible d'avoir une application inversible d'un ouvert de $\mathbb{R}^m$ vers un ouvert de $\mathbb{R}^n$ si $m \neq n$. Il n'y a donc pas de notion de difféomorphismes entre ouverts de dimensions différentes.

Lemme 6.225.

Si $f: U \rightarrow V$ est une difféomorphisme³⁶ alors pour tout $a \in U$, l'application df_a est inversible et

$$(df_a)^{-1} = (df^{-1})_{f(a)}. \quad (6.485)$$

Démonstration. Il suffit d'apercevoir qu'en vertu de la règle de différentiation en chaîne 6.465,

$$(df_a)(df^{-1})_{f(a)} = f(f \circ f^{-1})_{f(a)} = \text{Id}. \quad (6.486)$$

$\square$

Lemme 6.226 (Leibnitz pour les formes bilinéaires[5]).

Si $B: E \times F \rightarrow G$ est bilinéaire et continue, elle est C^∞ et

$$dB_{(x,y)}(u, v) = B(x, v) + B(u, y). \quad (6.487)$$

Démonstration. D'abord le membre de droite de (6.487) est une application linéaire et continue, donc c'est un bon candidat à être différentielle. Nous allons prouver que ça l'est, ce qui prouvera la différentiabilité de B . Avec ce candidat, le numérateur de la définition (6.450) s'écrit dans notre cas

$$B((x, y) + (u, v)) - B(x, y) - B(x, v) - B(u, y) = B(u, v). \quad (6.488)$$

Il reste à voir que

$$\lim_{(u,v) \rightarrow (0,0)} \frac{B(u, v)}{\|(u, v)\|} = 0 \quad (6.489)$$

Par l'équation (6.448) nous avons

$$\frac{\|B(u, v)\|}{\|(u, v)\|} \leq \frac{\|B\| \|u\| \|v\|}{\|u\|} = \|B\| \|v\| \quad (6.490)$$

parce que $\|(u, v)\| \geq \|u\|$. À partir de là il est maintenant clair que

$$\lim_{(u,v) \rightarrow (0,0)} \frac{\|B(u, v)\|}{\|(u, v)\|} = 0, \quad (6.491)$$

ce qu'il fallait. $\square$

36. Définition 6.223

Proposition 6.227 (Règle de Leibnitz[5]).

Soient E, F_1, F_2 des espaces vectoriels normés, U ouvert dans E et des applications de classe C^r ($r \geq 1$)

$$f_1: U \rightarrow F_1 \quad (6.492a)$$

$$f_2: U \rightarrow F_2 \quad (6.492b)$$

$$(6.492c)$$

et $B \in L(F_1 \times F_2, G)$. Alors l'application

$$\begin{aligned} \varphi: U &\rightarrow G \\ x &\mapsto B(f_1(x), f_2(x)) \end{aligned} \quad (6.493)$$

est de classe C^r et

$$d\varphi_x(u) = \varphi((df_1)_x(u), f_2(x)) + \varphi(f_1(x), (df_2)_x(u)). \quad (6.494)$$

Démonstration. Par hypothèse B est continue (c'est la définition de l'espace L), et donc C^∞ par le lemme 6.226. Par ailleurs la fonction $f_1 \times f_2$ est de classe C^r parce que f_1 et f_2 le sont et parce que la proposition 6.221 le dit. L'application composée $B \circ (f_1 \times f_2)$ est donc également de classe C^r par le théorème 6.222.

Il ne nous reste donc qu'à prouver la formule 6.494. En utilisant la différentielle du produit cartésien³⁷ nous avons

$$f(B \circ (f_1 \times f_2))_x(h) = dB_{(f_1 \times f_2)(x)}((df_1)_x(h), (df_2)_x(h)). \quad (6.495)$$

Nous développons cela en utilisant le lemme 6.226 :

$$d(B \circ (f_1 \times f_2))_x(h) = dB_{(f_1(x), f_2(x))}((df_1)_x(h), (df_2)_x(h)) \quad (6.496a)$$

$$= B(f_1(x), (df_2)_x(h)) + B((df_1)_x(h), f_2(x)), \quad (6.496b)$$

comme souhaité. $\square$

6.24.4 Différentielle partielle

Définition 6.228 (Différentielle partielle).

Soient E, F et G des espaces vectoriels normés et une fonction $f: E \times F \rightarrow G$. Nous définissons sa **différentielle partielle** sur l'espace E par

$$\begin{aligned} d_1 f_{(x_0, y_0)}: E &\rightarrow G \\ u &\mapsto \frac{d}{dt} \left[f(x_0 + tu, y_0) \right]_{t=0}. \end{aligned} \quad (6.497)$$

La différentielle d_2 se définit de la même façon.

Proposition 6.229 ([5]).

Soient E_1, E_2 et F des espaces vectoriels normés, soit un ouvert $U \subset E_1 \times E_2$ et une fonction $f: U \rightarrow F$.

(1) Si f est différentiable alors les différentielles partielles existent et

$$d_1 f_{(x_0, y_0)}(u) = df_{(x_0, y_0)}(u, 0) \quad (6.498a)$$

$$d_2 f_{(x_0, y_0)}(v) = df_{(x_0, y_0)}(0, v) \quad (6.498b)$$

où $u \in E_1$ et $v \in E_2$.

37. Proposition 6.221.

(2) Si f est différentiable alors

$$df_{(x_0, y_0)}(u, v) = d_1 f_{(x_0, y_0)}(u) + d_2 f_{(x_0, y_0)}(v). \quad (6.499)$$

Démonstration. Nous posons $\alpha = (x_0, y_0) \in U$ et

$$\begin{aligned} j_\alpha^{(1)}: E_1 &\rightarrow E_1 \times E_2 \\ x &\mapsto (x, y_0). \end{aligned} \quad (6.500)$$

C'est une fonction de classe C^∞ et

$$(dj_\alpha^{(1)})_{x_0}(u) = \frac{d}{dt} [j_\alpha^{(1)}(x_0 + tu)]_{t=0} = \frac{d}{dt} [(x_0 + tu, y_0)]_{t=0} = (u, 0). \quad (6.501)$$

D'autre part

$$(d_1 f)_\alpha(u) = \frac{d}{dt} [f(x_0 + tu, y_0)]_{t=0} \quad (6.502a)$$

$$= \frac{d}{dt} [(f \circ j_\alpha^{(1)})(x_0 + tu)]_{t=0} \quad (6.502b)$$

$$= (d(f \circ j_\alpha^{(1)}))_{x_0}(u). \quad (6.502c)$$

À ce moment nous utilisons la règle des différentielles composées 6.222 pour dire que

$$(d_1 f)_\alpha(u) = df_{j_\alpha^{(1)}(x_0)} \circ (dj_\alpha^{(1)})_{x_0}(u) = df_\alpha(u, 0). \quad (6.503)$$

Voilà qui prouve déjà le point (1).

Pour la suite nous considérons les fonctions

$$\begin{aligned} P_1(x, y) &= x, & J_1(u) &= (u, 0), \\ P_2(x, y) &= y, & J_2(v) &= (0, v) \end{aligned} \quad (6.504)$$

et nous avons l'égalité évidente

$$J_1 \circ P_1 + J_2 \circ P_2 = \mathbb{1} \quad (6.505)$$

sur $E_1 \times E_2$. En appliquant df_α à cette dernière égalité, en appliquant à (u, v) et en utilisant la linéarité de df_α nous trouvons

$$df_\alpha(u, v) = df_\alpha((J_1 \circ P_1)(u, v)) + df_\alpha((J_2 \circ P_2)(u, v)) \quad (6.506a)$$

$$= df_\alpha(u, 0) + df_\alpha(0, v) \quad (6.506b)$$

$$= (d_1 f)_\alpha(u) + (d_2 f)_\alpha(v) \quad (6.506c)$$

où nous avons utilisé le point (1) pour la dernière égalité. $\square$

6.24.5 Formule des accroissements finis

Il en existe plusieurs formes :

- (1) Une version adaptée aux espaces de dimension finie est le théorème 11.187.
- (2) Pour les fonctions $\mathbb{R} \rightarrow \mathbb{R}$ en le théorème 11.99.
- (3) Espaces vectoriels normés, théorème 6.231

Proposition 6.230.

Soient $a < b$ dans $\mathbb{R}$ et deux fonctions

$$f: [a, b] \rightarrow E \quad (6.507a)$$

$$g: [a, b] \rightarrow \mathbb{R} \quad (6.507b)$$

continues sur $[a, b]$ et dérivables sur $]a, b[$. Si pour tout $t \in]a, b[$ nous avons $\|f'(t)\| \leq g'(t)$ alors

$$\|f(b) - f(a)\| \leq g(b) - g(a). \quad (6.508)$$

Démonstration. Soit $\epsilon > 0$ et la fonction

$$\begin{aligned}\varphi_\epsilon: [a, b] &\rightarrow \mathbb{R} \\ t &\mapsto \|f(t) - f(a)\| - g(t) - \epsilon t.\end{aligned}\tag{6.509}$$

Cela est une fonction continue réelle à variable réelle. En particulier pour tout $u \in]a, b[$ la fonction φ_ϵ est continue sur le compact $[u, b]$ et donc y atteint son minimum en un certain point $c \in [u, b]$; c'est le bon vieux théorème de Weierstrass 5.133. Nous commençons par montrer que pour tout u , ledit minimum ne peut être que b . Pour cela nous allons montrer que si $t \in [u, b[$, alors $\varphi_\epsilon(s) < \varphi_\epsilon(t)$ pour un certain $s > t$. Par continuité si s est proche de t nous avons

$$\left\| \frac{f(s) - f(t)}{s - t} \right\| - \frac{\epsilon}{2} < \|f'(t)\| < g'(t) + \frac{\epsilon}{2} = \frac{g(s) - g(t)}{s - t} + \frac{\epsilon}{2}.\tag{6.510}$$

Ces inégalités proviennent de la limite

$$\lim_{s \rightarrow t} \frac{f(s) - f(t)}{s - t} = f'(t),\tag{6.511}$$

donc si s et t sont proches,

$$\left\| \frac{f(s) - f(t)}{s - t} - f'(t) \right\|\tag{6.512}$$

est petit. Si $s > t$ nous pouvons oublier des valeurs absolues et transformer l'inégalité en

$$\|f(s) - f(t)\| < g(s) - g(t) + \epsilon(s - t).\tag{6.513}$$

Utilisant cela et l'inégalité triangulaire,

$$\varphi_\epsilon(s) \leq \|f(s) - f(t)\| + \|f(t) - f(a)\| - g(s) - \epsilon s\tag{6.514a}$$

$$\leq g(s) - g(t) + \epsilon s - \epsilon t + \|f(t) - f(a)\| - g(s) - \epsilon s\tag{6.514b}$$

$$= \varphi_\epsilon(t).\tag{6.514c}$$

Donc nous avons bien $\varphi_\epsilon(s) < \varphi_\epsilon(t)$ avec l'inégalité stricte. Par conséquent pour tout $u \in]a, b[$ nous avons $\varphi_\epsilon(b) < \varphi_\epsilon(u)$ et en prenant la limite $u \rightarrow a$ nous avons

$$\varphi_\epsilon(b) \leq \varphi_\epsilon(a).\tag{6.515}$$

Cette inégalité donne immédiatement

$$\|f(b) - f(a)\| \leq g(b) - g(a) + \epsilon(b - a)\tag{6.516}$$

pour tout $\epsilon > 0$ et donc

$$\|f(b) - f(a)\| \leq g(b) - g(a).\tag{6.517}$$

□

Théorème 6.231 (Théorème des accroissements finis).

Soient E et F des espaces vectoriels normés, U ouvert dans E et une application différentiable $f: U \rightarrow F$. Pour tout segment $[a, b] \subset U$ nous avons

$$\|f(b) - f(a)\| \leq \left(\sup_{x \in [a, b]} \|df_x\| \right) \|b - a\|.\tag{6.518}$$

Démonstration. Nous prenons les applications

$$\begin{aligned}k: [0, 1] &\rightarrow E \\ t &\mapsto f((1 - t)a + tb)\end{aligned}\tag{6.519}$$

et

$$\begin{aligned} g: [0, 1] &\rightarrow \mathbb{R} \\ t &\mapsto t \sup_{x \in [a, b]} \|df_x\| \|b - a\|. \end{aligned} \quad (6.520)$$

Pour tout t nous avons $g'(t) = M\|b - a\|$ où il n'est besoin de dire ce qu'est M . D'un autre côté nous avons aussi

$$\begin{aligned} k'(t) &= \lim_{\epsilon \rightarrow 0} \frac{f((1-t-\epsilon)a + (t+\epsilon)b) - f((1-t)a + tb)}{\epsilon} \\ &= \frac{d}{d\epsilon} \left[f((1-t)a + tb + \epsilon(b-a)) \right]_{\epsilon=0} \\ &= df_{(1-t)a+tb}(b-a) \end{aligned} \quad (6.521)$$

où nous avons utilisé l'hypothèse de différentiabilité de f sur $[a, b]$ et donc en $(1-t)a + tb$. Nous avons donc

$$\|k'(t)\| \leq \|b - a\| \|df_{(1-t)a+tb}\| \leq M\|b - a\| = g'(t) \quad (6.522)$$

La proposition 6.230 est donc utilisable et

$$\|k(1) - k(0)\| = g(1) - g(0), \quad (6.523)$$

c'est à dire

$$\|f(b) - f(a)\| = M\|b - a\| \quad (6.524)$$

comme il se doit. $\square$

Proposition 6.232.

Soient E et F des espaces vectoriels normés, U ouvert dans E et une application $f: U \rightarrow F$. Soient $a, b \in U$ tels que $[a, b] \subset U$. Nous posons $u = (b - a)/\|b - a\|$ et nous supposons que pour tout $x \in [a, b]$, la dérivée directionnelle

$$\frac{\partial f}{\partial u}(x) = \frac{d}{dt} \left[f(x + tu) \right]_{t=0} \quad (6.525)$$

existe. Nous supposons de plus que $\frac{\partial f}{\partial u}(x)$ est continue en $x = a$. Alors

$$\|f(b) - f(a)\| \leq \left(\sup_{x \in [a, b]} \left\| \frac{\partial f}{\partial u}(x) \right\| \right) \|b - a\|. \quad (6.526)$$

Démonstration. Nous posons évidemment

$$M = \sup_{x \in [a, b]} \left\| \frac{\partial f}{\partial u}(x) \right\| \quad (6.527)$$

et nous considérons les fonctions

$$k(t) = f((1-t)a + tb) \quad (6.528)$$

et

$$g(t) = tM\|b - a\|. \quad (6.529)$$

Pour alléger les notations nous posons $x = (1-t)a + tb$ et nous calculons avec un petit changement de variables dans la limite :

$$k'(t) = \frac{d}{d\epsilon} \left[f(x + \epsilon(b-a)) \right]_{\epsilon=0} = \|b - a\| \frac{d}{d\epsilon} \left[f\left(x + \frac{\epsilon}{\|b-a\|}(b-a)\right) \right]_{\epsilon=0} = \|b - a\| \frac{\partial f}{\partial u}(x), \quad (6.530)$$

et donc encore une fois nous avons

$$\|k'(t)\| \leq g'(t), \quad (6.531)$$

ce qui donne

$$\|k(1) - k(0)\| = g(1) - g(0), \quad (6.532)$$

c'est à dire

$$\|f(b) - f(a)\| \leq \sup_{x \in [a, b]} \left\| \frac{\partial f}{\partial u}(x) \right\| \|b - a\|. \quad (6.533)$$

□

Théorème 6.233.

Soient E, V deux espaces vectoriels normés, une application $f: E \rightarrow V$, un point $a \in E$ tel que pour tout $u \in E$, la dérivée

$$\frac{d}{dt} \left[f(x + tu) \right]_{t=0} \quad (6.534)$$

existe pour tout $x \in B(a, r)$ et est continue (par rapport à x) en $x = a$. Nous supposons de plus que³⁸

$$\frac{\partial f}{\partial u}(a) = 0 \quad (6.535)$$

pour tout $u \in E$. Alors f est différentiable en a et

$$df_a = 0 \quad (6.536)$$

Démonstration. Soit $\epsilon > 0$. Pourvu que $\|h\|$ soit assez petit pour que $a + h \in B(a, r)$, la proposition 6.232 nous donne

$$\|f(a + h) - f(a)\| \leq \sup_{x \in [a, a+h]} \left\| \frac{\partial f}{\partial u}(x) \right\| \|h\| \quad (6.537)$$

où $u = h/\|h\|$. Par continuité de $\partial_u f(x)$ en $x = a$ et par le fait que cela vaut 0 en $x = a$, il existe un $\delta > 0$ tel que si $\|h\| < \delta$ alors

$$\left\| \frac{\partial f}{\partial u}(a + h) \right\| \leq \epsilon. \quad (6.538)$$

Pour de tels h nous avons

$$\|f(a + h) - f(a)\| \leq \epsilon \|h\|, \quad (6.539)$$

ce qui prouve que l'application linéaire $T(u) = 0$ convient parfaitement pour faire fonctionner la définition 6.212. □

6.24.6 L'inverse, sa différentielle

Si E est un espace de Banach, nous sommes intéressé à l'espace $\text{GL}(E)$ des endomorphismes inversibles de E sur E . Cet ensemble est métrique par la formule usuelle

$$\|T\| = \sup_{\|x\|=1} \|T(x)\|_E. \quad (6.540)$$

Théorème 6.234 (Inverse dans $\text{GL}(E)$ [93, 5]).

Soient E et F des espaces vectoriels normés.

(1) L'ensemble $\text{GL}(E)$ est ouvert dans $\text{End}(E)$.

(2) L'application inverse

$$\begin{aligned} i: \text{GL}(E, F) &\rightarrow \text{GL}(F, E) \\ u &\mapsto u^{-1} \end{aligned} \quad (6.541)$$

est de classe C^∞ et

$$di_{u_0}(h) = -u_0^{-1} \circ h \circ u_0^{-1} \quad (6.542)$$

pour tout $h \in \text{End}(E)$

Démonstration. Nous supposons que $\text{GL}(E, F)$ n'est pas vide, sinon ce n'est pas du jeu.

38. Je ne suis pas certain que cette hypothèse soit nécessaire, voir la question (19) de la page 60.

Cas de dimension finie Si la dimension de E et F est finie, elles doivent être égales, sinon il n'y a pas de fonctions inversibles $E \rightarrow F$. L'ensemble $\text{GL}(E, F)$ est donc naturellement $\text{GL}(n, \mathbb{R})$. Un élément de $\text{M}(n, \mathbb{R})$ est dans $\text{GL}(n, \mathbb{R})$ si et seulement si son déterminant est non nul. Le déterminant étant une fonction continue (polynomiale) en les entrées de la matrice, l'ensemble $\text{GL}(n, \mathbb{R})$ est ouvert dans $\text{M}(n, \mathbb{R})$.

Même idée pour la régularité de la fonction $i: \text{GL}(n, \mathbb{R}) \rightarrow \text{GL}(n, \mathbb{R}), X \mapsto X^{-1}$. Les entrées de X^{-1} sont les cofacteurs de X divisé par $\det(X)$, et donc des polynômes en les entrées de X divisés par un polynôme qui ne s'annule pas sur $\text{GL}(n, \mathbb{R})$, et donc sur un ouvert autour de X et de X^{-1} . Bref, tout est C^∞ .

Le reste de la preuve parle de la dimension infinie.

Ouvert autour de l'identité Nous commençons par prouver que $B(\mathbb{1}, 1) \subset \text{GL}(E)$. Pour cela il suffit de remarquer que si $\|u\| < 1$ alors le lemme 6.157 nous donne un inverse de $(1 + u)$ en la personne de $\sum_{k=0}^{\infty} (-u)^k$.

Ouvert en général Soit maintenant $u_0 \in \text{GL}(E)$. Si $\|u\| < \frac{1}{\|u_0^{-1}\|}$ alors $\|u_0^{-1}u\| < 1$, ce qui signifie que

$$\mathbb{1} + u_0^{-1}u \quad (6.543)$$

est inversible. Mais $u_0 + u = u_0(\mathbb{1} + u_0^{-1}u)$, donc $u_0 + u \in \text{GL}(E)$ ce qui signifie que

$$B\left(u_0, \frac{1}{\|u_0^{-1}\|}\right) \subset \text{GL}(E). \quad (6.544)$$

Différentielle en l'identité Nous commençons par prouver que $di_{\mathbb{1}}(u) = -u$. Pour cela nous posons

$$\alpha(h) = \sum_{k=2}^{\infty} (-1)^k h^k \quad (6.545)$$

et nous calculons

$$di_{\mathbb{1}}(u) = \frac{d}{dt} \left[i(\mathbb{1} + tu) \right]_{t=0} = \frac{d}{dt} \left[\mathbb{1} - tu + \alpha(tu) \right]_{t=0}. \quad (6.546)$$

Il suffit de prouver que $\frac{d}{dt} [\alpha(tu)]_{t=0} = 0$ pour conclure que $di_{\mathbb{1}}(u) = -u$. Pour cela, nous remarquons que $\alpha(0) = 0$ et donc que

$$\frac{d}{dt} [\alpha(tu)]_{t=0} = \lim_{t \rightarrow 0} \frac{\alpha(tu) - \alpha(0)}{t} \quad (6.547a)$$

$$= \lim_{t \rightarrow 0} \sum_{k=2}^{\infty} (-1)^k \frac{(tu)^k}{t} \quad (6.547b)$$

$$= - \lim_{t \rightarrow 0} u \sum_{k=1}^{\infty} (-1)^k t^k u^k. \quad (6.547c)$$

La norme de ce qui est dans la limite est majorée par

$$\|u\| \sum_{k=1}^{\infty} \|tu\|^k = \|u\| \left(\frac{1}{1 - \|tu\|} - 1 \right), \quad (6.548)$$

et cela tend vers zéro lorsque $t \rightarrow 0$. Nous avons utilisé la somme 6.348 de la série géométrique. Nous avons bien prouvé que $di_{\mathbb{1}}(u) = -u$.

Différentielle en général Soit maintenant $u_0 \in \text{GL}(E)$ et $h \in \text{End}(E)$ tel que $u_0 + h \in \text{GL}(E)$; par le premier point, il suffit de prendre $\|h\|$ suffisamment petit. Vu que $u_0 + h = u_0(\mathbb{1} + u_0^{-1}h)$ nous avons

$$(u_0 + h)^{-1} = (\mathbb{1} + u_0^{-1}h)^{-1} u_0^{-1}. \quad (6.549)$$

Nous pouvons donc calculer

$$(u_0 + h)^{-1} = (\mathbb{1} - u_0^{-1}h + \alpha(u_0^{-1}h))u_0^{-1} = u_0^{-1} - u_0^{-1}hu_0^{-1} + \alpha(u_0^{-1}h)u_0^{-1}, \quad (6.550)$$

et ensuite

$$di_{u_0}(h) = \frac{d}{dt} \left[i(u_0 + th) \right]_{t=0} = \frac{d}{dt} \left[u_0^{-1} - tu_0^{-1}hu_0^{-1} + \alpha(tu_0^{-1}h)u_0^{-1} \right]_{t=0}, \quad (6.551)$$

mais nous avons déjà vu que

$$\frac{d}{dt} \left[\alpha(th) \right]_{t=0} = 0, \quad (6.552)$$

donc

$$di_{u_0}(h) = -u_0^{-1}hu_0^{-1} \quad (6.553)$$

Cela donne la différentielle de l'application inverse.

Continuité de l'inverse L'application i est continue parce que différentiable.

L'inverse est C^∞ Nous allons écrire la fonction inverse comme une composée. Soient les applications

$$\begin{aligned} B: L(F, E) \times L(F, E) &\rightarrow L(L(E, F), L(F, E)) \\ B(\psi_1, \psi_2)(A) &= -\psi_1 \circ A \circ \psi_2 \end{aligned} \quad (6.554)$$

et

$$\begin{aligned} \Delta: L(F, E) &\rightarrow L(F, E) \times L(F, E) \\ \varphi &\mapsto (\varphi, \varphi) \end{aligned} \quad (6.555)$$

Nous avons alors

$$di = B \circ \Delta \circ i. \quad (6.556)$$

L'application Δ est de classe C^∞ . Nous devons voir que B l'est aussi. Pour le voir nous commençons par prouver qu'elle est bornée :

$$\begin{aligned} \|B\| &= \sup_{\|\psi_1\|, \|\psi_2\|=1} \|B(\psi_1, \psi_2)\|_{\mathcal{L}(L(E, F), L(F, E))} \\ &= \sup_{\|\psi_1\|, \|\psi_2\|=1} \sup_{\|A\|=1} \|\psi_1 \circ A \circ \psi_2\|_{L(F, E)} \\ &\leq \sup_{\|\psi_1\|, \|\psi_2\|=1} \sup_{\|A\|=1} \|\psi_1\| \|A\| \|\psi_2\| \\ &\leq 1. \end{aligned} \quad (6.557)$$

Donc B est bien bornée et par conséquent continue. Une application bilinéaire continue est C^∞ par le lemme 6.226. La décomposition $di = B \circ \Delta \circ i$ nous donne donc que $i \in C^\infty$ dès que i est continue, ce que nous avons déjà montré. □

6.24.7 Projection orthogonale

Le théorème suivant n'est pas indispensablissime parce qu'il est le même que le théorème de la projection sur les espaces de Hilbert³⁹. Cependant la partie existence est plus simple en se limitant au cas de dimension finie.

Théorème 6.235 (Théorème de la projection).

Soit E un espace vectoriel réel ou complexe de dimension finie, $x \in E$, et C un sous ensemble fermé convexe de E .

(1) Les deux conditions suivantes sur $y \in E$ sont équivalentes :

(a) $\|x - y\| = \inf \{\|x - z\| \text{ tel que } z \in C\}$,

39. Théorème 17.6

(b) pour tout $z \in C$, $\operatorname{Re}\langle x - y, z - y \rangle \leq 0$.

(2) Il existe un unique $y \in E$, noté $y = \operatorname{proj}_C(x)$ vérifiant ces conditions.

Démonstration. Nous commençons par prouver l'existence et l'unicité d'un élément dans C vérifiant la première condition. Ensuite nous verrons l'équivalence.

Existence Soit $z_0 \in C$ et $r = \|x - z_0\|$. La boule fermée $\overline{B}(x, r)$ est compacte⁴⁰ et intersecte C . Vu que C est fermé, l'ensemble $C' = C \cap \overline{B}(x, r)$ est compact. Tous les points qui minimisent la distance entre x et C sont dans C' ; la fonction

$$\begin{aligned} C' &\rightarrow \mathbb{R} \\ z &\mapsto d(x, z) \end{aligned} \quad (6.558)$$

est continue sur un compact et donc a un minimum qu'elle atteint⁴¹. Un point P réalisant ce minimum prouve l'existence d'un point vérifiant la première condition.

Unicité Soient y_1 et y_2 , deux éléments de C minimisant la distance avec x , et soit d ce minimum. Nous avons par l'identité du parallélogramme (6.209) que

$$\|y_1 - y_2\|^2 = -4 \left\| \frac{y_1 + y_2 - x}{2} \right\|^2 + 2\|y_1 - x\|^2 + 2\|y_2 - x\|^2 \leq -4d + 2d + 2d = 0. \quad (6.559)$$

Par conséquent $y_1 = y_2$.

(1)a $\Rightarrow$ (1)b Soit $z \in C$ et $t \in]0, 1[$; nous notons $P = \operatorname{proj}_C x$. Par convexité le point $z = ty + (1 - t)P$ est dans C , et par conséquent,

$$\|x - P\|^2 \leq \|x - tz - (1 - t)P\|^2 = \|(x - P) - t(z - P)\|^2. \quad (6.560)$$

Nous sommes dans un cas $\|a\|^2 \leq \|a - b\|^2$, qui implique $2\operatorname{Re}\langle a, b \rangle \leq \|b\|^2$. Dans notre cas,

$$2\operatorname{Re}\langle x - P, t(z - P) \rangle \leq t^2\|z - P\|^2. \quad (6.561)$$

En divisant par t et en faisant $t \rightarrow 0$ nous trouvons l'inégalité demandée :

$$2\operatorname{Re}\langle x - P, z - P \rangle \leq 0. \quad (6.562)$$

(1)b $\Rightarrow$ (1)a Soit un point $P \in C$ vérifiant

$$\operatorname{Re}\langle x - P, z - P \rangle \leq 0 \quad (6.563)$$

pour tout $z \in C$. Alors en notant $a = x - P$ et $b = P - z$,

$$\begin{aligned} \|x - z\|^2 &= \|x - P + P - z\|^2 = \|a + b\|^2 \\ &= \|a\|^2 + \|b\|^2 + 2\operatorname{Re}\langle a, b \rangle \\ &= \|a\|^2 + \|b\|^2 - 2\operatorname{Re}\langle x - P, z - P \rangle \\ &\geq \|b\|^2, \end{aligned} \quad (6.564)$$

ce qu'il fallait.

□

6.25 Polynôme d'endomorphismes

Soit A un anneau commutatif et $\mathbb{K}$, un corps commutatif. L'injection canonique $A \rightarrow A[X]$ se prolonge en une injection

$$\mathbb{M}(A) \rightarrow \mathbb{M}(A[X]). \quad (6.565)$$

40. C'est ceci qui ne marche plus en dimension infinie.

41. Théorème 5.110.

6.25.1 Polynômes d'endomorphismes

Soit $u \in \text{End}(E)$ où E est un $\mathbb{K}$ -espace vectoriel. Nous considérons l'application

$$\begin{aligned}\varphi_u: \mathbb{K}[X] &\rightarrow \text{End}(E) \\ P &\mapsto P(u).\end{aligned}\tag{6.566}$$

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 que endomorphisme de E .

Lemme 6.236.

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

$$(PQ)(u) = P(u) \circ Q(u).\tag{6.567}$$

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

$$\sum_l a_l b_{k-l}.\tag{6.568}$$

Par conséquent $(PQ)(u)$ contient $\sum_l a_l b_{k-l} u^k$. Par ailleurs $P(u) \circ Q(u)$ est donné par

$$\sum_i a_i u^i \left(\sum_j b_j u^j \right) (x) = \sum_{ij} a_i b_j u^{i+j}(x).\tag{6.569}$$

Le coefficient du terme en u^k est bien le même que celui donné par (6.568). $\square$

Théorème 6.237 (Décomposition des noyaux ou lemme des noyaux).

Soit u un endomorphisme du $\mathbb{K}$ -espace vectoriel E . Soit $P \in \mathbb{K}[X]$ un polynôme tel que $P(u) = 0$. Nous supposons que P s'écrit comme le produit $P = P_1 \dots P_n$ de polynômes deux à deux étrangers⁴². Alors

$$E = \ker P_1(u) \oplus \dots \oplus \ker P_n(u).\tag{6.570}$$

De plus les projecteurs associés à cette décomposition sont des polynômes en u .

Ce résultat est utilisé pour prouver que toute représentation est décomposable en représentations irréductibles, proposition 12.129 ainsi que pour le théorème 6.281 qui dit que si le polynôme minimal d'un endomorphisme est scindé à racine simple alors il est diagonalisable.

Démonstration. Nous posons

$$Q_i = \prod_{j \neq i} P_j.\tag{6.571}$$

Par le lemme 3.106 ces polynômes sont étrangers entre eux et le théorème de Bézout (théorème 3.105) donne l'existence de polynômes R_i tels que

$$R_1 Q_1 + \dots + R_n Q_n = 1.\tag{6.572}$$

Si nous appliquons cette égalité à u et ensuite à $x \in E$ nous trouvons

$$\sum_{i=1}^n (R_i Q_i)(u)(x) = x,\tag{6.573}$$

et en particulier si nous posons $E_i = \text{Image}(P_i Q_i(u))$ nous avons

$$E = \sum_{i=1}^n E_i.\tag{6.574}$$

42. Définition 3.104.

Cette dernière somme n'est éventuellement pas une somme directe. Si $i \neq j$, alors $Q_i Q_j$ est multiple de P et nous avons, en utilisant le lemme 6.236,

$$(R_i Q_i)(u) \circ (R_j Q_j)(u) = (R_i Q_i R_j Q_j)(u) = S_{ij}(u) \circ P(u) = 0 \quad (6.575)$$

où S_{ij} est un polynôme.

Nous pouvons voir E comme un $\mathbb{K}$ -module et appliquer le théorème 3.34. Les opérateurs $R_i Q_i(u)$ ont l'identité comme somme et sont orthogonaux, et nous avons donc la décomposition en somme directe :

$$E = \bigoplus_{i=1}^n R_i Q_i(u) E. \quad (6.576)$$

Afin de terminer la preuve, nous devons montrer que $R_i Q_i(u) E = \ker P_i(u)$. D'abord nous avons

$$P_i R_i Q_i(u) = (R_i P)(u) = R_i(u) \circ P(u) = 0, \quad (6.577)$$

par conséquent $\text{Image}(R_i Q_i(u)) \subset \ker P_i(u)$. Pour obtenir l'inclusion inverse, nous reprenons l'équation (6.573) avec $x \in \ker P_i(u)$. Elle se réduit à

$$(R_i Q_i)(u)x = x. \quad (6.578)$$

Par conséquent $x \in \text{Image}(R_i Q_i(u))$. □

Corollaire 6.238.

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

$$F = \bigoplus_{i=1}^r \ker M_i^{\alpha_i}(f) \cap F \quad (6.579)$$

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 (6.237) s'applique et

$$E = E_1 \oplus \cdots \oplus E_r. \quad (6.580)$$

Nous pouvons décomposer $x \in F$ en termes de cette somme :

$$x = x_1 + \cdots + x_r \quad (6.581)$$

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 $\text{proj}_i: E \rightarrow E_i$, et en appliquant proj_i à (6.581), $\text{proj}_i(x) = x_i$. Vu que $x \in F$, le membre de gauche est encore dans F et $x_i \in E_i \cap F$. Nous avons donc

$$F \subset \bigoplus_{i=1}^r F_i. \quad (6.582)$$

L'inclusion inverse est immédiate parce que $F_i \subset F$ pour chaque i . □

Lemme 6.239.

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 u pour la valeur propre $P(\lambda)$.

Démonstration. C'est un simple calcul de $P(u)x$ en ayant noté $P(X) = \sum_{k=0}^n c_k X^k$:

$$P(u)x = \sum_{k=0}^n c_k u^k(x) = \sum_{k=0}^n c_k \lambda^k u = P(\lambda)x. \quad (6.583)$$

□

6.25.2 Calcul effectif de l'exponentielle d'une matrice

Nous reprenons l'exemple de [94]. Soit A une matrice dont le polynôme minimum s'écrit

$$P(X) = (X - 1)^2(X - 2). \quad (6.584)$$

Par le théorème 6.237 de décomposition des noyaux nous avons

$$E = \ker(A - 1)^2 \oplus \ker(A - 2). \quad (6.585)$$

En suivant les notations de ce théorème nous avons $P_1(X) = (X - 1)^2$, $P_2(X) = X - 2$ et

$$Q_1(X) = X - 2 \quad (6.586a)$$

$$Q_2(X) = (X - 1)^2. \quad (6.586b)$$

Les polynômes R_i dont l'existence est assurée par le théorème de Bézout sont

$$\begin{aligned} R_1(X) &= -X \\ R_2(X) &= 1. \end{aligned} \quad (6.587)$$

Nous avons

$$R_1Q_1 + R_2Q_2 = 1. \quad (6.588)$$

Le projecteur p_i sur $\ker P_i$ est R_iQ_i :

$$\begin{aligned} p_1 &= -A(A - 2) = \text{proj}_{\ker(A-1)^2} \\ p_2 &= (A - 1)^2 = \text{proj}_{\ker(A-2)}. \end{aligned} \quad (6.589)$$

Passons maintenant au calcul de l'exponentielle. Nous avons évidemment

$$e^A = e^A p_1 + e^A p_2. \quad (6.590)$$

Étant donné que p_1 est le projecteur sur le noyau de $(A - 1)^2$, nous avons

$$e^A p_1 = e e^{A-1} p_1 = e p_1 + e(u - 1)1 = e p_1 = -A e(A - 2). \quad (6.591)$$

En effet $e^{A-1} p_1 = \sum_{k=0}^{\infty} (A - 1)^k \circ p_1$. De la même façon nous avons

$$e^A p_2 = e^2 e^{A-2} p_2 = e^2 p_2 = e^2 (A - 1)^2. \quad (6.592)$$

Au final,

$$e^A = -A e(A - 2) + e^2 (A - 1)^2. \quad (6.593)$$

6.25.3 Polynôme minimal et minimal ponctuel

Lemme-définition 6.240.

Soit un endomorphisme $f: E \rightarrow E$ d'un $\mathbb{K}$ -espace vectoriel de dimension finie. Il existe un unique polynôme annulateur normalisé de degré minimum.

Il est nommé le **polynôme minimal** de f et il est noté μ_f ou simplement μ lorsque la dépendance en f est claire.

Démonstration. Pour l'unicité, soient P et Q deux polynômes annulateur de f de même degré N et ayant tous deux 1 comme coefficient de x^N . Alors $P - Q$ est de degré $N - 1$ tout en étant encore annulateur.

Pour l'existence, les endomorphismes Id , f , f^2 , $\dots$ ne peuvent pas être tous linéairement indépendants parce que la dimension de $\text{End}(E)$ 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 $\varphi: \mathbb{K}[X] \rightarrow \text{End}(E)$ 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. $\square$

Remarque 6.241.

La preuve donnée ci-dessus montre que $\deg(\mu) \leq \dim(E)^2$. Comme conséquence du théorème de Caley-Hamilton 6.262 nous verrons qu'en réalité le degré du polynôme minimal est majoré par la dimension de l'espace.

Exemple 6.242(Pas en dimension infinie)

L'endomorphisme de dérivation

△

Dans la suite, l'endomorphisme f du $\mathbb{K}$ -espace vectoriel E de dimension n est fixé. Pour $x \in E$ nous notons

$$E_x = \{P(f)x \text{ tel que } P \in \mathbb{K}[X]\}. \quad (6.594)$$

Nous considérons le morphisme d'algèbres

$$\begin{aligned} \varphi: \mathbb{K}[X] &\rightarrow \text{End}(E) \\ P &\mapsto P(f) \end{aligned} \quad (6.595)$$

et si $x \in E$ est donné nous considérons le morphisme de $\mathbb{K}$ -espaces vectoriels

$$\begin{aligned} \varphi_x: \mathbb{K}[X] &\rightarrow E \\ P &\mapsto P(f)x. \end{aligned} \quad (6.596)$$

Les noyaux de ces applications sont des idéaux, entre autres par le lemme 6.236. Ils ont donc un unique générateur unitaire (chacun) par le théorème 3.110. En termes de vocabulaire, l'ensemble

$$\ker(\phi) = \{Q \in \mathbb{K}[X] \text{ tel que } Q(f) = 0\} \quad (6.597)$$

est l'**idéal annulateur** de f et un polynôme Q tel que $Q(f) = 0$ est une polynôme annulateur de f .

Définition 6.243.

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.

Nous notons μ le générateur unitaire du noyau de φ et μ_x celui de φ_x . Vu que $\mu \in \ker(\varphi_x)$ pour tout x nous avons $\mu_x \mid \mu$ pour tout x .

Exemple 6.244(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 16.50 donnera un habillage à peine subtil à cet exemple. △

Proposition 6.245.

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 $\ker(\varphi) = \{Q \in \mathbb{K}[X] \text{ tel que } Q(u) = 0\}$ est un idéal par le lemme 6.236. Le polynôme minimal de u est un élément de degré plus bas dans I et par conséquent $I = (\mu_u)$ par le théorème 3.110. Nous concluons que μ_u divise tous les éléments de I . □

La proposition suivante permet de caractériser le polynôme minimal.

Proposition 6.246 ([78]).

Soit une application linéaire f sur un $\mathbb{K}$ -espace vectoriel. Il existe un unique polynôme unitaire⁴³ $P \in \mathbb{K}[X]$ tel que

43. À mon avis, «unitaire» manque dans [78].

- (1) $P(f) = 0$;
 (2) l'application

$$\begin{aligned} \varphi: \frac{\mathbb{K}[X]}{(P)} &\rightarrow \text{End}(E) \\ \bar{Q} &\mapsto Q(f) \end{aligned} \quad (6.598)$$

est injective.

Démonstration. En ce qui concerne l'existence, il existe le polynôme minimal de f qui satisfait les conditions. Pour l'unicité nous travaillons maintenant.

Supposons que l'application (6.598) 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 3.110(3) nous dit alors que $P = \mu$ parce que μ est également générateur unitaire. $\square$

Lemme 6.247 ([95]).

Soit $f: E \rightarrow E$ 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 $E_i = \ker(P_i^{\alpha_i}(f))$. 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 6.237 nous donne la somme directe

$$E = \bigoplus_{i=1}^r \ker(P_i^{\alpha_i}(f)). \quad (6.599)$$

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 $Q(f)x_i \in E_j \cap E_i = \{0\}$. 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 $\mu_{x_i} = P_i^{\alpha_i}$.

Nous posons enfin $a = x_1 + \dots + x_r$; par définition du polynôme annulateur μ_a , nous avons

$$0 = \mu_a(f)a = \mu_a(f)x_1 + \dots + \mu_a(f)x_r. \quad (6.600)$$

Mais $\mu_a(f)x_j \in E_j$, et la somme des E_j est directe, donc l'annulation de la somme (6.600) 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 avons que le produit divise encore μ_a :

$$\prod_{i=1}^r \mu_{x_i} \mid \mu_a, \quad (6.601)$$

c'est à dire $\mu \mid \mu_a$. Comme nous avons aussi $\mu_a \mid \mu$, nous déduisons $\mu_a = \mu$. $\square$

Définition 6.248 (Matrices, endomorphismes et vecteurs cycliques).

Une matrice est **cyclique** si elle est semblable à une matrice compagnon. Un endomorphisme $f: E \rightarrow E$ 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 6.249.

Soit E un espace vectoriel de dimension finie et un endomorphisme cyclique⁴⁴ 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 6.245. Étant donné que v est cyclique, tout élément de E s'écrit sous la

44. Voir la définition 6.248.

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

$$P(f)x = (P(f) \circ Q(f))v = (Q(f) \circ P(f))v = 0 \quad (6.602)$$

où nous avons utilisé le lemme 6.236. $\square$

Lemme 6.250 ([95]).

Soit $a \in E$ tel que $\mu_a = \mu$. Alors E_a est un sous-espace stable pour 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 $e_1 = a, e_2 = f(a), \dots, e_l = f^{l-1}(a)$ forment une base de E_a . Nous pouvons la compléter en une base $\{e_1, \dots, e_n\}$ de E . Et nous posons⁴⁵

$$G = \{x \in E \text{ tel que } e_l^*(f^k(x)) = 0 \forall k \geq 0\} \quad (6.603a)$$

$$= \bigcap_{k \geq 0} \ker\{e_l^* \circ f^k\} \quad (6.603b)$$

$$= \bigcap_{k=0}^{l-1} \ker(e_l^* \circ f^k). \quad (6.603c)$$

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 $i \leq l-1$.

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 $f^j(a)$ ($j \leq l$). 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.

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

$$\sum_{j=0}^{l-1} \lambda_j (e_l^* \circ f^j) = 0 \quad (6.604)$$

et montrons que $\lambda_j = 0$ pour tout j est l'unique solution. Soit $x \in E$ et appliquons l'opération (6.604) au vecteur $f^i(x)$; le résultat est zéro :

$$0 = \sum_{j=0}^{l-1} \lambda_j (e_l^* \circ f^i \circ f^j) = (e_l^* \circ f^i)P(u) \quad (6.605)$$

où nous avons posé $P(X) = \sum_{j=0}^{l-1} \lambda_j X^j$. Appliquons cela à a : pour tout i nous avons

$$(e_l^* \circ f^i)(P(f)a) = 0. \quad (6.606)$$

Mais par définition de E_a , l'élément $P(f)a$ est dans E_a . Nous en déduisons que

$$P(f)a \in G \cap E_a = \{0\}, \quad (6.607)$$

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 . $\square$

Définition 6.251.

Un endomorphisme d'un espace vectoriel est **semi-simple** si tout sous-espace stable par u possède un supplémentaire stable.

45. ici, comme presque partout, e_l^* est le dual de e_l , c'est à dire l'application linéaire sur E donnée par $e_l^*(e_i) = \delta_{li}$.

Lemme 6.252.

Si le polynôme minimal d'un endomorphisme est irréductible, alors il est semi-simple⁴⁶.

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 problèmes. Sinon nous considérons $u_1 \in E \setminus F$ et

$$E_{u_1} = \{P(f)u_1 \text{ tel que } P \in \mathbb{K}[X]\}, \quad (6.608)$$

qui est un espace stable par f .

Montrons que $E_{u_1} \cap F = \{0\}$. Pour cela nous regardons l'idéal

$$I_{u_1} = \{P \in \mathbb{K}[X] \text{ tel que } P(f)u_1 = 0\}. \quad (6.609)$$

Cela 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 que 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 $y \neq 0$, ce la 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 Bézout (théorème 3.105) qui nous donne $A, B \in \mathbb{K}[X]$ tels que

$$AP + BP_{u_1} = 1. \quad (6.610)$$

Nous appliquons cette égalité à f et puis à u_1 :

$$u_1 = A(f) \circ \underbrace{P(f)u_1}_{=y} + B(f) \circ \underbrace{P_{u_1}(u_1)}_{=0} = A(f)y. \quad (6.611)$$

Mais $y \in F$, donc $A(f)y \in F$. Nous aurions donc $u_1 \in F$, ce qui est impossible par choix. Nous avons 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 $u_2 \in E \setminus (E_{u_1} \oplus F)$. Étant donné que E est de dimension finie, ce procédé s'arrête à un certain moment et nous aurons

$$E = F \oplus E_{u_1} \oplus \dots \oplus E_{u_k} \quad (6.612)$$

où chacun des E_{u_i} sont stables. □

Théorème 6.253.

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 $\mu_f = M_1^{\alpha_1} \dots M_r^{\alpha_r}$ 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 $\alpha_i \geq 1$ et $N \in \mathbb{K}[X]$ tel que $\mu_f = M^2 N$ où l'on a noté $M = M_i$. Nous étudions l'espace

$$F = \ker M(f) \quad (6.613)$$

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 $M(f)$,

$$M(f)(MN(f)x) = \mu_f(f)x = 0, \quad (6.614)$$

46. Définition 6.251.

ce qui signifie que $MN(f)x \in F$. Mais vu que S est stable par f nous avons aussi que $MN(f)x \in S$. Finalement $MN(f)x \in F \cap S = \{0\}$. Autrement dit, $MN(f)$ s'annule sur S .

Prenons maintenant $y \in F$. Nous avons

$$MN(f) = N(f)(M(f)y) = 0 \quad (6.615)$$

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 $m_f = M_1 \dots M_r$ 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

$$E_i = \ker(M_i(f)) \quad (6.616)$$

et $f_i = f|_{E_i}$. Par le lemme 6.238 nous avons

$$F = \bigoplus_{i=1}^r (F \cap E_i). \quad (6.617)$$

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 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 6.252.

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 :

$$E_i = S_i \oplus (F \cap E_i). \quad (6.618)$$

Étant donné que sur chaque S_i nous avons $f|_{S_i} = f_i$, l'espace $S = S_1 \oplus \dots \oplus S_r$ est stable par f . Du coup nous avons

$$E = E_1 \oplus \dots \oplus E_r \quad (6.619a)$$

$$= (S_1 \oplus (F \cap E_1)) \oplus \dots \oplus (S_r \oplus (F \cap E_r)) \quad (6.619b)$$

$$= \left(\bigoplus_{i=1}^r S_i \right) \oplus \left(\bigoplus_{i=1}^r F \cap E_i \right) \quad (6.619c)$$

$$= S \oplus F, \quad (6.619d)$$

ce qui montre que F a bien un supplémentaire stable par f et donc que f est semi-simple. $\square$

Exemple 6.254 (L'espace engendré par $\mathbb{1}, A, A^2, \dots$)

Soit A une matrice, et

$$V = \text{Span}\{A^k \text{ tel que } k \in \mathbb{N}\}. \quad (6.620)$$

Nous montrons que $\dim(V)$ est le degré du polynôme minimal de A .

D'abord l'idéal annulateur de A est engendré par le polynôme minimal⁴⁷ 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 cela serait un polynôme annulateur en A de degré plus petit que p . Donc $\dim(V) \geq p$.

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 $\dim(V) \leq p$). Soit un entier $q \geq \text{pet de division euclidienne}$ ⁴⁸ $np + r = q$ avec $r < p$. Nous avons $A^q = A^{np} A^r$. D'une part

$$A^{np} = (A^p)^n = f(A)^n \quad (6.621)$$

47. Proposition 6.245.

48. Théorème 2.22.

est de degré $n(p-1)$. Par conséquent

$$A^q = f(A)^n A^r \quad (6.622)$$

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 $\{1, A, \dots, A^{p-1}\}$ est génératrice de V .

La dimension de V est donc p , le degré du polynôme minimal. $\triangle$

Proposition 6.255.

Soit f un endomorphisme d'un espace vectoriel de dimension finie. Nous avons l'isomorphisme d'espace vectoriel

$$\mathbb{K}[f] \simeq \frac{\mathbb{K}[X]}{(\mu_f)} \quad (6.623)$$

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

$$\bar{P} = \{P + S\mu\}_{S \in \mathbb{K}[X]}. \quad (6.624)$$

Nous allons montrer que l'application suivante fournit l'isomorphisme :

$$\begin{aligned} \psi: \frac{\mathbb{K}[X]}{(\mu)} &\rightarrow \mathbb{K}[f] \\ \bar{P} &\mapsto P(f). \end{aligned} \quad (6.625)$$

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

$$\psi(\bar{Q}) = P(f) + (S\mu)(f). \quad (6.626)$$

Mais $\mu(f) = 0$ donc le deuxième terme est nul. Donc $\psi(\bar{P})$ est bien défini.

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 $\bar{P} = 0$.

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 corollaire 4.34 en parle déjà : une base est donné par les projections de $1, X, \dots, X^{\deg(\mu_a)-1}$. $\square$

6.25.4 Polynôme caractéristique

Définition 6.256.

Soit un anneau commutatif A . Si $u \in \mathbb{M}_n(A)$, nous définissons le **polynôme caractéristique** de u :

$$\chi_u(X) = \det(X\mathbb{1}_n - u). \quad (6.627)$$

Nous définissons de même le polynôme caractéristique d'un endomorphisme $u: E \rightarrow E$.

Lemme 6.257.

Le polynôme caractéristique χ_u est unitaire et a pour degré la dimension de l'espace vectoriel E .

Théorème 6.258.

Soit E un $\mathbb{K}$ -espace vectoriel de dimension finie n et un endomorphisme $u \in \text{End}(E)$. 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.

Définition 6.259.

Si $\lambda \in \mathbb{K}$ est une racine de χ_u , l'ordre de l'annulation est la **multiplicité algébrique** de la valeur propre λ de u . À ne pas confondre avec la **multiplicité géométrique** qui sera la dimension de l'espace propre.

Théorème 6.260.

Soit $u \in \text{End}(E)$ et $\lambda \in \mathbb{K}$. Les conditions suivantes sont équivalentes

- (1) $\lambda \in \text{Spec}(u)$
- (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 6.49(1) ou encore que λ est une racine du polynôme caractéristique de u .

(2) $\Leftrightarrow$ (3). Cela est une application directe du théorème 6.258 qui précise que le polynôme caractéristique a les mêmes racines dans $\mathbb{K}$ que le polynôme minimal. $\square$

Proposition 6.261 ([96]).

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

$$p_{f,x} = \dim E_{f,x} = \deg(\mu_{f,x}) \quad (6.628)$$

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

$$\chi_{f|_{E_{f,x}}}(f)x = \mu_{f,x}(f)x = 0. \quad (6.629)$$

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

$$B = \{f^k(x) \text{ tel que } 0 \leq k \leq p_{f,x} - 1\} \quad (6.630)$$

est libre. En effet une combinaison nulle des vecteurs de B donnerait un polynôme en f de degré inférieur à $p_{f,x}$ annihilant x . Nous écrivons

$$\mu_{f,x}(X) = X^{p_{f,x}} - \sum_{i=0}^{p_{f,x}-1} a_i X^i. \quad (6.631)$$

Étant donné que $\mu_{f,x}(f)x = 0$ et que la somme du membre de droite est dans $\text{Span}(B)$, nous avons $f^{p_{f,x}}(x) \in \text{Span}(B)$. Nous prouvons par récurrence que $f^{p_{f,x}+k}(x) \in \text{Span}(B)$. En effet en appliquant f^k à l'égalité

$$0 = f^{p_{f,x}}(x) - \sum_{i=0}^{p_{f,x}-1} a_i f^i(x) \quad (6.632)$$

nous trouvons

$$f^{p_{f,x}+k}(x) = \sum_{i=0}^{p_{f,x}-1} a_i f^{i+k}(x), \quad (6.633)$$

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

$$\mu_{f,x}(f)x = 0. \quad (6.634)$$

En y appliquant f^k et en profitant de la commutativité des polynômes sur les endomorphismes (proposition 6.236), nous avons

$$0 = f^k(\mu_{f,x}(f)x) = \mu_{f,x}(f)f^k(x), \quad (6.635)$$

de telle sorte que $\mu_{f,x}(f)$ est nul sur B et donc est nul sur $E_{f,x}$. Autrement dit,

$$\mu_{f,x}(f|_{E_{f,x}}) = 0. \quad (6.636)$$

Montrons que $\mu_{f,x}$ est même minimal pour $f|_{E_{f,x}}$. Soit Q , un polynôme non nul de degré $p_{f,x} - 1$ annulant $f|_{E_{f,x}}$. En particulier $Q(f)x = 0$, alors qu'une telle relation signifierait que B est un système lié, alors que nous avons montré que c'était un système libre. Nous concluons que $\mu_{f,x}$ est le polynôme minimal de $f|_{E_{f,x}}$. $\square$

Cette histoire de densité permet de donner une démonstration alternative du théorème de Cayley-Hamilton.

Théorème 6.262 (Cayley-Hamilton).

Le polynôme caractéristique est un polynôme annulateur.

Une démonstration plus simple via la densité des diagonalisables est donnée en théorème 12.24.

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

$$\chi_f = Q_x \chi_{f,x}, \quad (6.637)$$

et donc aussi

$$\chi_f(f)x = Q_x(f)(\chi_{f,x}(f)x) = 0 \quad (6.638)$$

parce que la proposition 6.261 nous indique que $\chi_{f,x}$ est un polynôme annulateur de $f|_{E_{f,x}}$. $\square$

Corollaire 6.263.

Le degré du polynôme minimal est majoré par la dimension de l'espace.

Démonstration. Le polynôme minimal engendre l'idéal des polynôme annulateurs (proposition 6.245), et divise donc le polynôme caractéristique. Or le degré du polynôme caractéristique est la dimension de l'espace par le lemme 6.257. $\square$

Exemple 6.264(Calcul de l'inverse d'un endomorphisme)

Le polynôme de Cayley-Hamilton donne un moyen de calculer l'inverse d'un endomorphisme inversible pourvu que l'on sache son polynôme caractéristique. En effet, supposons que

$$\chi_f(X) = \sum_{k=0}^n a_k X^k. \quad (6.639)$$

Nous aurons alors

$$0 = \chi_f(f) = \sum_{k=0}^n a_k f^k. \quad (6.640)$$

Nous appliquons f^{-1} à cette dernière égalité en sachant que $f^{-1}(0) = 0$:

$$0 = a_0 f^{-1} + \sum_{k=1}^n a_k f^{k-1}, \quad (6.641)$$

et donc

$$u^{-1} = -\frac{1}{\det(f)} \sum_{k=1}^n a_k f^{k-1} \quad (6.642)$$

où nous avons utilisé le fait que $a_0 = \chi_f(0) = \det(f)$. $\triangle$

Proposition 6.265.

Si $(X - z)^l$ ($l \geq 1$) est la plus grande puissance de $(X - z)$ dans le polynôme caractéristique d'un endomorphisme u alors

$$1 \leq \dim(E_z) \leq l. \quad (6.643)$$

C'est à dire que nous avons au moins un vecteur propre pour chaque racine du polynôme caractéristique.

Démonstration. Si $(X - z)$ divise χ_u alors en posant $\chi_u = (X - z)P(X)$ nous avons

$$\det(u - X\mathbb{1}) = (X - z)P(X), \quad (6.644)$$

ce qui, évalué en $X = z$, donne $\det(u - z\mathbb{1}) = 0$. L'annulation du déterminant étant équivalente à l'existence d'un noyau non trivial, nous avons $v \neq 0$ dans E tel que $(u - z\mathbb{1})v = 0$. Cela donne $u(v) = zv$ et donc que v est vecteur propre de u pour la valeur propre z . Donc aussi $\dim(E_z) \geq 1$.

Si $\dim(E_z) = k$ alors le théorème de la base incomplète 6.5 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 u est de la forme

$$\begin{pmatrix} z & & * \\ & \ddots & \vdots \\ & & z & * \\ & & & * \end{pmatrix} \quad (6.645)$$

où les étoiles représentent des blocs a priori non nuls. En tout cas il est vu sous cette forme que $(X - z\mathbb{1})^k$ divise χ_u . $\square$

6.26 Valeur propre et vecteur propre

Définition 6.266.

Soit un $\mathbb{K}$ -espace vectoriel E et un endomorphisme $A: V \rightarrow V$. Un **vecteur propre** de A est un vecteur $v \neq 0$ tel que $Av = \lambda v$ pour un certain $\lambda \in \mathbb{K}$. Dans ce cas, λ est la **valeur propre** de v .

L'**espace propre** de A pour la valeur λ ⁴⁹ est l'ensemble des vecteurs propres de A pour la valeur propre λ et zéro.

L'ensemble de valeurs propres de l'endomorphisme u est son **spectre** et est noté $\text{Spec}(u)$.

Remarque 6.267.

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 6.268.

Soit u un endomorphisme et $E_\lambda(u)$ ses espaces propres. La somme des V_λ est directe.

49. Nous laissons au lecteur le soin de vérifier que c'est bien un sous-espace vectoriel de E .

Démonstration. Soit $v_i \in V_{\lambda_i}$ un choix de vecteurs propres de u . Si la somme n'est pas directe, nous pouvons considérer une combinaison linéaire des v_i qui soit nulle :

$$v_1 + \dots + v_p = 0. \quad (6.646)$$

Appliquons $(A - \lambda_1 \mathbb{1})$ à cette égalité :

$$(\lambda_2 - \lambda_1)v_1 + \dots + (\lambda_p - \lambda_1)v_p = 0. \quad (6.647)$$

En appliquant encore successivement les opérateurs $(A - \lambda_i \mathbb{1})$ nous réduisons le nombre de termes jusqu'à obtenir $v_p = 0$. $\square$

Exemple 6.269

Sur $\mathbb{R}^2$, nous considérons la matrice $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ qui a pour polynôme caractéristique 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 :

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \quad (6.648)$$

entraîne $x = 0$.

Ici la multiplicité algébrique est différente de la multiplicité géométrique. $\triangle$

Proposition 6.270 ([96]).

Soit E , un espace vectoriel sur un corps infini et $(F_k)_{k=1,\dots,r}$, des sous-espaces vectoriels propres⁵⁰ de E tels que $\bigcup_{i=1}^r F_i = E$. Alors $E = F_k$ pour un certain k .

Autrement dit, l'union finie de sous-espaces propres ne peut être égal à l'espace complet.

La proposition suivante donne une utilisation amusante de la notion de polynôme caractéristique

Proposition 6.271 ([97]).

Soit un espace vectoriel V de dimension finie pour lequel il existe un endomorphisme $f: V \rightarrow V$ tel que $(f \circ f)(v) = -v$ pour tout $v \in V$. Alors la dimension de V est paire.

Démonstration. Cherchons les valeurs propres de f en résolvant l'équation $f(v) = \lambda v$. Nous appliquons f à cette égalité :

$$-v = \lambda f(v) = \lambda^2 v. \quad (6.649)$$

Donc λ ne peut pas être réel. Nous avons montré que f n'a pas de valeurs propres réelles. 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. $\square$

Une autre preuve possible est d'utiliser le déterminant : si la dimension de V est n nous avons :

$$\det(f^2) = \det(-\text{Id}) = (-1)^n. \quad (6.650)$$

Donc $(-1)^n$ est positif, ce qui montre que n est pair.

6.27 Espaces hermitiens

Définition 6.272.

Si E est un espace vectoriel sur $\mathbb{C}$, nous disons qu'une application $\langle \cdot, \cdot \rangle: E \times E \rightarrow \mathbb{C}$ est un **produit scalaire hermitien** si pour tout $u, v \in E$ nous avons

⁵⁰. Définition 6.266.

- (1) $\langle u, v \rangle = \overline{\langle v, u \rangle}$
- (2) $\lambda \langle u, v \rangle = \langle \lambda u, v \rangle = \langle u, \bar{\lambda} v \rangle$
- (3) $\langle u, u \rangle \in \mathbb{R}^+$ et $\langle u, u \rangle = 0$ si et seulement si $u = 0$.

Un espace vectoriel sur $\mathbb{C}$ muni d'un produit scalaire hermitien est un espace vectoriel hermitien.

Exemple 6.273

L'ensemble $E = \mathbb{C}^n$ vu comme espace vectoriel de dimension n sur $\mathbb{C}$ est muni d'une forme sesquilinéaire

$$\langle x, y \rangle = \sum_{k=1}^n x_k \bar{y}_k \quad (6.651)$$

pour tout $x, y \in \mathbb{C}^n$. Cela est un espace vectoriel hermitien. $\triangle$

Définition 6.274.

Soit E un espace vectoriel hermitien et $A \in \text{End}(E)$. L'opérateur **adjoint** de A est l'opérateur noté A^* défini par

$$\langle Av, w \rangle = \langle v, A^*w \rangle \quad (6.652)$$

pour tout $v, w \in \mathbb{C}^n$.

La prescription (6.652) définit bien l'opérateur A^* de façon unique. En effet si $\{e_i\}$ est une base orthonormée alors

$$\langle e_i, A^*e_j \rangle = (A^*e_j)_i = \langle Ae_i, e_j \rangle = (Ae_i)_j. \quad (6.653)$$

Autrement dit, $(A^*e_j)_i = (Ae_i)_j$.

Définition 6.275.

Un opérateur A est **hermitien** si $A^* = A$. On dit aussi **autoadjoint**.

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 réels⁵¹. 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 $\mathbb{R}$.

Remarque 6.276.

Le fait d'être hermitien n'implique en rien le fait d'être inversible.

6.28 Diagonalisation

Ici encore $\mathbb{K}$ est un corps commutatif.

6.28.1 Matrices semblables

Définition 6.277 (matrices semblables).

Sur l'ensemble $\mathbb{M}_n(\mathbb{K})$ des matrices $n \times n$ à coefficients dans $\mathbb{K}$ nous introduisons la relation d'équivalence $A \sim B$ si et seulement si il existe une matrice $P \in \text{GL}(n, \mathbb{K})$ telle que $B = P^{-1}AP$. Deux matrices équivalentes en ce sens sont dites **semblables**.

Le polynôme caractéristique est un invariant sous les similitudes. En effet si P est une matrice inversible,

$$\chi_{PAP^{-1}} = \det(PAP^{-1} - \lambda X) \quad (6.654a)$$

$$= \det(P^{-1}(PAP^{-1} - \lambda X)P) \quad (6.654b)$$

$$= \det(A - \lambda X). \quad (6.654c)$$

51. Voir la définition 6.379.

La permutation de lignes ou de colonnes ne sont pas de similitudes, comme le montrent les exemples suivants :

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}. \quad (6.655)$$

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.

6.28.2 Endomorphismes diagonalisables

Définition 6.278.

Une matrice est **diagonalisable** si elle est semblable à une matrice diagonale.

Lemme 6.279.

Une matrice triangulaire supérieure avec des 1 sur la diagonale n'est diagonalisable que si elle est diagonale (c'est à dire si elle 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 $A = \mathbb{1}$. $\square$

Lemme 6.280.

Soit F un sous-espace stable par u . Soit une décomposition du polynôme minimal

$$\mu_u = P_1^{n_1} \dots P_r^{n_r} \quad (6.656)$$

où les P_i sont des polynômes irréductibles unitaires distincts. Si nous posons $E_i = \ker P_i^{n_i}$, alors

$$F = (F \cap E_1) \oplus \dots \oplus (F \cap E_r). \quad (6.657)$$

Théorème 6.281.

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 simples⁵².
- (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.

(2) implique (3) Étant donné que $P(u) = 0$, il est dans l'idéal des polynôme annulateurs de u , et le polynôme minimal μ_u le divise parce que l'idéal des polynôme annulateurs est généré par μ_u par le théorème 3.110.

(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

$$\mu_u(X) = (X - \lambda_1) \dots (X - \lambda_r) \quad (6.659)$$

52. Le polynôme caractéristique, lui, n'a pas spécialement ses racines simples ; il peut encore être de la forme

$$\chi_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\alpha_i}, \quad (6.658)$$

mais alors $\dim(E_{\lambda_i}) = \alpha_i$.

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 6.237) nous enseigne que

$$E = \ker(u - \lambda_1) \oplus \dots \oplus \ker(u - \lambda_r). \quad (6.660)$$

Mais $\ker(u - \lambda_i)$ est l'espace propre $E_{\lambda_i}(u)$. Donc u est diagonalisable.

(1) implique (4) Soit $\{e_1, \dots, e_n\}$ une base qui diagonalise u , soit F un sous-espace de E un $\{f_1, \dots, f_r\}$ une base de F . Par le théorème 6.8 (qui généralise le théorème de la base incomplète), nous pouvons compléter la base de F par des éléments de la base $\{e_i\}$. Le complément ainsi construit est invariant par u .

(4) implique (1) En dimension un, tout endomorphisme est diagonalisable, nous supposons donc que $\dim E = n \geq 2$. 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 .

(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

$$P(x) = (X - \lambda_1) \dots (X - \lambda_r). \quad (6.661)$$

Alors $P(u) = 0$. En effet si e_i est un vecteur propre pour la valeur propre λ_i ,

$$P(u)e_i = \prod_{j \neq i} (u - \lambda_j) \circ (u - \lambda_i)e_i = 0 \quad (6.662)$$

par le lemme 6.236. Par conséquent $P(u)$ s'annule sur une base.

(5) implique (2) Si la matrice A est diagonale alors le polynôme $P = \prod_{i=1}^n (A - A_{ii}\mathbb{1})$ est annulateur de A .

(3) implique (5) le polynôme minimal de u s'écrit

$$\mu = (X - \lambda_1) \dots (X - \lambda_r), \quad (6.663)$$

et les espaces E_i du lemme 6.280 sont les espaces propres $E_i = \ker(u - \lambda_i)$. Nous avons donc une somme directe

$$E = E_1 \oplus \dots \oplus E_r. \quad (6.664)$$

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.

□

Corollaire 6.282.

Si u est diagonalisable et si F est une sous-espace stable par u , alors

$$F = \bigoplus_{\lambda} E_{\lambda}(u) \cap F \quad (6.665)$$

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 6.281, le polynôme μ_u est scindé et ne possède que des racines simples. Notons le

$$\mu_u(X) = (X - \lambda_1) \dots (X - \lambda_r). \quad (6.666)$$

Les espaces E_i du lemme 6.280 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 6.283.

Soit E un $\mathbb{K}$ -espace vectoriel et $u \in \text{End}(E)$. Si $\text{Card}(\text{Spec}(u)) = \dim(E)$ 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 6.268). Par conséquent $\text{Span}\{E_{\lambda_i}(u)\}$ est de dimension n et u est diagonalisable. $\square$

Voici un résultat de diagonalisation simultanée. Nous donnerons un résultat de trigonalisation simultanée dans le lemme 6.359.

Proposition 6.284 (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 $u_j(E_{\lambda}(u_i)) \subset E_{\lambda}(u_i)$.
- (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

$$u_i(u_j(x)) = u_j(u_i(x)) = \lambda u_j(x). \quad (6.667)$$

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

$$E_{\lambda_k}(u_0) \neq E, \quad (6.668)$$

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 :

$$E = \bigoplus_k E_{\lambda_k}(u_0). \quad (6.669)$$

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 $u_i : E_{\lambda_k}(u_0) \rightarrow E_{\lambda_k}(u_0)$, et nous pouvons considérer la famille d'opérateurs

$$\left(u_i|_{E_{\lambda_k}(u_0)} \right)_{i \in I}. \quad (6.670)$$

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 . $\square$

Exemple 6.285

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 (6.281). 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

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (6.671a)$$

$$A^1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (6.671b)$$

Ce A est donc une involution mais n'est pas diagonalisable. $\triangle$

6.28.3 Diagonalisation : cas complexe

Lemme 6.286 (Théorème spectral hermitien).

Pour un opérateur hermitien⁵³,

- (1) le spectre est réel,
- (2) deux vecteurs propres à des valeurs propres distinctes sont orthogonaux⁵⁴.

Démonstration. Soit v un vecteur de valeur propre λ . Nous avons d'une part

$$\langle Av, v \rangle = \lambda \langle v, v \rangle = \lambda \|v\|^2, \quad (6.672)$$

et d'autre part, en utilisant le fait que A est hermitien,

$$\langle Av, v \rangle = \langle v, A^*v \rangle = \langle v, Av \rangle = \bar{\lambda} \|v\|^2, \quad (6.673)$$

par conséquent $\lambda = \bar{\lambda}$ parce que $v \neq 0$.

Soient λ_i et v_i ($i = 1, 2$) deux valeurs propres de A avec leurs vecteurs propres correspondants. Alors d'une part

$$\langle Av_1, v_2 \rangle = \lambda_1 \langle v_1, v_2 \rangle, \quad (6.674)$$

et d'autre part

$$\langle Av_1, v_2 \rangle = \langle v_1, Av_2 \rangle = \lambda_2 \langle v_1, v_2 \rangle. \quad (6.675)$$

Nous avons utilisé le fait que λ_2 était réel. Par conséquent, soit $\lambda_1 = \lambda_2$, soit $\langle v_1, v_2 \rangle = 0$. $\square$

Remarque 6.287.

Un opérateur de la forme A^*A est évidemment hermitien. De plus ses valeurs propres sont toutes positives parce que si $A^*Ax = \lambda v$ alors

$$0 \leq \langle Av, Av \rangle = \langle A^*Av, v \rangle = \lambda \langle v, v \rangle. \quad (6.676)$$

Donc $\lambda \geq 0$.

Le lemme suivant est utile en soi et dit que toute matrice complexe est trigonalisable. Une démonstration alternative passant par le polynôme caractéristique sera présentée dans la remarque 6.352 utilisant la proposition 6.351.

Lemme 6.288 (Lemme de Schur complexe[98]).

Si $A \in \mathbb{M}(n, \mathbb{C})$, il existe une matrice unitaire U telle que UAU^{-1} soit triangulaire supérieure.

Démonstration. Étant donné que $\mathbb{C}$ est algébriquement clos, nous pouvons toujours considérer un vecteur propre v_1 de A , de valeur propre λ_1 . Nous pouvons utiliser un procédé de Gram-Schmidt pour construire une base orthonormée $\{v, u_2, \dots, u_n\}$ de $\mathbb{R}^n$, et la matrice (unitaire)

$$Q = \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ v & u_2 & \cdots & u_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix}. \quad (6.677)$$

Nous avons $Q^{-1}AQe_1 = Q^{-1}Av = \lambda Q^{-1}v = \lambda e_1$, par conséquent la matrice $Q^{-1}AQ$ est de la forme

$$Q^{-1}AQ = \begin{pmatrix} \lambda_1 & * \\ 0 & A_1 \end{pmatrix} \quad (6.678)$$

où $*$ représente une ligne quelconque et A_1 est une matrice de $\mathbb{M}(n-1, \mathbb{C})$. Nous pouvons donc répéter le processus sur A_1 et obtenir une matrice triangulaire supérieure (nous utilisons le fait qu'un produit de matrices orthogonales est une matrice orthogonale). $\square$

53. Définition 6.275.

54. Pour la forme (6.651).

En particulier les matrices hermitiennes, anti-hermitiennes et unitaires sont trigonalisables par une matrice unitaire, qui peut être choisie de déterminant 1.

Corollaire 6.289.

Le polynôme caractéristique⁵⁵ sur $\mathbb{C}$ d'une matrice s'écrit sous la forme

$$\chi_A(X) = \prod_{i=1}^r (X - \lambda_i)^{m_i} \quad (6.679)$$

où les λ_i sont les valeurs propres distinctes de A et m_i sont les multiplicités correspondantes.

Démonstration. Le lemme 6.288 nous donne l'existence d'une base de trigonalisation ; dans cette base les valeurs propres de A sont sur la diagonale et nous avons

$$\chi_A(X) = \det(A - X\mathbb{1}) = \det \begin{pmatrix} X - \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & X - \lambda_r \end{pmatrix}, \quad (6.680)$$

qui vaut bien le produit annoncé. $\square$

Théorème 6.290 (Théorème spectral pour les matrices normales[99, 100, 101]).

Soit $A \in \mathbb{M}(n, \mathbb{C})$ une matrice de valeurs propres $\lambda_1, \dots, \lambda_n$ (non spécialement distinctes). Alors les conditions suivantes sont équivalentes :

- (1) A est normale,
- (2) A se diagonalise par une matrice unitaire,
- (3) $\sum_{i,j=1}^n |A_{ij}|^2 = \sum_{j=1}^n |\lambda_j|^2$,
- (4) il existe une base orthonormale de vecteurs propres de A .

Démonstration. Nous allons nous contenter de prouver (1) $\Leftrightarrow$ (2).

Soit Q la matrice unitaire donnée par la décomposition de Schur (lemme 6.288) : $A = QTQ^{-1}$. Étant donné que A est normale nous avons

$$QTT^*Q^{-1} = QT^*TQ^{-1}, \quad (6.681)$$

ce qui montre que T est également normale. Or une matrice triangulaire supérieure normale est diagonale. En effet nous avons $T_{ij} = 0$ lorsque $i > j$ et

$$(TT^*)_{ii} = (T^*T)_{ii} = \sum_{k=1}^n |T_{ki}|^2 = \sum_{k=1}^n |T_{ik}|^2. \quad (6.682)$$

Écrivons cela pour $i = 1$ en tenant compte de $|T_{k1}|^2 = 0$ pour $k = 2, \dots, n$,

$$|T_{11}|^2 = |T_{11}|^2 + |T_{12}|^2 + \dots + |T_{1n}|^2, \quad (6.683)$$

ce qui implique que T_{11} est le seul non nul parmi les T_{1k} . En continuant de la sorte avec $i = 2, \dots, n$ nous trouvons que T est diagonale.

Dans l'autre sens, si A se diagonalise par une matrice unitaire, $UAU^* = D$, nous avons

$$DD^* = UAA^*U^* \quad (6.684)$$

et

$$D^*D = UA^*AU^*, \quad (6.685)$$

qui prouve que A est normale. $\square$

55. Définition 6.256.

6.28.4 Diagonalisation : cas réel

Lemme 6.291 (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

$$Q^{-1}AQ = \begin{pmatrix} \lambda_1 & * & * & * & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \lambda_r & * & * \\ 0 & 0 & 0 & \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} & * \\ 0 & 0 & 0 & 0 & \begin{pmatrix} a_s & b_s \\ c_s & d_s \end{pmatrix} \end{pmatrix}. \quad (6.686)$$

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 la 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

$$Au + iAv = A(u + iv) = (\alpha + i\beta)(u + iv) = \alpha u - \beta v + i(\alpha v + \beta u), \quad (6.687)$$

et en égalisant les parties réelles et imaginaires,

$$Au = \alpha u - \beta v \quad (6.688a)$$

$$Av = \alpha v + \beta u. \quad (6.688b)$$

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 avons 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 $\{q_1, q_2, q_3, \dots, q_n\}$ de $\mathbb{R}^n$. Nous considérons à présent la matrice orthogonale dont les colonnes sont formées de ces vecteurs : $Q = [q_1 \ q_2 \ \dots \ q_n]$.

L'espace $\text{Span}\{e_1, e_2\}$ est stable par $Q^{-1}AQ$, en effet nous avons

$$Q^{-1}AQe_1 = Q^{-1}Aq_1 = Q^{-1}(aq_1 + bq_2) = ae_1 + be_2. \quad (6.689)$$

La matrice $Q^{-1}AQ$ est donc de la forme

$$Q^{-1}AQ = \begin{pmatrix} \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix} & C_1 \\ 0 & A_1 \end{pmatrix} \quad (6.690)$$

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 conjuguées.

En ce qui concerne les valeurs propres, il est facile de voir en regardant (6.686) 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 . $\square$

Théorème 6.292 (Théorème spectral, matrice symétrique[1]).

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. 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 $\lambda = \bar{\lambda}$.

Le lemme de Schur réel 6.291 donne une matrice orthogonale qui trigonalise A . Les valeurs propres étant toutes réelles, la matrice $Q A Q^{-1}$ est même triangulaire (il n'y a pas de blocs dans la forme (6.686)). Prouvons que $Q A Q^{-1}$ est symétrique :

$$(Q A Q^{-1})^t = (Q^{-1})^t A^t Q^t = Q A^t Q^{-1} = Q A Q^{-1} \quad (6.691)$$

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 $\{e_i\}_{i=1,\dots,n}$ la base canonique de $\mathbb{R}^n$ et Q une matrice orthogonale telle que $A = Q^t D Q$ avec D diagonale. Nous posons $f_i = Q^t e_i$ et en tenant compte du fait que $Q^t = Q^{-1}$ nous avons $A f_i = Q^t D Q Q^t e_i = Q^t \lambda_i e_i = \lambda_i f_i$. Donc les f_i sont des vecteurs propres de A . De plus ils sont orthonormés parce que

$$\langle f_i, f_j \rangle = \langle Q^t e_i, Q^t e_j \rangle = \langle e_i, Q^t Q e_j \rangle = \langle e_i, e_j \rangle = \delta_{ij}. \quad (6.692)$$

□

Le théorème spectral pour les opérateurs auto-adjoints sera traité plus bas parce qu'il a besoin de choses sur les formes bilinéaires, théorème 6.380.

Remarque 6.293.

Une matrice symétrique est diagonalisable par une matrice orthogonale. Nous pouvons en réalité nous arranger pour diagonaliser par une matrice de $SO(n)$. Plus généralement si A est une matrice diagonalisable par une matrice $P \in GL^+(n, \mathbb{R})$ alors elle est diagonalisable par une matrice de $GL^-(n, \mathbb{R})$ en changeant le signe de la première ligne de P . Et inversement.

En effet, si nous avons $P^t D P = A$, alors en notant $*$ les quantités qui ne dépendent pas de a , b ou c ,

$$\begin{aligned} \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{pmatrix} \begin{pmatrix} a & b & c \\ * & * & * \\ * & * & * \end{pmatrix} &= \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \begin{pmatrix} \lambda_1 a & \lambda_1 b & \lambda_1 c \\ * & * & * \\ * & * & * \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 a^2 + * & \lambda_1 ab + * & \lambda_1 ac + * \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{pmatrix}. \end{aligned} \quad (6.693)$$

Nous voyons donc que si nous changeons les signes de a , b et c en même temps, le résultat ne change pas.

Définition 6.294 (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.

Afin d'éviter l'une ou l'autre confusion, nous disons souvent *strictement* définie positive pour positive.

Nous notons $S^+(n, \mathbb{R})$ l'ensemble des matrices réelles $n \times n$ semi-définies positives. L'ensemble $S^{++}(n, \mathbb{R})$ est l'ensemble des matrices symétriques strictement définies positives.

Remarque 6.295.

Nous ne définissons pas la notion de matrice définie positive pour une matrice non symétrique.

Lemme 6.296.

La matrice symétrique M est strictement définie positive si et seulement si $\langle x, Mx \rangle > 0$ pour tout x non nul dans $\mathbb{R}^n$.

Démonstration. Soit $\{e_i\}_{i=1,\dots,n}$ une base orthonormée de vecteurs propres de M dont l'existence est assurée par le théorème spectral 6.292. Nous nommons x_i les coordonnées de x dans cette base. Alors,

$$\langle x, Mx \rangle = \sum_{i,j} x_i \langle e_i, x_j M e_j \rangle = \sum_{i,j} x_i x_j \langle e_i, \lambda_j e_j \rangle = \sum_{i,j} x_i x_j \lambda_j \delta_{ij} = \sum_i \lambda_i x_i^2 \quad (6.694)$$

où les λ_i sont les valeurs propres de M . Cela est strictement positif pour tout x si et seulement si tous les λ_i sont positifs. $\square$

Corollaire 6.297.

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 6.296. $\square$

6.28.5 Pseudo-réduction simultanée**Corollaire 6.298** (Pseudo-réduction simultanée[102]).

Soient $A, B \in S(n, \mathbb{R})$ avec A définie positive⁵⁶. Alors il existe $Q \in GL(n, \mathbb{R})$ tel que $Q^t B Q$ soit diagonale et $Q^t A Q = \mathbb{1}$.

Démonstration. Nous allons noter $x \cdot y$ le produit scalaire usuel de $\mathbb{R}^n$ et $\{e_i\}_{i=1,\dots,n}$ sa base canonique.

Vu que A est définie positive, nous avons que l'expression⁵⁷ $\langle x, y \rangle = x \cdot Ay$ est un produit scalaire sur $\mathbb{R}^n$. Autrement dit, E muni de cette forme bilinéaire symétrique est un espace euclidien, ce qui fait dire à la proposition 6.77 qu'il existe une base de $\mathbb{R}^n$ orthonormée $\{f_i\}_{i=1,\dots,n}$ pour ce produit scalaire, c'est à dire qu'il existe une matrice $P \in GL(n, \mathbb{R})$ telle que $P^t A P = \mathbb{1}$. Ici, P est la matrice de changement de base de la base canonique à notre base orthonormée, c'est à dire la matrice qui fait $P e_i = f_i$ pour tout i . Voyons cela avec un peu de détails.

Pour savoir ce que valent les éléments de la matrice $P^t A P$, nous nous souvenons que $P^t A P e_j$ est un vecteur dont les coordonnées sont les éléments de la j^e colonne de $P^t A P$. Nous avons donc $(P^t A P)_{ij} = e_i \cdot P^t A P e_j$. Calculons :

$$(P^t A P)_{ij} = e_i \cdot P^t A P e_j = P e_i \cdot A P e_j = f_i \cdot A f_j = \langle f_i, f_j \rangle = \delta_{ij} \quad (6.695)$$

où nous avons utilisé le fait que A était auto-adjointe pour la passer de l'autre côté du produit scalaire (usuel). Au final nous avons effectivement $P^t A P = \mathbb{1}$.

La matrice $P^t B P$ est une matrice symétrique, donc le théorème spectral 6.292 nous donne une matrice $R \in O(n, \mathbb{R})$ telle que $R^t P^t B P R$ soit diagonale. En posant maintenant $Q = P R$ nous avons la matrice cherchée. $\square$

Note : nous avons prouvé la pseudo-réduction simultanée comme corollaire du théorème de diagonalisation des matrices symétriques 6.292. Il aurait aussi pu être vu comme un corollaire du théorème spectral 6.380 sur les opérateurs auto-adjoints via son corollaire 6.381.

⁵⁶. Définition 6.294.

⁵⁷. On peut aussi l'écrire de façon plus matricielle sous la forme $\langle x, y \rangle = x^t A y$.

6.29 Sous espaces caractéristiques

Lorsqu'un opérateur n'est pas diagonalisable, les valeurs propres jouent quand même un rôle important.

Définition 6.299.

Soit E un $\mathbb{K}$ -espace vectoriel $f \in \text{End}(E)$. Pour $\lambda \in \mathbb{K}$ nous définissons

$$F_\lambda(f) = \{v \in E \text{ tel que } (f - \lambda \mathbb{1})^n v = 0, n \in \mathbb{N}\} \quad (6.696)$$

et nous appelons ça 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 6.300.

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 . Inversement si v est une valeur 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

$$(f - \lambda \mathbb{1})^n f(x) = f((f - \lambda \mathbb{1})^n x) = 0, \quad (6.697)$$

par conséquent $f(x) \in F_\lambda(f)$. □

Remarque 6.301.

Toute matrice sur $\mathbb{C}$ n'est pas diagonalisable : nous en avons déjà donné un exemple simple en 6.358. Nous en voyons maintenant un moins simple. Considérons en effet l'endomorphisme f donné par la matrice

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \quad (6.698)$$

où $a \neq b$, $\alpha \neq 0$, β et γ sont des nombres complexes quelconques. Son polynôme caractéristique est

$$\chi_f(\lambda) = (a - \lambda)^2(b - \lambda), \quad (6.699)$$

et les valeurs propres sont donc a et b . Nous trouvons les vecteurs propres pour la valeur a en résolvant

$$\begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax \\ ay \\ az \end{pmatrix}. \quad (6.700)$$

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

$$\begin{pmatrix} \frac{1}{b-a} \left(\beta + \frac{\alpha\gamma}{b-a} \right) \\ \frac{\gamma}{b-a} \\ 1 \end{pmatrix}. \quad (6.701)$$

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

$$(f - a \mathbb{1})^2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a & \alpha & \beta \\ 0 & a & \gamma \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} a\alpha \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad (6.702)$$

de telle sorte que le vecteur $(0, 1, 0)$ soit 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.

6.29.1 Théorèmes de décomposition

Théorème 6.302 (Théorème spectral, décomposition primaire).

Soit E espace vectoriel de dimension finie sur le corps algébriquement clos $\mathbb{K}$ et $f \in \text{End}(E)$. Alors

$$E = F_{\lambda_1}(f) \oplus \dots \oplus F_{\lambda_k}(f) \quad (6.703)$$

où la somme est sur les valeurs propres distinctes de f .

Les projecteurs sur les espaces caractéristique forment un système complet et orthogonal.

Démonstration. Soit P le polynôme caractéristique de f et une décomposition

$$P = (f - \lambda_1)^{\alpha_1} \dots (f - \lambda_r)^{\alpha_r} \quad (6.704)$$

en facteurs irréductibles. La le théorème de noyaux (6.237) nous avons

$$E = \ker(f - \lambda_1)^{\alpha_1} \oplus \dots \oplus \ker(f - \lambda_r)^{\alpha_r}. \quad (6.705)$$

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

$$\ker(f - \lambda_i)^{\alpha_i} \subset F_{\lambda_i}(f) \quad (6.706)$$

est évidente. Nous devons montrer l'inclusion inverse. Prouvons que la somme des $F_{\lambda_i}(f)$ est directe. Si $v \in F_{\lambda_i}(f) \cap F_{\lambda_j}(f)$, alors il existe $v_1 = (f - \lambda_i)^n v \neq 0$ avec $(f - \lambda_i)v_1 = 0$. Étant donné que $(f - \lambda_i)$ commute avec $(f - \lambda_j)$, ce v_1 est encore dans $F_{\lambda_j}(f)$ et par conséquent il existe $w = (f - \lambda_j)^m v_1$ non nul tel que

$$\begin{cases} (f - \lambda_i)w = 0 \\ (f - \lambda_j)w = 0. \end{cases} \quad \begin{matrix} (6.707a) \\ (6.707b) \end{matrix}$$

Ce w serait donc un vecteur propre simultanément pour les valeurs propres λ_i et λ_j , ce qui est impossible parce que les espaces propres sont linéairement indépendants. Les espaces F_{λ_i} sont donc en somme directe et

$$\sum_i \dim F_{\lambda_i}(f) \leq \dim E. \quad (6.708)$$

En tenant compte de l'inclusion (6.706) nous avons même

$$\dim E = \sum_i \dim \ker(f - \lambda_i)^{\alpha_i} \leq \sum_i \dim F_{\lambda_i}(f) \leq \dim E. \quad (6.709)$$

Par conséquent nous avons $\dim \ker(f - \lambda_i)^{\alpha_i} = \dim F_{\lambda_i}(f)$ et l'égalité des deux espaces. $\square$

Problèmes et choses à faire

Dans le cas où le corps n'est pas algébriquement clos, il paraît qu'il faut remplacer «diagonalisable» par «semi-simple».

Si l'espace vectoriel est sur un corps algébriquement clos, alors les endomorphismes semi-simples⁵⁸ sont les endomorphismes diagonaux.

Théorème 6.303 (Décomposition de Dunford).

Soit E un espace vectoriel sur le corps algébriquement clos $\mathbb{K}$ et $u \in \text{End}(E)$ un endomorphisme de E .

⁵⁸ Définition 6.251.

(1) L'endomorphisme u se décompose de façon unique sous la forme

$$u = s + n \quad (6.710)$$

où s est diagonalisable, n est nilpotent et $[s, n] = 0$.

(2) Les endomorphismes s et n sont des polynômes en u et commutent avec u .

(3) Les parties s et n sont données par

$$s = \sum_i \lambda_i p_i \quad (6.711a)$$

$$n = \sum_i (s - \lambda_i \mathbb{1}) p_i \quad (6.711b)$$

où les sommes sont sur les valeurs propres distinctes⁵⁹ de f et où $p_i: E \rightarrow F_{\lambda_i}(u)$ est la projection de E sur $F_{\lambda_i}(u)$.

Démonstration. Le théorème spectral 6.302 nous indique que

$$E = \bigoplus_i F_{\lambda_i}(f). \quad (6.712)$$

Nous considérons l'endomorphisme s de E qui consiste à dilater d'un facteur λ l'espace caractéristique $F_{\lambda}(f)$:

$$s = \sum_i \lambda_i p_i \quad (6.713)$$

où $p_i: E \rightarrow F_{\lambda_i}(u)$ 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

$$f - s: F_{\lambda}(f) \rightarrow F_{\lambda}(f). \quad (6.714)$$

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

$$s'u = s'^2 + s'n' = s'^2 + n's' = (s' + n')s' = us', \quad (6.715)$$

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 diagonalisabilité.

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 et s' sont alors deux endomorphismes diagonalisables qui commutent. Par la proposition 6.284, ils sont simultanément diagonalisables. Dans la base de simultanée diagonalisation, 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,

$$(A + B)^n = \sum_{k=0}^n \binom{n}{k} A^k B^{n-k}. \quad (6.716)$$

Si n est assez grand, au moins un parmi A^k ou B^{n-k} est nul.

Maintenant que $n - n'$ est diagonal et nilpotent, il est nul et $n = n'$. Nous avons alors immédiatement aussi $s = s'$.

□

59. C'est à dire sur les sous-espaces caractéristiques.

6.29.2 Diverses conséquences

Théorème 6.304.

Soit une matrice $A \in \mathbb{M}(n, \mathbb{C})$. On a que la suite $(A^k x)$ tend vers zéro pour tout x si et seulement si $\rho(A) < 1$ où $\rho(A)$ est le rayon spectral de A .

Démonstration. Dans le sens direct, il suffit de prendre comme x , un vecteur propre de A . Dans ce cas nous avons $A^k x = \lambda^k x$. Mais $\lambda^k x$ ne tend vers zéro que si $|\lambda| < 1$. Donc toutes les valeurs propres de A doivent être plus petites que 1 et $\rho(A) < 1$.

Pour l'autre sens nous utilisons la décomposition de Dunford (théorème 6.303) : il existe une matrice inversible P telle que

$$A = P^{-1}(D + N)P \quad (6.717)$$

où D est diagonale, N est nilpotente et $[D, N] = 0$. Étant donné que $D + N$ est triangulaire, son polynôme caractéristique que

$$\chi_{D+N}(\lambda) = \prod_i (D_{ii} - \lambda). \quad (6.718)$$

Par similitude, c'est le même polynôme caractéristique que celui de A et nous savons alors que la diagonale de D contient les valeurs propres de A .

Par ailleurs nous avons

$$A^k = P^{-1}(D + N)^k P \quad (6.719a)$$

$$= P^{-1} \sum_{j=0}^k \binom{k}{j} D^{k-j} N^j P \quad (6.719b)$$

$$= P^{-1} \sum_{j=0}^{n-1} \binom{k}{j} D^{k-j} N^j P \quad (6.719c)$$

où nous avons utilisé le fait que D et N commutent ainsi que $N^{n-1} = 0$ parce que N est nilpotente. Nous utilisons la norme matricielle usuelle, pour laquelle $\|D\| = \rho(D) = \rho(A)$. Nous avons alors

$$\|(D + N)^k\| \leq \sum_{j=0}^k \binom{k}{j} \rho(D)^{k-j} \|N\|^j. \quad (6.720)$$

Du coup si $\rho(D) < 1$ alors $\|(D + N)^k\| \rightarrow 0$ (et c'est même un si et seulement si). $\square$

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 16.79 une formule pour le logarithme sous forme d'une série ; ce logarithme sera réel.

Proposition 6.305.

Toute matrice inversible complexe est une exponentielle.

Démonstration. Soit $A \in \text{GL}(n, \mathbb{C})$; nous allons donner une matrice $B \in \mathbb{M}(n, \mathbb{C})$ telle que $A = \exp(B)$. D'abord remarquons qu'il suffit de prouver le résultat pour une matrice par classe de similitude. En effet si $A = \exp(B)$ et si M est inversible alors

$$\exp(MBM^{-1}) = \sum_k \frac{1}{k!} (MBM^{-1})^k \quad (6.721a)$$

$$= \sum_k \frac{1}{k!} MB^k M^{-1} \quad (6.721b)$$

$$= M \exp(B) M^{-1}. \quad (6.721c)$$

Donc $MAM^{-1} = \exp(MBM^{-1})$. Nous pouvons donc nous contenter de trouver un logarithme pour les blocs de Jordan. Nous supposons donc que $A = (\mathbb{1} + N)$ avec $N^m = 0$. En nous inspirant de (16.76), nous posons

$$D(t) = tN - \frac{t^2}{2}N^2 + \dots + (-1)^m \frac{t^{m-1}}{m-1}N^{m-1} \quad (6.722)$$

et nous allons prouver que $e^{D(1)} = \mathbb{1} + N$. Notons que N étant nilpotente, cette somme ainsi que toutes celles qui viennent sont finies. Il n'y a donc pas de problèmes de convergences dans cette preuve (si ce n'est les passages des équations (6.721)).

Nous posons $S(t) = e^{D(t)}$ (la somme est finie), et nous avons

$$S'(t) = D'(t)e^{D(t)} \quad (6.723)$$

Afin d'obtenir une expression qui donne S' en termes de S , nous multiplions par $(\mathbb{1} + tN)$ en remarquant que $(\mathbb{1} + tN)D'(t) = N$ nous avons

$$(\mathbb{1} + tN)S'(t) = NS(t). \quad (6.724)$$

En dérivant à nouveau,

$$(\mathbb{1} + tN)S''(t) = 0. \quad (6.725)$$

La matrice $(\mathbb{1} + tN)$ est inversible parce que son noyau est réduit à $\{0\}$. En effet si $(\mathbb{1} + tN)x = 0$, alors $Nx = -\frac{1}{t}x$, ce qui est impossible parce que N est nilpotente. Ce que dit l'équation (6.725) est alors que $S''(t) = 0$. Si nous développons $S(t)$ en puissances de t nous nous arrêtons au terme d'ordre 1 et nous avons

$$S(t) = S(0) + tS'(0) = \mathbb{1} + tD'(0) = \mathbb{1} + tN. \quad (6.726)$$

En $t = 1$ nous trouvons $S(1) = \mathbb{1} + N$. La matrice $D(1)$ donnée est donc bien un logarithme de $\mathbb{1} + N$. $\square$

Proposition 6.306 ([35]).

Si $A \in \mathbb{M}(n, \mathbb{C})$ est telle que $\rho(A) < 1$, alors $A^n \rightarrow 0$.

Démonstration. Nous nous plaçons dans une base des espaces caractéristiques de A , c'est à dire que nous supposons que la matrice A a la forme

$$A = \begin{pmatrix} \lambda_1 \mathbb{1} + N_1 & & \\ & \ddots & \\ & & \lambda_s \mathbb{1} + N_s \end{pmatrix} \quad (6.727)$$

où les λ_i sont les valeurs propres de A et les N_i sont nilpotentes. En effet nous savons que l'espace caractéristique F_{λ_i} est l'espace de nilpolence de $A - \lambda_i \mathbb{1}$. Si nous notons A_i la restriction de A à cet espace, la matrice $N_i = A_i - \lambda_i \mathbb{1}$ est nilpotente. Du coup $A_i = \lambda_i \mathbb{1} + N_i$ et nous avons bien la décomposition (6.727).

Nous avons donc $A^n \rightarrow 0$ si et seulement si $(N_i + \lambda_i \mathbb{1})^n \rightarrow 0$ pour tout i . Soit donc N nilpotente et $\lambda < 1$ (parce que nous savons que toutes les valeurs propres de A sont inférieures à un). Nous avons

$$(\lambda \mathbb{1} + N)^n = \sum_{k=0}^n \binom{n}{k} \lambda^{n-k} N^k = \sum_{k=0}^{r-1} \binom{n}{k} \lambda^{n-k} N^k. \quad (6.728)$$

Nous voyons que le nombre de termes dans la somme ne dépend pas de n . De plus pour chacun de termes, la puissance de N ne dépend pas non plus de n . Le terme

$$\binom{n}{k} \lambda^{n-k} \leq P(n) \lambda^{n-k} \quad (6.729)$$

où P est un polynôme tend vers zéro lorsque n devient grand parce que c'est une cas polynôme fois exponentielle. $\square$

6.29.3 Diagonalisabilité d'exponentielle

Proposition 6.307 ([35]).

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.

Démonstration. Si A est diagonalisable, alors il existe une matrice inversible M telle que $D = M^{-1}AM$ soit diagonale (c'est la définition 6.278). Dans ce cas nous avons aussi $(M^{-1}AM)^k = M^{-1}A^kM$ et donc $M^{-1}e^AM = e^{M^{-1}AM} = e^D$ qui est diagonale.

La partie difficile est donc le contraire.

Qui est diagonalisable et comment ? Nous supposons que e^A est diagonalisable et nous écrivons la décomposition de Dunford (théorème 6.303) :

$$A = S + N \quad (6.730)$$

où S est diagonalisable, N est nilpotente, $[S, N] = 0$. Nous avons besoin de prouver que $N = 0$.

Les matrices A et S commutent ; en passant au développement nous en déduisons que A et e^S commutent, puis encore en passant au développement que e^A et e^S commutent. Vu que S est diagonalisable, e^S l'est et par hypothèse e^A est également diagonalisable. Donc e^A et e^{-S} sont simultanément diagonalisables par la proposition 6.284.

Étant donné que A et S commutent, nous avons $e^N = e^{A-S} = e^A e^{-S}$, et nous en déduisons que e^N est diagonalisable vu que les deux facteurs e^A et e^{-S} sont simultanément diagonalisables.

Unipotence Si r est le degré de nilpotence de N , nous avons

$$e^N - \mathbb{1} = N + \frac{N^2}{2} + \dots + \frac{N^{r-1}}{(r-1)!}. \quad (6.731)$$

Donc

$$(e^N - \mathbb{1})^k = \left(N + \frac{N^2}{2} + \dots + \frac{N^{r-1}}{(r-1)!} \right)^k \quad (6.732)$$

où le membre de droite est un polynôme en N dont le terme de plus bas degré est de degré k . Donc $(e^N - \mathbb{1})$ est nilpotente et e^N est unipotente.

Si M est la matrice qui diagonalise e^N , alors la matrice diagonale $M^{-1}e^N M$ est tout autant unipotente que e^N elle-même. En effet,

$$(M^{-1}e^N M - \mathbb{1})^r = \sum_{k=0}^r \binom{r}{k} (-1)^{r-k} M^{-1}(e^N)^k M \quad (6.733a)$$

$$= M^{-1} \left(\sum_{k=0}^r \binom{r}{k} (-1)^{r-k} (e^N)^k \right) M \quad (6.733b)$$

$$= M^{-1}(e^N - \mathbb{1})^r M \quad (6.733c)$$

$$= 0. \quad (6.733d)$$

La matrice $M^{-1}e^N M$ est donc une matrice diagonale et unipotente ; donc $M^{-1}e^N M = \mathbb{1}$, ce qui donne immédiatement que $e^N = \mathbb{1}$.

Polynômes annulateurs En reprenant le développement (6.731) sachant que $e^N = \mathbb{1}$, nous savons que

$$N + \frac{N^2}{2} + \dots + \frac{N^{r-1}}{(r-1)!} = 0. \quad (6.734)$$

Dit en termes pompeux (mais non moins porteurs de sens), le polynôme

$$Q(X) = X + \frac{X^2}{2} + \dots + \frac{X^{r-1}}{(r-1)!} \quad (6.735)$$

est un polynôme annulateur de N .

La proposition 6.245 stipule que le polynôme minimal d'un endomorphisme divise tous les polynômes annulateurs. Dans notre cas, X^r est un polynôme annulateur et donc le polynôme minimal de N est de la forme X^k . Donc il est X^r lui-même.

Nous avons donc $X^r \mid Q$. Mais Q est un polynôme contenant le monôme X donc X^r ne peut diviser Q que si $r = 1$. Nous en concluons que X est un polynôme annulateur de N . C'est à dire que $N = 0$.

Conclusion Vu que Dunford⁶⁰ dit que $A = S + N$ et que nous venons de prouver que $N = 0$, nous concluons que $A = S$ avec S diagonalisable.

□

6.29.4 Valeurs singulières

Définition 6.308.

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 existent des vecteurs unitaires $u \in \mathbb{K}^m$, $v \in \mathbb{K}^n$ tels que

$$Mv = \sigma u \quad (6.736a)$$

$$M^*u = \sigma v. \quad (6.736b)$$

Théorème 6.309 (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

$$M = ADB \quad (6.737)$$

où il existe deux matrices unitaires $A \in \mathbb{U}(m \times m)$, $B \in \mathbb{U}(n \times n)$ et une matrice (pseudo)diagonale $D \in \mathbb{M}(m \times n)$ tels que

- (1) $A \in \mathbb{U}(m \times m)$, $B \in \mathbb{U}(n \times n)$ 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 de M .

Corollaire 6.310.

Soit $M \in \mathbb{M}(n, \mathbb{C})$. Il existe un isomorphisme $f: \mathbb{C}^n \rightarrow \mathbb{C}^n$ 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. □

6.30 Extension du corps de base

Nous avons discuté dans la section 4.3 de ce qui arrive au corps lorsqu'on l'étend. Dans cette sections 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 $\mathbb{L}$.

Soit donc un corps $\mathbb{K}$ et deux $\mathbb{K}$ -espaces vectoriels E et F , et entrons dans le vif du sujet⁶¹. Soit $\mathbb{K}$ un corps (commutatif) et une extension $\mathbb{L}$ de $\mathbb{K}$. Soient E et F , des $\mathbb{K}$ -espaces vectoriels de dimension finie.

⁶⁰. Théorème 6.303.

⁶¹. Le sujet étant le corps étendu.

6.30.1 Extension des applications linéaires

Définition 6.311 ([103]).

L'espace vectoriel obtenu par **extension du corps de base** de E est l'espace vectoriel

$$E_{\mathbb{L}} = \mathbb{L} \otimes_{\mathbb{K}} E. \quad (6.738)$$

Ce dernier est le quotient $\mathbb{L} \otimes_{\mathbb{K}} E = (\mathbb{L} \times E) / \sim$ par la relation d'équivalence

$$(\lambda, v) \sim (a\lambda, \frac{1}{a}v) \quad (6.739)$$

pour tout $a \in \mathbb{K}$. Nous noterons $[\lambda, v]$ ou $\lambda \otimes v$ ou encore $\lambda \otimes_{\mathbb{K}} v$ la classe de (λ, v) .

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 $f: E \rightarrow F$ est une applications linéaire nous définissons

$$\begin{aligned} f_{\mathbb{L}}: E_{\mathbb{L}} &\rightarrow F_{\mathbb{L}} \\ [\lambda, v] &\mapsto [\lambda, f(v)]. \end{aligned} \quad (6.740)$$

Remarque 6.312.

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.

Nous définissons aussi l'injection canonique

$$\begin{aligned} \iota: E &\rightarrow E_{\mathbb{L}} \\ v &\mapsto [1, v]. \end{aligned} \quad (6.741)$$

Proposition 6.313 ([78]).

Injectivité et surjectivité respectées.

- (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. Supposons pour commencer que $f_{\mathbb{L}}$ est injective. Le diagramme

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \tau \downarrow & & \downarrow \tau \\ E_{\mathbb{L}} & \xrightarrow{f_{\mathbb{L}}} & F_{\mathbb{L}} \end{array} \quad (6.742)$$

est un diagramme commutatif. En effet

$$(\tau \circ f)(v) = [1, f(v)] \quad (6.743)$$

tandis que

$$(f_{\mathbb{L}} \circ \tau)(v) = f_{\mathbb{L}}[1, v] = [1, f(v)]. \quad (6.744)$$

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 $E_{\mathbb{L}}$.

Réciproquement, nous supposons que f est injective et nous prouvons que $f_{\mathbb{L}}$ est injective. Par le lemme 6.22(1), nous savons qu'il existe $g: F \rightarrow E$ telle que $f \circ g = \text{Id}|_F$. Nous en déduisons que $f_{\mathbb{L}} \circ g_{\mathbb{L}} = \text{Id}|_{F_{\mathbb{L}}}$ parce que si $[\lambda, v] \in F_{\mathbb{L}}$ alors

$$(f_{\mathbb{L}} \circ g_{\mathbb{L}})[\lambda, v] = f_{\mathbb{L}}[\lambda, g(v)] = [\lambda, (f \circ g)(v)] = [\lambda, v]. \quad (6.745)$$

Notons que g est injective, donc $g_{\mathbb{L}}$ est injective et l'égalité $f_{\mathbb{L}} \circ g_{\mathbb{L}} = \text{Id}|_{F_{\mathbb{L}}}$ implique que $f_{\mathbb{L}}$ est également injective. $\square$

Proposition 6.314 ([104]⁶²).

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

$$\lambda \otimes ke_i = \frac{\lambda}{k} \otimes e_i = \frac{\lambda}{k} (1 \otimes e_i). \quad (6.746)$$

Cela pour introduire que l'application

$$\begin{aligned} \psi: \mathbb{L} \otimes_{\mathbb{K}} E &\rightarrow \bigoplus_i \mathbb{L}(1 \otimes e_i) \\ \sum_k \lambda_k \otimes v_k &\mapsto \bigoplus_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) \end{aligned} \quad (6.747)$$

où $v_k = \sum_i v_{ik}e_i$ avec $v_{ik} \in \mathbb{K}$ est un isomorphisme de $\mathbb{L}$ -espaces vectoriels. La surjectivité est facile. En ce qui concerne l'injectivité, si

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = 0 \quad (6.748)$$

alors les choses suivantes sont nulles également :

$$\sum_i \sum_k (\lambda_k v_{ik})(1 \otimes e_i) = \sum_{ik} (\lambda_k \otimes v_{ik}e_i) = \sum_k (\lambda_k \otimes \sum_i v_{ik}e_i) = \sum_k (\lambda_k \otimes v_k). \quad (6.749)$$

Le dernier est l'argument de ψ . Le fait que ce soit nul implique que ψ est injective. $\square$

Remarque 6.315.

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, vu qu'il y a plusieurs façons de noter un élément de $E_{\mathbb{L}}$ sous la forme de tels termes.

Corollaire 6.316.

La $\mathbb{L}$ -dimension de $E_{\mathbb{L}}$ est égale à la $\mathbb{K}$ -dimension de E .

6.30.2 Projections

Problèmes et choses à faire

Nous allons définir $\text{proj}: \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \rightarrow \mathcal{L}(E, F)$ en faisant appel à des bases et en prouvant que les choses définies ne dépendent pas des bases choisies. Il y a sûrement 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 4.42). 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

$$\mathbb{L} = \mathbb{K} \oplus V. \quad (6.750)$$

Nous avons alors naturellement une projection $\text{proj}: \mathbb{L} \rightarrow \mathbb{K}$.

Soit $\{e_i\}$ une base de E et $\{e_a\}$ une de F . Nous noterons également e_i et e_a les éléments τe_i et τe_a correspondants. Grâce à la proposition 6.314, ce sont des bases de $E_{\mathbb{L}}$ et $F_{\mathbb{L}}$. Si la fonction $f: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ s'écrit dans ces bases comme

$$f(e_i) = \sum_a f_{ai} e_a \quad (6.751)$$

alors nous définissons $\text{proj}(f)$ par

$$(\text{proj } f)e_i = \sum_a \text{proj}(f_{ai})e_a. \quad (6.752)$$

62. Attention : dans ce texte, l'auteur se place dans un cadre nettement plus général. J'ai tenté de suivre et d'adapter. Jene suis même pas tout à fait certain que l'énoncé soit correct (ici). Si vous êtes expert en extension de corps, vous devriez m'écrire pour me dire ce que vous pensez de ce que vous aller lire ici.

Proposition 6.317 ([8]).

L'application $\mathbf{proj}$ définie en (6.752) 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 choses qui se notent $\mathbf{proj}$. La première est la projection $\mathbf{proj}: \mathbb{L} \rightarrow \mathbb{K}$ qui ne dépend que d'un choix de supplémentaire et que nous supposons fixée ici. D'autre part il y a $\mathbf{proj}: E_{\mathbb{L}} \rightarrow E$ qui dépend a priori des bases choisies.

Nous choisissons de nouvelles bases qui sont liées aux anciennes bases par

$$\begin{cases} e'_b = \sum_a B_{ab} e_a \\ e'_i = \sum_j A_{ji} e_j. \end{cases} \quad (6.753a)$$

$$(6.753b)$$

Les matrices A et B sont dans $\mathrm{GL}(\mathbb{K})$. Nous allons écrire l'opérateur $\mathbf{proj}'$ qui correspond à ces bases et montrer que pour toute application linéaire $f: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ nous avons $\mathbf{proj}(f) = \mathbf{proj}'(f)$. Nous avons :

$$f(e'_j) = \sum_i A_{ji} f(e_i) \quad (6.754a)$$

$$= \sum_a \sum_b \sum_i A_{ji} f_{ai} (B^{-1})_{ba} e'_b \quad (6.754b)$$

$$= \sum_b \left(\sum_{ai} A_{ji} f_{ai} (B^{-1})_{ba} \right) e'_b, \quad (6.754c)$$

ce qui fait que

$$(\mathbf{proj}' f) e'_j = \sum_b \left(\mathbf{proj} (A_{ji} f_{ai} (B^{-1})_{ba}) \right) e'_b. \quad (6.755)$$

Nous calculons maintenant $(\mathbf{proj}' f) e_j$ en substituant $e_j = \sum_l (A^{-1})_{lj} e'_l$ et en utilisant (6.755) et la linéarité de $\mathbf{proj}'$ et la $\mathbb{K}$ -linéarité de $\mathbf{proj}: \mathbb{L} \rightarrow \mathbb{K}$:

$$(\mathbf{proj}' f) \left(\sum_l (A^{-1})_{lj} e'_l \right) = \sum_l (A^{-1})_{lj} \sum_b \sum_{ai} \mathbf{proj} (A_{li} f_{ai} (B^{-1})_{ba}) e_b \quad (6.756a)$$

$$= \sum_a \mathbf{proj} (f_{aj}) e_a \quad (6.756b)$$

$$= (\mathbf{proj} f) e_j. \quad (6.756c)$$

Donc $\mathbf{proj} = \mathbf{proj}'$. □

Note au passage comme toujours : 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 6.318 ([8]).

L'opération $\mathbf{proj}: \mathcal{L}(E_{\mathbb{L}}, F_{\mathbb{L}}) \rightarrow \mathcal{L}(E, F)$ ne dépend pas des bases choisies un peu partout. Mais elle dépend de l'application $pr: \mathbb{L} \rightarrow \mathbb{K}$ déjà construite. Et celle-là dépend du choix d'un supplémentaire V qui fournit $\mathbb{L} = \mathbb{K} \oplus V$.

Si $\mathbf{proj}(\lambda) = 0$ pour un de ces choix, cela n'implique nullement que $\lambda = 0$. Penser à $i \in \mathbb{C}$ si la projection $\mathbf{proj}: \mathbb{C} \rightarrow \mathbb{R}$ est l'application $(x + iy) \mapsto x$ parallèle à l'axe des imaginaires.

Par contre si $\mathbf{proj}(\lambda) = 0$ 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 $\mathbf{proj}(\lambda) = 0$ nous en déduirons $\lambda = 0$.

Proposition 6.319.

Si $f: E \rightarrow F$ 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

$$(1) \quad \mathbf{proj} f_{\mathbb{L}} = f,$$

(2) $(f_{\mathbb{L}})_{ja} = f_{ja} \in \mathbb{K}$.

Démonstration. Nous avons

$$f_{\mathbb{L}}(e_i) = \sum_a f_{ai}(1 \otimes e_a) = \sum_a f_{ai}\tau(e_a), \quad (6.757)$$

donc

$$(\text{proj } f_{\mathbb{L}})e_i = \sum_a \text{proj}(f_{ai})e_a = \sum_a f_{ai}e_a = f(e_i). \quad (6.758)$$

Cela prouve que $\text{proj } f_{\mathbb{L}} = f$.

Par ailleurs,

$$f_{\mathbb{L}}(\tau e_i) = f_{\mathbb{L}}(1 \otimes e_i) = 1 \otimes f(e_i) = \tau(f(e_i)) = \sum_a f_{ai}\tau(e_a) \quad (6.759)$$

alors que par définition,

$$f_{\mathbb{L}}(\tau e_i) = \sum_a (f_{\mathbb{L}})_{ai}\tau(e_a). \quad (6.760)$$

Les éléments $\tau(e_a)$ formant une base⁶³, la comparaison de (6.759) avec (6.760) donne $(f_{\mathbb{L}})_{ai} = f_{ai} \in \mathbb{K}$. $\square$

Lemme 6.320.

Soient

- (1) Une base $\{e_i\}$ de E et une application linéaire $f: E \rightarrow F$;
- (2) une base $\{e_a\}$ de F et une application linéaire $g: G \rightarrow F$;
- (3) une base $\{e_\alpha\}$ de G et une application linéaire $\tilde{h}: G_{\mathbb{L}} \rightarrow E_{\mathbb{L}}$.

Alors nous avons

$$\text{proj}(f_{\mathbb{L}} \circ \tilde{h}) = \text{proj}(f_{\mathbb{L}}) \circ \text{proj}(\tilde{h}). \quad (6.761)$$

Démonstration. Pour écrire $\text{proj}(f_{\mathbb{L}} \circ \tilde{h})$ à partir de la définition (6.752) nous commençons par écrire

$$(f_{\mathbb{L}} \circ \tilde{h})e_\alpha = \sum_a (f_{\mathbb{L}} \circ \tilde{h})_{a\alpha}e_a = \sum_{ai} (f_{\mathbb{L}})_{ai}(\tilde{h})_{i\alpha}e_a = \sum_a \left(\sum_i f_{ai}(\tilde{h})_{i\alpha} \right) e_a \quad (6.762)$$

où nous avons utilisé le fait que $(f_{\mathbb{L}})_{ai} = f_{ai}$. Donc, en utilisant la $\mathbb{K}$ -linéarité de proj ,

$$\text{proj}(f_{\mathbb{L}} \circ \tilde{h})e_\alpha = \sum_a \sum_i \text{proj} \left(f_{ai}(\tilde{h})_{i\alpha} \right) e_a = \sum_a \sum_i f_{ai} \text{proj} \left((\tilde{h})_{i\alpha} \right) e_a. \quad (6.763)$$

D'autre part,

$$\begin{aligned} \text{proj}(f_{\mathbb{L}}) \circ \text{proj}(\tilde{h})e_\alpha &= \text{proj}(f_{\mathbb{L}}) \sum_i \text{proj} \left((\tilde{h})_{i\alpha} \right) e_i \\ &= \sum_i \text{proj} \left((\tilde{h})_{i\alpha} \right) \sum_a f_{ai}e_a \\ &= \sum_{ai} \text{proj} \left((\tilde{h})_{i\alpha} \right) f_{ai}e_a, \end{aligned} \quad (6.764)$$

et c'est égal à (6.763). $\square$

Remarque 6.321.

Nous n'avons en général pas $\text{proj}(xy) = \text{proj}(x)\text{proj}(y)$ pour tout $x, y \in \mathbb{L}$. Par exemple si $\mathbb{K} = \mathbb{R}$ et $\mathbb{L} = \mathbb{C}$ avec la projection canonique,

$$\text{proj}(i \cdot i) = \text{proj}(-1) = -1 \quad (6.765)$$

alors que $\text{proj}(i) = 0$.

63. Encore la proposition 6.314.

Proposition 6.322.

Soit $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, E)$. Alors il existe $h: G \rightarrow E$ tel que $f \circ h = g$ si et seulement si il existe $\tilde{g}: G_{\mathbb{L}} \rightarrow E_{\mathbb{L}}$ tel que $f_{\mathbb{L}} \circ \tilde{g} = g_{\mathbb{L}}$.

Démonstration. Dans le sens direct, il suffit de poser $\tilde{h} = h_{\mathbb{L}}$.

Dans le sens inverse, si nous avons $\tilde{h}: G_{\mathbb{L}} \rightarrow E_{\mathbb{L}}$ tel que $f_{\mathbb{L}} \circ \tilde{h} = g_{\mathbb{L}}$ alors en appliquant proj des deux côtés et en utilisant le lemme 6.320,

$$\text{proj}(f_{\mathbb{L}}) \circ \text{proj}(\tilde{h}) = \text{proj}(g_{\mathbb{L}}) \quad (6.766)$$

c'est à dire

$$f \circ \text{proj}(\tilde{h}) = g, \quad (6.767)$$

c'est à dire que l'application $\text{proj} \tilde{h}: G \rightarrow E$ est la réponse à la proposition. $\square$

6.30.3 Rang, polynôme minimal, polynôme caractéristique**Proposition 6.323** (Stabilité du rang par extension des scalaires[78]).

Si $f: E \rightarrow F$ est linéaire alors nous avons

$$\text{rang}(f) = \text{rang}(f_{\mathbb{L}}). \quad (6.768)$$

où à droite nous considérons le rang de l'application $\mathbb{L}$ -linéaire $f_{\mathbb{L}}: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$.

Démonstration. Il existe un supplémentaire V tel que $E = \ker(f) \oplus V$ avec $\dim(V) = \text{rang}(f)$. Nous pouvons factoriser f en

$$f = f_2 \circ f_1 \quad (6.769)$$

avec $f_1: E \rightarrow V$ est la projection parallèle à $\ker(f)$ et est surjective (vers V) parce que $\dim(V) = \text{rang}(f) = \dim(\text{Image}(f))$. De plus $f_2: V \rightarrow F$ est injective parce que si $v \in V$ est tel que $f_2(v) = 0$ alors on aurait

$$f(v) = (f_2 \circ f_1)(v) = f_2(v) = 0. \quad (6.770)$$

Cela donne $v \in \ker(f) \cap V = \{0\}$. Par la proposition 6.313, les applications $(f_1)_{\mathbb{L}}$ et $(f_2)_{\mathbb{L}}$ sont respectivement surjective et injective.

L'application $(f_2)_{\mathbb{L}}: V_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ est forcément surjective sur son image, donc

$$(f_2)_{\mathbb{L}}: V_{\mathbb{L}} \rightarrow \text{Image}(f_{\mathbb{L}}) \quad (6.771)$$

est un isomorphisme de $\mathbb{L}$ -espaces vectoriels. Nous avons alors les égalités

$$\dim_{\mathbb{L}}(V_{\mathbb{L}}) = \dim_{\mathbb{L}}(\text{Image}(f_{\mathbb{L}})) = \text{rang}(f_{\mathbb{L}}). \quad (6.772)$$

Mais aussi, par les définitions posées plus haut,

$$\dim(V) = \text{rang}(f) = \dim(\text{Image}(f)). \quad (6.773)$$

Mais le corollaire 6.316 nous dit que $\dim_{\mathbb{L}}(V_{\mathbb{L}}) = \dim_{\mathbb{K}}(V)$. Donc il y a égalité des deux lignes (6.772) et (6.773) donne $\text{rang}(f) = \text{rang}(f_{\mathbb{L}})$. $\square$

Proposition 6.324.

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 6.319(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 6.256) : 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 $\mathbb{K}$. $\square$

La situation est très différente avec le polynôme minimal⁶⁴. Autant il existe une «recette» pour

64. Définition 4.38.

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 polynôme en les coefficients de la matrice). La proposition suivante montre que le polynôme minimal est conservé par extension de corps, mais que pour le voir, il faut travailler plus.

Proposition 6.325 ([78, 8]).

Soit $\mathbb{L}$ une extension du corps $\mathbb{K}$ et une application linéaire $f: E \rightarrow F$ entre deux $\mathbb{K}$ -espaces vectoriels. Alors $\mu_f = \mu_{f_{\mathbb{L}}}$.

Démonstration. Nous allons montrer que l'application

$$\begin{aligned} \tilde{g}: \frac{\mathbb{L}[X]}{(\mu)} &\rightarrow \text{End}(E_{\mathbb{L}}) \\ \bar{P} &\mapsto P(f_{\mathbb{L}}) \end{aligned} \quad (6.774)$$

est bien définie et injective. La proposition 6.246 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 $P(f_{\mathbb{L}}) = P(f)_{\mathbb{L}}$:

$$P(f_{\mathbb{L}})\lambda \otimes v = \sum_k a_k f_{\mathbb{L}}^k \lambda \otimes v \quad (6.775a)$$

$$= \lambda \otimes \sum_k a_k f^k(v) \quad (6.775b)$$

$$= \lambda \otimes P(f)v \quad (6.775c)$$

$$= P(f)_{\mathbb{L}}\lambda \otimes v. \quad (6.775d)$$

Par conséquent $\mu(f_{\mathbb{L}}) = 0$ et l'application est bien définie.

Sur $\mathbb{L}[X]/(\mu)$ nous considérons la base $\{1, \bar{X}, \dots, \bar{X}^{\deg(\mu)-1}\}$, et $\text{End}(E_{\mathbb{L}})$ nous considérons une base qui commence⁶⁵ 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

$$\sum_k \text{proj}(\lambda_k f_{\mathbb{L}}^k) = 0. \quad (6.776)$$

Pour détailler ce que cela implique, nous calculons ceci :

$$(\lambda f_{\mathbb{L}})(\tau e_i) = \lambda f_{\mathbb{L}}(\tau e_i) = \sum_a \lambda f_{ia} e_a, \quad (6.777)$$

par conséquent $\text{proj}(\lambda f_{\mathbb{L}})e_i = \sum_a \text{proj}(\lambda f_{ia})e_a$, et comme proj est $\mathbb{K}$ -linéaire et que $f_{ai} \in \mathbb{K}$,

$$\text{proj}(\lambda f_{\mathbb{L}})e_i = \text{proj}(\lambda) \sum_a f_{ai} e_a = \text{proj}(\lambda) \text{proj}(f_{\mathbb{L}})e_i = \text{proj}(\lambda) f(e_i). \quad (6.778)$$

Appliquer la projection proj à l'équation (6.776) donne alors $\sum_k \text{proj}(\lambda_k) f^k = 0$. Mais comme les f^k sont linéairement indépendantes sur $\mathbb{K}$ nous avons pour tout k : $\text{proj}(\lambda_k) = 0$ (égalité dans $\mathbb{K}$). En nous souvenant de la remarque 6.318 nous en déduisons $\lambda_k = 0$ dans $\mathbb{L}$.

Dans les choix de bases faits, l'application $\tilde{g}$ a la forme

$$\tilde{g} = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \\ * & * & * \\ * & * & * \\ * & * & * \end{pmatrix}, \quad (6.779)$$

qui est injective.

Vu que $\tilde{g}$ est injective, μ est le polynôme minimal de $f_{\mathbb{L}}$ et donc $\mu = \mu_{\mathbb{L}}$. □

⁶⁵. Théorème de la base incomplète 6.5(2).

6.31 Frobenius et Jordan

6.31.1 Matrice compagnon

Définition 6.326.

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 P est la matrice donnée par

$$C(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & a_0 \\ 1 & 0 & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix} \quad (6.780)$$

si $n \geq 2$ et par (a_0) si $n = 1$.

Une matrice est dite *compagnon* si elle a cette forme.

Proposition 6.327.

Si f est l'endomorphisme associé à la matrice $C(P)$ nous avons

$$f(e_i) = \begin{cases} e_{i+1} & \text{si } i < n \\ (a_0, \dots, a_{n-1}) & \text{si } i = n. \end{cases} \quad (6.781)$$

De plus l'endomorphisme f vérifie $P(f)e_1 = 0$.

Lemme 6.328 ([105]).

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 , $(f^i(e_1))_{i=1, \dots, n-1}$ est libre, donc le polynôme minimal ponctuel en e_1 est de degré n au minimum. En reprenant les notations du théorème 3.110, 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. $\square$

Remarque 6.329.

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 égale au polynôme minimal sont denses dans les 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.

6.31.2 Réduction de Frobenius

Lemme 6.330.

Soit un endomorphisme $f: E \rightarrow E$ 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 6.343 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 combinaison 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 6.262), donc il est le polynôme minimal. $\square$

Théorème 6.331 (Réduction de Frobenius [106, 107, 108]).

Soit E , un $\mathbb{K}$ -espace vectoriel, et $f \in \text{End}(E)$. 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

$$\chi_f = \prod_{i=1}^r \mu_i \quad (6.782a)$$

$$\mu_f = \mu_1 \quad (6.782b)$$

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 caractéristique des $f|_{E_i}$, mais ces derniers endomorphismes étant cycliques⁶⁶, leurs polynôme caractéristique sont égaux à leurs polynômes minimaux (lemme 6.330). Cela prouve l'égalité (6.782a). Ensuite tous les μ_i doivent diviser le polynôme minimal, donc $\text{ppcm}(\mu_1, \dots, \mu_r)$ 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 $\text{ppcm}(\mu_1, \dots, \mu_r) = \mu_f$. Mais par ailleurs $\mu_1 = \text{ppcm}(\mu_1, \dots, \mu_r)$ 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 6.247). Le plus petit espace stable sous f contenant y est

$$E_y = \text{Span}\{y, f(y), \dots, f^{d-1}(y)\}. \quad (6.783)$$

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'étaient pas linéairement indépendants, alors nous aurions des a_k tels que $\sum_k a_k e_k = 0$ et avec lesquels

$$\left(\sum_k a_k X^k\right)(f)y = 0, \quad (6.784)$$

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 étendre⁶⁷ $\{e_1, \dots, e_d\}$ en une base $\{e_1, \dots, e_n\}$ de E . Ensuite nous allons montrer que

$$E = E_y \oplus F \quad (6.785)$$

avec

$$F = \{x \in E \text{ tel que } e_d^*(f^k(x)) = 0 \forall k \in \mathbb{N}\}. \quad (6.786)$$

Par construction, F est invariant sous f . Montrons pour commencer que $E_y \cap F = \{0\}$. Un élément de E_y s'écrit

$$z = a_1 e_1 + \dots + a_k e_k \quad (6.787)$$

avec $k \leq d$. Étant donné que f décale les vecteurs de base, nous avons $e_d^*(f^{d-k}(z)) = a_k$. Du coup $z \in F$ si et seulement si $a_1 = \dots = a_d = 0$, c'est à dire que $E_y \cap F = \{0\}$.

⁶⁶. Définition 6.248.

⁶⁷. Pour autant que j'aie compris, cette extension manque dans [106]. Corrigez moi si je me trompe.

Nous montrons maintenant que $\dim F = n - d$. Pour cela nous considérons l'application

$$\begin{aligned} T: \mathbb{K}[F] &\rightarrow E^* \\ g &\mapsto e_d^* \circ g. \end{aligned} \quad (6.788)$$

Cette application est injective. En effet un élément général de $\mathbb{K}[f]$ est

$$g = a_1 \text{Id} + a_2 f + \dots + a_p f^{p-1} \quad (6.789)$$

avec $p \leq d$. Si $T(g) = 0$, alors nous avons en particulier

$$0 = T(g)e_{d-p+1} = e_d^*(a_1 e_{d-p+1} + a_2 e_{d-p+2} + \dots + a_p e_d) = a_p. \quad (6.790)$$

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, $\dim \text{Image}(T) = d$. Nous regardons l'orthogonal de l'image :

$$(\text{Image}(T))^\perp = \{x \in E \text{ tel que } T(g)x = 0 \forall g \in \mathbb{K}[f]\} \quad (6.791a)$$

$$= \{x \in E \text{ tel que } e_d^*(g(x)) = 0 \forall g \in \mathbb{K}[f]\} \quad (6.791b)$$

$$= F. \quad (6.791c)$$

Par conséquent $F^\perp = \text{Image}(T)$. Vu que $\dim \text{Image}(T) = d$, 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 6.249 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 $F_1, \dots, F_r$ et $G_1, \dots, G_s$ de sous-espaces stables par f et vérifiant

$$(1) \quad E = \bigoplus_{i=1}^r F_i,$$

$$(2) \quad f|_{F_i} \text{ est cyclique,}$$

$$(3) \quad \mu_{f|_{F_{i+1}}} \text{ divise } \mu_{f|_{F_i}},$$

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 (6.782). Nous supposons que $P_i = Q_i$ pour $i \leq 1 \leq j-1$ et nous tentons de montrer que $P_j = Q_j$.

Nous avons

$$P_j(f) = P_j(f)|_{F_1} \oplus \dots \oplus P_j(f)|_{F_{j-1}}. \quad (6.792)$$

En effet étant donné que P_{j+k} divise P_j , nous avons⁶⁸ $P_j(f) = A(f) \circ P_{j+k}(f)$, mais $P_{j+k}(f)F_{j+k} = 0$, donc $P_j(f)F_{j+k} = 0$. Les espaces G_i n'ayant a priori aucun rapport avec les polynômes P_i , nous écrivons

$$P_j(f) = P_j(f)|_{G_1} \oplus \dots \oplus P_j(f)|_{G_{j-1}} \oplus P_j(f)|_{G_j} \oplus \dots \oplus P_j(f)|_{G_s}. \quad (6.793)$$

Pour $1 \leq i \leq j-1$, nous avons supposé $P_i = Q_i$. Étant donné que $f|_{F_i}$ est semblable à C_i et $f|_{G_i}$ est semblable à C_{Q_i} , la matrice de $f|_{E_i}$ est semblable à la matrice de $f|_{G_i}$. En particulier,

$$\dim P_j(f)F_i = \dim P_j(f)G_i. \quad (6.794)$$

En prenant les dimensions des images dans les égalités (6.792) et (6.793), nous trouvons que

$$P_j(f)|_{G_j} = \dots = P_j(f)|_{G_s} = 0. \quad (6.795)$$

68. En vertu du lemme 6.236.

Par conséquent $P_j \in I_{f|G_j}$ et donc P_j divise Q_j , qui est générateur de $I_{f|G_j}$. 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. □

Remarque 6.332.

Sous forme matricielle, ce théorème dit que toute matrice est semblable à une matrice de la forme bloc-diagonale

$$f = \begin{pmatrix} C_{\mu_1} & & \\ & \ddots & \\ & & C_{\mu_r} \end{pmatrix} \quad (6.796)$$

où les C_{μ_i} sont les matrices compagnon (définition 6.326).

En particulier, et ceci est très important, deux applications sont semblables si et seulement si elles ont même suite d'invariants de similitude.

Remarque 6.333.

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.

6.31.3 Forme normale de Jordan

Il existe une preuve directe de la réduction de Jordan ne nécessitant pas la réduction de Frobenius[99]. Cette dernière passe par les espaces caractéristiques⁶⁹ 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 Frobenius.

Théorème 6.334 (Réduction de Jordan).

Soit E un espace vectoriel sur $\mathbb{K}$, et $f \in \text{End}(E)$ un endomorphisme dont le polynôme caractéristique χ_f est scindé⁷⁰. Il existe une base de E dans laquelle la matrice de f s'écrit sous la forme

$$M = \begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_k}(\lambda_k) \end{pmatrix} \quad (6.797)$$

où les λ_i sont les valeurs propres de f (avec éventuelle répétitions) et $J_n(\lambda)$ représente le bloc $n \times n$

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \lambda & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}. \quad (6.798)$$

En d'autres termes, $J_n(\lambda)_{ii} = \lambda$ 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 .

⁶⁹. Aussi appelés «espaces propres généralisés».

⁷⁰. C'est pour cette hypothèse que $\mathbb{K} = \mathbb{R}$ n'est pas le bon cadre.

Nous savons par le lemme 6.328 que (la matrice de) f est semblable à sa matrice compagnon. En l'occurrence pour f nous avons

$$C_{X^m} = \begin{pmatrix} 0 & & 0 \\ 1 & \ddots & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix}. \quad (6.799)$$

Ensuite le changement de base (qui est une similitude) $(e_1, \dots, e_n) \mapsto (e_n, \dots, e_1)$ 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

$$\chi_f = (X - \lambda_1)^{l_1} \dots (X - \lambda_m)^{l_m}. \quad (6.800)$$

Le lemme des noyaux (théorème 6.237) nous enseigne que

$$E = \bigoplus_{i=1}^m \underbrace{\ker(f - \mu_i \mathbb{1})^{l_i}}_{F_i}. \quad (6.801)$$

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

$$f|_{F_i} = (f - \lambda_i \mathbb{1})|_{F_i} + \lambda_i \mathbb{1}_{F_i}, \quad (6.802)$$

nous voyons que $f|_{F_i}$ s'écrit comme un bloc de Jordan avec λ_i sur la diagonale. $\square$

Remarque 6.335.

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 Frobenius, elle, est disponible sur tout corps, y compris $\mathbb{R}$.

6.32 Commutant et endomorphismes cycliques

6.32.1 Endomorphisme cyclique

Lemme 6.336.

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

$$E_{f,x} = \text{Span}\{f^k(x) \text{ tel que } k \in \mathbb{N}\}. \quad (6.803)$$

Définition 6.337.

Soit E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et un endomorphisme $f: E \rightarrow E$. Le **commutant** de f est l'ensemble des endomorphismes de E qui commutent avec f :

$$\mathcal{C}(f) = \{g \in \mathcal{L}(E, E) \text{ tel que } g \circ f = f \circ g\}. \quad (6.804)$$

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.

6.32.2 Commutant : cas diagonalisable

Proposition 6.338 ([109]).

Si f est diagonalisable, alors

$$\dim(\mathcal{C}(f)) = \sum_{\lambda \in \text{Spec}(f)} \dim(E_\lambda)^2. \quad (6.805)$$

où les E_λ sont les espaces propres de f .

Démonstration. D'abord si $g \in \mathcal{C}(f)$ alors E_λ est stable par g . En effet si $v \in E_\lambda$ alors $f(g(v)) = g(f(v)) = g(\lambda v) = \lambda g(v)$, 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

$$\begin{aligned} \psi: \mathcal{C}(f) &\rightarrow \text{End}(E_1) \times \dots \times \text{End}(E_r) \\ g &\mapsto g|_{E_1} \times \dots \times g|_{E_r} \end{aligned} \quad (6.806)$$

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 .

ψ est injective Supposons que $g, h \in \mathcal{C}(f)$ tels que $\psi(g) = \psi(h)$. Vu que f est diagonalisable nous pouvons décomposer $x \in E$ en ses composantes sur les espaces propres⁷¹ :

$$x = \sum_{\lambda \in \text{Spec}(f)} x_\lambda \quad (6.807)$$

avec $x_\lambda \in E_\lambda$. Nous avons alors

$$g(x) = \sum_{\lambda} g(x_\lambda) = \sum_{\lambda} \psi(g)_\lambda(x_\lambda). \quad (6.808)$$

Vu que nous avons $\psi(g)_\lambda = \psi(h)_\lambda$, nous avons aussi

$$g(x) = \sum_{\lambda} \psi(g)_\lambda(x_\lambda) = \sum_{\lambda} \psi(h)_\lambda(x_\lambda) = \sum_{\lambda} h(x_\lambda) = h(x). \quad (6.809)$$

Cela prouve $g = h$ et donc que ψ est injective.

ψ est surjective Si nous avons pour chaque $\lambda \in \text{Spec}(f)$ un endomorphisme g_λ de E_λ alors en posant

$$g(x) = \sum_{\lambda \in \text{Spec}(f)} g_\lambda(x_\lambda) \quad (6.810)$$

alors nous avons bien

$$\psi(g) = (g_{\lambda_1}, \dots, g_{\lambda_r}). \quad (6.811)$$

Nous pouvons donc conclure en écrivant

$$\dim(\mathcal{C}(f)) = \sum_{\lambda \in \text{Spec}(f)} \dim(\text{End}(E_\lambda)) = \sum_{\lambda \in \text{Spec}(f)} \dim(E_\lambda)^2. \quad (6.812)$$

□

Remarque 6.339.

Nous avons alors immédiatement

$$\dim(\mathcal{C}(f)) \geq \dim(E) \quad (6.813)$$

lorsque f est diagonalisable.

⁷¹. Théorème 6.281(5).

En suivant la notation (6.594), un endomorphisme est cyclique lorsqu'il existe $x \in E$ tel que $E_x = E$.

Proposition 6.340 ([109]).

Si f est un endomorphisme diagonalisable d'un espace vectoriel E de dimension n . Nous avons équivalence entre les faits suivants.

- (1) Le polynôme minimal est égal au polynôme caractéristique : $\mu_f = \chi_f$
- (2) L'endomorphisme f est cyclique.
- (3) $\mathcal{C}(f) = \mathbb{K}[f]$.
- (4) $\dim(\mathcal{C}(f)) = n$
- (5) L'endomorphisme f possède n valeurs propres distinctes.
- (6) $\dim(\mathbb{K}[f]) = n$

Démonstration. Le point important de cette proposition sont les équivalences (1)-(3). Les autres sont des intermédiaires. En particulier, dans le cas diagonalisable, nous allons voir que le point (5) est essentiellement une reformulation de (1).

(4) implique (5) Par la formule (6.805), les espaces propres de f ont dimension 1. Par conséquent f possède n valeurs propres distinctes.

(5) implique (6) Le théorème 6.281 nous dit que le polynôme minimal est scindé à racines simples. Vu que f possède n valeurs propres distinctes, μ est de degré n . Par l'isomorphisme $\mathbb{K}[f] = \mathbb{K}[X]/(\mu)$ de la proposition 6.255 nous avons $\dim(\mathbb{K}[f]) = \deg(\mu) = n$ par la proposition 4.34.

(6) implique (1) Par l'isomorphisme $\mathbb{K}[f] = \mathbb{K}[X]/(\mu)$ de la proposition 6.255 et la proposition 4.34 nous avons $n = \dim(\mathbb{K}[f]) = \deg(\mu)$. Vu que χ est un polynôme annulateur (Caley-Hamilton 6.262), il est divisé par μ . Maintenant μ et χ sont des polynômes unitaires de degré n et μ divise χ . Ils sont donc égaux.

(1) implique (2) Le fait que f soit diagonalisable permet d'utiliser le théorème 6.281 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 $v = e_1 + \dots + e_n$ est cyclique. Nous avons

$$f^k(v) = \sum_{i=1}^n \lambda_i^k e_i. \quad (6.814)$$

Pour prouver que cette famille (avec $k = 0, \dots, n-1$) est libre⁷² nous en prenons une combinaison linéaire nulle et nous prouvons que les coefficients sont tous nuls. Soit donc

$$0 = \sum_{l=0}^{n-1} a_l f^l(v) = \sum_{l=0}^{n-1} a_l \sum_{i=1}^n \lambda_i^l e_i = \sum_{i=1}^n \left(\sum_{l=0}^{n-1} a_l \lambda_i^l \right) e_i. \quad (6.815)$$

Vu que cela est nul, nous avons pour tout i :

$$\sum_{l=0}^{n-1} a_l \lambda_i^l = 0. \quad (6.816)$$

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 et elle est $a_j = 0$ pour tout j . Nous devons donc calculer le déterminant

$$\det \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \cdots & \lambda_n^{n-1} \end{pmatrix}. \quad (6.817)$$

⁷². Ce sera alors une base parce que n vecteurs libres dans un espace de dimension n est toujours une base, théorème 6.8(3).

Il s'agit du déterminant de Vandermonde déjà étudié par la proposition 6.50. Nous avons $\det(A) = \prod_{1 \leq i < j \leq n} (\lambda_j - \lambda_i)$. Cela est bien non nul du fait que toutes les valeurs propres soient distinctes.

(2) implique (3) Soit v un vecteur cyclique de f . Un endomorphisme g donne lieu à un polynôme par le fait suivant : il existe des uniques a_k ($k = 0, \dots, n-1$) tels que

$$g(v) = \sum_{k=0}^{n-1} a_k f^k(v). \quad (6.818)$$

Cela donne une application linéaire

$$\begin{aligned} \psi: \mathcal{C}(f) &\rightarrow \mathbb{K}[f] \\ g &\mapsto P \text{ tel que } P(f)v = g(v). \end{aligned} \quad (6.819)$$

C'est une application injective parce que si $\psi(g) = 0$ alors $g(v) = 0$ et pour tout k nous avons $g(f^k(v)) = f^k(g(v)) = 0$. L'endomorphisme g s'annulant sur une base, est nul.

(3) implique (4) Si $n_1, \dots, n_r$ sont les dimensions des différents espaces propres de f , nous avons les inégalités

$$\dim(\mathbb{K}[f]) = \deg(\mu) \leq n = n_1 + \dots + n_r \leq n_1^2 + \dots + n_r^2 = \dim(\mathcal{C}(f)). \quad (6.820)$$

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 $\dim(\mathcal{C}(f)) = n$.

Nous avons fini de prouver toutes les équivalences demandées. $\square$

Exemple 6.341

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 exemples 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. $\triangle$

6.32.3 Commutant : cas général

Nous considérons encore un espace vectoriel E de dimension finie n et un endomorphisme $f: E \rightarrow E$. Nous notons μ son polynôme minimal et μ_x le polynôme minimal ponctuel en x .

Lemme 6.342 ([110, 106, 78]).

Nous avons

$$\dim(\mathcal{C}(f)) \geq \dim(E) \quad (6.821)$$

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 $AX - XA = 0$.

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 supérieures. 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

$$(AX - XA)_{kk} = \sum_i (A_{ki}X_{ik} - X_{ki}A_{ik}) = \sum_{k \leq i \leq k} (A_{ki}X_{ik} - X_{ki}A_{ik}) = 0. \quad (6.822)$$

Nous avons donc au maximum

$$\frac{n(x+1)}{2} - n \quad (6.823)$$

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.

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 6.331. 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 $\text{End}(E_i)$. Mais en prolongeant par 0 sur E , ça reste libre en tant que partie de $\text{End}(E)$.

Bien entendu les f_j^k et les f_i^k ($i \neq j$) sont linéairement indépendants dans $\text{End}(E)$ 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 $\text{End}(E)$ composée d'endomorphismes qui commutent avec f . Il y en a en tout

$$\sum_{i=1}^r \deg(\mu_i) = \deg(\chi_f) = n. \quad (6.824)$$

Par conséquent $\dim(\mathcal{C}(f)) \geq \dim(E)$.

□

Théorème 6.343 ([95]).

Soit un endomorphisme $f: E \rightarrow E$ sur l'espace vectoriel de dimension finie n . Nous notons μ et χ les polynômes minimal et caractéristique. Nous avons équivalence entre les faits suivants :

- (1) $\mu = \chi$,
- (2) f est cyclique,
- (3) $\mathcal{C}(f) = \mathbb{K}[f]$.

Démonstration. Plusieurs implications. Notons que (1) implique (1) a déjà été démontré par le lemme 6.330.

(1) implique (2) Conformément à ce que nous permet le lemme 6.247 nous choisissons ⁷³ $a \in E$ de telle sorte à avoir $\mu_a = \mu$. De plus pour $x \in E$ nous considérons l'application

$$\begin{aligned} \varphi_x: \mathbb{K}[X] &\rightarrow E \\ P &\mapsto P(f)x. \end{aligned} \quad (6.825)$$

Nous avons $\varphi_a(P) = P(f)a$ et vu que E_a est engendré par les $f^k(a)$ nous avons $\varphi_a(\mathbb{K}[X]) = E_a$. 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

$$\bar{P} = \{P + Q\mu_a\}_{Q \in \mathbb{K}[X]}. \quad (6.826)$$

Nous considérons donc l'application

$$\varphi_a: \frac{\mathbb{K}[X]}{(\mu_a)} \rightarrow E_a \quad (6.827)$$

et nous prouvons que c'est un isomorphisme d'espace vectoriel.

⁷³. Dans toute la suite, nous devrions écrire μ_f et $\mu_{f,a}$ mais nous omettons d'indiquer explicitement la dépendance en f .

Linéaire Parce que $(\lambda P + Q)(f) = (\lambda P)(f) + Q(f)$.

Injectif Si $\varphi_a(\bar{P}) = 0$ alors $\varphi_a(P) = 0$ (dans la deuxième, φ_a est l'application définie sur les polynômes et non sur les classes), ce qui montre que P est annulateur de a . Mais par définition 6.243 du polynôme minimal ponctuel, μ_a est générateur de $\ker(\varphi_a)$; donc il existe $Q \in \mathbb{K}[X]$ tel que $P = Q\mu_a$. En d'autres termes, du point de vue du quotient, $\bar{P} = 0$.

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 $x = P(f)a = \varphi_a(P)$.

Mais par hypothèse et par choix de a nous avons $\mu_a = \mu = \chi$, donc en fait $E_a = \mathbb{K}[X]/(\chi)$. Mais nous savons que $\deg(\chi) = \dim(E)$ et que $\dim(\mathbb{K}[X]/P) = \deg(P)$ par la proposition 6.255. 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 .

(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 $g = P(f)$. Soit $y \in E$ et un polynôme Q tel que $y = Q(f)v$; en notant que g commute avec $P(f)$ nous avons

$$g(y) = g(Q(f)v) = Q(f)(g(v)) = Q(f)(P(f)v) = P(f)Q(f)v = P(f)y. \quad (6.828)$$

Donc $g = P(f)$.

(3) implique (1) Nous avons les inégalités :

$$n \leq \dim(\mathcal{C}(f)) = \dim(\mathbb{K}[f]) = \deg(\mu) \leq \deg(\chi) = n. \quad (6.829)$$

La première est le lemme 6.342. Toutes les inégalités sont 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 .

□

Corollaire 6.344 ([78]).

En suivant les notations sur les extensions de corps de base de la section 6.30, l'endomorphisme $f: E \rightarrow F$ est cyclique si et seulement si l'endomorphisme $f_{\mathbb{L}}: E_{\mathbb{L}} \rightarrow F_{\mathbb{L}}$ est cyclique.

Démonstration. Nous savons par le théorème 6.343 qu'un endomorphisme est cyclique si et seulement si son polynôme minimal est égal à son polynôme caractéristique. Or par les propositions 6.324 et 6.325, nous savons que ces polynômes sont identiques pour f et pour $f_{\mathbb{L}}$. □

Théorème 6.345 (Similitude et extension de corps[78]).

Les applications linéaires $f, g: E \rightarrow E$ 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 $m \in \text{GL}(E)$ tel que $f = mgm^{-1}$ alors il suffit d'appliquer le lemme 6.320 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 6.331. Il existe une unique suite de polynômes unitaires μ_i ($i = 1, \dots, s$) tels que $\mu_i \mid \mu_{i+1}$ et pour laquelle nous avons une décomposition $E = E_1 \oplus \dots \oplus E_s$ pour laquelle $f|_{E_i}: E_i \rightarrow E_i$ est cyclique et de polynôme minimal μ_i .

Nous avons aussi $E_{\mathbb{L}} = (E_1)_{\mathbb{L}} \oplus \dots \oplus (E_s)_{\mathbb{L}}$ et les $(E_i)_{\mathbb{L}}$ sont stables sous $f_{\mathbb{L}}$ qui y sera également cyclique (corollaire 6.344). 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 6.332 nous permet de conclure que f et g sont semblables si et seulement si $f_{\mathbb{L}}$ et $g_{\mathbb{L}}$ le sont. □

6.33 Endomorphismes nilpotents et trigonalisables

6.33.1 Endomorphismes nilpotents

La **trace** d'une matrice $A \in \mathbb{M}(n, \mathbb{K})$ est la somme de ses éléments diagonaux :

$$\mathrm{Tr}(A) = \sum_{i=1}^n A_{ii}. \quad (6.830)$$

Une propriété importante est son invariance cyclique.

Lemme 6.346.

Si A et B sont des matrices carrées, alors $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

La trace est un invariant de similitude.

Démonstration. C'est un simple calcul :

$$\mathrm{Tr}(AB) = \sum_{ik} A_{ik} B_{ki} = \sum_{ik} A_{ki} B_{ik} = \sum_{ik} B_{ik} A_{ki} = \sum_i (BA)_{ii} = \mathrm{Tr}(BA) \quad (6.831)$$

où nous avons simplement renommé les indices $i \leftrightarrow k$.

En particulier, la trace est un invariant de similitude parce que $\mathrm{Tr}(ABA^{-1}) = \mathrm{Tr}(A^{-1}AB) = \mathrm{Tr}(B)$. $\square$

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.

Lemme 6.347 ([35]).

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 (6.627) est

$$\chi_u = (-1)^n X^\alpha (X - \lambda_1)^{\alpha_1} \dots (X - \alpha_r)^{\alpha_r}. \quad (6.832)$$

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 (6.832), nous voyons que le coefficient du terme X^{n-1} dans le polynôme caractéristique est

$$0 = \mathrm{Tr}(u^p) = \alpha_1 \lambda_1^p + \dots + \alpha_r \lambda_r^p. \quad (6.833)$$

Donc les nombres $(\alpha_1, \dots, \alpha_r)$ est une solution non triviale⁷⁴ du système

$$\begin{cases} \alpha_1 X_1 + \dots + \lambda_r X_r = 0 & (6.834a) \\ \vdots & (6.834b) \\ \lambda_1^r X_1 + \dots + \lambda_r^r X_r = 0. & (6.834c) \end{cases}$$

Cela sont les équations (6.833) écrites avec $p = 1, \dots, r$. Le déterminant de ce système est

$$\lambda_1 \dots \lambda_r \det \begin{pmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_1 \\ \vdots & & \vdots \\ \lambda_1^{r-1} & \dots & \lambda_r^{r-1} \end{pmatrix} \neq 0, \quad (6.835)$$

74. Si $\alpha_1 = \dots = \alpha_r = 0$, alors les valeurs propres sont toutes nulles et la matrice est en réalité nulle dès le départ.

qui est un déterminant de Vandermonde (proposition 6.50) valant

$$0 = \lambda_1 \dots \lambda_r \prod_{1 \leq i \leq j \leq r} (\lambda_i - \lambda_j). \quad (6.836)$$

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 (6.834). $\square$

Proposition 6.348 ([111]).

Soit un $\mathbb{K}$ -espace vectoriel E . Un endomorphisme $u \in \text{End}(E)$ est nilpotent si et seulement si il existe une base de E dans laquelle la matrice de u est strictement triangulaire supérieure.

Démonstration. $\Rightarrow$ Nous faisons la démonstration par récurrence sur la dimension de E . Lorsque $n = 1$ nous avons $u = (a)$ avec $a \in \mathbb{K}$. Vu que $a^k = 0$ pour un certain k nous avons $a = 0$ parce qu'un corps est toujours un anneau intègre⁷⁵.

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

$$\{x, e_2, \dots, e_n\} \quad (6.837)$$

donnée par le théorème de la base incomplète 6.5. La matrice de u dans cette base s'écrit

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A & \\ 0 & & & \end{array} \right). \quad (6.838)$$

Un tout petit peu de calcul de produit de matrice montre que la matrice de u^k est de la forme

$$\left(\begin{array}{c|ccc} 0 & * & * & * \\ \hline 0 & & & \\ 0 & & A^k & \\ 0 & & & \end{array} \right). \quad (6.839)$$

Étant donné que u est nilpotente, 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).

$\Leftarrow$ Lorsqu'une matrice est triangulaire supérieure stricte, elle applique

$$\text{Span}\{e_1, \dots, e_k\} \rightarrow \text{Span}\{e_1, \dots, e_{k-1}\}. \quad (6.840)$$

Donc tout vecteur finit sur zéro si on lui applique u assez souvent. $\square$

Proposition 6.349.

Soit $A \in \text{GL}(n, \mathbb{C})$. La suite $(A^k)_{k \in \mathbb{Z}}$ est bornée si et seulement si A est diagonalisable et $\text{Spec}(A) \subset \mathbb{S}^1$.

Démonstration. Si A est diagonalisable avec les valeurs propres λ_i de norme 1 dans $\mathbb{C}$, alors A^k est la matrice diagonale avec les λ_i^k sur la diagonale. Cela reste borné pour toute valeur entière de k .

En ce qui concerne l'autre sens, nous supposons encore que

$$A = \begin{pmatrix} \lambda_1 \mathbb{1} + N_1 & & \\ & \ddots & \\ & & \lambda_s \mathbb{1} + N_s \end{pmatrix}, \quad (6.841)$$

⁷⁵. Lemme 4.2.

et nous regardons un des blocs. Nous voulons prouver que $N = 0$ et que $|\lambda| = 1$.

Nous commençons par regarder ce qu'implique le fait que $(\lambda \mathbb{1} + N)^n$ reste borné pour $n > 0$. En notant r l'ordre de nilpotence de N , nous avons le développement

$$(\lambda \mathbb{1} + N)^n = \sum_{k=0}^{r-1} \binom{n}{k} N^k \lambda^{n-k}. \quad (6.842)$$

Par la proposition 6.348, une matrice nilpotente s'écrit dans une base sous la forme

$$N = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix} \quad (6.843)$$

et effectuer A^k revient à décaler la diagonale de 1. Donc la famille

$$\{\mathbb{1}, N, \dots, N^{r-1}\} \quad (6.844)$$

est libre. Par conséquent la suite $(\lambda \mathbb{1} + N)^n$ restera bornée si et seulement si chacun des termes

$$\binom{n}{k} N^k \lambda^{n-k} \quad (6.845)$$

reste borné. Le premier terme étant $\lambda^n \mathbb{1}$, nous avons obligatoirement $|\lambda| \leq 1$. Si $|\lambda| < 1$, alors le coefficient $\binom{n}{k} \lambda^{n-k}$ tend vers zéro. Si $|\lambda| = 1$ par contre ce coefficient tend vers l'infini et la seule façon pour que (6.845) reste borné est que $N = 0$. Nous avons donc deux possibilités :

- $|\lambda| < 1$
- $|\lambda| = 1$ et $N = 0$.

Nous nous tournons maintenant sur la contrainte que $(\lambda \mathbb{1} + N)^n$ doive rester borné pour $n < 0$. Nous avons

$$\lambda \mathbb{1} + N = \lambda(\mathbb{1} + \lambda^{-1}N), \quad (6.846)$$

et nous pouvons appliquer la proposition 6.157 à l'opérateur nilpotent $-\lambda^{-1}N$ pour avoir

$$(\mathbb{1} + \lambda^{-1}N)^{-1} = \mathbb{1} + \sum_{k=1}^{\infty} (-\lambda)^{-1} N^k. \quad (6.847)$$

Ceci pour dire que $(\lambda \mathbb{1} + N)^{-1} = \lambda^{-1}(\mathbb{1} + \lambda^{-1}N')$ pour une autre matrice nilpotente N' . Le travail déjà fait, appliqué à λ^{-1} et N' , nous donne deux possibilités :

- $|\lambda^{-1}| < 1$
- $|\lambda^{-1}| = 1$ et $N' = 0$.

La possibilité $|\lambda^{-1}| < 1$ est exclue parce qu'elle impliquerait $|\lambda| > 1$ qui avait déjà été exclu. Il ne reste donc que la possibilité $|\lambda| = 1$ et $N = N' = 0$. $\square$

6.33.2 Endomorphismes trigonalisables

Définition 6.350 ([112]).

Une matrice dans $\mathbb{M}(n, \mathbb{K})$ est **trigonalisable** lorsqu'elle est semblable⁷⁶ à une matrice triangulaire supérieure.

Proposition 6.351.

Soit u un endomorphisme d'un espace vectoriel E sur le corps $\mathbb{K}$. Les faits suivants sont équivalents.

- (1) L 'endomorphisme u est trigonalisable (auquel cas les valeurs propres sont sur la diagonale).

⁷⁶. Définition 6.277.

(2) Le polynôme caractéristique de u est scindé⁷⁷.

Démonstration. (2)⇒(1) Nous avons par hypothèse que

$$\chi_u(X) = \prod_{i=1}^r (X - \lambda_i)^{\alpha_i} \quad (6.848)$$

où les λ_i sont les valeurs propres de u . Le théorème de Cayley-Hamilton 6.262 dit que $\chi_u(u) = 0$, ce qui permet d'utiliser le théorème de décomposition des noyaux 6.237 :

$$E = \ker(X - \lambda_1)^{\alpha_1} \oplus \dots \oplus \ker(X - \lambda_r)^{\alpha_r}. \quad (6.849)$$

Les espaces $F_{\lambda_i}(u) = \ker(X - \lambda_i)^{\alpha_i}$ sont les espaces caractéristiques de u , ce qui fait que $u - \lambda_i \mathbb{1}$ est nilpotent sur $F_{\lambda_i}(u)$. L'endomorphisme $u - \lambda_i \mathbb{1}$ est donc strictement trigonalisable supérieur sur son bloc⁷⁸. Cela signifie que u est triangulaire supérieure avec les valeurs propres sur la diagonale.

(1)⇒(2) C'est immédiat parce que le déterminant d'une matrice triangulaire est le produit des éléments de sa diagonale. □

Remarque 6.352.

Si $\mathbb{K}$ est algébriquement clos (comme $\mathbb{C}$ par exemple), alors tous les polynômes sont scindés et toutes les matrices sont trigonalisables⁷⁹. Un exemple un peu simple de cela est la matrice

$$u = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \quad (6.850)$$

Le polynôme caractéristique est $\chi_u(X) = X^2 + 1$ et les valeurs propres sont $\pm i$. Il est vite vu que dans la base

$$\left\{ \begin{pmatrix} i \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ i \end{pmatrix} \right\} \quad (6.851)$$

de $\mathbb{C}^2$, la matrice u se note $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

Remarque 6.353.

Cela nous donne une autre façon de prouver qu'une matrice nilpotente de $M(n, \mathbb{C})$ ou $M(n, \mathbb{R})$ est trigonalisable[113]. D'abord dans $M(n, \mathbb{C})$, toutes les matrices sont trigonalisables⁸⁰, et les valeurs propres arrivent sur la diagonale. Mais comme les valeurs propres d'une matrice nilpotente sont zéro, elle est triangulaire stricte. Par ailleurs son polynôme caractéristique est alors X^n .

Ensuite si $u \in M(n, \mathbb{R})$ nous pouvons voir u comme une matrice dans $M(n, \mathbb{C})$ et y calculer son polynôme caractéristique qui sera tout de même X^n . Ce polynôme étant scindé, la proposition 6.351 nous assure que u est trigonalisable. Une fois de plus, les valeurs propres étant sur la diagonale, elle est triangulaire supérieure stricte.

Remarque 6.354.

La méthode des pivots de Gauss⁸¹ certes permet de trigonaliser n'importe quoi, mais elle ne correspond pas à un changement de base. Autrement dit, les pivots de Gauss ne sont pas de similitudes.

C'est là qu'il faut bien avoir en tête la différence entre *équivalence* et *similarité* (définition 6.14). Lorsqu'on parle de changement de base, de matrice trigonalisable ou diagonalisable, nous parlons de similarité et non d'équivalence.

⁷⁷. Définition 3.99.

⁷⁸. Proposition 6.348.

⁷⁹. Le lemme de Schur complexe 6.288 va un peu plus loin et précise que la trigonalisation peut être faite par une matrice unitaire.

⁸⁰. Parce que le polynôme caractéristique est scindé, voir remarque 6.352.

⁸¹. Le lemme 6.15.

6.33.3 Théorème de Burnside

Lemme 6.355.

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 6.356.

Toute représentation d'un groupe abélien d'exposant fini sur $\mathbb{C}^n$ a une image finie.

Démonstration. Dans le cas d'un groupe abélien, la démonstration est facile. 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 6.355 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 6.281). 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

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}. \quad (6.852)$$

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. $\square$

Théorème 6.357 (Burnside[35, 114]).

Un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$ est fini si et seulement si il est d'exposant⁸² fini.

Démonstration. Soit G un sous-groupe de $\mathrm{GL}(n, \mathbb{C})$. Si G est fini, l'ordre de ses éléments divise $|G|$ (corollaire 2.40) au théorème de Lagrange et l'exposant est le PPCM qui est donc fini également.

Nous supposons maintenant que l'ordre de G est fini. Nous notons e l'exposant de G . En particulier, tous les éléments de G sont des racines du polynôme $X^e - 1$.

Générateurs Le groupe G est une partie de $\mathbb{M}(n, \mathbb{C})$ dont nous considérons l'algèbre engendrée (définition 4.4) $\mathcal{G}$. Soit $C_1, \dots, C_r$ une famille génératrice de $\mathcal{G}$ constituée d'éléments de G et la fonction

$$\begin{aligned} \tau: G &\rightarrow \mathbb{C}^r \\ A &\mapsto (\mathrm{Tr}(AC_1), \dots, \mathrm{Tr}(AC_r)). \end{aligned} \quad (6.853)$$

τ est injective Supposons que $\tau(A) = \tau(B)$. Alors pour tout générateur C_i nous avons $\mathrm{Tr}(AC_i) = \mathrm{Tr}(BC_i)$ et par linéarité de la trace, nous avons

$$\mathrm{Tr}(AM) = \mathrm{Tr}(BM) \quad (6.854)$$

pour tout $M \in G$. Notons par ailleurs

$$N = AB^{-1} - \mathbb{1}, \quad (6.855)$$

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 $P(AB^{-1} - \mathbb{1})P^{-1} = D - \mathbb{1}$ qui est encore diagonale. Donc N est diagonalisable.

Par ailleurs nous avons

$$\mathrm{Tr}((AB^{-1})^p) = \mathrm{Tr}(AB^{-1}(AB^{-1})^{p-1}) \quad (6.856a)$$

$$= \mathrm{Tr}(BB^{-1}(AB^{-1})^{p-1}) \quad (6.854) \quad (6.856b)$$

$$= \mathrm{Tr}((AB^{-1})^{p-1}). \quad (6.856c)$$

82. Définition 2.12.

En continuant nous obtenons

$$\operatorname{Tr}((AB^{-1})^p) = \operatorname{Tr}(\mathbb{1}) = n. \quad (6.857)$$

D'autre part,

$$N^k = (AB^{-1} - \mathbb{1})^k = \sum_{p=0}^k \binom{k}{p} (-1)^{k-p} (AB^{-1})^p \quad (6.858)$$

En prenant la trace, et en tenant compte du fait que $\operatorname{Tr}((AB^{-1})^p) = n$,

$$\operatorname{Tr}(N^k) = \sum_{p=0}^k \binom{k}{p} (-1)^{k-p} n = n(1-1)^k = 0. \quad (6.859)$$

Donc la trace de N^k est nulle et le lemme 6.347 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.

Nombre fini de valeurs Les éléments de G sont annulés par $X^e - 1$ qui est un polynôme scindé à racines simples. Donc le polynôme minimal d'un élément de G est (a fortiori) scindé à racines simples et le théorème 6.281 nous assure alors que ces éléments sont diagonalisables. Du coup les valeurs propres des matrices de G sont des racines e èmes 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 èmes de l'unité. Mais vu que les C_i sont dans G , nous avons

$$\operatorname{Image}(\tau) = \{\operatorname{Tr}(A) \text{ tel que } A \in G\}^r, \quad (6.860)$$

qui est un ensemble fini. Par conséquent G est fini parce que τ est injective. □

6.33.4 Théorème de Lie-Kolchin

Contrairement à ce que l'on peut parfois 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 6.358

Le théorème 6.281 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

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (6.861)$$

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

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \quad (6.862)$$

qui revient au système

$$\begin{cases} x + y = x \\ y = y. \end{cases} \quad (6.863a)$$

$$(6.863b)$$

La première équation donne directement $y = 0$. Le seul espace propre est de dimension 1 et est engendré par $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. △

La remarque 6.301 donne un exemple un peu plus avancé, qui montre la multiplicité algébrique et géométrique d'une racine d'un polynôme caractéristique.

Lemme 6.359 (Trigonalisation simultanée).

Une famille de matrices de $\mathrm{GL}(n, \mathbb{C})$ commutant deux à deux est simultanément trigonalisable.

Démonstration. Commençons par enfoncer une porte ouverte par la proposition 6.351 : sur $\mathrm{GL}(n, \mathbb{C})$ toutes les matrices sont trigonalisables parce que tous les polynômes sont scindés.

Nous effectuons la démonstration par récurrence sur la dimension. Si $n = 1$ alors toutes les matrices sont triangulaires et nous ne nous posons pas de questions. Nous supposons donc $n > 1$.

Soit la famille $(A_i)_{i \in I}$ dans $\mathrm{GL}(n, \mathbb{C})$ et A_0 un de ses éléments. Nous nommons $\lambda_1, \dots, \lambda_r$ les valeurs propres distinctes de A_0 . Le théorème de décomposition primaire 6.302 nous donne la somme directe d'espaces caractéristiques⁸³

$$E = F_{\lambda_1}(A_0) \oplus \dots \oplus F_{\lambda_r}(A_0). \quad (6.864)$$

Nous pouvons supposer que cette somme n'est pas réduite à un seul terme. En effet si tel était le cas, A_0 serait un multiple de l'identité parce que A_0 n'aurait qu'une seule valeur propre et les sommes dans la décomposition de Dunford 6.303(3) se réduisent à un seul terme (et $p_i = \mathrm{Id}$). En particulier les dimensions des espaces $F_{\lambda}(A_0)$ sont strictement plus petites que n .

Vu que tous les A_i commutent avec A_0 , les espaces $F_{\lambda}(A_0)$ sont stables par les A_i et nous pouvons trigonaliser les A_i simultanément sur chacun des $F_{\lambda}(A_0)$ en utilisant l'hypothèse de récurrence. $\square$

Théorème 6.360 (Lie-Kolchin[2]).

Tout sous-groupe connexe et résoluble de $\mathrm{GL}(n, \mathbb{C})$ est conjugué à un groupe de matrices triangulaires.

Démonstration. Soit G un sous-groupe connexe et résoluble de $\mathrm{GL}(n, \mathbb{C})$.

Si sous-espace non trivial stable par G Nous commençons par voir ce qu'il se passe si il existe un sous-espace vectoriel non trivial V de $\mathbb{C}^n$ stabilisé par G . Pour cela nous considérons une base de $\mathbb{C}^n$ dont les premiers éléments forment une base de V (base incomplète, théorème 6.5). Les éléments de G s'écrivent, dans cette base,

$$\begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix}. \quad (6.865)$$

Les matrices g_1 et g_2 sont carrés. Nous considérons alors l'application ψ définie par

$$\begin{aligned} \psi: G &\rightarrow \mathrm{GL}(V) \\ g &\mapsto g_1. \end{aligned} \quad (6.866)$$

Cela est un morphisme de groupes parce que

$$\begin{pmatrix} g_1 & * \\ 0 & g_2 \end{pmatrix} \begin{pmatrix} h_1 & * \\ 0 & h_2 \end{pmatrix} = \begin{pmatrix} g_1 h_1 & * \\ 0 & g_2 h_2 \end{pmatrix}, \quad (6.867)$$

de telle sorte que $\psi(gh) = \psi(g)\psi(h)$.

Le groupe $\psi(G)$ est connexe et résoluble. En effet $\psi(G)$ est connexe en tant qu'image d'un connexe par une application continue (proposition 5.69). Et il est résoluble en tant qu'image d'un groupe résoluble par un homomorphisme par la proposition 2.55. Vu que $\psi(G)$ est un sous-groupe résoluble et connexe de $\mathrm{GL}(V)$ et que la dimension de V est strictement plus petite que celle de $\mathbb{C}^n$, une récurrence sur la dimension indique que $\psi(G)$ est conjugué à un groupe de matrices triangulaires. C'est à dire qu'il existe une base de V dans laquelle toutes les matrices g_1 (avec $g \in G$) sont triangulaires supérieures.

On fait de même avec l'application $g \mapsto g_2$, ce qui donne une base du supplémentaire de V dans laquelle les matrices g_2 sont triangulaires.

En couplant ces deux bases, nous obtenons une base de $\mathbb{C}^n$ dans laquelle toutes les matrices (6.865) (c'est à dire toutes les matrices de G) sont triangulaires supérieures.

83. Définition 6.299.

Sinon Nous supposons à présent que $\mathbb{C}^n$ n'a pas de sous-espaces non triviaux stables sous G . Nous posons $m = \min\{k \text{ tel que } D^k(G) = \{e\}\}$, qui existe parce que G est résoluble et que sa suite dérivée termine sur e (proposition 2.54).

Si $m = 1$ Si $m = 1$ alors G est abélien et il existe une base de G dans laquelle toutes les matrices de G sont triangulaires (lemme 6.359). Le premier vecteur d'une telle base serait stable par G , mais comme nous avons supposé qu'il n'y avait pas de sous-espaces non triviaux stabilisés par G , il faut déduire que ce vecteur stable est à lui tout seul non trivial, c'est à dire que $n = 1$. Dans ce cas, le théorème est démontré.

Si $m > 1$ Nous devons maintenant traiter le cas où $m > 1$. Nous posons $H = D^{m-1}(G)$; cela est un sous-groupe normal et abélien de G . Encore une fois le résultat de trigonalisation simultanée 6.359 donne une base dans laquelle tous les éléments de H sont triangulaires. En particulier le premier élément de cette base est un vecteur propre commun à toutes les matrices de H .

Soit V le sous-espace engendré par tous les vecteurs propres communs de H . Nous venons de voir que V n'est pas vide. Nous allons montrer que V est stable par G . Soient $h \in H$, $v \in V$ et $g \in G$:

$$h(g(v)) = g \underbrace{g^{-1}hg}_{\in H}(v) = g(\lambda v) = \lambda g(v) \quad (6.868)$$

parce que v est vecteur propre de $g^{-1}hg$. Ce que le calcul (6.868) montre est que $g(v)$ est vecteur propre de h pour la valeur propre λ . Donc $g(v) \in V$ et V est stabilisé par G . Mais comme il n'existe pas d'espaces non triviaux stabilisés par G , nous en déduisons que $V = \mathbb{C}^n$. Donc tous les vecteurs de $\mathbb{C}^n$ sont vecteurs propres communs de H . Autrement dit on a une base de diagonalisation simultanée de H .

H est dans le centre de G Montrons à présent que H est dans le centre de G , c'est à dire que pour tout $g \in G$ et $h \in H$ il faut $ghg^{-1} = h$. D'abord ghg^{-1} est une matrice diagonale (parce que elle est dans H) ayant les mêmes valeurs propres que h . En effet si λ est valeur propre de ghg^{-1} pour le vecteur propre v , alors

$$(ghg^{-1})(v) = \lambda v \quad (6.869a)$$

$$h(g^{-1}v) = \lambda(g^{-1}v), \quad (6.869b)$$

c'est à dire que λ est également valeur propre de h , pour le vecteur propre $g^{-1}v$. Mais comme h a un nombre fini de valeurs propres, il n'y a qu'un nombre fini de matrices diagonales ayant les mêmes valeurs propres que h . L'ensemble $\mathbf{Ad}(G)h$ est donc un ensemble fini. D'autre part, l'application $g \mapsto g^{-1}hg$ est continue, et G est connexe, donc l'ensemble $\mathbf{Ad}(G)h$ est connexe. Un ensemble fini et connexe dans $\mathrm{GL}(n, \mathbb{C})$ est nécessairement réduit à un seul point. Cela prouve que $ghg^{-1} = h$ pour tout $g \in G$ et $h \in H$.

Espaces propres stables pour tout G Soit $h \in H$ et W un espace propre de h (ça existe non vide parce que H est triangularisé, voir plus haut). Alors nous allons prouver que W est stable pour tous les éléments de G . En effet si $w \in W$ avec $h(w) = \lambda w$ alors en permutant g et h ,

$$hg(w) = g(hw) = \lambda g(w), \quad (6.870)$$

donc $g(w)$ est aussi vecteur propre de h pour la valeur propre λ , c'est à dire que $g(w) \in W$. Vu que nous supposons que $\mathbb{C}^n$ n'a pas d'espaces invariants non triviaux, nous devons conclure que $W = \mathbb{C}^n$, c'est à dire que H est composé d'homothéties. C'est à dire que pour tout $h \in H$ nous avons $h = \lambda_h \mathbb{1}$.

Contradiction sur la minimalité de m Les éléments d'un groupe dérivé sont de déterminant 1 parce que $\det(g_1 g_2 g_1^{-1} g_2^{-1}) = 1$. Par conséquent pour tout h , le nombre λ_h est une racine n^{e} de l'unité. Vu qu'il n'y a qu'une quantité finie de racines n^{e} de l'unité, le groupe H est fini et connexe et donc une fois de plus réduit à un élément, c'est à dire $H = \{e\}$. Cela contredit la minimalité de m et donc produit une contradiction. Nous devons donc avoir $m = 1$.

Conclusion Nous avons vu que si $\mathbb{C}^n$ avait un sous-espace non trivial fixé par G alors le théorème était démontré. Par ailleurs si $\mathbb{C}^n$ n'a pas un tel sous-espace, soit $m = 1$ (et alors le théorème est également prouvé), soit $m > 1$ et alors on a une contradiction.

Bref, le théorème est prouvé sous peine de contradiction.

□

6.34 Formes bilinéaires et quadratiques

6.34.1 Généralités

Définition 6.361 ([115]).

Soit un espace vectoriel E et $\mathbb{F}$ un corps de caractéristique différente de 2. Une **forme quadratique** sur E est une application $q: V \rightarrow \mathbb{F}$ pour laquelle il existe une forme bilinéaire symétrique $b: V \times V \rightarrow \mathbb{F}$ satisfaisant $q(x) = b(x, x)$ pour tout $x \in V$.

L'ensemble des formes quadratiques réelles sur E est noté $Q(E)$.

Lemme 6.362.

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** :

$$b(x, y) = \frac{1}{2}(q(x) + q(y) - q(x - y)). \quad (6.871)$$

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.

6.34.2 Topologie

La topologie considérée sur $Q(E)$ est celle de la norme

$$N(q) = \sup_{\|x\|_E=1} |q(x)|, \quad (6.872)$$

qui du point de vue de $S_n(\mathbb{R})$ est

$$N(A) = \sup_{\|x\|_E=1} |x^t A x|. \quad (6.873)$$

Notons que à droite, c'est la valeur absolue usuelle sur $\mathbb{R}$.

6.34.3 Matrice associée

Proposition 6.363.

Soit M , une matrice symétrique. Nous avons

- (1) $\det M > 0$ et $\text{Tr}(M) > 0$ implique M définie positive,
- (2) $\det M > 0$ et $\text{Tr}(M) < 0$ 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.

Si une base $\{e_i\}_{i=1,\dots,n}$ de l'espace vectoriel E est donnée, la **matrice associée** à la forme bilinéaire b sur E est la matrice d'éléments

$$B_{ij} = b(e_i, e_j). \quad (6.874)$$

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.

Si B_{ij} est la matrice associée à la forme bilinéaire b alors la valeur de $b(u, v)$ se calcule avec la formule

$$b(x, y) = \sum_{i,j} B_{ij} x_i y_j \quad (6.875)$$

lorsque x_i et y_j sont les coordonnées de x et y dans la base choisie.

Proposition 6.364.

Soit $\{e_i\}$ une base de E . L'application

$$\begin{aligned} \phi: Q(E) &\rightarrow S(n, \mathbb{R}) \\ q &\mapsto (b(e_i, e_j))_{i,j} \end{aligned} \quad (6.876)$$

où b est forme bilinéaire associée à q est une bijection linéaire et continue.

Démonstration. Si $\phi(q) = \phi(q')$; alors

$$q(x) = \sum_{i,j} \phi(q)_{ij} x_i x_j = \sum_{i,j} \phi(q')_{ij} x_i x_j = q'(x). \quad (6.877)$$

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

$$q(x) = \sum_{i,j} B_{ij} x_i x_j \quad (6.878)$$

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

$$\sup_{\|x\|=1} |q_n(x)| \rightarrow 0. \quad (6.879)$$

Nous rappelons l'identité de polarisation :

$$b_n(x, y) = \frac{1}{2} (q_n(x - y) - q_n(x) - q_n(y)). \quad (6.880)$$

En ce qui concerne deux des trois termes, il n'y a pas de problèmes :

$$|\phi(q_n)_{ij}| = |b_n(e_i, e_j)| \leq \frac{1}{2} |b_n(e_i - e_j)| + \frac{1}{2} |q_n(e_i)| + \frac{1}{2} |q_n(e_j)|. \quad (6.881)$$

Si n est assez grand, nous avons tout de suite

$$|\phi(q_n)_{ij}| \leq \frac{1}{2} |q_n(e_i - e_j)| + \epsilon. \quad (6.882)$$

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

$$q_n(e_i - e_j) = \alpha_{ij}^2 q_n(e_{ij}) \leq \alpha^2 q_n(e_{ij}). \quad (6.883)$$

Il suffit maintenant de prendre n assez grand pour avoir $\sup_{\|x\|=1} |q_n(x)| \leq \frac{\epsilon}{\alpha^2}$ pour avoir

$$|\phi(q_n)_{ij}| \leq \frac{\epsilon}{2} + \frac{\epsilon}{\alpha^2}. \quad (6.884)$$

□

Proposition 6.365.

Dans la base de diagonalisation de sa matrice associée, une forme quadratique a la forme

$$q(x) = \sum_i \lambda_i x_i^2 \quad (6.885)$$

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 de la matrice de b alors dans cette base nous avons

$$q(x) = b(x, x) = \sum_{i,j} x_i x_j b(f_i, f_j) = \sum_i \lambda_i x_i^2 \quad (6.886)$$

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 changent pas (à part l'ordre éventuellement). Cela pour dire que nous nous permettrons de parler des **valeurs propres** d'une forme quadratique comme étant les valeurs propres de la matrice associée.

Proposition 6.366.

Une application linéaire est définie positive si et seulement si sa matrice associée l'est.

6.34.4 Dégénérescence

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 6.367.

Une forme bilinéaire est **non dégénérée** $b(x, z) = 0$ pour tout z implique $x = 0$.

Lemme 6.368.

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

$$b(x - y, z) = 0 \quad (6.887)$$

pour tout z , ce qui implique $x - y = 0$. □

Proposition 6.369.

La forme bilinéaire b est non-dégénérée 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 6.292). 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 $(e_k)_j = \delta_{kj}$:

$$b(x, e_k) = \sum_{i,j} x_i (e_k)_j = \sum_i b_{ik} x_i = b_{kk} x_k. \quad (6.888)$$

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. □

Définition 6.370 (Isotropie).

Un vecteur est **isotrope** pour b si il est perpendiculaire à lui-même; en d'autres termes, x est isotrope si et seulement si $b(x, x) = 0$. Un sous-espace $W \subset E$ est **totalelement 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 :

$$C(b) = \{x \in E \text{ tel que } b(x, x) = 0\}. \quad (6.889)$$

Nous introduisons quelques notations. D'abord pour $y \in E$ nous notons

$$\begin{aligned} \Phi_y: E &\rightarrow \mathbb{R} \\ x &\mapsto b(x, y) \end{aligned} \quad (6.890)$$

et ensuite

$$\begin{aligned} \Phi: E &\rightarrow E^* \\ y &\mapsto \Phi_y. \end{aligned} \quad (6.891)$$

Définition 6.371.

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

$$\ker(b) = \{z \in E \text{ tel que } b(z, y) = 0 \forall y \in E\}. \quad (6.892)$$

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.

Proposition 6.372 ([116]).

Soit b une forme bilinéaire et symétrique. Alors

- (1) $\ker(b) \subset C(b)$ (cône d'isotropie, définition 6.370)
- (2) si b est positive alors $\ker(b) = C(b)$.

Démonstration. (1) Si $z \in \ker(b)$ alors pour tout $y \in E$ nous avons $b(z, y) = 0$. En particulier pour $y = z$ nous avons $b(z, z) = 0$ et donc $z \in C(b)$.

- (2) Soit b positive et $x \in C(b)$. Par l'inégalité de Cauchy-Schwarz (proposition 6.66) nous avons

$$|b(x, y)| \leq \sqrt{b(x, x)b(y, y)} = 0. \quad (6.893)$$

Donc pour tout y nous avons $b(x, y) = 0$.

□

6.34.5 Inégalité de Minkowski

Ce qui est couramment nommé «inégalité de Minkowski» est la proposition 18.23 dans les espaces L^p . Nous allons en donner ici un cas très particulier.

Proposition 6.373.

Si q est une forme quadratique sur $\mathbb{R}^n$ et si $x, y \in \mathbb{R}^n$ alors

$$\sqrt{q(x+y)} \leq \sqrt{q(x)} + \sqrt{q(y)}. \quad (6.894)$$

Démonstration. La proposition 6.365 nous permet de «diagonaliser» la forme quadratique q . Quitte à ne plus avoir une base orthonormale, nous pouvons renormaliser les vecteurs de base pour avoir

$$q(x) = \sum_i x_i^2. \quad (6.895)$$

Le résultat n'est donc rien d'autre que l'inégalité triangulaire pour la norme euclidienne usuelle, laquelle est démontrée dans la proposition 6.68. □

6.34.6 Ellipsoïde

Lemme 6.374.

Toute matrice peut être décomposée de façon unique en une partie symétrique et une partie antisymétrique. Cette décomposition est donnée par

$$S = \frac{M + M^t}{2}, \quad A = \frac{M - M^t}{2} \quad (6.896)$$

Démonstration. L'existence est une vérification immédiate de $S + A = M$ en utilisant (6.896). 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 $A = A'$. $\square$

Définition 6.375.

Un **ellipsoïde** dans $\mathbb{R}^n$ centré en v est le lieu des points x vérifiant l'équation

$$(x - v)^t M (x - v) = 1 \quad (6.897)$$

où M est une matrice symétrique strictement définie positive⁸⁴.

Lorsque nous parlons d'ellipsoïde plein, il suffit de changer l'égalité en une inégalité.

Une autre façon d'écrire la relation (6.897) est d'écrire $\langle (x - v), M(x - v) \rangle$ en utilisant le produit scalaire.

Remarque 6.376.

Le fait que M soit symétrique n'est pas tout à fait obligatoire ; la chose importante est que toutes les valeurs propres soient strictement positives. En effet si M a toutes ses valeurs propres strictement positives, nous nommons S la partie symétrique de M et A la partie antisymétrique (lemme 6.374). Alors pour tout $x \in \mathbb{R}^n$ nous avons

$$x^t A x = \langle x, A x \rangle = \langle A^t x, x \rangle = -\langle A x, x \rangle = -\langle x, A x \rangle, \quad (6.898)$$

donc $x^t A x = 0$. L'équation $x^t M x = 1$ est donc équivalente à $x^t S x = 1$ (elles ont les mêmes solutions).

De plus S reste strictement définie positive parce que pour tout $x \in \mathbb{R}^n$ nous avons

$$0 < x^t M x = x^t S x. \quad (6.899)$$

Proposition 6.377.

Si $\mathcal{E}$ est un ellipsoïde centrée à l'origine, il existe une base de $\mathbb{R}^n$ dans laquelle son équation est :

$$\sum_{i=1}^n \frac{x_i^2}{a_i^2} = 1. \quad (6.900)$$

Démonstration. Nous avons une matrice symétrique strictement définie positive S telle que l'équation soit $\langle x, S x \rangle = 1$. Le théorème spectral 6.292 nous fournit une base orthonormale $\{e_i\}$ dans laquelle $S e_i = \lambda_i e_i$ avec $\lambda_i > 0$. En substituant dans l'équation $\langle x, S x \rangle = 1$ nous trouvons l'équation

$$\sum_i \lambda_i x_i^2 = 1. \quad (6.901)$$

En posant $a_i = \frac{1}{\sqrt{\lambda_i}}$, nous trouvons le résultat. Cette définition des a_i est toujours possible parce que $\lambda_i > 0$. $\square$

Corollaire 6.378.

Un ellipsoïde plein centré en l'origine admet une équation de la forme $q(x) \leq 1$ où q est une forme quadratique strictement définie positive.

84. Définition 6.294.

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

$$\sum_{i=1}^n \frac{x_i^2}{a_i^2} \leq 1. \quad (6.902)$$

Nous considérons la forme quadratique

$$\begin{aligned} q: \mathbb{R}^n &\rightarrow \mathbb{R} \\ x &\mapsto \sum_{i=1}^n \frac{\langle x, e_i \rangle^2}{a_i^2}. \end{aligned} \quad (6.903)$$

Nous avons évidemment $\mathcal{E} = \{x \in \mathbb{R}^n \text{ tel que } q(x) \leq 1\}$. 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 $q(x) > 0$. $\square$

6.35 Théorème spectral auto-adjoint

Définition 6.379.

Si E est un espace euclidien, un endomorphisme $f: E \rightarrow E$ est **auto-adjoint** si pour tout $x, y \in E$ nous avons $\langle x, f(y) \rangle = \langle f(x), y \rangle$.

L'ensemble des opérateurs auto-adjoints de E est noté $S(E)$. Cette notation provient du fait que dans $\mathbb{R}^n$ muni du produit scalaire usuel, les opérateurs auto-adjoints sont les matrices symétriques.

Théorème 6.380 (Théorème spectral auto-adjoint).

Un endomorphisme auto-adjoint d'un espace euclidien

- (1) est diagonalisable dans une base orthonormée,
- (2) a son spectre réel.

Démonstration. Nous procédons par récurrence sur la dimension de E , et nous commençons par $n = 1$ ⁸⁵. Soit donc $f: E \rightarrow E$ avec $\langle f(x), y \rangle = \langle x, f(y) \rangle$. Étant donné que f est également linéaire, il existe $\lambda \in \mathbb{R}$ tel que $f(x) = \lambda x$ pour tout $x \in E$. Tous les vecteurs de E sont donc vecteurs propres de f .

Passons à la récurrence. Nous considérons $\dim(E) = n + 1$ et $f \in S(E)$. Nous considérons la forme bilinéaire symétrique Φ_f et la forme quadratique associée ϕ_f . Pour rappel,

$$\Phi_f(x, y) = \langle x, f(y) \rangle \quad (6.904a)$$

$$\phi_f(x) = \Phi_f(x, x). \quad (6.904b)$$

Et nous allons laisser tomber les indices f pour noter simplement Φ et ϕ . Étant donné que $\overline{B(0, 1)}$ est compacte et que ϕ est continue, il existe $x_0 \in \overline{B(0, 1)}$ tel que

$$\lambda = \phi(x_0) = \sup_{x \in \overline{B(0, 1)}} \phi(x). \quad (6.905)$$

Notons aussi que $\|x_0\| = 1$: le maximum est pris sur le bord. Nous posons

$$g = \lambda \text{Id} - f \quad (6.906)$$

ainsi que

$$\Phi_1(x, y) = \langle x, g(y) \rangle. \quad (6.907)$$

⁸⁵. Dans [1], l'auteur commence avec $n = 0$ mais moi je n'en ai pas le courage..

Cela est une forme bilinéaire et symétrique parce que

$$\Phi_1(y, x) = \langle y, g(x) \rangle = \langle g(y), x \rangle = \langle x, g(y) \rangle = \Phi_1(x, y) \quad (6.908)$$

où nous avons utilisé le fait que g était auto-adjoint et la symétrie du produit scalaire. De plus Φ_1 est semi-définie positive parce que

$$\Phi_1(x, x) = \langle x, \lambda x - f(x) \rangle = \lambda \|x\|^2 - \phi(x). \quad (6.909)$$

Vu que λ est le maximum, nous avons tout de suite $\Phi_1(x) \geq 0$ tant que $\|x\| = 1$. Et si x n'est pas de norme 1, c'est le même prix parce qu'on se ramène à $\|x\| = 1$ en multipliant par un nombre positif. Attention cependant :

$$\Phi_1(x_0, x_0) = \lambda \|x_0\|^2 - \phi(x_0) = 0. \quad (6.910)$$

Donc Φ_1 a un noyau contenant x_0 par la proposition 6.372. Nous en déduisons que $\text{Image}(g) \neq E$ en effet, $x_0 \in \text{Image}(g)^\perp$, mais nous avons la proposition 6.28 sur les dimensions :

$$\dim E = \dim(\text{Image}(g)) + \dim(\text{Image}(g)^\perp). \quad (6.911)$$

Vu que $\text{Image}(g)^\perp$ est un espace vectoriel non réduit à $\{0\}$, la dimension de $\text{Image}(g)$ ne peut pas être celle de E . L'endomorphisme g n'étant pas surjectif, il ne peut pas être injectif non plus parce que nous sommes en dimension finie ; il existe donc $e_1 \in E$ tel que $g(e_1) = 0$ et tant qu'à faire nous choisissons $\|e_1\| = 1$ (ici la norme est bien celle de l'espace euclidien considéré). Par définition,

$$f(e_1) = \lambda e_1, \quad (6.912)$$

c'est à dire que $\lambda \in \text{Spec}(f)$. Et ϕ étant une forme quadratique réelle nous avons $\lambda \in \mathbb{R}$.

Nous posons à présent $H = \text{Span}\{e_1\}^\perp$. C'est un sous-espace stable par f parce que si $x \in H$ alors

$$\langle e_1, f(x) \rangle = \langle f(e_1), x \rangle = \lambda \langle e_1, x \rangle = 0. \quad (6.913)$$

Nous pouvons donc considérer la restriction de f à H : $f_H : H \rightarrow H$. Cet endomorphisme est bilinéaire et symétrique sur l'espace H de dimension inférieure à celle de E , donc la récurrence nous donne une base orthonormée

$$\{e_2, \dots, e_n\} \quad (6.914)$$

de vecteurs propres de f_H . De plus les valeurs propres sont réelles, toujours par récurrence. Donc

$$\text{Spec}(f) = \{\lambda\} \cup \text{Spec}(f_H) \subset \mathbb{R}. \quad (6.915)$$

Notons pour être complet que si $i \geq 2$ alors

$$\langle e_1, e_i \rangle = 0 \quad (6.916)$$

parce que le vecteur e_i est par construction choisit dans l'espace $H = e_1^\perp$. Nous avons donc bien une base orthonormée de E construite sur des vecteurs propres de f . $\square$

Corollaire 6.381.

Soit E un espace vectoriel ainsi que ϕ et ψ des formes quadratiques sur E avec ψ définie positive. Alors il existe une base ψ -orthonormale dans laquelle ϕ est diagonale.

Démonstration. Il suffit de considérer l'espace euclidien E muni du produit scalaire $\langle x, y \rangle = \psi(x, y)$. Ensuite nous diagonalisons la matrice (symétrique) de ϕ pour ce produit scalaire à l'aide du théorème 6.380. $\square$

Définition 6.382.

*Dans le cas de $V = \mathbb{R}^m$ nous avons un produit scalaire canonique. Soient u et v , deux vecteurs de $\mathbb{R}^m$. Le **produit scalaire** de u et v , noté $\langle u, v \rangle$ ou $u \cdot v$ est le réel*

$$\langle u, v \rangle = \sum_{k=1}^m u_k v_k = u_1 v_1 + u_2 v_2 + \dots + u_m v_m. \quad (6.917)$$

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

$$\langle e_i, e_j \rangle = \sum_{k=1}^m \delta_{ik} \delta_{jk}. \quad (6.918)$$

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 :

$$\langle e_i, e_j \rangle = \delta_{ii} \delta_{ji} = \delta_{ji}. \quad (6.919)$$

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 6.383.

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.

$$v \cdot e_j = \sum_{i=1}^m \langle v_i e_i, e_j \rangle = \sum_{i=1}^m v_i \langle e_i, e_j \rangle = \sum_{i=1}^m v_i \delta_{ij} \quad (6.920)$$

En effectuant la somme sur i dans le membre de droite de l'équation (6.920), tous les termes sont nuls sauf celui où $i = j$; il reste donc

$$v \cdot e_j = v_j. \quad (6.921)$$

□

Le produit scalaire ne dépend en réalité pas de la base orthogonale choisie.

Lemme 6.384.

Si $\{e_i\}$ est la base canonique, et si $\{f_i\}$ est une autre base orthonormale, alors si u et v sont deux vecteurs de $\mathbb{R}^m$, nous avons

$$\sum_i u_i v_j = \sum_i u'_i v'_j \quad (6.922)$$

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

$$\begin{aligned} \sum_i u'_i v'_j &= \sum_i \left(\sum_j A_{ij} u_j \right) \left(\sum_k A_{ik} v_k \right) \\ &= \sum_{ijk} A_{ij} A_{ik} u_j v_k \\ &= \sum_{jk} \underbrace{\sum_i (A^t)_{ji} A_{ik}}_{=\delta_{jk}} u_j v_k \\ &= \sum_{jk} \delta_{jk} u_j v_k \\ &= \sum_k u_j v_k. \end{aligned} \quad (6.923)$$

□

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 regardons les vecteurs.

Nous dirons que deux vecteurs sont **orthogonaux** lorsque leur produit scalaire est nul. Nous écrivons que $u \perp v$ lorsque $\langle u, v \rangle = 0$.

Définition 6.385.

La **norme euclidienne** d'un élément de $\mathbb{R}^m$ est définie par $\|u\| = \sqrt{u \cdot u}$.

Cette définition est motivée par le fait que le produit scalaire $u \cdot u$ donne exactement la norme usuelle donnée par le théorème de Pythagore :

$$u \cdot u = \sum_{i=1}^m u_i u_i = \sum_{i=1}^m u_i^2 = u_1^2 + u_2^2 + \dots + u_m^2. \quad (6.924)$$

Le fait que $e_i \cdot e_j = \delta_{ij}$ signifie que la base canonique est **orthonormée**, c'est à dire que les vecteurs de la base canonique sont orthogonaux deux à deux et qu'ils ont tout 1 comme norme.

Lemme 6.386.

Pour tout $u \in \mathbb{R}^m$, il existe un $\xi \in \mathbb{R}^m$ tel que $\|u\| = \xi \cdot u$ et $\|\xi\| = 1$.

Démonstration. Vérifions que le vecteur $\xi = u/\|u\|$ ait les propriétés requises. D'abord $\|\xi\| = 1$ parce que $u \cdot u = \|u\|^2$. Ensuite

$$\xi \cdot u = \frac{u \cdot u}{\|u\|} = \frac{\|u\|^2}{\|u\|} = \|u\|. \quad (6.925)$$

□

6.36 Mini introduction au produit tensoriel

6.36.1 Définitions

Soit E , un espace vectoriel de dimension finie. Si α et β sont deux formes linéaires sur un espace vectoriel E , nous définissons $\alpha \otimes \beta$ comme étant la 2-forme donnée par

$$(\alpha \otimes \beta)(u, v) = \alpha(u)\beta(v). \quad (6.926)$$

Si a et b sont des vecteurs de E , ils sont vus comme des formes sur E via le produit scalaire et nous avons

$$(a \otimes b)(u, v) = (a \cdot u)(b \cdot v). \quad (6.927)$$

Cette dernière équation nous incite à pousser un peu plus loin la définition de $a \otimes b$ et de simplement voir cela comme la matrice de composantes

$$(a \otimes b)_{ij} = a_i b_j. \quad (6.928)$$

Cette façon d'écrire a l'avantage de ne pas demander de se souvenir qui est un vecteur ligne, qui est un vecteur colonne et où il faut mettre la transposée. Évidemment $(a \otimes b)$ est soit ab^t soit $a^t b$ suivant que a et b soient ligne ou colonne.

6.36.2 Application d'opérateurs

Lemme 6.387.

Soient $x, y \in E$ et A, B deux opérateurs linéaires sur E vus comme matrices. Alors

$$(Ax \otimes By) = A(x \otimes y)B^t. \quad (6.929)$$

Démonstration. Calculons la composante ij de la matrice $(Ax \otimes By)$. Nous avons

$$(Ax \otimes By)_{ij} = (Ax)_i (By)_j \quad (6.930a)$$

$$= \sum_{kl} A_{ik} x_k B_{jl} y_l \quad (6.930b)$$

$$= A_{ik} (x \otimes y)_{kl} B_{jl} \quad (6.930c)$$

$$= (A(x \otimes y)B^t)_{ij}. \quad (6.930d)$$

□

6.37 Coordonnées cylindriques et sphériques

Les **coordonnées cylindriques** sont un perfectionnement des coordonnées polaires. Il s'agit simplement de donner le point (x, y, z) en faisant la conversion $(x, y) \mapsto (r, \theta)$ et en gardant le z . Les formules de passage sont

$$\begin{cases} x = r \cos(\theta) & (6.931a) \\ y = r \sin(\theta) & (6.931b) \\ z = z. & (6.931c) \end{cases}$$

Les **coordonnées sphériques** sont ce qu'on appelle les «méridiens» et «longitudes» en géographie. Les formules de transformation sont

$$\begin{cases} x = \rho \sin(\theta) \cos(\varphi) & (6.932a) \\ y = \rho \sin(\theta) \sin(\varphi) & (6.932b) \\ z = \rho \cos(\theta) & (6.932c) \end{cases}$$

avec $0 \leq \theta \leq \pi$ et $0 \leq \varphi < 2\pi$.

Remarque 6.388.

Attention : d'un livre à l'autre les conventions sur les noms des angles changent. N'essayez donc pas d'étudier par cœur des formules concernant les coordonnées sphériques trouvées autre part. Par exemple sur le premier dessin de wikipédia, l'angle φ est noté θ et l'angle θ est noté Φ . Mais vous noterez que sur cette même page, les convention de noms de ces angles changent plusieurs fois.

Trouvons le changement inverse, c'est à dire trouvons ρ , θ et φ en termes de x , y et z . D'abord nous avons

$$\rho = \sqrt{x^2 + y^2 + z^2}. \quad (6.933)$$

Ensuite nous savons que

$$\cos(\theta) = \frac{z}{\rho} \quad (6.934)$$

détermine de façon unique⁸⁶ un angle $\theta \in [0, \pi]$. Dès que ρ et θ sont connus, nous pouvons poser $r = \rho \sin \theta$ et alors nous nous trouvons avec les équations

$$\begin{cases} x = r \cos(\varphi) & (6.935a) \\ y = r \sin(\varphi), & (6.935b) \end{cases}$$

qui sont similaires à celles déjà étudiées dans le cas des coordonnées polaires.

6.38 Méthode de Gauss pour résoudre des systèmes d'équations linéaires

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 :

⁸⁶. Le problème $\rho = 0$ ne se pose pas ; pourquoi ?

(a) Remplacer une ligne par elle-même + un multiple d'une autre ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 2 & 3 & 5 \\ 1 & 2 & 4 \end{array} \right) \xrightarrow{L_1 - 2L_2 \mapsto L'_1} \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array} \right)$$

(b) Remplacer une ligne par un multiple d'elle-même ;

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & -1 & -3 \\ 1 & 2 & 4 \end{array} \right) \xrightarrow{-L_1 \mapsto L'_1} \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 2 & 4 \end{array} \right)$$

(c) Permuter des lignes.

$$\text{p.ex. } \left(\begin{array}{cc|c} 0 & 1 & 3 \\ 1 & 0 & -2 \end{array} \right) \xrightarrow{L_1 \mapsto L'_2 \text{ et } L_2 \mapsto L'_1} \left(\begin{array}{cc|c} 1 & 0 & -2 \\ 0 & 1 & 3 \end{array} \right)$$

(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 6.389. — 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 :

$$\text{p.ex. } \left(\begin{array}{ccc|c} 1 & 0 & -2 & 2 \\ 0 & 1 & 3 & 0 \end{array} \right) \Leftrightarrow \begin{cases} x - 2z = 2 \\ y + 3z = 0 \end{cases} \Leftrightarrow \begin{cases} x = 2 + 2\lambda \\ y = -3\lambda \\ z = \lambda \end{cases}$$

Chapitre 7

Tribus, théorie de la mesure

7.1 Tribus

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 7.23 sur un espace mesuré avec une tribu, définition 7.1.
- (2) Une mesure extérieure est la définition 7.17
- (3) Une algèbre de partie : définition 7.18. Une mesure sur une algèbre de parties : définition 7.20. L'intérêt est que si on connaît une mesure sur une algèbre de parties, elle se prolonge en une mesure sur la tribu engendrée par le théorème de prolongement de Hahn 7.60.
- (4) Un λ -système : définition 7.37.
- (5) Une mesure complexe : définition 13.7.

7.1.1 Généralités

Définition 7.1 (Tribu, espace mesurable[117]).

Si Ω est un ensemble, un ensemble $\mathcal{A}$ de sous-ensembles de Ω est une **tribu** si

- (1) $\Omega \in \mathcal{A}$;
- (2) $\complement A \in \mathcal{A}$ pour tout $A \in \mathcal{A}$;
- (3) si $(A_i)_{i \in \mathbb{N}}$ une suite dénombrable d'éléments de $\mathcal{A}$, alors $\bigcup_{i \in \mathbb{N}} A_i \in \mathcal{A}$.

Le couple $(\Omega, \mathcal{A})$ est alors un **espace mesurable**.

Remarque 7.2.

Nous trouvons parfois la notation

$$\bigcup_{k \in \mathbb{N}} A_k = \sup_{k \geq 0} A_k. \quad (7.1)$$

Lemme 7.3.

Opérations ensemblistes sur les tribus.

- (1) Une tribu est stable par intersections au plus dénombrables.
- (2) Une tribu est stable par différence ensembliste.

Démonstration. Soit $(A_i)_{i \in I}$ une famille au plus dénombrable d'éléments de la tribu $\mathcal{A}$. Nous devons prouver que $\bigcap_{i \in I} A_i$ est également un élément de $\mathcal{A}$. Pour cela nous passons au complémentaire :

$$\complement \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} \complement A_i. \quad (7.2)$$

La définition d'une tribu implique que le membre de droite est un élément de la tribu. Par stabilité d'une tribu par complémentaire, l'ensemble $\bigcap_{i \in I} A_i$ est également un élément de la tribu.

La seconde assertion est immédiate à partir de la première parce que $A \setminus B = A \cap \complement B$. $\square$

Si $(\mathcal{A}_i)_{i \in I}$ est un ensemble de tribus (indexé par un ensemble I quelconque) alors

$$\mathcal{A} = \bigcap_{i \in I} \mathcal{A}_i \quad (7.3)$$

est également une tribu.

Définition 7.4.

Soit $\mathcal{D}$ un ensemble de parties de Ω . La **tribu engendrée** par $\mathcal{D}$ est l'intersection de toutes les tribus de Ω contenant $\mathcal{D}$. C'est la plus petite tribu contenant $\mathcal{D}$. Nous la noterons le plus souvent $\sigma(\mathcal{A})$

Note : une tribu engendrée par une application sera la définition 7.69.

Proposition 7.5 ([118]).

Soit S un ensemble et $\mathcal{F}$ une tribu de S . Soit une classe $\mathcal{N} \subset \mathcal{P}(S)$ telle que

- (1) Si $A \in \mathcal{N}$ alors il existe $Y \in \mathcal{F} \cap \mathcal{N}$ tel que $A \subset Y$.
- (2) Si $A \in \mathcal{N}$ et $B \subset A$ alors $B \in \mathcal{N}$.
- (3) La classe $\mathcal{N}$ est stable par union dénombrable.

Alors la classe

$$\mathcal{T} = \{X \cup A \text{ avec } A \in \mathcal{N} \text{ et } X \in \mathcal{F}\} \quad (7.4)$$

est une tribu.

Démonstration. L'ensemble $\mathcal{T}$ est stable par union dénombrable parce que $\mathcal{F}$ et $\mathcal{N}$ le sont. De plus S et $\emptyset$ sont dans $\mathcal{F}$ et donc dans $\mathcal{T}$. Nous devons voir que $\mathcal{T}$ est stable par complémentarité.

Soit donc $A \in \mathcal{N}$ et $X \in \mathcal{F}$; nous savons que $(A \cup X)^c = A^c \cap X^c$. De plus il existe $Y \in \mathcal{F} \cap \mathcal{N}$ tel que $A \subset Y$ et nous pouvons exprimer A^c en termes de Y : $A^c = Y^c \cup (Y \setminus A)$. Donc

$$(A \cup X)^c = (Y^c \cup (Y \setminus A)) \cap X^c = \underbrace{(Y^c \cap X^c)}_{\in \mathcal{F}} \cup \underbrace{((Y \setminus A) \cap X^c)}_{\in \mathcal{N}}. \quad (7.5)$$

Le fait que la seconde partie soit dans $\mathcal{N}$ est due au fait que ce soit une partie de $Y \in \mathcal{N}$. Nous avons donc bien $(A \cup X)^c \in \mathcal{T}$. $\square$

7.1.1.1 Tribu induite

Proposition 7.6.

Soit un espace mesurable $(S, \mathcal{F})$ et une partie $R \subset S$. L'ensemble

$$\mathcal{F}_R = \{A \cap R \text{ tel que } A \in \mathcal{F}\} \quad (7.6)$$

est une tribu.

Démonstration. D'abord R et $\emptyset$ sont dans $\mathcal{F}_R$. Si $C \in \mathcal{F}_R$ alors $C = A \cap R$ pour un certain $A \in \mathcal{F}$ et nous devons prouver que $R \cap C^c$ est dans $\mathcal{F}_R$ (le complémentaire de C dans R). Nous avons

$$R \cap C^c = R \cap (A \cap R)^c = R \cap A^c \in \mathcal{F}_R \quad (7.7)$$

parce que $A^c \in \mathcal{F}$. Enfin si $C_i \in \mathcal{F}_R$ alors $C_i = R \cap A_i$ pour des A_i dans $\mathcal{F}$. Nous avons

$$\bigcup_{i \in \mathbb{N}} C_i = \bigcup_{i \in \mathbb{N}} (R \cap A_i) = R \cap \left(\bigcup_{i \in \mathbb{N}} A_i \right), \quad (7.8)$$

mais $\bigcup_i A_i \in \mathcal{F}$ donc $\bigcup_i C_i \in \mathcal{F}_R$. $\square$

Définition 7.7.

Soit un espace mesurable $(S, \mathcal{F})$ et une partie $R \subset S$. L'ensemble

$$\mathcal{F}_R = \{A \cap R \text{ tel que } A \in \mathcal{F}\} \quad (7.9)$$

est la **tribu induite** de R depuis S .

7.1.1.2 Tribu borélienne

Définition 7.8 (Tribu borélienne).

La tribu des **boréliens**, notée $\mathcal{Bor}(\mathbb{R}^d)$ est la tribu engendrée par les ouverts de $\mathbb{R}^d$. Plus généralement si Y est un espace topologique, la tribu des boréliens est la tribu engendrée par les ouverts de Y .

Proposition 7.9.

La tribu engendrée par une base dénombrable de la topologie est celle des boréliens.

Démonstration. Si une base de topologie est donnée, tout ouvert peut être écrit comme union d'élément de la base, proposition 5.16. Dans le cas d'une base dénombrable, cette union sera forcément dénombrable. Une tribu étant stable par union dénombrable, tout ouvert est dans la tribu engendrée par la base de topologie. Les autres boréliens suivent automatiquement.

Dit avec plus de lettres et moins de phrases, si $\mathcal{D}$ est une base dénombrable de la topologie de X , et si $\mathcal{O}$ est un ouvert de X , nous avons $\mathcal{O} = \bigcup_{i=1}^{\infty} A_i$ avec $A_i \in \mathcal{D}$. Vu qu'une tribu est stable par union dénombrable¹, nous avons $\mathcal{O} \in \sigma(\mathcal{D})$. En conséquence de quoi $\mathcal{Bor}(X) \subset \sigma(\mathcal{D})$.

Mais comme $\mathcal{D} \subset \mathcal{Bor}(X)$ l'inclusion inverse est automatique. D'où l'égalité $\mathcal{Bor}(X) = \sigma(\mathcal{D})$. $\square$

7.1.1.3 Les boréliens de $\mathbb{R}$

Nous rappelons que la topologie de $\mathbb{R}$ est celle des boules donnée par le théorème 5.20. Nous rappelons (voir la proposition 5.43 et sa preuve) que les boules ouvertes de la forme $B(q, r)$ avec $q, r \in \mathbb{Q}$ forment une base dénombrable de la topologie de $\mathbb{R}$.

Lemme 7.10.

Soit $\{q_i\}$ une énumération des rationnels. La tribu engendrée par les ouverts $\sigma_i =]q_i, \infty[$ est la tribu des boréliens.

Démonstration. Si $a < b$ dans $\mathbb{Q}$ alors $\sigma_a \setminus \sigma_b =]a, b]$. Ensuite

$$\bigcup_{n \in \mathbb{N}^*} \sigma_a \setminus \sigma_{b - \frac{1}{n}} = \bigcup_{n \in \mathbb{N}^*}]a, b - \frac{1}{n}] =]a, b[. \quad (7.10)$$

Par union dénombrable, tous les intervalles $]a, b[$ avec $a, b \in \mathbb{Q}$ sont dans la tribu engendrée par les σ_i .

Ces boules ouvertes forment une base de la topologie de $\mathbb{R}$ par la proposition 5.43 et la proposition 7.9 conclu. $\square$

Exemple 7.11

Les singletons sont des boréliens de $\mathbb{R}$ parce que

$$\{x\} = \left(]-\infty, x[\cup]x, +\infty[\right)^c. \quad (7.11)$$

Vu qu'une tribu est stable par union dénombrable, l'ensemble $\mathbb{Q}$ est un borélien de $\mathbb{R}$. Et comme les tribus sont stables par différence ensembliste (7.3(2)), l'ensemble des irrationnels est un borélien de $\mathbb{R}$. $\triangle$

7.1.2 Tribu de Baire

Définition 7.12.

Une partie d'un espace topologique est **rare** si elle est contenue dans un fermé d'intérieur vide.

Une partie est **maigre** si elle est réunion finie ou dénombrable de parties rares.

1. Définition 7.1(3)

Exemple 7.13

L'ensemble $\mathbb{Q}$ dans $\mathbb{R}$ est maigre mais n'est pas rare parce que $\bar{\mathbb{Q}} = \mathbb{R}$. $\triangle$

Proposition 7.14 ([118]).

Soit X un espace topologique. L'ensemble de parties

$$\mathcal{Ba}(X) = \{B \cup A \text{ avec } B \text{ borélien et } A \text{ maigre}\} \quad (7.12)$$

est une tribu. Elle est appelée la **tribu de Baire** de l'espace X .

Démonstration. Nous allons montrer que les boréliens et les maigres vérifient les conditions de la proposition 7.5.

- (1) Si A est maigre, il s'écrit comme $A = \bigcup_{i \in \mathbb{N}} R_i$ où les R_i sont rares. Il existe donc des fermés d'intérieur vide F_i tels que $R_i \subset F_i$; en particulier $A \subset \bigcup_i F_i$. En tant que fermés, $F_i \in \mathcal{Bor}(X)$; de plus chaque F_i est rare, donc $\bigcup_i F_i$ est maigre. L'ensemble A est donc bien contenu dans un ensemble maigre et borélien.
- (2) Soit A maigre et $B \subset A$. Nous avons, avec les mêmes notations, $A = \bigcup_i R_i$ et $B = \bigcup_i (R_i \cap B)$. Les ensembles $R_i \cap B$ sont encore rares, donc B est une union dénombrable d'ensembles rares. L'ensemble B est donc maigre.
- (3) Si les ensembles (A_i) sont maigres, alors ils sont unions dénombrables de rares : $A_i = \bigcup_k R_k^{(i)}$. Nous avons alors

$$\bigcup_i A_i = \bigcup_{(i,k) \in \mathbb{N}^2} R_k^{(i)}, \quad (7.13)$$

et donc $\bigcup_i A_i$ est encore une union dénombrable d'ensembles rares. $\square$

Proposition 7.15 ([118]).

Une partie B de l'espace topologique X est dans la tribu de Baire de X si et seulement si il existe un ouvert U tel que $B \Delta U$ est maigre.

Démonstration. Nous définissons la relation d'équivalence² suivante sur $\mathcal{P}(X)$: nous disons que $A \sim B$ si et seulement si $A \Delta B$ est maigre.

Réflexive Nous avons $A \Delta A = \emptyset$, donc $A \sim A$.

symétrique Nous avons $A \Delta B = B \Delta A$, donc $\sim$ est symétrique.

transitive Si A, B, C sont des parties de X alors nous avons toujours

$$A \Delta C \subset (A \cup B \cup C) \setminus (A \cap B \cap C) = (A \Delta B) \cup (B \Delta C). \quad (7.14)$$

Donc si $A \sim B$ et $B \sim C$ alors $A \Delta C$ est contenu dans une union de maigres et est donc maigre.

Autres propriétés de $\sim$ De plus la relation d'équivalence $\sim$ vérifie $A \sim B$ si et seulement si $A^c \sim B^c$, par le lemme 1.9(1).

Pour compléter les propriétés de $\sim$ mentionnons encore le fait que si F est fermé alors $F \sim \text{Int}(F)$. En effet $F \cup \text{Int}(F) = F$ et $F \cap \text{Int}(F) = \text{Int}(F)$, de telle sorte que $F \Delta \text{Int}(F) = F \setminus \text{Int}(F)$. Cela est un fermé parce que son complémentaire est $F^c \cup \text{Int}(F)$ qui est une union d'ouverts. De plus $F \subset \text{Int}(F)$ est d'intérieur vide, de telle sorte qu'il est rare et donc maigre.

Pour la suite de la preuve nous posons

$$\mathcal{F} = \{A \subset X \text{ tel que il existe ouvert } U \text{ avec } U \sim A\}, \quad (7.15)$$

et nous devons prouver que $\mathcal{F} = \mathcal{Ba}(X)$.

2. Définition 1.10

$\mathcal{F} \subset \mathcal{Ba}(X)$ Soit $A \in \mathcal{F}$ et un ouvert U tel que $U \sim A$. Alors nous posons $M = U \Delta A$ qui est maigre. En vertu du lemme 1.9(2), nous avons

$$A = M \Delta U = (M \cup U) \setminus (M \cap U), \quad (7.16)$$

ce qui prouve que A est dans la tribu engendrée par les ouverts et les maigres, laquelle tribu est contenue dans $\mathcal{Ba}(X)$.

$\mathcal{Ba}(X) \subset \mathcal{F}$ Nous allons montrer que $\mathcal{F}$ est une tribu contenant tous les ouverts et tous les maigres. Alors en particulier $\mathcal{F}$ contiendra $\mathcal{Ba}(X)$. Si U est ouvert, $U \sim U$ et donc $U \in \mathcal{F}$. Si M est maigre, alors $M \sim \emptyset$ et donc $M \in \mathcal{F}$. Il reste à prouver que $\mathcal{F}$ est une tribu.

Vide et ensemble Cela est facile : X et $\emptyset$ sont dans $\mathcal{F}$.

Complémentaire Commençons par nous souvenir que $F \sim \text{Int}(F)$ dès que F est fermé. Si $A \in \mathcal{F}$ alors il existe un ouvert U tel que $A \sim U$ et donc aussi $A^c \sim U^c$. D'autre part U^c est fermé, donc $U^c \sim \text{Int}(U^c)$, donc

$$A^c \sim U^c \sim \text{Int}(U^c), \quad (7.17)$$

ce qui implique que $A^c \in \mathcal{F}$.

Union dénombrable Soit $A_n \in \mathcal{F}$ et $M_n = A_n \Delta U_n$ avec M_n maigre et U_n ouvert. Nous allons prouver que

$$\bigcup_n A_n \sim \bigcup_n U_n. \quad (7.18)$$

Pour cela il faut remarque que

$$\left(\bigcup_n A_n \right) \Delta \left(\bigcup_n U_n \right) \subset \bigcup_n (A_n \Delta U_n) = \bigcup_n M_n. \quad (7.19)$$

Le terme le plus à droite est maigre, ce qui signifie que celui le plus à gauche est contenu dans un maigre et donc est maigre lui-même.

□

Proposition 7.16.

Si B est un borélien de X , alors il existe un ouvert U et un maigre M tels que

- (1) $B \Delta U$ est maigre,
- (2) $M \Delta U = B$,
- (3) $D \Delta M$ est ouvert.

Démonstration. Vu que B est borélien, il est aussi dans la tribu de Baire et il existe par la proposition 7.15 un ouvert U tel que $M = B \Delta U$ est maigre. En prenant ce U et ce M , les trois conditions sont vérifiées parce que

$$M \Delta U = (B \Delta U) \Delta U = B \quad (7.20)$$

et

$$B \Delta M = M \Delta B = (U \Delta B) \Delta B = U. \quad (7.21)$$

Tout par le lemme 1.9(2).

□

7.2 Théorie de la mesure

Définition 7.17 ([119]).

Une **mesure extérieure** sur un ensemble S est une application $m^*: \mathcal{P}(S) \rightarrow [0, \infty]$ telle que

- (1) $m^*(\emptyset) = 0$,
- (2) Si $A \subset B$ dans S alors $m^*(A) \leq m^*(B)$
- (3) Si les A_n sont des parties de S alors

$$m^*\left(\bigcup_{n \in \mathbb{N}} A_n\right) \leq \sum_{n \in \mathbb{N}} m^*(A_n). \quad (7.22)$$

La différence avec une mesure est que nous ne demandons pas que (7.22) soit une égalité lorsque les A_n sont disjoints.

7.2.1 Mesure et algèbre de parties

Définition 7.18 (Algèbre de parties[119]).

Soit S , un ensemble. Une classe $\mathcal{D}$ de parties de S est une **algèbre de parties** de S si

- (1) $S \in \mathcal{D}$ et $\emptyset \in \mathcal{D}$,
- (2) si $A \in \mathcal{D}$ alors $A^c \in \mathcal{D}$,
- (3) si $A, B \in \mathcal{D}$ alors $A \cup B \in \mathcal{D}$.

Les algèbre de parties ne sont pas des classes si sauvages que ça ; en témoigne le lemme suivant.

Lemme 7.19.

Une algèbre de partie est stable par intersection (finie) et par différence ensembliste.

Démonstration. Il suffit de remarquer que $A \cap B = (A^c \cup B^c)^c$ et que $A \setminus B = A \cap B^c$. □

Définition 7.20 (Mesure sur une algèbre de parties).

Soit S un ensemble et $\mathcal{D}$ une algèbre de parties de S . Une **mesure positive** sur $(S, \mathcal{D})$ est une application $\mu: \mathcal{D} \rightarrow [0, \infty]$ telle que

- (1) $\mu(\emptyset) = 0$,
- (2) Si $A_n \in \mathcal{D}$ sont des ensembles deux à deux disjoints et tels que $\bigcup_n A_n \in \mathcal{D}$ alors

$$\mu\left(\bigcup_n A_n\right) = \sum_n \mu(A_n). \quad (7.23)$$

La mesure est **finie** si $\mu(S) < \infty$ et σ -finie si il existe une suite (S_n) dans $\mathcal{D}$ telle que $S = \bigcup_n S_n$ et $\mu(S_n) < \infty$.

Lemme 7.21 ([119]).

Si $\mathcal{D}$ est une algèbre de parties de S et si μ est une mesure sur $(S, \mathcal{D})$ alors

- (1) si $A, B \in \mathcal{D}$ avec $A \subset B$ alors $\mu(A) \leq \mu(B)$
- (2) si $A_n \in \mathcal{D}$ et $\bigcup_n A_n \in \mathcal{D}$ alors

$$\mu\left(\bigcup_n A_n\right) \leq \sum_n \mu(A_n). \quad (7.24)$$

La propriété (2) est la σ -sous-additivité.

Démonstration. Si $A \subset B$ alors $B = A \cup (B \setminus A)$ avec A et $B \setminus A$ disjoints donc

$$\mu(B) = \mu(A) + \mu(B \setminus A) \geq \mu(A). \quad (7.25)$$

Pour la seconde, on passe par les compléments deux à deux : nous posons

$$\begin{cases} B_0 = \emptyset \\ B_n = A_n \setminus \bigcup_{k < n} B_k. \end{cases} \quad (7.26a)$$

$$(7.26b)$$

Ces ensembles sont deux à deux disjoints et $\bigcup_n B_n = \bigcup_n A_n \in \mathcal{D}$, donc

$$\mu\left(\bigcup_n A_n\right) = \sum_n \mu\left(A_n \setminus \bigcup_{k < n} B_k\right) \leq \sum_n \mu(A_n), \quad (7.27)$$

où nous avons utilisé la première partie du lemme. □

Proposition 7.22 (Mesure extérieure à partir d'une algèbre de parties[119]).

Soit $\mathcal{D}$ une algèbre de partie sur l'ensemble S et μ une mesure sur $(S, \mathcal{D})$. Alors l'application

$$\begin{aligned} \mu^* : \mathcal{P}(S) &\rightarrow [0, +\infty] \\ X &\mapsto \inf \left\{ \sum_n \mu(A_n) \text{ tel que } A_n \in \mathcal{D}, X \subset \bigcup_n A_n \right\} \end{aligned} \quad (7.28)$$

est une mesure extérieure³ sur S et pour tout $A \in \mathcal{D}$ nous avons $\mu^*(A) = \mu(A)$.

Démonstration. Ceci est une phrase servant à aligner correctement le **description** qui suit.

La définition est bonne Notons d'abord que la définition est bonne : l'ensemble sur lequel l'infimum est pris n'est pas vide : il suffit de prendre $A_1 = S$ et $A_{n \geq 2} = \emptyset$.

Le vide D'abord $\mu^*(\emptyset) = 0$ parce que $\emptyset \in \mathcal{D}$. Prendre $A_n = \emptyset$.

Inégalité d'inclusion Soient $X \subset Y$ dans $\mathcal{P}(S)$. Si $Y \subset A$ alors $X \subset A$, donc

$$\left\{ \sum_n \mu(A_n) \text{ tel que } A_n \in \mathcal{D}, Y \subset \bigcup_n A_n \right\} \subset \left\{ \sum_n \mu(A_n) \text{ tel que } A_n \in \mathcal{D}, X \subset \bigcup_n A_n \right\}, \quad (7.29)$$

ce qui prouve que $\mu^*(X) \leq \mu^*(Y)$.

Inégalité par union dénombrable Soit $(X_n)_{n \in \mathbb{N}}$ une suite de parties de S . Si il existe n_0 tel que $\mu^*(X_{n_0}) = \infty$ alors nous avons automatiquement $\sum_n \mu^*(X_n) = \infty$ et l'inégalité demandée est évidente parce que n'importe quoi est plus petit ou égal à ∞ . Nous supposons donc que $\mu^*(X_n) < \infty$ pour tout n .

Soit $\epsilon > 0$. Pour tout $n \geq 1$ il existe une suite $(B_k^{(n)})_{k \in \mathbb{N}}$ dans $\mathcal{D}$ tels que $X_n \subset \bigcup_k B_k^{(n)}$ et

$$\mu^*(X_n) + \frac{\epsilon}{2^n} \geq \sum_k \mu(B_k^{(n)}). \quad (7.30)$$

Étant donné que

$$\bigcup_n X_n \subset \bigcup_n \left(\bigcup_k B_k^{(n)} \right), \quad (7.31)$$

nous avons

$$\mu^*\left(\bigcup_n X_n\right) \leq \sum_n \sum_k \mu^*(B_k^{(n)}) \leq \sum_n \left(\mu^*(X_n) + \frac{\epsilon}{2^n} \right) = \sum_n \mu^*(X_n) + \epsilon. \quad (7.32)$$

Cette inégalité étant valable pour tout ϵ , nous avons bien

$$\mu^*\left(\bigcup_n X_n\right) = \sum_n \mu^*(X_n). \quad (7.33)$$

Restriction Soit $A \in \mathcal{D}$. Nous avons automatiquement $\mu^*(A) \leq \mu(A)$ parce que $\mu(A)$ est dans l'ensemble dont nous prenons l'infimum (prendre $A_1 = A$ et $A_{n \geq 2} = \emptyset$).

En ce qui concerne l'inégalité inverse nous considérons une suite A_n dans $\mathcal{D}$ telle que $A \subset \bigcup_n A_n$. Vu que $A \in \mathcal{D}$ et que $\mathcal{D}$ est une algèbre de parties nous avons $A \cap A_n \in \mathcal{D}$ et $\bigcup_n (A \cap A_n) = A \in \mathcal{D}$. Par conséquent

$$\mu(A) = \mu\left(\bigcup_n (A \cap A_n)\right) \leq \sum_n \mu(A \cap A_n) \leq \sum_n \mu(A_n). \quad (7.34)$$

Donc tous les éléments de l'ensemble sur lequel nous prenons l'infimum sont plus grands que $\mu(A)$. Nous en déduisons que $\mu^*(A) \geq \mu(A)$.

□

3. Définition 7.17.

7.2.2 Mesure sur un espace mesurable

Définition 7.23 (Mesure positive).

Une **mesure positive** sur l'espace mesurable⁴ $(\Omega, \mathcal{A})$ est une application $\mu: \mathcal{A} \rightarrow [0, \infty]$ telle que

(1) $\mu(A) \geq 0$ pour tout $A \in \mathcal{A}$;

(2) $\mu(\bigcup_{i=0}^{\infty} A_i) = \sum_{i=0}^{\infty} \mu(A_i)$ si les A_i sont des éléments de $\mathcal{A}$ deux à deux disjoints.

Le triple $(\Omega, \mathcal{A}, \mu)$ est alors un **espace mesuré**.

Une mesure est **σ -finie** si il existe un recouvrement dénombrable de Ω par des ensembles de mesure finie. Si la mesure est σ -finie, nous disons que l'espace $(\Omega, \mathcal{A}, \mu)$ est un **espace mesuré σ -fini**.

La mesure μ sur Ω est **finie** si $\mu(\Omega) < \infty$.

Remarque 7.24.

La définition implique automatiquement que $\mu(\emptyset) = 0$. En effet si A est une partie mesurable, $\mu(A \cup \emptyset) = \mu(A)$, mais A et $\emptyset$ sont disjoints, donc $\mu(A \cup \emptyset) = \mu(A) + \mu(\emptyset)$.

Si $(\Omega, \mathcal{A}, \mu)$ et $(S, \mathcal{F}, \nu)$ sont deux espaces mesurés, alors nous notons

$$(\Omega, \mathcal{A}, \mu) \subset (S, \mathcal{F}, \nu) \quad (7.35)$$

lorsque $\Omega \subset S$, $\mathcal{A} \subset \mathcal{F}$ et pour tout $A \in \mathcal{A}$, $\mu(A) = \nu(A)$.

Définition 7.25 (Ensemble mesurable).

Les éléments de $\mathcal{A}$ sont les ensembles **mesurables** pour la mesure μ .

Si la mesure est σ -finie, nous pouvons choisir le recouvrement croissant pour l'inclusion. En effet si $(E_n)_{n \in \mathbb{N}}$ est le recouvrement, il suffit de considérer $F_n = \bigcup_{k \leq n} E_k$. Ces ensembles F_n forment tout autant un recouvrement dénombrable, mais il est évidemment croissant.

Le lemme suivant complète la propriété 7.23(2) lorsque les ensembles ne sont pas disjoints.

Lemme 7.26.

Si $A \subset B$ sont deux ensembles μ -mesurables de mesure finie alors

$$\mu(B \setminus A) = \mu(B) - \mu(A) \quad (7.36)$$

et en particulier

$$\mu(B) \geq \mu(A). \quad (7.37)$$

Si (M_n) est une suite d'éléments de $\mathcal{A}$ pas spécialement disjoints, alors

$$\mu\left(\bigcup_k M_k\right) \leq \sum_k \mu(M_k). \quad (7.38)$$

Démonstration. Vu que les ensembles $B \setminus A$ et A sont disjoints par la propriété (2) de la définition de mesure nous avons

$$\mu((B \setminus A) \cup A) = \mu(B \setminus A) + \mu(A) \quad (7.39)$$

et donc

$$\mu(B) = \mu(B \setminus A) + \mu(A) \quad (7.40)$$

comme demandé.

Pour la seconde partie nous considérons la suite disjointe

$$\begin{cases} M'_0 = \emptyset \\ M'_k = M_k \setminus M'_{k-1}. \end{cases} \quad (7.41a)$$

$$(7.41b)$$

Nous avons $\bigcup_k M'_k = \bigcup_k M_k$. Le calcul suivant est alors immédiat :

$$\mu\left(\bigcup_k M_k\right) = \mu\left(\bigcup_k M'_k\right) = \sum_k \mu(M'_k) = \sum_k \mu(M_k \setminus M'_{k-1}) \leq \sum_k \mu(M_k). \quad (7.42)$$

□

4. Les définitions de tribus et d'espaces mesurables sont en 7.1.

Lemme 7.27 ([8]).

Résultats sur les unions croissantes d'ensembles mesurables dans $(S, \mathcal{A}, \mu)$.

(1) Si (A_k) est une suite croissante d'ensembles μ -mesurables dont l'union est mesurable, alors

$$\lim_{n \rightarrow \infty} \mu(A_k) = \mu\left(\bigcup_k A_k\right). \quad (7.43)$$

(2) Soit K_n , une suite emboîtée d'éléments de $\mathcal{A}$ tels que $K_n \rightarrow S$. Si $A \in \mathcal{A}$ alors

$$\lim_{n \rightarrow \infty} \mu(A \cap K_n) = \mu(A). \quad (7.44)$$

Démonstration. Pour prouver (1), nous faisons le coup de l'union télescopique, en posant $A_0 = \emptyset$:

$$\bigcup_{k=1}^{\infty} A_k = \bigcup_{k=1}^{\infty} (A_k \setminus A_{k-1}). \quad (7.45)$$

Les ensembles $A_k \setminus A_{k-1}$ sont deux à deux disjoints, donc la propriété (2) de la définition d'une mesure donne

$$\mu\left(\bigcup_{k=1}^{\infty} A_k\right) = \mu\left(\bigcup_{k=1}^{\infty} (A_k \setminus A_{k-1})\right) \quad (7.46a)$$

$$= \sum_{k=1}^{\infty} \mu(A_k \setminus A_{k-1}) \quad (7.46b)$$

$$= \sum_{k=1}^{\infty} (\mu(A_k) - \mu(A_{k-1})) \quad (7.46c)$$

$$= \lim_{k \rightarrow \infty} \mu(A_k) - \mu(A_0) \quad (7.46d)$$

$$= \lim_{k \rightarrow \infty} \mu(A_k). \quad (7.46e)$$

où pour obtenir 7.46c, nous avons utilisé le lemme 7.26.

Le point (2) est une application du point (1). $\square$

Définition 7.28 (mesure de comptage).

Soit $(S, \mathcal{F})$ un ensemble mesurable. La **mesure de comptage** sur $(S, \mathcal{F})$ est la mesure définie par

$$m(A) = \begin{cases} \text{Card}(A) & \text{si } A \text{ est fini} \\ +\infty & \text{sinon.} \end{cases} \quad (7.47)$$

Cette mesure est utilisée pour voir des séries comme des intégrales sur $(\mathbb{N}, \mathcal{P}(\mathbb{N}), m)$.

Exemple 7.29

La mesure de comptage m sur $\mathbb{N}$ est σ -finie parce que $E_n = \{0, \dots, n\}$ est de mesure finie et $\bigcup_{n \in \mathbb{N}} E_n = \mathbb{N}$. $\triangle$

Exemple 7.30

L'intervalle $I = [0, 1]$ muni de la tribu de toutes ses parties et de la mesure de comptage est un espace mesuré non σ -fini. $\triangle$

Exemple 7.31

L'intégration à la Riemann n'est pas dans la théorie des espaces mesurés. En effet l'ensemble

$$\mathcal{A} = \{A \subset [0, 1] \text{ tel que } \mathbb{1}_A \text{ est intégrable au sens de Riemann}\} \quad (7.48)$$

n'est pas une tribu. Par exemple les singletons en font partie tandis que $[0, 1] \cap \mathbb{Q}$ n'en fait pas partie malgré que ce soit une union dénombrable de singletons. $\triangle$

Définition 7.32.

Si μ est une mesure nous disons qu'une propriété est vraie μ -**presque partout** si elle est fausse seulement sur un ensemble de mesure nulle.

Par exemple la fonction de Dirichlet est presque partout égale à la fonction 1 (pour la mesure de Lebesgue).

Définition 7.33 (fonction mesurable).

Une application entre espace mesurés

$$f: (\Omega, \mathcal{A}) \rightarrow (\Omega', \mathcal{A}') \quad (7.49)$$

est **mesurable** si pour tout $B \in \mathcal{A}'$, l'ensemble $f^{-1}(B)$ est dans $\mathcal{A}$.

Lemme 7.34.

Une union dénombrable d'ensemble de mesure nulle est de mesure nulle.

Démonstration. C'est une conséquence immédiate du point (2) de la définition d'une mesure : si les A_i sont de mesure nulle,

$$\mu \left(\bigcup_{i=1}^{\infty} A_i \right) \leq \mu(A_i) = 0 \quad (7.50)$$

□

Définition 7.35.

Si (A_n) est une suite croissante d'ensembles alors la **limite** est

$$\lim_n A_n = \bigcup_{i=0}^{\infty} A_i. \quad (7.51)$$

Si la suite est décroissante alors la limite est

$$\lim_n A_n = \bigcap_{i=0}^{\infty} A_i. \quad (7.52)$$

Proposition 7.36 ([120]).

Soit μ une mesure sur Ω et (S_n) une suite croissante d'ensembles μ -mesurables de Ω . Nous notons

$$S = \lim_n S_n. \quad (7.53)$$

Alors pour tout ensemble mesurable⁵ $A \subset \Omega$ nous avons

$$\mu(A \cap S) = \lim_{n \rightarrow \infty} \mu(A \cap S_n). \quad (7.54)$$

Note : dans la référence le résultat fonctionne pour tout ensemble A (et non seulement les mesurables) parce que la définition de la mesurabilité est un peu différente.

Démonstration. L'inégalité $\lim \mu(A \cap S_n) \leq \mu(A \cap S)$ est simple à prouver. En effet pour tout n nous avons $A \cap S_n \subset A \cap S$ et donc par le lemme 7.26 nous avons

$$\mu(A \cap S_n) \leq \mu(A \cap S). \quad (7.55)$$

En passant à la limite (qui respecte les inégalités) nous avons l'inégalité.

Nous passons à l'inégalité dans l'autre sens. D'abord si $\mu(A \cap S_n) = \infty$ pour un certain n , alors il cela vaut encore ∞ pour tous les n suivants et la limite est ∞ sans problèmes. Donc nous

5. Définition 7.25

supposons que $\mu(A \cap S_n) < \infty$ pour tout $n \in \mathbb{N}$. De plus, quitte à renommer les indices, nous pouvons supposer que $S_0 = \emptyset$.

Un élément x est dans S si et seulement si il existe $n \geq 0$ tel que $x \in S_{n+1}$. En prenant le plus petit de ces n nous avons $x \in S_n$ (éventuellement $n = 0$) et donc

$$S = \bigcup_{n=0}^{\infty} (S_{n+1} \setminus S_n). \quad (7.56)$$

Par conséquent

$$A \cap S = A \cap \bigcup_{n=0}^{\infty} (S_{n+1} \setminus S_n) = \bigcup_{n=0}^{\infty} A \cap (S_{n+1} \setminus S_n) \quad (7.57)$$

Étant donné que les ensembles $A \cap (S_{n+1} \setminus S_n)$ sont disjoints,

$$\mu(A \cap S) = \sum_{n=0}^{\infty} \mu(A \cap (S_{n+1} \setminus S_n)) \quad (7.58a)$$

$$= \sum_{n=0}^{\infty} \mu((A \cap S_{n+1}) \setminus (A \cap S_n)) \quad (7.58b)$$

$$= \sum_{n=0}^{\infty} [\mu(A \cap S_{n+1}) - \mu(A \cap S_n)] \quad (7.58c)$$

$$= \lim_{n \rightarrow \infty} \mu(A \cap S_{n+1}) - \underbrace{\mu(A \cap S_0)}_{=0} \quad (7.58d)$$

$$= \lim_{n \rightarrow \infty} \mu(A \cap S_n). \quad (7.58e)$$

Dans ce calcul nous avons utilisé plusieurs fois le fait que les S_n et A étaient mesurables (et la propriété de tribu qui dit que $A \cap S_n$ est également mesurable) ainsi que le lemme 7.26. Nous avons aussi utilisé la série télescopique dans $\mathbb{R}$ pour obtenir (7.58d). $\square$

Définition 7.37 (λ -système[121]).

Soit E un ensemble. Un ensemble $\mathcal{D}$ de parties de E est un λ -**système** lorsqu'il vérifie les conditions suivantes :

- (1) si $A, B \in \mathcal{D}$ avec $A \subset B$ alors $B \setminus A \in \mathcal{D}$,
- (2) si $(A_k)_{k \geq 1}$ est une suite croissante d'éléments de $\mathcal{D}$ alors $\bigcup_k A_k \in \mathcal{D}$.

Note : une tribu est un λ -système.

Lemme 7.38 ([121]).

Une intersection quelconque de λ -systèmes dans E est un λ -système dans E .

Démonstration. Soient $\{\mathcal{D}_l\}_{l \in L}$ des λ -systèmes indicés par un ensemble L . Si $A, B \in \bigcap_{l \in L} \mathcal{D}_l$ alors $B \setminus A \in \mathcal{D}_l$ pour tout $l \in L$ et donc $A \setminus B \in \bigcap_{l \in L} \mathcal{D}_l$. De la même façon si (A_k) est une suite croissante dans $\bigcap_{l \in L} \mathcal{D}_l$ alors pour tout $l \in L$ nous avons $\bigcup_k A_k \in \mathcal{D}_l$. Donc $\bigcup_k A_k \in \bigcap_l \mathcal{D}_l$. $\square$

Ce lemme est ce qui permet de définir le λ -système **engendré** par une classe $\mathcal{A}$ de parties de E : c'est l'intersection de tous les λ -systèmes de E contenant $\mathcal{A}$.

Lemme 7.39 ([121]).

Soit $\mathcal{C}$ une classe de parties de E (contenant E lui-même) qui soit stable par intersection finie. Alors le λ -système engendré par $\mathcal{C}$ coïncide avec la tribu engendrée par $\mathcal{C}$.

Démonstration. Nous notons $\mathcal{E}$ le λ -système engendré par $\mathcal{C}$ et $\mathcal{F}$ la tribu engendrée par $\mathcal{C}$. Étant donné que $\mathcal{F}$ est un λ -système nous avons $\mathcal{E} \subset \mathcal{F}$. Pour montrer l'inclusion inverse nous allons prouver que $\mathcal{E}$ est une tribu.

D'abord pour $C \in \mathcal{C}$ nous posons

$$\mathcal{G}_C = \{A \in \mathcal{E} \text{ tel que } A \cap C \in \mathcal{E}\}. \quad (7.59)$$

et pour $F \in \mathcal{E}$,

$$\mathcal{H}_F = \{A \in \mathcal{E} \text{ tel que } A \cap F \in \mathcal{E}\}. \quad (7.60)$$

Nous allons montrer que $\mathcal{G}_C$ et $\mathcal{H}_F$ sont des λ -systèmes et que $\mathcal{G}_C = \mathcal{H}_F = \mathcal{E}$.

Nous commençons par $\mathcal{G}_C$. Si $A, B \in \mathcal{G}_C$ avec $A \subset B$ alors

$$(B \setminus A) \cap C = \underbrace{(B \cap C)}_{\in \mathcal{E}} \setminus \underbrace{(A \cap C)}_{\in \mathcal{E}}. \quad (7.61)$$

Vu que $\mathcal{E}$ est un λ -système et que $(A \cap C) \subset (B \cap C)$ nous avons bien $(B \setminus A) \cap C \in \mathcal{E}$ et donc $B \setminus A \in \mathcal{G}_C$. Soit maintenant (A_k) une suite croissante dans $\mathcal{G}_C$. Nous avons

$$\left(\bigcup_{k=1}^{\infty} A_k \right) \cap C = \bigcup_{k=1}^{\infty} (A_k \cap C) \quad (7.62)$$

qui est une union d'une suite croissante d'éléments de $\mathcal{E}$. Donc $\bigcup_{k=1}^{\infty} (A_k \cap C) \in \mathcal{E}$, ce qui signifie que $\bigcup_{k=1}^{\infty} A_k \in \mathcal{G}_C$. Cela termine la preuve du fait que $\mathcal{G}_C$ soit un λ -système.

Étant donné que $\mathcal{C}$ est stable par intersection finie, si $K \in \mathcal{C}$ nous avons $C \cap K \in \mathcal{C}$, ce qui signifie que $K \in \mathcal{G}_C$. Nous avons donc $\mathcal{C} \subset \mathcal{G}_C$. Donc $\mathcal{G}_C$ est un λ -système vérifiant $\mathcal{C} \subset \mathcal{G}_C \subset \mathcal{E}$. Mais comme $\mathcal{E}$ est le plus petit λ -système contenant $\mathcal{C}$ nous avons en fait $\mathcal{G}_C = \mathcal{E}$.

Nous montrons à présent que $\mathcal{H}_F$ est un λ -système. Si $A, B \in \mathcal{H}_F$ avec $A \subset B$ alors $(B \setminus A) \cap F = (B \cap F) \setminus (A \cap F)$. Vu que $\mathcal{E}$ est un λ -système et que $A \cap F$ et $B \cap F$ sont dans $\mathcal{E}$ avec $A \cap F \subset B \cap F$, nous avons

$$(B \cap F) \setminus (A \cap F) \in \mathcal{H}_F. \quad (7.63)$$

Soit maintenant $(A_k)_{k \geq 1}$ une suite croissante dans $\mathcal{H}_F$. Pour tout k nous avons $A_k \cap F \in \mathcal{E}$, ce qui donne

$$\left(\bigcap_{k=1}^{\infty} A_k \right) \cap F = \bigcap_{k=1}^{\infty} (A_k \cap F) \in \mathcal{E}. \quad (7.64)$$

Donc $\mathcal{H}_F$ est un λ -système vérifiant $\mathcal{C} \subset \mathcal{H}_F \subset \mathcal{E}$. Nous en concluons que pour tout $C \in \mathcal{C}$ et pour tout $F \in \mathcal{E}$,

$$\mathcal{G}_C = \mathcal{H}_F = \mathcal{E}. \quad (7.65)$$

Nous allons maintenant prouver que $\mathcal{E}$ est une tribu⁶.

- (1) Si $F \in \mathcal{E}$ alors $E \cap F = F \in \mathcal{E}$, ce qui signifie que $E \in \mathcal{H}_F = \mathcal{E}$.
- (2) Si $A \in \mathcal{E}$ alors $E \setminus A \in \mathcal{E}$ parce que $\mathcal{E}$ est un λ -système et $E \in \mathcal{E}$. Donc $\complement A \in \mathcal{E}$.
- (3) Montrons que $\mathcal{E}$ est stable par union finie en considérant $A, B \in \mathcal{E}$. Vu que E est également un élément de $\mathcal{E}$ nous avons

$$E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B) \in \mathcal{E}. \quad (7.66)$$

Cela prouve que $\complement(A \cup B) \in \mathcal{E}$. Par complémentarité nous avons aussi $A \cup B \in \mathcal{E}$.

Soient $A_k \in \mathcal{E}$, et nommons $B_p = A_1 \cup \dots \cup A_p$. Les ensembles B_p forment une suite croissante d'éléments de $\mathcal{E}$. L'union est donc dans $\mathcal{E}$ et ce dernier est au final stable par union dénombrable.

Maintenant que $\mathcal{E}$ est une tribu nous avons $\mathcal{F} \subset \mathcal{E}$ parce que $\mathcal{F}$ est la plus petite tribu contenant $\mathcal{C}$. Nous en déduisons que $\mathcal{E} = \mathcal{F}$, ce qu'il fallait démontrer. $\square$

Le théorème suivant permet de prouver que la mesure de Lebesgue est l'unique mesure possible ayant les bonnes valeurs sur les intervalles (théorème 7.159).

6. Définition 7.1.

Théorème 7.40 (Unicité des mesures[121]).

Soient μ et ν , deux mesures sur $(E, \mathcal{A})$ et une classe $\mathcal{E}$ de parties de E telles que

- (1) La tribu engendrée par $\mathcal{E}$ soit $\mathcal{A}$.
- (2) si $A, B \in \mathcal{E}$ alors $A \cap B \in \mathcal{E}$
- (3) il existe une suite croissante (E_n) dans $\mathcal{E}$ telle que $E = \lim E_n$.

Alors si les mesures μ et ν coïncident sur $\mathcal{E}$, elles coïncident sur $\mathcal{A}$ en entier.

Démonstration. Soit (E_n) la suite des hypothèses ; nous considérons μ_n et ν_n , les restrictions de μ et ν à E_n , c'est à dire

$$\mu_n(A) = \mu(A \cap E_n) \quad (7.67a)$$

$$\nu_n(A) = \nu(A \cap E_n). \quad (7.67b)$$

Vu que les E_n sont dans $\mathcal{E} \subset \mathcal{A}$ ils sont mesurables au sens de μ et ν . Par la proposition 7.36, pour tout $A \in \mathcal{E}$ nous avons alors

$$\lim_{n \rightarrow \infty} \mu_n(A) = \mu(A) \quad (7.68a)$$

$$\lim_{n \rightarrow \infty} \nu_n(A) = \nu(A) \quad (7.68b)$$

Nous devons donc seulement montrer que pour tout $A \in \mathcal{A}$ et pour tout $n \in \mathbb{N}$, $\mu_n(A) = \nu_n(A)$. Pour cela nous nous fixons un n et nous considérons la classe

$$\mathcal{D} = \{A \in \mathcal{A} \text{ tel que } \mu_n(A) = \nu_n(A)\}. \quad (7.69)$$

Le but sera de prouver que $\mathcal{D} = \mathcal{A}$.

Par hypothèse $A \cap E_n \in \mathcal{E}$ et donc

$$\mu(A \cap E_n) = \nu(A \cap E_n) < \infty, \quad (7.70)$$

c'est à dire que $\mu_n = \nu_n$ sur $\mathcal{E}$. Par ailleurs, $E \cap E_n = E_n \in \mathcal{E}$, donc

$$\mu_n(E) = \nu_n(E) < \infty. \quad (7.71)$$

Par conséquent $\mu_n = \nu_n$ sur la classe $\mathcal{E}' = \mathcal{E} \cup \{E\} : \mathcal{E}' \subset \mathcal{D}$.

Montrons que $\mathcal{D}$ est un λ -système. Soient $A, B \in \mathcal{D}$ avec $A \subset B$. Alors, étant donné que les mesures μ_n et ν_n sont finies, le lemme 7.26 nous donne

$$\mu_n(B \setminus A) = \mu_n(B) - \mu_n(A) \quad (7.72a)$$

$$\nu_n(B \setminus A) = \nu_n(B) - \nu_n(A). \quad (7.72b)$$

Donc $\mu_n(B \setminus A) = \nu_n(B \setminus A)$ et $B \setminus A \in \mathcal{D}$.

Soit par ailleurs une suite croissante $(A_k)_{k \geq 1}$ d'éléments de $\mathcal{D}$. En posant $B_p = \bigcup_{k=1}^p A_k$, le lemme 7.27(1) nous donne

$$\mu_n\left(\bigcup_{k=1}^{\infty} A_k\right) = \lim_{p \rightarrow \infty} \mu_n(A_p). \quad (7.73)$$

Mais vu que pour chaque p nous avons $\mu_n(A_p) = \nu_n(A_p)$, nous avons aussi

$$\mu_n\left(\bigcup_{p=1}^{\infty} A_p\right) = \nu_n\left(\bigcup_{p=1}^{\infty} A_p\right). \quad (7.74)$$

Donc $\mathcal{D}$ est bel et bien un λ -système contenant $\mathcal{E}'$. Par le lemme 7.39, le λ -système engendré par $\mathcal{E}'$ est égal à la tribu engendrée par $\mathcal{E}'$, mais par hypothèse la tribu engendrée par $\mathcal{E}$ est $\mathcal{A}$, donc le λ -système engendré par $\mathcal{E}'$ est $\mathcal{A}$. Vu que $\mathcal{D}$ est un λ -système contenant $\mathcal{E}'$, nous avons alors $\mathcal{A} \subset \mathcal{D}$ et donc $\mathcal{A} = \mathcal{D}$, ce qu'il fallait. $\square$

Exemple 7.41

La partie $\mathcal{E}$ des intervalles de $\mathbb{R}$ de la forme $]a, b[$ engendre les boréliens par la proposition 5.43. Par conséquent pour vérifier que deux mesures sont égales sur les boréliens de $\mathbb{R}$ il suffit de prouver qu'elles sont égales sur les intervalles ouverts. $\triangle$

7.2.3 Mesure extérieure

Nous avons déjà défini la notion de mesure extérieure en la définition 7.17.

Lemme 7.42 ([119]).

Soit $(S, \mathcal{F}, \mu)$ un espace mesuré et $X \subset S$. Alors

$$\inf_{\substack{A \in \mathcal{F} \\ X \subset A}} \mu(A) = \inf \left\{ \sum_n \mu(A_n) \text{ tel que } A_n \in \mathcal{F}, X \subset \bigcup_k A_k \right\}. \quad (7.75)$$

Démonstration. Pour montrer l'inégalité $\geq$, nous remarquons qu'il y a plus d'éléments dans l'ensemble du second membre que dans le premier. En effet si $A \in \mathcal{F}$ avec $X \subset A$ alors dans le membre de gauche nous pouvons prendre $A_1 = A$ et $A_{n \geq 1} = \emptyset$.

Pour l'inégalité dans l'autre sens, nous montrons que tout élément de

$$\left\{ \sum_n \mu(A_n) \text{ tel que } A_n \in \mathcal{F}, X \subset \bigcup_k A_k \right\} \quad (7.76)$$

est plus grand qu'un élément de

$$\{\mu(A) \text{ tel que } A \in \mathcal{F}, X \subset A\}. \quad (7.77)$$

En effet si $A_n \in \mathcal{F}$ avec $X \subset \bigcup_k A_k$ alors en posant $A = \bigcup_k A_k$ nous avons $A \in \mathcal{F}$ avec $X \subset A$ ainsi que $\mu(A) \leq \sum_n \mu(A_n)$. Cela prouve que l'élément $\sum_n \mu(A_n)$ de (7.76) est plus grand que l'élément $\mu(A)$ de (7.77). $\square$

Proposition 7.43 ([119]).

Soit un espace mesuré $(S, \mathcal{F}, \mu)$ et l'application

$$\begin{aligned} \mu^* : \mathcal{P}(S) &\rightarrow [0, \infty] \\ X &\mapsto \inf \{ \mu(A) \text{ tel que } A \in \mathcal{F}, X \subset A \}. \end{aligned} \quad (7.78)$$

Alors μ^* est une mesure extérieure sur S et sa restriction à $\mathcal{F}$ est égale à μ .

Cela est un cas particulier de 7.22 en utilisant 7.42. Nous en donnons cependant une preuve directe, qui est presque identique à celle de 7.22, mais avec une ou deux simplifications.

Démonstration. Notons que la définition est bonne parce que l'ensemble sur lequel l'infimum est pris n'est pas vide : prendre $A = S$.

Le vide D'abord $\mu^*(\emptyset) = 0$ parce que $\emptyset \in \mathcal{F}$.

Inégalité d'inclusion Soient $X \subset Y$ dans $\mathcal{P}(S)$. Si $Y \subset A$ alors $X \subset A$, donc

$$\inf \{ \mu(A) \text{ tel que } A \in \mathcal{F}, X \subset A \} \leq \inf \{ \mu(A) \text{ tel que } A \in \mathcal{F}, Y \subset A \}, \quad (7.79)$$

ce qui signifie que $\mu^*(X) \leq \mu^*(Y)$.

Inégalité par union dénombrable Soit $(X_n)_{n \in \mathbb{N}}$ une suite de parties de S . Si il existe n_0 tel que $\mu^*(X_{n_0}) = \infty$ alors nous avons automatiquement $\sum_n \mu^*(X_n) = \infty$ et l'inégalité demandée est évidente parce que n'importe quoi est plus petit ou égal à ∞ . Nous supposons donc que $\mu^*(X_n) < \infty$ pour tout n .

Soit $\epsilon > 0$ et par définition pour chaque n , il existe un $A_n \in \mathcal{F}$ tel que $X_n \subset A_n$ et $\mu(A_n) \leq \mu^*(X_n) + \frac{\epsilon}{2^n}$. Bien entendu nous avons

$$\bigcup_n X_n \subset \bigcup_n A_n \in \mathcal{F}. \quad (7.80)$$

Nous en déduisons que

$$\mu^*\left(\bigcup_n X_n\right) \leq \mu\left(\bigcup_n A_n\right). \quad (7.81)$$

Mais $(S, \mathcal{F}, \mu)$ étant un espace mesuré,

$$\mu\left(\bigcup_n A_n\right) \leq \sum_n \mu(A_n). \quad (7.82)$$

Au final nous avons les inégalités

$$\mu^*\left(\bigcup_n X_n\right) \leq \mu\left(\bigcup_n A_n\right) \leq \sum_n \mu(A_n) \leq \sum_n \mu^*(X_n) + \epsilon \sum_n \frac{1}{2^n} = \sum_n \mu^*(X_n) + \epsilon. \quad (7.83)$$

Cela étant vrai pour tout ϵ ,

$$\mu^*\left(\bigcup_n X_n\right) \leq \sum_n \mu^*(X_n), \quad (7.84)$$

ce qui prouve que μ^* est une mesure extérieure.

Restriction Supposons que $X \in \mathcal{F}$. Alors si $X \subset A$ nous avons $\mu(X) \leq \mu(A)$; mais en même temps, $\mu(X)$ est dans l'infimum qui définit $\mu^*(X)$ donc

$$\mu^*(X) \leq \mu(X) \leq \inf\{\mu(A) \text{ tel que } A \in \mathcal{F}, X \subset A\} \leq \mu(X) \leq \mu^*(X). \quad (7.85)$$

Donc nous avons égalité de tous les éléments de cette chaîne d'inégalité.

□

Définition 7.44.

Soit S un ensemble et m^* une mesure extérieure sur S . Une partie $A \subset X$ est m^* -mesurable si pour tout $X \subset S$,

$$m^*(X) = m^*(X \cap A) + m^*(X \cap A^c). \quad (7.86)$$

Remarque 7.45.

L'inégalité

$$m^*(X) \leq m^*(X \cap A) + m^*(X \cap A^c) \quad (7.87)$$

étant toujours vraie, pour prouver qu'un ensemble est m^* -mesurable, il est suffisant de prouver l'inégalité inverse :

$$m^*(X) \geq m^*(X \cap A) + m^*(X \cap A^c) \quad (7.88)$$

La définition 7.44 est motivée par la proposition suivante.

Proposition 7.46.

Soit un espace mesuré $(S, \mathcal{F}, \mu)$ et μ^* la mesure extérieure qui va avec. Alors tous les éléments de $\mathcal{F}$ sont μ^* -mesurables.

En d'autres termes, pour tout $A \in \mathcal{F}$ et tout $X \subset S$ nous avons

$$\mu^*(X) = \mu^*(X \cap A) + \mu^*(X \cap A^c). \quad (7.89)$$

Démonstration. Vu que $X = (X \cap A) \cup (X \cap A^c)$, et que μ^* est une mesure extérieure,

$$\mu^*(X) \leq \mu^*(X \cap A) + \mu^*(X \cap A^c). \quad (7.90)$$

Nous devons montrer l'inégalité inverse.

Soit $B \in \mathcal{F}$ tel que $X \subset B$. D'une part nous avons $X \cap A \subset B \cap A \in \mathcal{F}$, donc

$$\mu^*(X \cap A) \leq \mu^*(B \cap A) = \mu(B \cap A). \quad (7.91)$$

Et d'autre part, $X \cap A^c \subset B \cap A^c \in \mathcal{F}$, donc

$$\mu^*(X \cap A^c) \leq \mu(B \cap A^c). \quad (7.92)$$

En remettant ensemble,

$$\mu^*(X \cap A) + \mu^*(X \cap A^c) \leq \mu(B \cap A) + \mu(B \cap A^c) = \mu(B). \quad (7.93)$$

La dernière égalité est le fait que $B \cap A$ et $B \cap A^c$ sont disjoints et que μ est une mesure. L'inégalité (7.93) étant vraie pour tout $B \in \mathcal{F}$ tel que $X \subset B$, elle est encore vraie pour l'infimum :

$$\mu^*(X \cap A) + \mu^*(X \cap A^c) \leq \inf\{\mu(B) \text{ tel que } B \in \mathcal{F}, X \subset B\} = \mu^*(X). \quad (7.94)$$

Nous avons donc prouvé que

$$\mu^*(X \cap A) + \mu^*(X \cap A^c) \leq \mu^*(X). \quad (7.95)$$

□

Remarque 7.47.

Notons la duplicité du vocabulaire. Les ensembles μ -mesurables sont les éléments de $\mathcal{F}$, qui sont a priori les seuls sur lesquels μ est calculable⁷, alors que les μ^* -mesurables sont les parties de S qui vérifient une certaine propriété (et μ^* est calculable sur toutes les parties de S).

7.2.4 Espace mesuré complet

Définition 7.48.

Soit un espace mesuré $(X, \mathcal{A}, \mu)$. Une partie N de X est **négligeable** pour μ si il existe $Y \in \mathcal{A}$ tel que $N \subset Y$ et $\mu(Y) = 0$.

Lemme 7.49.

L'ensemble des parties négligeables est stable par union dénombrable.

Démonstration. Si les ensembles N_i sont négligeables, alors pour chaque i nous avons $Y_i \in \mathcal{A}$ tel que $N_i \subset Y_i$ et $\mu(Y_i) = 0$. Alors bien entendu $\bigcup_i N_i \subset \bigcup_i Y_i$ et en utilisant (7.38),

$$\mu\left(\bigcup_i Y_i\right) \leq \sum_i \mu(Y_i) = 0. \quad (7.96)$$

□

Définition 7.50.

L'espace mesuré $(X, \mathcal{F}, \mu)$ est **complet** si tout ensemble μ -négligeable est dans $\mathcal{F}$.

Notons que la proposition 7.5 s'applique si $(X, \mathcal{F}, \mu)$ est un espace mesuré et $\mathcal{N}$ est l'ensemble des parties μ -négligeables. C'est ce qui permet de donner le théorème suivant, que nous redémontrons de façon indépendante de la proposition 7.5.

Théorème 7.51 (Complétion d'espace mesuré[119, 122, 123]).

Soit un espace mesuré $(X, \mathcal{F}, \mu)$ et $\mathcal{N}$ l'ensemble des parties μ -négligeables de X .

(1) Les ensembles suivants sont égaux :

$$\mathcal{A} = \{A \subset X \text{ tel que } \exists B, C \in \mathcal{F} \text{ tel que } B \subset A \subset C, \mu(C \setminus B) = 0\} \quad (7.97a)$$

$$\mathcal{B} = \{B \cup N \text{ tel que } B \in \mathcal{F}, N \in \mathcal{N}\} \quad (7.97b)$$

$$\mathcal{C} = \{A \subset X \text{ tel que } \exists B \in \mathcal{F} \text{ tel que } A \Delta B \in \mathcal{N}\}. \quad (7.97c)$$

Ici $A \Delta B$ est la différence symétrique de A et B , définition 1.8.

(2) L'ensemble $\hat{\mathcal{F}} = \mathcal{A} = \mathcal{B} = \mathcal{C}$ est une tribu.

7. «calculable» au sens où μ y vaut un nombre bien défini ; après, que ce soit facile ou pas à calculer dans la pratique, c'est une autre histoire.

(3) *La définition*

$$\begin{aligned} \mu' : \mathcal{B} &\rightarrow [0, \infty] \\ A \cup N &\mapsto \mu(A) \end{aligned} \quad (7.98)$$

est cohérente.

(4) *L'application μ' ainsi définie est une mesure sur $(X, \mathcal{A})$.*

(5) *L'espace $(X, \mathcal{A}, \mu')$ est complet.*

(6) *La mesure μ' prolonge μ .*

(7) *La mesure μ' est minimale au sens où toute mesure complète prolongeant μ prolonge μ' .*

Démonstration. Commençons par prouver que les trois ensembles $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ sont égaux.

$\mathcal{A} \subset \mathcal{B}$. Soit $A \in \mathcal{A}$. Alors nous avons des ensembles $B, C \in \mathcal{F}$ tels que $B \subset A \subset V$ avec $\mu(C \setminus B) = 0$. Alors nous avons aussi $A = B \cup (C \setminus B)$, ce qui prouve que $A \in \mathcal{B}$.

$\mathcal{B} \subset \mathcal{C}$. Soit $A \in \mathcal{B}$, c'est à dire que $A = B \cup N$ avec $B \in \mathcal{F}$ et $N \in \mathcal{N}$. Nous avons évidemment $A \cup B = A$ et donc

$$A \Delta B = (A \cup B) \setminus (A \cap B) = A \setminus (A \cap B) = (B \cup N) \setminus (A \cap B) \subset N. \quad (7.99)$$

Pour comprendre la dernière inclusion, si x appartient à $A = B \cup N$ sans être dans N alors $x \in B$ et donc $x \in A \cap B$. Par conséquent nous avons $A \Delta B \subset N$ et donc $A \Delta B \in \mathcal{N}$.

$\mathcal{C} \subset \mathcal{A}$ Soit donc $A \in \mathcal{C}$; il existe $B \in \mathcal{F}$ tel que $A \Delta B \in \mathcal{N}$ ou encore, il existe $D \in \mathcal{F}$ tel que $A \Delta B \subset D$ avec $\mu(D) = 0$. Si nous posons $B' = B \cap D^c$ et $C' = B \cup D$ alors nous prétendons avoir

$$B' \subset A \subset C'. \quad (7.100)$$

Et nous le prouvons. En effet si $x \in B \cap D^c$ alors en remarquant que B se divise en

$$B = (B \cap A) \cup (B \cap (A \Delta B)), \quad (7.101)$$

et en nous souvenant que $B \cap (A \Delta B) \subset D$, il vient que $B \cap D^c \subset B \cap A$. Et en particulier $x \in A$. D'autre part

$$A \subset B \cup (A \Delta B) \subset B \cup D. \quad (7.102)$$

Nous avons donc bien $B' \subset A \subset C'$. Par stabilité de la tribu $\mathcal{F}$ sous les intersections et complémentaires nous avons aussi $B', C' \in \mathcal{F}$. De plus

$$C' \setminus B' = (B \cup D) \setminus (B \cap D^c) \subset D, \quad (7.103)$$

et donc

$$\mu(C' \setminus B') \leq \mu(D) = 0. \quad (7.104)$$

Nous avons donc prouvé que $\mathcal{A} \subset \mathcal{B} \subset \mathcal{C} \subset \mathcal{A}$, et donc que $\mathcal{A} = \mathcal{B} = \mathcal{C}$. Nous allons donc maintenant noter $\mathcal{A}$ indifféremment les trois ensembles. Nous prouvons à présent que c'est une tribu.

Tribu : le vide Pas de problèmes à $\emptyset \in \mathcal{A}$

Tribu : complémentaire Soit $A \in \mathcal{A}$. Alors il existe $B, C \in \mathcal{F}$ tels que $B \subset A \subset C$ avec $\mu(C \setminus B) = 0$. En passant au complémentaire,

$$C^c \subset A^c \subset B^c. \quad (7.105)$$

Mais $B^c \setminus C^c = C \setminus B$, donc $\mu(B^c \setminus C^c) = 0$.

Tribu : union dénombrable Soit (A_n) des éléments de $\mathcal{A}$. Pour chaque n nous avons des ensembles $B_n, C_n \in \mathcal{F}$ tels que $B_n \subset A_n \subset C_n$ avec $\mu(C_n \setminus B_n) = 0$. En ce qui concerne les unions nous avons

$$\bigcup_n B_n \subset \bigcup_n A_n \subset \bigcup_n C_n, \quad (7.106)$$

et

$$\left(\bigcup_n C_n\right) \setminus \left(\bigcup_n B_n\right) \subset \bigcup_n (C_n \setminus B_n). \quad (7.107)$$

Par conséquent, en utilisant (7.38),

$$\mu\left(\left(\bigcup_n C_n\right) \setminus \left(\bigcup_n B_n\right)\right) \leq \mu\left(\bigcup_n (C_n \setminus B_n)\right) \leq \sum_n \mu(C_n \setminus B_n) = 0. \quad (7.108)$$

Cela prouve que $\bigcup_n A_n \in \mathcal{A}$, et donc que $\mathcal{A}$ est une tribu.

Définition cohérente Soient $A, A' \in \mathcal{F}$ et $N, N' \in \mathcal{N}$ tels que $A \cup N = A' \cup N'$. Nous considérons $Y, Y' \in \mathcal{F}$ tel que $N \subset Y$, $N' \subset Y'$ et $\mu(Y) = \mu(Y') = 0$. En vertu de (7.38) nous avons

$$\mu(A) \leq \mu(A \cup Y) \leq \mu(A' \cup Y \cup Y') \leq \mu(A') + \mu(Y) + \mu(Y') = \mu(A'). \quad (7.109)$$

En écrivant la même chose en échangeant les primes nous prouvons également $\mu(A') \leq \mu(A)$. Au final $\mu(A) = \mu(A')$, c'est à dire

$$\mu'(A \cup N) = \mu'(A' \cup N'). \quad (7.110)$$

La définition de μ' est donc cohérente.

μ' est une mesure Le fait que μ' soit positive et que $\mu'(\emptyset)$ soit nul ne pose pas de problèmes.

Il faut voir l'union dénombrable disjointe. Si les ensembles $A_i = B_i \cup N_i$ sont disjoints, alors les B_i et les N_i sont tous disjoints deux à deux. De plus l'ensemble $\bigcup_i N_i$ est négligeable parce que nous avons déjà vu que $\mathcal{N}$ était stable par union dénombrable (7.38). Donc

$$\mu'\left(\bigcup_i B_i \cup N_i\right) = \mu'\left(\underbrace{\left(\bigcup_i B_i\right) \cup \left(\bigcup_i N_i\right)}_{\in \mathcal{N}}\right) = \mu\left(\bigcup_i B_i\right) = \sum_u \mu(B_i) = \sum_i \mu'(B_i \cup N_i). \quad (7.111)$$

Espace complet Un ensemble μ' -négligeable est automatiquement μ -négligeable. En effet si H est μ' -négligeable, il existe $B \in \mathcal{F}$ et $N \in \mathcal{N}$ tels que $H \subset B \cup N$ avec $\mu(B) = 0$. Vu que N est μ -négligeable, il existe $Y \in \mathcal{F}$ tel que $N \subset Y$ et $\mu(Y) = 0$. Donc $H \subset B \cup N \subset B \cup Y$ avec $\mu(B \cup Y) = 0$.

Tous les ensembles μ -négligeables faisant partie de $\mathcal{B}$, tous les ensembles μ' -négligeables font partie de $\mathcal{A}$.

Prolongement La mesure μ' prolonge μ . En effet si $A \in \mathcal{F}$ alors $A = A \cup \emptyset \in \mathcal{B}$ et A est μ' -mesurable. De plus $\mu'(A) = \mu'(A \cup \emptyset) = \mu(A)$.

Minimalité Soit un espace mesuré complet $(X, \mathcal{M}, \nu)$ prolongeant $(X, \mathcal{F}, \mu)$. Pour $A \in \mathcal{A}$ nous devons prouver que $A \in \mathcal{M}$ et que $\mu'(A) = \nu(A)$. Il existe $B \in \mathcal{F}$ et $N \in \mathcal{N}$ tels que $A = B \cup N$. Vu que N est μ -négligeable, il est également ν -négligeable et donc ν -mesurable parce que ν est complète : $A \in \mathcal{M}$. En ce qui concerne l'égalité $\mu'(A) = \nu(A)$ nous avons

$$\nu(B) \leq \nu(B \cup N) \leq \nu(B) + \nu(N) = \nu(B), \quad (7.112)$$

donc $\nu(A) = \nu(B \cup N) = \nu(B) = \mu(B)$. La dernière égalité est le fait que ν prolonge μ . Mais par définition de μ' nous avons aussi $\mu'(A) = \mu'(B \cup N) = \mu(B)$. Au final $\mu'(A) = \nu(A)$.

□

Définition 7.52.

L'espace mesuré complet $(X, \mathcal{A}, \mu')$ défini par le théorème 7.51 est l'espace mesuré complétée de $(X, \mathcal{F}, \mu)$.

Nous noterons le complété de $(S, \mathcal{F}, \mu)$ par $(S, \hat{\mathcal{F}}, \hat{\mu})$

Théorème 7.53 (Carathéodory[119]).

Soit S un ensemble et m^* une mesure extérieure sur S . Alors

- (1) l'ensemble $\mathcal{M}$ des parties m^* -mesurables est une tribu,
- (2) la restriction de m^* est une mesure sur $(S, \mathcal{M})$,
- (3) l'espace mesuré $(S, \mathcal{M}, m^*)$ est complet⁸.

Démonstration. Une grosse partie de la preuve sera de prouver la stabilité de $\mathcal{M}$ par union dénombrable quelconque ; cela sera divisé en plusieurs parties.

Tribu : le vide L'ensemble vide est m^* -mesurable.

Tribu : complémentaire Soit $A \in \mathcal{M}$ et $X \in S$. La condition qui dirait $A^c \in \mathcal{M}$ est :

$$m^*(X) = m^*(X \cap A^c) + m^*(X \cap A), \quad (7.113)$$

qui est la même que celle qui dit que A est dans $\mathcal{M}$.

Tribu : union finie Soient $A, B \in \mathcal{M}$ et $X \subset S$. Alors, vu que m^* est une mesure extérieure,

$$m^*(X) \leq m^*(X \cap (A \cup B)) + m^*(X \cap (A \cup B)^c) \quad (7.114a)$$

$$= m^*((X \cap A) \cup (X \cap B)) + m^*(X \cap A^c \cap B^c). \quad (7.114b)$$

Mais nous pouvons écrire la première union sous forme d'une union disjointe de la façon suivante :

$$(X \cap A) \cup (X \cap B) = (X \cap A) \cup (X \cap B \cap A^c), \quad (7.115)$$

ce qui donne

$$m^*(X) \leq m^*(X \cap A) + m^*(X \cap B \cap A^c) + m^*(X \cap A^c \cap B^c) \quad (7.116a)$$

$$= m^*(X \cap A) + m^*(X \cap A^c) \quad (7.116b)$$

$$= m^*(X) \quad (7.116c)$$

parce que les deux dernier termes de (7.116a) se somment à $m^*(X \cap A^c)$ parce que $B \in \mathcal{M}$. La dernière ligne est le fait que A soit m^* -mesurable.

Union finie disjointe Soient $\{A_1, \dots, A_n\}$ des éléments deux à deux disjoints de $\mathcal{M}$. Nous allons maintenant prouver par récurrence que

$$m^*\left(X \cap \left(\bigcup_{k=1}^n A_k\right)\right) = \sum_{k=1}^n m^*(X \cap A_k). \quad (7.117)$$

Si $n = 1$ le résultat est évident. Sinon, le fait que A_{n+1} soit m^* -mesurable donne

$$m^*\left(X \cap \left(\bigcup_{k=1}^{n+1} A_k\right)\right) = m^*\left(X \cap \left(\bigcup_{k=1}^{n+1} A_k\right) \cap A_{n+1}\right) + m^*\left(X \cap \left(\bigcup_{k=1}^{n+1} A_k\right) \cap A_{n+1}^c\right). \quad (7.118)$$

Le fait que les A_k soient disjoints implique aussi que

$$X \cap \left(\bigcup_{k=1}^{n+1} A_k\right) \cap A_{n+1} = X \cap A_{n+1} \quad (7.119)$$

8. Définition 7.50.

et

$$X \cap \left(\bigcup_{k=1}^{n+1} A_k \right) \cap A_{n+1}^c = X \cap \left(\bigcup_{k=1}^n A_k \right) \quad (7.120)$$

et donc

$$m^* \left(X \cap \left(\bigcup_{k=1}^{n+1} A_k \right) \right) = m^*(X \cap A_{n+1}) + m^* \left(X \cap \left(\bigcup_{k=1}^n A_k \right) \right) \quad (7.121a)$$

$$\stackrel{rec.}{=} m^*(X \cap A_{n+1}) + \sum_{k=1}^n m^*(X \cap A_k) \quad (7.121b)$$

$$= \sum_{k=1}^{n+1} m^*(X \cap A_k). \quad (7.121c)$$

La relation (7.117) est prouvée.

Notons qu'en particulierisant à $X = S$ nous avons

$$m^* \left(\bigcup_{k=1}^n A_k \right) = \sum_{k=1}^n m^*(A_k) \quad (7.122)$$

dès que les A_k sont des éléments deux à deux disjoints de $\mathcal{M}$.

Union dénombrable disjointe Soit $(A_n)_{n \in \mathbb{N}}$ une suite d'éléments deux à deux disjoints dans $\mathcal{M}$. Nous allons prouver les choses suivantes :

- $\bigcup_n A_n \in \mathcal{M}$
- $m^* \left(\bigcup_n A_n \right) = \sum_n m^*(A_n)$

où toutes les sommes et union sur n sont entre 1 et ∞ .

Nous posons $A = \bigcup_k A_k$ et $B_n = \bigcup_{k=1}^n A_k$. Nous savons que $B_n \in \mathcal{M}$ pour tout n par le point précédent. Donc si $X \in S$ nous avons

$$m^*(X) = m^*(X \cap B_n) + m^*(X \cap B_n^c) \quad (7.123a)$$

$$= \sum_{k=1}^n m^*(X \cap A_k) + m^*(X \cap B_n^c) \quad (7.123b)$$

$$\geq \sum_{k=1}^n m^*(X \cap A_k) + m^*(X \cap A^c) \quad (7.123c)$$

où nous avons utilisé la relation (7.117) sur les B_n ainsi que le fait que $A^c \subset B_n^c$ (parce que $B_n \subset A$). L'inégalité (7.123a) étant vraie pour tout n , elle est vraie à la limite :

$$m^*(X) \geq \sum_{k=1}^{\infty} m^*(X \cap A_k) + m^*(X \cap A^c) \quad (7.124a)$$

$$\geq m^* \left(\bigcup_k (X \cap A_k) \right) + m^*(X \cap A^c) \quad (7.124b)$$

$$= m^* \left(X \cap \left(\bigcup_k A_k \right) \right) + m^*(X \cap A^c) \quad (7.124c)$$

$$= m^*(X \cap A) + m^*(X \cap A^c), \quad (7.124d)$$

ce qui signifie que $A \in \mathcal{M}$. La première des deux choses que nous voulions montrer est faite. En la particulierisant à $X = A$ et en tenant compte des faits que $A \cap A_k = A_k$ et $A \cap A^c = \emptyset$,

$$m^*(A) \geq \sum_{k=1}^{\infty} m^*(A \cap A_k) + m^*(A \cap A^c), \quad (7.125)$$

c'est à dire que pour tout n nous avons

$$m^*\left(\bigcup_{k \in \mathbb{N}} A_k\right) \geq \sum_{k=1}^n m^*(A_k). \quad (7.126)$$

L'inégalité est encore vraie à la limite, et l'inégalité inverse étant toujours vraie pour une mesure extérieure,

$$m^*\left(\bigcup_{k \in \mathbb{N}} A_k\right) = \sum_{k=1}^{\infty} m^*(A_k). \quad (7.127)$$

Union dénombrable quelconque Soit maintenant une suite $(A_n)_{n \in \mathbb{N}}$ d'éléments de $\mathcal{M}$ que nous ne supposons plus être disjoints. Nous nous ramenons au cas disjoint en posant

$$\begin{cases} B_1 = A_1 \\ B_n = A_n \cap \left(\bigcup_{k=1}^{n-1} A_k\right)^c, \end{cases} \quad (7.128a)$$

$$(7.128b)$$

c'est à dire que nous mettons dans B_n les éléments de A_n qui ne sont dans aucun des A_k précédents. Autrement dit, nous posons $B_0 = \emptyset$ et $B_n = A_n \setminus B_{n-1}$. L'ensemble $\mathcal{M}$ étant stable par réunion finie, par complément et par intersection finie nous avons $B_n \in \mathcal{M}$. De plus les B_n sont disjoints, donc

$$\bigcup_{k=1}^{\infty} A_k = \bigcup_{k=1}^{\infty} B_k \in \mathcal{M}. \quad (7.129)$$

La première égalité se justifie de la façon suivante : si $x \in \bigcup_{k=1}^{\infty} A_k$ alors nous notons n_0 le plus petit n tel que $x \in A_n$ et alors $x \in B_{n_0}$.

Espace complet Nous prouvons à présent que $(S, \mathcal{M}, m^*)$ est un espace mesuré complet. Soit N une partie m^* -négligeable de S et $Y \in \mathcal{M}$ tel que $m^*(Y) = 0$ et $N \subset Y$. D'abord $m^*(N) = 0$ parce que

$$m^*(N) \leq m^*(Y) = 0. \quad (7.130)$$

Si $X \subset S$ nous avons

$$X \cap N \subset N \Rightarrow m^*(X \cap N) = 0 \quad (7.131a)$$

$$X \cap N^c \subset X \Rightarrow m^*(X \cap N^c) \leq m^*(X). \quad (7.131b)$$

Donc

$$m^*(X \cap N) + m^*(X \cap N^c) \leq m^*(X), \quad (7.132)$$

ce qui montre que N est m^* -mesurable.

□

7.54.

Ce théorème nous pousse à adopter de la notation. Lorsqu'un espace mesuré $(S, \mathcal{F}, \mu)$ est donné, nous noterons

$$(S, \mathcal{M}, \mu^*) \quad (7.133)$$

l'espace mesuré construit de la façon suivante. D'abord μ^* est la mesure extérieure associée à μ par la proposition 7.43. Ensuite $\mathcal{M}$ est la tribu des parties μ^* -mesurables, qui est bien une tribu parce que μ^* est une mesure extérieure (7.53). La proposition (7.46) dit alors que $\mathcal{F} \subset \mathcal{M}$. De plus 7.53 nous explique que si $A \in \mathcal{F}$ alors $\mu(A) = \mu^*(A)$. Tout cela pour dire que

$$(S, \mathcal{F}, \mu) \subset (S, \mathcal{M}, \mu^*). \quad (7.134)$$

Et enfin, 7.53 nous dit que l'espace mesuré $(S, \mathcal{M}, \mu^*)$ est complet.

Exemple 7.55

Montrons un cas dans lequel $(S, \mathcal{M}, \mu^*)$ n'est pas σ -fini. Soit S un ensemble non dénombrable et $\mathcal{F}$ la tribu des parties de S qui sont soit fini ou dénombrables soit de complémentaire fini ou dénombrable. Nous y mettons la mesure

$$\mu(A) = \begin{cases} 0 & \text{si } A \text{ est au plus dénombrable} \\ \infty & \text{sinon.} \end{cases} \quad (7.135)$$

Cette mesure n'est pas σ -finie parce qu'aucune union de dénombrables est non dénombrable. De plus $(S, \mathcal{F}, \mu)$ est complet parce que toute partie contenue dans un ensemble fini ou dénombrable est fini ou dénombrable (1.12).

$\mathcal{F}$ n'est pas $\mathcal{P}(S)$ La tribu $\mathcal{F}$ est différente de $\mathcal{P}(S)$. En effet S étant infini, il existe par 1.6 une bijection $\varphi: \{1, 2\} \times S \rightarrow S$. Alors l'ensemble $\varphi(\{1\} \times S)$ est non dénombrable et son complémentaire

$$\varphi(\{1\} \times S)^c = \varphi(\{2\} \times S) \quad (7.136)$$

n'est pas dénombrable non plus. Cet ensemble n'est donc pas de $\mathcal{F}$.

$\mathcal{M}$ est $\mathcal{P}(S)$ En effet, soit $A \subset S$; il faut prouver que pour tout $X \subset S$ nous avons

$$\mu^*(X) = \mu^*(X \cap A) + \mu^*(X \cap A^c). \quad (7.137)$$

Nous prouvons cela en séparant les cas suivant que X est dénombrable ou non.

Si X est fini ou dénombrable, alors $X \cap A$ et $X \cap A^c$ le sont également et nous avons $\mu^*(X) = \mu(X) = 0$ ainsi que $\mu^*(X \cap A) = \mu^*(X \cap A^c) = 0$.

Si au contraire X n'est pas dénombrable,

$$\mu^*(X) = \inf_{\substack{A \in \mathcal{F} \\ X \subset A}} \mu(A) = \infty, \quad (7.138)$$

parce que X n'étant pas dénombrable, l'ensemble A ne l'est pas non plus et $\mu(A) = \infty$. Mais comme X n'est pas dénombrable, soit $X \cap A$ soit $X \cap A^c$ (soit les deux) n'est pas dénombrable non plus; par conséquent

$$\mu^*(X \cap A) + \mu^*(X \cap A^c) = \infty. \quad (7.139)$$

Par conséquent $(S, \mathcal{F}, \mu) \neq (S, \mathcal{M}, \mu^*)$. Mais vu que $(S, \mathcal{F}, \mu)$ est complété nous devons avoir $(S, \mathcal{F}, \mu) = (S, \hat{\mathcal{F}}, \hat{\mu})$. Tout cela pour dire que nous avons un exemple avec

$$(S, \mathcal{M}, \mu^*) \neq (S, \hat{\mathcal{F}}, \hat{\mu}). \quad (7.140)$$

△

Nous avons deux façons de créer un espace complet à partir de $(S, \mathcal{F}, \mu)$.

- (1) Partir de la mesure extérieure μ^* et construire $(S, \mathcal{M}, \mu^*)$.
- (2) Partir des ensembles μ -négligeables, construire $\hat{\mathcal{F}}$ et ensuite $(S, \hat{\mathcal{F}}, \hat{\mu})$.

Ces deux façons ne sont pas équivalentes en général comme le montre l'exemple 7.55. Mais il sera montré par la proposition 7.59 que si $(S, \mathcal{F}, \mu)$ est σ -fini alors les deux sont équivalent.

Lemme 7.56.

Soit $(S, \mathcal{F}, \mu)$ un espace mesuré. Alors pour tout $X \subset S$ tel que $\mu^*(X) < \infty$ il existe $A \in \mathcal{F}$ tel que $X \subset A$ et $\mu^*(X) = \mu(A)$.

C'est à dire que μ^* a beau être défini sur toutes les parties de S , ce qu'il faut rajouter pour être μ -mesurable, c'est pas grand chose.

Démonstration. Par définition de la mesure extérieure associée à μ en tant qu'infimum, pour tout $n \geq 1$, il existe $A_n \in \mathcal{F}$ tel que $X \subset A_n$ et $\mu(A_n) \leq \mu^*(X) + \frac{1}{2^n}$. Nous posons $A = \bigcap_{n \geq 1} A_n$ et nous vérifions que ce A fait l'affaire.

D'abord $A \in \mathcal{F}$ parce qu'une tribu est stable par union dénombrable. Ensuite pour tout $n \geq 1$ nous avons

$$\mu(A) \leq \mu(A_n) \leq \mu^*(X) + \frac{1}{2^n}, \quad (7.141)$$

et à la limite $\mu(A) \leq \mu^*(X)$. Mais $X \subset A$ implique $\mu^*(X) \leq \mu(A)$ parce que $\mu^*(X)$ l'infimum d'un ensemble contenant $\mu(A)$. $\square$

Corollaire 7.57.

Soit une mesure μ et la mesure extérieure μ^* associée⁹. Une partie N de X est négligeable si et seulement si $\mu^*(N) = 0$.

Démonstration. Si μ^* est la mesure extérieure associée à μ et si N est μ -négligeable alors $\mu^*(N) = 0$ parce que

$$\mu^*(N) \leq \mu^*(Y) = \mu(Y) = 0 \quad (7.142)$$

pour un certain Y mesurable de mesure nulle contenant N .

D'autre part si $\mu^*(N) = 0$ alors le lemme 7.56 donne une partie mesurable A telle que $N \subset A$ et $\mu(A) = 0$, c'est à dire que N est négligeable. $\square$

Lemme 7.58.

Si l'espace mesuré $(S, \mathcal{F}, \mu)$ est σ -fini alors l'espace mesuré $(S, \mathcal{M}, \mu^*)$ est également σ -fini.

Démonstration. Vu que $(S, \mathcal{F}, \mu)$ est σ -fini, nous avons une suite croissante A_n d'éléments de $\mathcal{F}$ tels que $\bigcup_n A_n = S$ et telle que $\mu(A_n) < \infty$ pour tout n . Étant donné que $\mathcal{F} \subset \mathcal{M}$, cette suite convient également pour montrer que $(S, \mathcal{M}, \mu^*)$ est σ -fini parce que $\mu^*(A_n) = \mu(A_n) < \infty$. $\square$

La proposition suivante montre que si $(S, \mathcal{F}, \mu)$ est σ -finie alors nous avons l'égalité.

Proposition 7.59.

Soit $(S, \mathcal{F}, \mu)$ un espace mesuré σ -fini, μ^* la mesure extérieure associée et $\mathcal{M}$ la tribu des ensembles μ^* -mesurables¹⁰. Alors

$$(S, \mathcal{M}, \mu^*) = (S, \hat{\mathcal{F}}, \hat{\mu}). \quad (7.143)$$

Démonstration. La proposition 7.46 indique que tous les éléments de $\mathcal{F}$ sont μ^* -mesurables, c'est à dire que $\mathcal{F} \subset \mathcal{M}$. Mais l'espace $(S, \mathcal{M}, \mu^*)$ est complet par le théorème de Carathéodory 7.53, donc par minimalité du complété (7.51(7)),

$$(S, \hat{\mathcal{F}}, \hat{\mu}) \subset (S, \mathcal{M}, \mu^*) \quad (7.144)$$

au sens où $\hat{\mathcal{F}} \subset \mathcal{M}$ et si $A \in \hat{\mathcal{F}}$ alors $\hat{\mu}(A) = \mu^*(A)$. Notons que cette inclusion est vraie même si la mesure n'est pas σ -finie.

Nous passons à l'inclusion inverse. Soit $A \in \mathcal{M}$, c'est à dire que pour tout $Y \subset S$ nous avons

$$\mu^*(Y) = \mu^*(Y \cap A) + \mu^*(Y \cap A^c). \quad (7.145)$$

Nous allons montrer que $A \in \hat{\mathcal{F}}$ en séparant les cas suivant que $\mu^*(A) = \infty$ ou non.

Si $\mu^*(A) < \infty$ Par le lemme 7.56, il existe $X \in \mathcal{F}$ tel que $A \subset X$ et $\mu^*(A) = \mu(X)$. Vu que $(S, \mathcal{F}, \mu) \subset (S, \mathcal{M}, \mu^*)$ nous avons alors

$$\mu^*(A) = \mu(X) = \mu^*(X). \quad (7.146)$$

Nous écrivons la relation (7.145) avec ce X en guise de Y , et en nous souvenant que $X \cap A = A$ et $X \cap A^c = X \setminus A$:

$$\mu^*(X) = \mu^*(A) + \mu^*(X \setminus A). \quad (7.147)$$

9. Par la proposition 7.43.

10. C'est bien une tribu par 7.53(1).

En tenant compte de (7.146) et du fait que $\mu^*(A) < \infty$, nous pouvons simplifier et trouver $\mu^*(X \setminus A) = 0$. Le lemme 7.56 nous donne alors $B \in \mathcal{F}$ tel que $X \setminus A \subset B$ et $\mu(B) = \mu^*(X \setminus A) = 0$, c'est à dire que $X \setminus A$ est μ -négligeable. Par conséquent $X \setminus A \in \hat{\mathcal{F}}$. En écrivant

$$A = X \setminus (X \setminus A), \quad (7.148)$$

nous avons écrit A comme différence de deux éléments de $\hat{\mathcal{F}}$ et nous concluons que $A \in \hat{\mathcal{F}}$.

Si $\mu^*(A) < \infty$ Le lemme 7.58 nous indique que $(S, \mathcal{M}, \mu^*)$ est σ -fini et il existe donc une suite $(S_n)_{n \geq 1}$ dans $\mathcal{M}$ telle que $\bigcup_n S_n = S$ et $\mu^*(S_n) < \infty$. L'ensemble $A \cap S_n$ est un élément de $\mathcal{M}$ vérifiant

$$\mu^*(A \cap S_n) \leq \mu^*(A) < \infty, \quad (7.149)$$

ce qui implique que $A \cap S_n \in \hat{\mathcal{F}}$ par la première partie. Maintenant $A = \bigcup_n (A \cap S_n) \in \hat{\mathcal{F}}$ par union dénombrable d'éléments de la tribu $\hat{\mathcal{F}}$. □

7.2.5 Prolongement

Théorème 7.60 (Prolongement de Hahn[119]).

Soit $\mathcal{A}$ une algèbre de parties d'un ensemble S et μ une mesure sur $(S, \mathcal{A})$. Soit $\mathcal{F} = \sigma(\mathcal{A})$ la tribu engendrée par $\mathcal{A}$. Alors

- (1) La mesure μ se prolonge en une mesure m sur $\mathcal{F}$.
- (2) Si μ est σ -finie alors le prolongement est unique et m est σ -finie.
- (3) Si μ est finie, alors m l'est aussi.

Démonstration. La proposition 7.22 nous donne une mesure extérieure μ^* sur S dont la restriction à $\mathcal{A}$ est μ . Si $\mathcal{M}$ est la tribu des parties μ^* -mesurables de S alors le théorème de Carathéodory 7.53 nous dit que $(S, \mathcal{M}, \mu^*)$ est un espace mesuré.

$\mathcal{A} \subset \mathcal{M}$ Cette partie est une adaptation de ce qui a déjà été fait dans la preuve de la proposition 7.46. Soit $A \in \mathcal{A}$ et $X \in S$; nous devons prouver la relation de la définition 7.44. Vu que μ^* est une mesure extérieure nous avons automatiquement

$$\mu^*(A) \leq \mu^*(X \cap A) + \mu^*(X \cap A^c). \quad (7.150)$$

Il reste à prouver l'inégalité inverse. Soit une suite B_k d'éléments de $\mathcal{A}$ telle que $X \subset \bigcup_k B_k$; nous avons alors

$$\mu^*(X \cap A) \leq \mu^*\left(\bigcup_{k=1}^{\infty} B_k \cap A\right) \leq \sum_{k=1}^{\infty} \mu^*(B_k \cap A) = \sum_k \mu(B_k \cap A) \quad (7.151)$$

où nous avons utilisé la définition 7.17(3) ainsi que le lemme 7.19. De la même façon,

$$\mu^*(X \cap A^c) \leq \sum_k \mu(B_k \cap A^c). \quad (7.152)$$

Mettant les deux bouts ensemble, en remarquant que $B_k \cap A \in \mathcal{A}$ et donc que $\mu^*(B_k \cap A) = \mu(B_k \cap A)$,

$$\mu^*(X \cap A) + \mu^*(X \cap A^c) \leq \sum_k \mu(B_k \cap A) + \mu(B_k \cap A^c) = \sum_k \mu(B_k). \quad (7.153)$$

La somme $\mu^*(X \cap A) + \mu^*(X \cap A^c)$ est donc inférieure à chacun des éléments de l'ensemble sur lequel on prend l'infimum pour définir ¹¹ $\mu^*(X)$, donc

$$\mu^*(X \cap A) + \mu^*(X \cap A^c) \leq \mu^*(X). \quad (7.154)$$

11. Définition 7.28.

A fortiori nous avons $\sigma(\mathcal{A}) \subset \mathcal{M}$ et donc $(S, \sigma(\mathcal{A}), \mu^*)$ est un espace mesuré. Cela prouve l'existence d'une mesure prolongeant μ à $\sigma(\mathcal{A})$.

Unicité Nous supposons à présent que μ est σ -finie. Soient m_1 et m_2 deux mesures prolongeant μ et définies sur une tribu contenant $\mathcal{A}$. Nous posons

$$\mathcal{C} = \{A \in \mathcal{A} \text{ tel que } \mu(A) < \infty\}. \quad (7.155)$$

Dans l'optique d'utiliser le théorème d'unicité des mesures 7.40, nous prouvons que $\sigma(\mathcal{A}) = \sigma(\mathcal{C})$. Vu que μ est σ -finie, il existe une suite croissante (S_n) d'éléments de $\mathcal{A}$ telle que $S = \bigcup_n S_n$ et $\mu(S_n) \in \mathcal{C}$. Alors si $A \in \mathcal{A}$ nous avons $A = \bigcup_n (A \cap S_n)$, et donc $A \in \sigma(\mathcal{C})$. Donc $\mathcal{A} \subset \sigma(\mathcal{C})$. Mais étant donné que $\mathcal{C} \subset \mathcal{A}$ nous avons aussi $\sigma(\mathcal{C}) \subset \sigma(\mathcal{A})$. Au final $\sigma(\mathcal{A}) = \sigma(\mathcal{C})$.

Les mesures m_1 et m_2 sont des mesures sur $\sigma(\mathcal{C})$ coïncidant sur $\mathcal{C}$ (parce que $\mathcal{C} \subset \mathcal{A}$). De plus la classe $\mathcal{C}$ est stable par intersection finie et contient une suite croissante dont l'union est S (parce que μ est σ -finie).

Le théorème 7.40 nous dit alors que m_1 et m_2 coïncident sur $\sigma(\mathcal{C}) = \sigma(\mathcal{A})$.

Extension finie et σ -finie Enfin si μ est σ -finie il existe $S_n \in \mathcal{A}$ avec $\mu(S_n) < \infty$ et $\bigcup_n S_n = S$.

Ces ensembles vérifient tout autant $m(S_n) = \mu(S_n) < \infty$ pour tout prolongement m de μ .

Idem si μ est finie, tout prolongement est fini.

□

Exemple 7.61([119])

Soit $\mathcal{A}$, l'algèbre de parties de $\mathbb{R}$ formée par les réunions finies d'intervalles de la forme $]-\infty, a[$, $[a, b[$ et $[b, +\infty[$ avec $-\infty < a \leq b < +\infty$. Notons que les singletons ne font pas partie de $\mathcal{A}$ parce que $[a, a[= \emptyset$. Nous posons

$$\mu(A) = \begin{cases} 0 & \text{si } A = \emptyset \\ \infty & \text{sinon.} \end{cases} \quad (7.156)$$

Cela donne une mesure (non σ -finie) sur $(\mathbb{R}, \mathcal{A})$.

Nous allons prouver que la tribu engendrée par $\mathcal{A}$ est la tribu des boréliens et que μ accepte (au moins) deux prolongements distincts à $\sigma(\mathcal{A})$.

D'abord nous avons

$$]a, b[= (-\infty, a[\cup [b, +\infty[) \cap [a, b[, \quad (7.157)$$

donc toutes les boules ouvertes appartiennent à $\sigma(\mathcal{A})$. Ces dernières comprenant une base dénombrable de la topologie de $\mathbb{R}$ (par la proposition 5.43), tous les ouverts de $\mathbb{R}$ sont dans $\sigma(\mathcal{A})$. Par conséquent $\mathcal{Bor}(\mathbb{R}) \subset (\mathbb{R}^d)$. Mais en même temps tous les éléments de $\mathcal{A}$ sont des boréliens, donc $\mathcal{Bor}(\mathbb{R}) = \sigma(\mathcal{A})$ parce que la fermeture en tant qu'algèbre de parties est plus petite que la fermeture en tant que tribu.

La mesure de comptage prolonge μ parce qu'à part l'ensemble vide, tous les éléments de $\mathcal{A}$ sont infinis. Notons que les singletons sont dans $\sigma(\mathcal{A})$, donc la mesure de comptage prend d'autres valeurs que 0 et $+\infty$.

Par ailleurs la mesure

$$\mu'(A) = \begin{cases} 0 & \text{si } A = \emptyset \\ +\infty & \text{sinon} \end{cases} \quad (7.158)$$

est également une mesure prolongeant μ à $\sigma(\mathcal{A}) = \mathcal{Bor}(\mathbb{R})$.

La mesure de comptage et μ' sont deux prolongements distincts de μ .

△

Exemple 7.62([119])

Nous montrons maintenant une mesure non σ -finie qui se prolonge en deux mesures distinctes, toutes deux σ -finies.

Nous considérons la même algèbre $\mathcal{A}$ de parties que celle donnée dans l'exemple 7.61, mais cette fois vue sur $\mathbb{Q}$ uniquement. La mesure de comptage m sur $(\mathbb{Q}, \mathcal{A})$ n'est pas σ -finie.

Vu que les singletons sont des boréliens nous avons $\sigma(\mathcal{A}) = \mathcal{P}(\mathbb{Q})$, ce qui fait que $(\mathbb{Q}, \sigma(\mathcal{A}), m)$ est un prolongement σ -fini de m . L'espace mesuré $(\mathbb{Q}, \sigma(\mathcal{A}), 2m)$ est également σ -fini et est un prolongement distinct de $(\mathbb{Q}, \mathcal{A}, m)$. $\triangle$

7.3 Applications mesurables

7.3.1 Propriétés

Définition 7.63 (Fonction mesurable).

Soit $(E, \mathcal{A})$ et $(F, \mathcal{F})$ deux espaces mesurés. Une fonction $f: E \rightarrow F$ est **mesurable** si pour tout $\mathcal{O} \in \mathcal{F}$, l'ensemble $f^{-1}(\mathcal{O})$ est dans $\mathcal{A}$.

Définition 7.64 (Fonction borélienne).

Une application $f: (\Omega, \mathcal{A}) \rightarrow (\mathbb{R}^d, \text{Bor}(\mathbb{R}^d))$ est **borélienne** si elle est mesurable, c'est à dire si pour tout $B \in \text{Bor}(\mathbb{R}^d)$ nous avons $f^{-1}(B) \in \mathcal{A}$.

Si rien n'est précisé, une application entre deux espaces topologiques est borélienne lorsqu'elle est mesurable en considérant la tribu borélienne sur les deux espace.

Si $\mathcal{A}$ est une tribu sur un ensemble E , nous notons $m(\mathcal{A})$ l'ensemble des fonctions qui sont $\mathcal{A}$ -mesurables.

Le plus souvent lorsque nous parlerons de fonctions $f: X \rightarrow Y$ où Y est un espace topologique, nous considérons la tribu borélienne sur Y . Ce sera en particulier le cas dans la théorie de l'intégration.

Remarque 7.65.

Lorsque nous considérons des fonctions à valeurs réelles $f: X \rightarrow \mathbb{R}$ nous utiliserons toujours la tribu borélienne sur $\mathbb{R}$. Pour X , cela peut dépendre des contextes. En théorie de l'intégration, nous mettrons sur X la tribu des ensembles mesurables au sens de Lebesgue sur X , tout en gardant celle des boréliens sur l'ensemble d'arrivée.

Pour toute la partie sur l'intégration, une fonction $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ sera mesurable si pour tout borélien A de $\mathbb{R}^m$ l'ensemble $f^{-1}(A)$ est Lebesgue-mesurable dans $\mathbb{R}^n$.

Étant donné qu'il est franchement difficile de créer des ensembles non mesurables au sens de Lebesgue, il est franchement difficile de créer des fonction non mesurables à valeurs réelles. L'hypothèse de mesurabilité est donc toujours satisfaite dans les cas pratiques.

Proposition 7.66.

Soient $(S_i, \mathcal{F}_i)$ ($i = 1, 2, 3$) des espaces mesurables et des fonctions mesurables $f: S_1 \rightarrow S_2$ et $g: S_2 \rightarrow S_3$. Alors la fonction $g \circ f: S_1 \rightarrow S_3$ est mesurable.

Démonstration. Soit $B \in \mathcal{F}_3$. Alors

$$(g \circ f)^{-1}(B) = f^{-1}(g^{-1}(B)) \in f^{-1}(\mathcal{F}_2) \subset \mathcal{F}_1. \quad (7.159)$$

□

7.3.2 D'une tribu à l'autre

Lemme 7.67 ([124]).

Soit une application $f: S_1 \rightarrow S_2$ et une tribu $\mathcal{F}_2$ sur S_2 . Alors $f^{-1}(\mathcal{F}_2)$ est une tribu sur S_1

Démonstration. Il faut prouver les trois propriétés de la définition 7.1 d'une tribu.

- (1) D'abord f est défini sur tout S_1 , donc $f^{-1}(S_2) = S_1$ alors que $S_2 \in \mathcal{F}_2$.

- (2) Soit $A \in f^{-1}(\mathcal{F}_2)$, c'est à dire $A = f^{-1}(B)$ pour un certain $B \in \mathcal{F}_2$. En ce qui concerne le complémentaire :

$$A^c = f^{-1}(B)^c = S_1 \setminus f^{-1}(B) = f^{-1}(S_2 \setminus B) = f^{-1}(B^c). \quad (7.160)$$

- (3) Si $(A_i)_{i \in \mathbb{N}}$ sont des éléments de $f^{-1}(\mathcal{F}_2)$ avec $A_i = f^{-1}(B_i)$ alors

$$\bigcup_i A_i = \bigcup_i f^{-1}(B_i) = f^{-1}\left(\bigcup_i B_i\right). \quad (7.161)$$

Ce qui est dans la dernière parenthèse est dans $\mathcal{F}_2$ parce que cette dernière est une tribu. $\square$

Lemme 7.68 ([124]).

Soit une application $f: S_1 \rightarrow S_2$ et $\mathcal{F}$ une tribu de S_1 . Alors

- (1) L'ensemble

$$\mathcal{F}_f = \{B \subset S_2 \text{ tel que } f^{-1}(B) \in \mathcal{F}\} \quad (7.162)$$

est une tribu sur S_2 .

- (2) C'est la plus grande tribu de S_2 pour laquelle f est mesurable.

Démonstration. Encore les trois propriétés à vérifier.

- (1) $S_2 \in \mathcal{F}$, sont $S_1 = f^{-1}(S_2) \in \mathcal{F}_f$.

- (2) Si $A \in \mathcal{F}_f$ alors $A = f^{-1}(B)$ pour un certain $B \in \mathcal{F}$. Nous avons alors aussi $B^c \in \mathcal{F}$ et donc

$$f^{-1}(B^c) = f^{-1}(B)^c = A^c. \quad (7.163)$$

Par conséquent A^c est dans $\mathcal{F}_f$.

- (3) Si (A_i) sont des éléments de $\mathcal{F}_f$ avec $A_i = f^{-1}(B_i)$ pour $B_i \in \mathcal{F}$ alors $\bigcup_i B_i \in \mathcal{F}$ et

$$f^{-1}\left(\bigcup_i B_i\right) = \bigcup_i f^{-1}(B_i) \in \mathcal{F}_f. \quad (7.164)$$

En ce qui concerne la maximalité, si $R \subset S_2$ n'est pas dans $\mathcal{F}_f$ alors $f^{-1}(R)$ n'est pas dans $\mathcal{F}$ et donc f ne serait pas mesurable. $\square$

Définition 7.69 (Tribu engendrée).

Soit une application $f: S_1 \rightarrow S_2$ et $\mathcal{F}$ une tribu de S_1 . Alors conformément au lemme 7.68 l'ensemble

$$\mathcal{F}_f = \{B \subset S_2 \text{ tel que } f^{-1}(B) \in \mathcal{F}\} \quad (7.165)$$

est la **tribu engendrée**.

Lemme 7.70 (Lemme de transfert).

Soit $f: S_1 \rightarrow S_2$ une application et une classe $\mathcal{C}$ de parties de S_2 . Alors

$$\sigma(f^{-1}(\mathcal{C})) = f^{-1}(\sigma(\mathcal{C})). \quad (7.166)$$

Démonstration. Vu que $\sigma(\mathcal{C})$ est une tribu, dans S_2 alors le lemme 7.68 dit que $f^{-1}(\sigma(\mathcal{C}))$ est une tribu qui contient en particulier $f^{-1}(\mathcal{C})$. Nous en déduisons que $\sigma(f^{-1}(\mathcal{C})) \subset f^{-1}(\sigma(\mathcal{C}))$.

Réciproquement. Dans S_1 nous avons la tribu $\sigma(f^{-1}(\mathcal{C}))$. Nous pouvons alors considérer la tribu

$$\mathcal{F}_f = \{B \subset S_2 \text{ tel que } f^{-1}(B) \in \sigma(f^{-1}(\mathcal{C}))\}. \quad (7.167)$$

Montrons que $\mathcal{C} \subset \mathcal{F}_f$. Lorsque $B \in \mathcal{C}$ nous avons $f^{-1}(B) \in f^{-1}(\mathcal{C}) \subset \sigma(f^{-1}(\mathcal{C}))$. Du coup $B \in \mathcal{F}_f$. Nous avons alors, en passant aux tribus engendrées :

$$\sigma(\mathcal{C}) \subset \sigma(\mathcal{F}_f) = \mathcal{F}_f. \quad (7.168)$$

Si maintenant $B \in \sigma(\mathcal{C})$, nous avons $f^{-1}(B) \in \sigma(f^{-1}(\mathcal{C}))$, ce qui signifie que

$$f^{-1}(\sigma(\mathcal{C})) \subset \sigma(f^{-1}(\mathcal{C})). \quad (7.169)$$

□

Le théorème suivant est important pour prouver qu'une application est mesurable. En effet, il permet de ne tester si une application est mesurable uniquement sur une partie génératrice de la tribu d'arrivée¹².

Théorème 7.71.

Soient des espaces mesurables $(S_1, \mathcal{F}_1)$ et $(S_2, \mathcal{F}_2)$ ainsi qu'une application $f: S_1 \rightarrow S_2$. Si il existe un ensemble de parties $\mathcal{C}$ de S_2 tel que

- $\sigma(\mathcal{C}) = \mathcal{F}_2$
- $f^{-1}(B) \in \mathcal{F}_1$ pour tout $B \in \mathcal{C}$

alors f est mesurable.

Démonstration. Par hypothèse, $\sigma(\mathcal{C}) = \mathcal{F}_2$ et $f^{-1}(\mathcal{C}) \subset \mathcal{F}_1$ et nous pouvons utiliser le lemme de transfert 7.70 :

$$\sigma(f^{-1}(\mathcal{C})) = f^{-1}(\sigma(\mathcal{C})) \quad (7.170)$$

qui s'écrit ici

$$\sigma(f^{-1}(\mathcal{C})) = f^{-1}(\mathcal{F}_2). \quad (7.171)$$

Mais vu que $f^{-1}(\mathcal{C}) \subset \mathcal{F}_1$, nous avons aussi $\sigma(f^{-1}(\mathcal{C})) \subset \mathcal{F}_1$, ce qui signifie que

$$f^{-1}(\mathcal{F}_2) \subset \mathcal{F}_1. \quad (7.172)$$

Cela est exactement le fait que f soit mesurable. □

Le théorème suivant est très important parce qu'en pratique c'est souvent lui, en conjonction avec la proposition 7.111 qui permet de déduire qu'une fonction est borélienne.

Théorème 7.72 ([124]).

Soient X et Y deux espaces topologiques. Alors toute application continue $f: X \rightarrow Y$ est borélienne¹³.

Démonstration. Pour vérifier que f est borélienne, nous devons prouver que $f^{-1}(B)$ est borélien pour tout borélien B de Y . Heureusement, le théorème 7.71 nous permet de limiter la vérification aux B appartenant à une classe engendrant les boréliens de Y .

La classe en question est toute trouvée : ce sont les ouverts. Si $\mathcal{O}$ est un ouvert de Y alors $f^{-1}(\mathcal{O})$ est un ouvert de X et donc un borélien de X . □

Le théorème suivant donne une importante compatibilité entre l'induction de tribu et l'induction de topologie : la tribu induite à partir des boréliens sur un sous-espace topologique est la tribu des boréliens pour la topologie induite.

Théorème 7.73 ([124]).

Soit X , un espace topologique et $Y \subset X$ une partie munie de la topologie induite. Alors

$$\mathcal{Bor}(Y) = \mathcal{Bor}(X)_Y \quad (7.173)$$

où $\mathcal{Bor}(X)_Y$ est la tribu sur Y induite de $\mathcal{Bor}(X)$ par la définition 7.7.

Démonstration. Nous notons τ_X et τ_Y les topologies de X et Y .

¹². Typiquement les ouverts pour les boréliens.

¹³. Définition 7.64.

Bor(Y) $\subset$ **Bor**(X) $_Y$ Si $A \in \tau_Y$ alors $A = Y \cap \Omega$ pour un $\Omega \in \tau_X$. Mais vu que Ω est un ouvert de X , il est un borélien de X , ce qui donne que $Y \cap \Omega$ est un élément de **Bor**(X) $_Y$. Cela prouve que $\tau_Y \subset \text{Bor}(X)_Y$, c'est à dire que **Bor**(X) $_Y$ est une tribu sur Y contenant les ouverts de Y . Nous avons donc

$$\text{Bor}(X) \subset \text{Bor}(X)_Y. \quad (7.174)$$

Réciproquement L'application $\text{Id}: (Y, \tau_Y) \rightarrow (X, \tau_X)$ est continue parce que si Ω est ouvert de X alors $\text{Id}^{-1}(\Omega) = \Omega \cap Y \in \tau_Y$. Par conséquent l'identité est une application borélienne (théorème 7.72), ce qui signifie que $\text{Id}^{-1}(\text{Bor}(X)) \subset \text{Bor}(Y)$, ou encore que si $B \in \text{Bor}(X)$, alors $\text{Id}^{-1}(B) = B \cap Y \in \text{Bor}(Y)$. Cela signifie que

$$\text{Bor}(X)_Y \subset \text{Bor}(Y). \quad (7.175)$$

□

Corollaire 7.74.

Si U est un borélien de l'espace topologique X , alors les boréliens de U sont les boréliens de X inclus à U :

$$\text{Bor}(U) = \{B \in \text{Bor}(X) \text{ tel que } B \subset U\}. \quad (7.176)$$

Démonstration. Si $B' \in \text{Bor}(U)$, le théorème 7.73 donne un borélien $B \in \text{Bor}(X)$ tel que $B' = B \cap U$. Mais U étant borélien de X , l'intersection $B \cap U$ est encore un borélien de X . □

Ce corollaire s'applique en particulier lorsque U est un ouvert.

7.3.3 Mesure image

Le produit d'une mesure par une fonction est défini par la propriété 7.137.

Proposition-définition 7.75 (Mesure image[124]).

Soient $(S_1, \mathcal{F}_1)$ et $(S_2, \mathcal{F}_2)$ des espaces mesurables. Soit $\varphi: S_1 \rightarrow S_2$ une application mesurable. Si m_1 est une mesure positive sur S_1 alors l'application définie par

$$m_2(A_2) = m_1(\varphi^{-1}(A_2)) \quad (7.177)$$

est une mesure positive sur $(S_2, \mathcal{F}_2)$.

La mesure m_2 ainsi définie est la **mesure image** de m_1 par l'application φ . Elle est notée $\varphi(m_1)$.

Démonstration. Il y a deux choses à vérifier pour avoir une mesure positive¹⁴. D'abord pour l'ensemble vide :

$$m_2(\emptyset) = m_1(\varphi^{-1}(\emptyset)) = m_1(\emptyset) = 0. \quad (7.178)$$

Ensuite pour l'additivité. Soient A_n dans $\mathcal{F}_2$ des parties deux à deux disjointes et telles que $\bigcup_n A_n \in \mathcal{F}_2$. Alors nous avons

$$m_2\left(\bigcup_n A_n\right) = m_1\left(\varphi^{-1}\left(\bigcup_n A_n\right)\right) \quad (7.179a)$$

$$= m_1\left(\bigcup_n \varphi^{-1}(A_n)\right) \quad (7.179b)$$

$$= \sum_n m_1(\varphi(A_n)) \quad (7.179c)$$

$$= \sum_n m_2(A_n). \quad (7.179d)$$

□

14. Définition 7.23

Lemme 7.76.

Soient deux espaces mesurables $(S_1, \mathcal{F}_1)$ et $(S_2, \mathcal{F}_2)$ ainsi que deux mesures μ et ν sur $(S_1, \mathcal{F}_1)$. Si $\varphi: S_1 \rightarrow S_2$ est mesurable et si $\mu \leq \nu$ alors $\varphi(\mu) \leq \varphi(\nu)$.

Démonstration. Soit B mesurable dans $(S_2, \mathcal{F}_2)$ (c'est à dire $B \in \mathcal{F}_2$). Alors

$$\varphi(\mu)(B) = \mu(\varphi^{-1}(B)) \leq \nu(\varphi^{-1}(B)) = \varphi(\nu)(B). \quad (7.180)$$

□

Il est naturel de se demander comment il faut intégrer par rapport à une mesure image. La réponse sera dans le théorème 13.55.

7.3.4 Régularité d'une mesure

Certaines mesures ont de la compatibilité avec la topologie. Nous allons étudier ça.

Théorème 7.77 ([124]).

Soit X un espace métrique et m une mesure positive bornée sur $(X, \mathcal{Bor}(X))$. Alors si B est un borélien,

- (1) Régularité extérieure : $m(B) = \inf\{m(\Omega) \text{ où } \Omega \text{ est un ouvert contenant } B\}$
- (2) Régularité intérieure : $m(B) = \sup\{m(F) \text{ où } F \text{ est un fermé, } F \subset B\}$.

Démonstration. Soit $\mathcal{F}$ l'ensemble des $B \in \mathcal{Bor}(X)$ tels que pour tout $\epsilon > 0$, il existe Ω_ϵ ouvert et F_ϵ fermé tels que $F_\epsilon \subset B \subset \Omega_\epsilon$ et $m(\Omega_\epsilon \setminus F_\epsilon) \leq \epsilon$. Nous allons montrer que cela est une tribu contenant les ouverts. Comme cela est inclus à la tribu borélienne, nous en déduirons que $\mathcal{F} = \mathcal{Bor}(X)$.

$\mathcal{F}$ contient les ouverts Soit Ω un ouvert de X . Alors Ω^c est fermé et $d(x, \Omega^c) = 0$ si et seulement si $x \in \Omega^c$ par la proposition 5.128. Nous pouvons donc écrire

$$\Omega^c = \bigcap_{n \geq 1} \{x \in X \text{ tel que } d(x, \Omega^c) < \frac{1}{n}\}. \quad (7.181)$$

En passant au complémentaire et en posant $F_n = \{x \in X \text{ tel que } d(x, \Omega^c) \geq \frac{1}{n}\}$ nous avons

$$\Omega = \bigcup_{n \geq 1} F_n. \quad (7.182)$$

Chacun des F_n est fermé parce que F_n est l'image réciproque du fermé $[\frac{1}{n}, \infty[$ par l'application $x \mapsto d(x, \Omega^c)$ qui est continue. De plus les F_n forment une suite croissante, donc le lemme 7.27 nous assure que $m(\Omega) = \lim_{n \rightarrow \infty} m(F_n)$. Et le lemme 7.26 que $m(\Omega \setminus F_n) = m(\Omega) - m(F_n)$.

Soit $\epsilon > 0$. Il existe alors $n_\epsilon \geq 1$ tel que

$$m(\Omega \setminus F_{n_\epsilon}) = m(\Omega) - m(F_{n_\epsilon}) \leq \epsilon. \quad (7.183)$$

Bref si Ω est ouvert nous considérons $\Omega_\epsilon = \Omega$ et $F_\epsilon = F_{n_\epsilon}$ et nous avons

$$F_\epsilon \subset \Omega \subset \Omega_\epsilon \quad (7.184)$$

avec $m(\Omega_\epsilon \setminus F_\epsilon) \leq \epsilon$.

L'ensemble $\mathcal{F}$ contient les ouverts.

$\mathcal{F}$ est une tribu Il y a à vérifier les trois conditions de la définition 7.1.

Les ensembles faciles Les ensembles X et $\emptyset$ sont dans $\mathcal{F}$ parce qu'ils sont ouverts et fermés.

Complémentaire Soit $B \in \mathcal{F}$, soit $\epsilon > 0$ et les ensembles F_ϵ et Ω_ϵ qui vont avec. Alors en passant au complémentaire nous avons

$$\Omega_\epsilon^c \subset B^c \subset F_\epsilon^c \quad (7.185)$$

De plus

$$F_\epsilon^c \setminus \Omega_\epsilon^c = F_\epsilon^c \cap (\Omega_\epsilon^c)^c = F_\epsilon^c \cap \Omega_\epsilon = \Omega_\epsilon \setminus F_\epsilon. \quad (7.186)$$

Par conséquent

$$m(F_\epsilon^c \setminus \Omega_\epsilon^c) = m(\Omega_\epsilon \setminus F_\epsilon) \leq \epsilon. \quad (7.187)$$

Cela montre que $B^c \in \mathcal{F}$.

Union dénombrable Soient (B_n) une suite d'éléments de $\mathcal{F}$ et $\epsilon > 0$. Pour chaque n nous choisissons un ouvert Ω_n et un fermé F_n tels que $F_n \subset B_n \subset \Omega_n$ et

$$m(\Omega_n \setminus F_n) \leq \frac{\epsilon}{2^{n+2}}. \quad (7.188)$$

Vu que $\Omega_n \setminus B_n \subset \Omega_n \setminus F_n$ nous avons aussi

$$m(\Omega_n \setminus B_n) \leq m(\Omega_n \setminus F_n) \leq \frac{\epsilon}{2^{n+2}}. \quad (7.189)$$

Nous posons $\Omega = \bigcup_{n \geq 1} \Omega_n$ (un ouvert) et $B = \bigcup_{n \geq 1} B_n$ ainsi que $A = \bigcup_{n \geq 1} F_n$ (qui n'est pas spécialement fermé).

Le but est de majorer $m(\Omega \setminus A)$ où A est un fermé qui est encore à déterminer. Calculons déjà ceci :

$$\Omega \setminus A = \bigcup_n \Omega_n \cap \left(\bigcup_k B_k \right)^c \quad (7.190a)$$

$$= \bigcup_n \left(\Omega_n \cap \left(\bigcap_k B_k^c \right) \right) \quad (7.190b)$$

$$\subset \bigcup_n (\Omega_n \cap B_n^c) \quad (7.190c)$$

$$= \bigcup_n (\Omega_n \setminus B_n) \quad (7.190d)$$

où l'union n'est pas spécialement disjointe. Par conséquent,

$$m(\Omega \setminus A) \leq \sum_{n=1}^{\infty} m(\Omega_n \setminus B_n) \leq \sum_{n=1}^{\infty} \frac{\epsilon}{2^{n+2}} = \frac{\epsilon}{4}. \quad (7.191)$$

De la même façon nous avons

$$B \setminus A = \left(\bigcup_{n=1}^{\infty} B_n \right) \cap \left(\bigcup_{k=1}^{\infty} F_k \right)^c \subset \bigcup_{n=1}^{\infty} B_n \setminus F_n. \quad (7.192)$$

Nous avons alors les inégalités de mesures

$$m(B \setminus A) \leq \sum_{n=1}^{\infty} m(B_n \setminus F_n) \quad (7.193a)$$

$$\leq \sum_{n=1}^{\infty} m(\Omega_n \setminus F_n) \quad (7.193b)$$

$$\leq \frac{\epsilon}{4}. \quad (7.193c)$$

C'est vraiment dommage que A ne soit pas en générale un fermé, sinon il répondrait à la question. Nous posons $F'_1 = F_1$ et $F'_n = \bigcup_{k=1}^n F_k$. En tant qu'unions finies de fermés,

les F'_n sont des fermés (lemme 5.2(2)). De plus la suite (F'_n) est croissante et l'union est A . Par le lemme 7.27(1) nous avons

$$m(A) = m\left(\bigcup_n F'_n\right) = \lim_{n \rightarrow \infty} m(F'_n). \quad (7.194)$$

Il existe donc n_ϵ tel que

$$m(A) - m(F'_{n_\epsilon}) \leq \epsilon \quad (7.195)$$

Nous posons $F = F'_{n_\epsilon}$. Vu que $F \subset A$ nous avons aussi $m(A \setminus F) = m(A) - m(F) \leq \epsilon$. Et en plus $F \subset A \subset B \subset \Omega$, ce qui donne bien la propriété voulue $F \subset B \subset \Omega$. Il reste à nous assurer de $m(\Omega \setminus F)$. Nous avons d'abord

$$m(B \setminus F) = m((B \setminus A) \cup (A \setminus F)) = m(B \setminus A) + m(A \setminus F) \leq \frac{5\epsilon}{4}. \quad (7.196)$$

Et enfin :

$$m(\Omega \setminus F) = m((\Omega \setminus B) \cup (B \setminus F)) = m(\Omega \setminus B) + m(B \setminus F) \leq \frac{6\epsilon}{4}. \quad (7.197)$$

Et donc à redéfinition près de ϵ c'est d'accord.

Il est donc établi que $\mathcal{F}$ est une tribu. Qui plus est, l'ensemble $\mathcal{F}$ est une tribu incluse aux boréliens et contenant les ouverts. Ergo $\mathcal{F} = \mathcal{Bor}(X)$.

Régularité extérieure Soit B un borélien et $\epsilon > 0$. Alors il existe F_ϵ fermé et Ω_ϵ ouvert tels que $F_\epsilon \subset B \subset \Omega_\epsilon$ et $m(\Omega_\epsilon \setminus F_\epsilon) \leq \epsilon$. Vu que $B \subset \Omega_\epsilon$ pour tout ϵ , nous avons aussi

$$m(B) \leq \inf_\epsilon m(\Omega_\epsilon). \quad (7.198)$$

Mais comme $\mu(\Omega_\epsilon) \geq m(B)$ pour tout ϵ , nous avons en réalité $m(B) = \inf_\epsilon m(\Omega_\epsilon)$.

Soit maintenant un ouvert Ω tel que $B \subset \Omega$. Nous devons prouver l'existence d'un $\epsilon > 0$ tel que $m(\Omega_\epsilon) \leq m(\Omega)$. Cela permettra de conclure que l'infimum sur tous les ouverts contenant B est égal à l'infimum sur les ouverts de la forme Ω_ϵ .

Nous posons $m(\Omega) = m(B) + \delta$ et avec $\epsilon \leq \delta$ nous avons

$$m(\Omega_\epsilon \setminus B) \leq m(\Omega_\epsilon \setminus F_\epsilon) \leq \epsilon \quad (7.199)$$

et donc aussi

$$m(\Omega_\epsilon) \leq m(B) + \epsilon \leq m(B) + \delta = m(\Omega). \quad (7.200)$$

Régularité intérieure Elle se fait de même.

□

Définition 7.78.

Soit X un espace topologique et m une mesure positive sur $(X, \mathcal{Bor}(X))$.

- (1) m est une **mesure de Borel** si elle est finie sur tout compact.
- (2) m est **régulière extérieurement** si $\forall B \in \mathcal{Bor}(X)$,

$$m(B) = \inf\{m(\Omega) \text{ tel que } \Omega \text{ est ouvert et } B \subset \Omega\} \quad (7.201)$$

- (3) m est **régulière intérieurement** si $\forall B \in \mathcal{Bor}(X)$,

$$m(B) = \sup\{m(K) \text{ tel que } K \text{ est compact et } K \subset B\} \quad (7.202)$$

- (4) m est une **mesure régulière** si elle est régulière dans les deux sens.

- (5) m est une **mesure de Radon** si elle est de Borel et régulière.

Proposition 7.79.

Soit X un espace localement compact et dénombrable à l'infini¹⁵ Alors toute mesure de Borel sur $(X, \mathcal{Bor}(X))$ est de Radon.

Démonstration. Nous avons une suite exhaustive¹⁶ de compacts X_k tels que

$$X = \bigcup_{k \geq 1} X_k = \bigcup_{k \geq 1} \text{Int}(X_k). \quad (7.203)$$

Régularité intérieure Soit B , un borélien de X ; nous avons $B = \bigcup_{k \geq 1} (B \cap X_k)$ et comme cette union est croissante,

$$m(B) = \lim_{k \rightarrow \infty} m(B \cap X_k) \quad (7.204)$$

par le lemme 7.27(1). Dans la suite, il va y avoir beaucoup de considérations sur les topologies induites. Nous nommons τ_k la topologie de X_k induite depuis celle de X . Il ne faudra pas confondre les expressions «un compact *de* X_k » et «un compact *dans* X_k ». La première parle d'un compact pour la topologie τ_k . La seconde parle d'un compact pour la topologie de X , inclus à X_k .

Si $a < m(B)$ alors il existe $k \geq 1$ tel que $a < m(B \cap X_k)$, c'est à dire

$$a < m(B \cap X_k) \leq m(B). \quad (7.205)$$

Mais (X_k, m) est un espace mesuré borné parce que m est de Borel et X_k est compact. Par conséquent la (restriction de la) mesure m est régulière sur l'espace mesuré $(X_k, \mathcal{Bor}(X_k))$ par le théorème 7.77. De plus l'ensemble $B \cap X_k$ est un borélien de (X_k, τ_k) parce que

$$B \cap X_k \in \mathcal{Bor}(X)_{X_k} = \mathcal{Bor}(X_k) \quad (7.206)$$

où nous avons utilisé la propriété de compatibilité entre topologie induite et tribu des borélien du théorème 7.73. Il existe donc un fermé F_ϵ de (X_k, τ_k) tel que

$$\begin{cases} F_\epsilon \subset B \cap X_k \\ m(B \cap X_k) \leq m(F_\epsilon) + \epsilon. \end{cases} \quad (7.207a)$$

$$(7.207b)$$

En mettant bout à bout les inégalités nous avons trouvé

$$a < m(B \cap X_k) \leq m(F_\epsilon) + \epsilon < m(F_\epsilon), \quad (7.208)$$

et donc en particulier $a < m(F_\epsilon)$. L'ensemble F_ϵ est en plus un compact de (X, τ_X) . En effet X_k étant fermé de (X, τ_X) , le lemme 5.66 nous dit que F_ϵ est un fermé de (X, τ_X) . Mais X_k étant compact, F_ϵ est un fermé inclus à un compact, il est donc compact (lemme 5.58).

Pour tout $a < m(B)$ nous avons trouvé un compact F_ϵ inclus à B dont la mesure est plus grande que a . Cela prouve la régularité intérieure de la mesure m .

Régularité extérieure Soit un borélien B de X . Si $m(B) = \infty$ alors tous les ouverts contenant B ont mesure infinie et $m(B)$ en est évidemment le supremum. Nous supposons donc que $m(B) < \infty$.

Nous notons τ_k la topologie induite de X sur $\text{Int}(X_k)$. Nous posons $B_k = B \cap \text{Int}(X_k)$. L'espace $(\text{Int}(X_k), m)$ est un espace mesuré borné et $B_k \in \mathcal{Bor}(\text{Int}(X_k))$. Il existe donc un ouvert Ω_k de $(\text{Int}(X_k), \tau_k)$ tel que $B_k \subset \Omega_k$ et

$$m(\Omega_k \setminus B_k) \leq \frac{\epsilon}{2^k}. \quad (7.209)$$

De plus $\text{Int}(X_k)$ est un ouvert de (X, τ_X) , donc en réalité Ω_k est un ouvert de X . Nous posons

$$\Omega = \bigcup_{k=1}^{\infty} \Omega_k \quad (7.210)$$

15. Définitions 5.12 et 5.14.

16. Définition 5.141.

qui est encore un ouvert de (X, τ_X) .

Il est temps de voir que Ω vérifie $m(\Omega \setminus B) \leq \epsilon$. Pour cela,

$$\Omega \setminus B = \left(\bigcup_k \Omega_k \right) \cap \left(\bigcup_l B_l \right)^c \quad (7.211a)$$

$$= \left(\bigcup_k \Omega_k \right) \cap \left(\bigcap_l B_l^c \right) \quad (7.211b)$$

$$\subset \bigcup_k (\Omega_k \cap B_k^c) \quad (7.211c)$$

$$= \bigcup_k (\Omega_k \setminus B_k), \quad (7.211d)$$

ce qui donne au niveau des mesures :

$$m(\Omega \setminus B) \leq \sum_{k=1}^{\infty} m(\Omega_k \setminus B_k) \leq \sum_{k=1}^{\infty} \frac{\epsilon}{2^k} = \epsilon. \quad (7.212)$$

□

Remarque 7.80.

Exprimé sur $\mathbb{R}^N$, la proposition 7.79 s'exprime en disant que toute mesure de Borel sur $\mathbb{R}^N$ est régulière. Typiquement, l'espace X dont il est question est un ouvert de $\mathbb{R}^N$.

7.3.5 Théorème de récurrence

Soit X un espace mesurable, μ une mesure finie sur X et $\phi: X \rightarrow X$ une application mesurable préservant la mesure, c'est à dire que pour tout ensemble mesurable $A \subset X$,

$$\mu(\phi^{-1}(A)) = \mu(A). \quad (7.213)$$

Si $A \subset X$ est un ensemble mesurable, un point $x \in A$ est dit **récurrent** par rapport à A si et seulement si pour tout $p \in \mathbb{N}$, il existe $k \geq p$ tel que $\phi^k(x) \in A$.

Théorème 7.81 (Théorème de récurrence de Poincaré.).

Si A est mesurable dans X , alors presque tous les points de A sont récurrents par rapport à A .

Démonstration. Soit $p \in \mathbb{N}$ et l'ensemble

$$U_p = \bigcup_{k=p}^{\infty} \phi^{-k}(A) \quad (7.214)$$

des points qui repasseront encore dans A après p itérations de ϕ . C'est un ensemble mesurable en tant que union d'ensembles mesurables (pour rappel, les tribus sont stables par union dénombrable, comme demandé à la définition 7.1), et nous avons donc

$$\mu(U_p) \leq \mu(X) < \infty. \quad (7.215)$$

De plus $U_p = \phi^{-p}(U_0)$, donc $\mu(U_p) = \mu(U_0)$. Vu que $U_p \subset U_0$, nous avons

$$\mu(U_0 \setminus U_p) = 0. \quad (7.216)$$

Étant donné que $A \subset U_0$ nous avons a fortiori que

$$\{x \in A \text{ tel que } x \notin U_p\} \subset U_0 \setminus U_p, \quad (7.217)$$

et donc

$$\mu\{x \in A \text{ tel que } x \notin U_p\} = 0. \quad (7.218)$$

Cela signifie exactement que l'ensemble des points x de A tels que aucun des $\phi^k(x)$ avec $k \geq p$ n'est dans A est de mesure nulle. □

7.4 Mesurabilité des fonctions à valeurs réelles

Nous allons parler de la mesurabilité de fonctions

$$f: (S, \mathcal{F}) \rightarrow (\bar{\mathbb{R}}, \mathcal{B}or(\bar{\mathbb{R}})) \quad (7.219)$$

où $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$.

7.4.1 Quelques mots à propos de $\bar{\mathbb{R}}$

7.82.

Nous convenons que $0 \times \pm\infty = 0$ parce que nous voulons qu'une droite (qui est un rectangle dont une mesure est 0 et l'autre ∞) soit de mesure nulle dans $\mathbb{R}^2$.

Les produits et sommes $\pm\infty \pm \pm\infty$ et $\pm\infty \times \pm\infty$ sont ceux que l'on croit. Sauf bien entendu $+\infty - \infty$ et $1/0$ qui ne sont toujours pas définis.

Définition 7.83 (Topologie sur $\bar{\mathbb{R}}$).

La topologie sur $\bar{\mathbb{R}}$ est celle sur $\mathbb{R}$ à laquelle nous ajoutons les voisinages de $\pm\infty$ de la façon suivante. Une partie V de $\bar{\mathbb{R}}$ est un voisinage de $+\infty$ si il existe $m > 0$ tel que $]m, +\infty] \subset V$.

Lemme 7.84.

L'ensemble B est un borélien de $\bar{\mathbb{R}}$ si et seulement si il existe un borélien B_0 de $\mathbb{R}$ tel que B soit B_0 ou $B_0 \cup \{-\infty\}$ ou $B_0 \cup \{-\infty\}$ ou $B_0 \cup \{+\infty, -\infty\}$.

Démonstration. Vu que la topologie usuelle sur $\mathbb{R}$ est la topologie induite de celle sur $\bar{\mathbb{R}}$, la tribu induite l'est aussi par le théorème 7.72. Donc si B est un borélien de $\bar{\mathbb{R}}$, l'ensemble $B \cap \mathbb{R}$ est un borélien de $\mathbb{R}$. $\square$

Lemme 7.85 ([124]).

Si $\mathcal{S}_0$ est l'ensemble des intervalles du type

$$]\alpha, \beta[, \quad [-\infty, \beta[, \quad]\alpha, +\infty] \quad (7.220)$$

avec $-\infty < \alpha < \beta < +\infty$ alors $\sigma(\mathcal{S}_0) = \mathcal{B}or(\bar{\mathbb{R}})$.

Démonstration. Les intervalles $]\alpha, \beta[$ engendrent la topologie de $\mathbb{R}$ ¹⁷, donc $\mathcal{B}or(\mathbb{R}) \subset \sigma(\mathcal{S}_0)$. De plus le lemme 7.3 nous autorise à dire que

$$\bigcap_{n \geq 1} [n, +\infty] = \{+\infty\} \in \sigma(\mathcal{S}_0). \quad (7.221)$$

Par conséquent tous les ensembles énumérés dans le lemme 7.84 font partie de $\sigma(\mathcal{S}_0)$. Cela implique que $\mathcal{B}or(\bar{\mathbb{R}}) \subset \sigma(\mathcal{S}_0)$.

Pour l'inclusion inverse, $\sigma(\mathcal{S}_0)$ est engendré par des parties qui font partie de $\mathcal{B}or(\bar{\mathbb{R}})$, donc $\sigma(\mathcal{S}_0) \subset \mathcal{B}or(\bar{\mathbb{R}})$. $\square$

Pour la suite nous utilisons la notation (pratique en probabilité)

$$\{f < a\} = \{x \in S \text{ tel que } f(x) < a\}. \quad (7.222)$$

7.4.2 Limite supérieure et inférieure

Définition 7.86.

Soit (a_n) une suite dans $\bar{\mathbb{R}}$. Nous définissons la **limite supérieure** et la **limite inférieure** par

$$\limsup_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} \left(\sup_{k \geq n} a_k \right) \quad (7.223)$$

et

$$\liminf_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} \left(\inf_{k \geq n} a_k \right). \quad (7.224)$$

¹⁷. Parce toutes les boules sont des intervalles de ce type et que les boules forment une base de topologie, proposition 5.43.

7.87.

En ce qui concerne les suites d'ensembles, utiles en théorie des probabilités, nous définissons de même. Si les A_n sont des parties de Ω , nous définissons la **limite supérieure** et la **limite inférieure** de la suite A_n par

$$\limsup_{n \rightarrow \infty} A_n = \bigcap_{n \geq 1} \bigcup_{k \geq n} A_k \quad (7.225)$$

et

$$\liminf_{n \rightarrow \infty} A_n = \bigcup_{n \geq 1} \bigcap_{k \geq n} A_k \quad (7.226)$$

Nous avons

$$\limsup A_n = \{\omega \in \Omega \text{ tel que } \omega \in A_n \text{ pour une infinité de } n\}. \quad (7.227)$$

Lemme 7.88.

Nous avons les formules pratiques suivantes :

$$\limsup a_n = \inf_{n \geq 1} \left(\sup_{k \geq n} a_k \right) \quad (7.228a)$$

$$\liminf a_n = \sup_{n \geq 1} \left(\inf_{k \geq n} a_k \right). \quad (7.228b)$$

Démonstration. La suite $n \mapsto \sup_{k \geq n} a_k$ est une suite décroissante, donc la limite est l'infimum. Même argument pour l'autre. $\square$

Lemme 7.89.

La suite (a_n) dans $\mathbb{R}$ converge si et seulement si

$$\limsup a_n = \liminf a_n. \quad (7.229)$$

Dans ce cas, $\lim a_n = \limsup a_n = \liminf a_n$.

Démonstration. Nous commençons par supposer que $\limsup a_n = \liminf a_n = l$, et nous prouvons que $\lim a_n$ existe et vaut l . Soit $\epsilon > 0$. Il existe N tel que si $n \geq N$ nous avons

$$\left| \sup_{k \geq n} a_k - l \right| < \epsilon \quad (7.230)$$

et

$$\left| \inf_{k \geq n} a_k - l \right| < \epsilon. \quad (7.231)$$

Pour tout $k \geq N$ nous avons alors $a_k \leq l + \epsilon$ et $a_k \geq l - \epsilon$. Cela donne $a_n \in B(l, \epsilon)$, c'est à dire $a_k \rightarrow l$ par la proposition 5.73.

Dans l'autre sens, nous supposons que $\lim_n a_n = l$ et nous prouvons que les limites supérieures et inférieures sont toutes deux égales à l . Soit $\epsilon > 0$ et N_ϵ tel que $|a_n - l| < \epsilon$ pour tout $n \geq N_\epsilon$. Si $n \geq N_\epsilon$ nous avons

$$\left| \sup_{k \geq n} a_k - l \right| \leq \epsilon \quad (7.232)$$

et donc la limite de $\sup_{k \geq n} a_k$ lorsque $n \rightarrow \infty$ est bien l . $\square$

7.4.3 Fonctions à valeurs réelles sur un espace mesurable**Théorème 7.90.**

Soit un espace mesurable $(S, \mathcal{F})$ et une fonction $f: S \rightarrow \bar{\mathbb{R}}$. Les faits suivants sont équivalents.

- (1) La fonction f est mesurable.
- (2) L'ensemble $\{f < a\}$ est dans $\mathcal{F}$ pour tout $a \in \mathbb{R}$
- (3) L'ensemble $\{f \leq a\}$ est dans $\mathcal{F}$ pour tout $a \in \mathbb{R}$

Démonstration. Plusieurs implications à prouver.

(1)⇒(2) Vu que f est mesurable et que $[-\infty, a[\in \mathcal{B}or(\bar{\mathbb{R}})$, nous avons $f^{-1}([-\infty, a[) \in \mathcal{F}$.

(2)⇒(1) Nous posons $\mathcal{A} = \{[-\infty, a[\text{ tel que } a \in \mathbb{R}\}$.

Nous avons $\mathcal{A} \subset \mathcal{S}_0$ (le $\mathcal{S}_0$ du lemme 7.85). Et de plus,

$$]\alpha, \beta[= [-\infty, \beta[\setminus [-\infty, \alpha] = [-\infty, \beta[\setminus \bigcap_{n \geq 1} [-\infty, \alpha + \frac{1}{n}[. \quad (7.233)$$

Donc $]\alpha, \beta[\in \sigma(\mathcal{A})$.

Et aussi :

$$]\alpha, +\infty[= \bar{\mathbb{R}} \setminus [-\infty, \alpha + \frac{1}{n}[, \quad (7.234)$$

ce qui donne $]\alpha, +\infty[\in \sigma(\mathcal{A})$.

Au final, $\mathcal{S}_0 \subset \sigma(\mathcal{A})$ et donc $\sigma(\mathcal{S}_0) \subset \sigma(\mathcal{A})$. Le lemme 7.85 nous dit que $\sigma(\mathcal{S}_0) = \mathcal{B}or(\bar{\mathbb{R}})$. Nous avons donc bien $\sigma(\mathcal{S}_0) = \sigma(\mathcal{A}) = \mathcal{B}or(\bar{\mathbb{R}})$.

par ailleurs, nous savons que $f^{-1}(\mathcal{A}) \subset \mathcal{F}$ parce que les éléments de $\mathcal{A}$ sont de la forme $\{f < a\}$. Cela donne $\sigma(f^{-1}(\mathcal{A})) = \mathcal{F}$. Mais $\sigma(f^{-1}(\mathcal{A}))$ peut aussi s'exprimer par le lemme de transfert 7.70 : $\sigma(f^{-1}(\mathcal{A})) = f^{-1}(\sigma(\mathcal{A}))$. En combinant les deux,

$$f^{-1}(\sigma(\mathcal{A})) = \mathcal{F}, \quad (7.235)$$

et en remplaçant $\sigma(\mathcal{A})$ par $\mathcal{B}or(\bar{\mathbb{R}})$ nous avons ce que nous voulions :

$$f^{-1}(\mathcal{B}or(\bar{\mathbb{R}})) \in \mathcal{F}, \quad (7.236)$$

ce qui signifie que f est mesurable.

(3)⇒(2) Nous avons

$$\{f < a\} = \bigcup_{n \geq 1} \{f \leq a - \frac{1}{n}\}. \quad (7.237)$$

donc cela est une union dénombrable d'éléments de $\mathcal{F}$. Donc $\{f < a\}$ est dans $\mathcal{F}$.

(1)⇒(3) Nous avons

$$\{f \leq a\} = \{f < a\} \cup f^{-1}([-\infty, a]). \quad (7.238)$$

Le premier ensemble est dans $\mathcal{F}$ par (2). Ensuite $[-\infty, a]$ est un fermé de $\bar{\mathbb{R}}$ et donc un borélien de $\bar{\mathbb{R}}$. Son image réciproque est donc un élément de $\mathcal{F}$ parce que f est mesurable. Au final nous avons bien $\{f \leq a\} \in \mathcal{F}$.

□

Lemme 7.91 ([125]).

Une fonction $f: X \rightarrow \mathbb{R}$ est mesurable si et seulement si $f^{-1}(I)$ est mesurable pour tout I de la forme $]a, \infty[$.

Démonstration. Nous devons prouver que $f^{-1}(A)$ est mesurable dans X pour tout borélien A de $\mathbb{R}$. Nous posons

$$S = \{A \subset \mathbb{R} \text{ tel que } f^{-1}(A) \text{ est mesurable dans } X\} \quad (7.239)$$

et nous prouvons que cela est une tribu. D'abord $f^{-1}(\mathbb{R}) = X$, et X est mesurable, donc $\mathbb{R} \in S$. Ensuite si $A \in S$ alors $f^{-1}(A^c) = f^{-1}(A)^c$. En tant que complémentaire d'un mesurable de X , l'ensemble $f^{-1}(A)^c$ est mesurable dans X . Et enfin si $A_n \in S$ alors $f^{-1}(\bigcup_n A_n) = \bigcup_n f^{-1}(A_n)$ qui est encore mesurable dans X en tant qu'union de mesurables.

Donc S est une tribu qui contient tous les ensembles de la forme $]a, \infty[$. Le lemme 7.10 conclut que S contient tous les boréliens de $\mathbb{R}$. □

Lemme 7.92 ([125]).

Soit $f_n: X \rightarrow \mathbb{R}$ une suite de fonctions mesurables¹⁸. Alors $\sup_n f_n$ est mesurable.

18. Ici X est un espace mesuré et $\mathbb{R}$ est muni des boréliens.

Démonstration. Nous avons

$$(\sup f_n)^{-1}(]a, \infty]) = \{x \in X \text{ tel que } (\sup f_n)(x) > a\} \quad (7.240a)$$

$$= \bigcup_n \{x \in X \text{ tel que } f_n(x) > a\} \quad (7.240b)$$

$$= \bigcup_n f_n^{-1}(]a, \infty]). \quad (7.240c)$$

Étant donné que f_n est mesurable et que $]a, \infty]$ est mesurable, chacun des $f_n^{-1}(]a, \infty])$ est mesurable dans X . Nous sommes en présence d'une union dénombrable de mesurables, donc $(\sup f_n)^{-1}(]a, \infty])$ est mesurable.

Le lemme 7.91 conclut que $\sup f_n$ est mesurable. $\square$

Proposition 7.93.

Si f_n est une suite de fonctions mesurables et positives, alors la fonction $\sum_n f_n$ est mesurable.

Démonstration. Nous considérons les fonctions $s_k(x) = \sum_{n=0}^k f_n(x)$ qui vaut éventuellement ∞ en certains points. Nous avons

$$\sum_n f_n(x) = \sup_k s_k(x), \quad (7.241)$$

donc le lemme 7.92 nous donne la mesurabilité de la somme de f_n . $\square$

Définition 7.94.

*Soit $(S, \mathcal{F})$ un espace mesurable. Une **partition mesurable dénombrable** de S est une suite $(S_n)_{n \geq 1}$ de parties de S telles que*

- (1) $S_n \in \mathcal{F}$ pour tout n ,
- (2) $S_n \cap S_k = \emptyset$ si $n \neq k$,
- (3) $S = \bigcup_{n \geq 1} S_n$.

Lemme 7.95 (Lemme de recollement).

Soit (S_n) une partition mesurable dénombrable de l'espace mesurable $(S, \mathcal{F})$. Soit $(S', \mathcal{F}')$ un autre espace mesurable et des fonctions mesurables

$$f_n: (S_n, \mathcal{F}_{S_n}) \rightarrow (S', \mathcal{F}') \quad (7.242)$$

où $\mathcal{F}_{S_n}$ est la tribu induite¹⁹. Alors la fonction

$$\begin{aligned} f: (S, \mathcal{F}) &\rightarrow (S', \mathcal{F}') \\ x &\mapsto f_n(x) \text{ si } x \in S_n \end{aligned} \quad (7.243)$$

est mesurable.

Démonstration. Soit $A' \in \mathcal{F}'$; nous devons prouver que $f^{-1}(A') \in \mathcal{F}$. Nous savons que

$$f^{-1}(A') = \bigcup_{n \geq 1} f_n^{-1}(A'), \quad (7.244)$$

qui est une union dénombrable d'éléments $f_n^{-1}(A') \in \mathcal{F}_{S_n}$.

Vu que $S_n \in \mathcal{F}$ nous avons $\mathcal{F}_{S_n} \subset \mathcal{F}$ parce qu'un élément de $\mathcal{F}_{S_n}$ est de la forme $S_n \cap B$ avec $B \in \mathcal{F}$. Du coup pour chaque n nous avons

$$f_n^{-1}(A') \in \mathcal{F}_{S_n} \subset \mathcal{F}. \quad (7.245)$$

Au final l'égalité (7.244) écrit $f^{-1}(A')$ comme une union d'éléments de $\mathcal{F}$ et est donc un élément de $\mathcal{F}$. $\square$

¹⁹. Définition 7.7.

Proposition 7.96.

Soit $(S, \mathcal{F})$ un espace mesurable et des applications mesurables $f, g: S \rightarrow \bar{\mathbb{R}}$. Alors les fonctions suivantes sont mesurables :

- (1) λf pour tout $\lambda \in \mathbb{R}$
- (2) $f + g$ si elle existe.
- (3) $1/f$ si elle existe.
- (4) fg .

Démonstration. Commençons par clarifier « si elle existe ». La fonction $f + g$ n'existe pas au point $x \in S$ si $f(x) = +\infty$ et $g(x) = -\infty$. La fonction $1/f$ n'existe pas au point $x \in S$ si $f(x) = 0$. Voir le point 7.82.

La partie où $f + g$ existe est mesurable La partie de S sur laquelle $f + g$ existe est

$$\{x \in S \text{ tel que } (f(x), g(x)) \neq (+\infty, -\infty), (f(x), g(x)) \neq (-\infty, +\infty)\}. \quad (7.246)$$

Nous avons

$$\{(f, g) = (+\infty, -\infty)\} = \{f = \infty\} \cap \{g = -\infty\} \quad (7.247)$$

qui est un ensemble mesurable parce que, par exemple,

$$\{+\infty\} = \bigcap_{n \geq 1} [n, +\infty]. \quad (7.248)$$

Le cas $(-\infty, +\infty)$ est identique, et au final la partie de S sur laquelle $f + g$ n'existe pas est mesurable. Par complémentarité la partie sur laquelle $f + g$ existe est également mesurable²⁰.

Idem pour la partie sur laquelle $1/f$ existe Idem.

Mesurabilité de λf Si $\lambda = 0$, nous avons une fonction constante dont la mesurabilité est évidente²¹. Nous supposons $\lambda > 0$. Alors

$$\{\lambda f < a\} = \{f < a/\lambda\} \in \mathcal{F}. \quad (7.249)$$

Pour $\lambda < 0$ nous avons de la même manière

$$\{\lambda f < a\} = \{f > a/\lambda\} \in \mathcal{F}. \quad (7.250)$$

Ce dernier point est suffisant pour que λf soit mesurable par la théorème 7.90(3) et par complémentarité.

Mesurabilité de $f + g$ Soit $a \in \mathbb{R}$; le théorème 7.90 nous demande d'avoir envie de prouver que $\{f + g < a\} \in \mathcal{F}$. Nous avons

$$f(x) + g(x) < a \quad (7.251)$$

si et seulement si

$$f(x) < a - g(x) \quad (7.252)$$

si et seulement si

$$\exists q \in \mathbb{Q} \text{ tel que } f(x) < q < a - g(x). \quad (7.253)$$

Donc

$$\{f + g < a\} = \bigcup_{q \in \mathbb{Q}} (\{f < q\} \cap \{g < a - r\}), \quad (7.254)$$

qui est une union dénombrable d'éléments de $\mathcal{F}$. Donc $\{f + g < a\} \in \mathcal{F}$ et $f + g$ est mesurable.

Note qu'en toute rigueur il faudrait « $\cap$ là où $f + g$ est définie» un peu partout, mais cela ne change rien parce que l'intersection de deux parties mesurables est mesurable.

20. Parfois on a envie de dire que l'affirmation « A est mesurable» ne passe pas le test de Popper.

21. Prenez quand même le temps d'y penser.

Mesurabilité de $1/f$ Soit $a \in \mathbb{R}$. Si $a > 0$ alors

$$\{1/f < a\} = \{f < 0\} \cup \{f > \frac{1}{a}\} \in \mathcal{F}. \quad (7.255)$$

et si $a < 0$ alors

$$\{1/f < a\} = \{f < 0\} \cap \{f > \frac{1}{a}\} \in \mathcal{F}. \quad (7.256)$$

Mesurabilité de fg Nous allons la prouver en plusieurs fois.

Si f est mesurable alors f^2 est mesurable Si $a \leq 0$ alors $\{f^2 < a\} = \emptyset$. Si $a > 0$ nous avons

$$\{f^2 < a\} = \{-\sqrt{a} < f < \sqrt{a}\} \in \mathcal{F}. \quad (7.257)$$

$f\mathbb{1}_A$ est mesurable Soit $A \in \mathcal{F}$, et prouvons que $f\mathbb{1}_A$ est mesurable. Par définition,

$$(f\mathbb{1}_A)(x) = \begin{cases} f(x) & \text{si } x \in A \\ 0 & \text{si } x \notin A. \end{cases} \quad (7.258)$$

Nous posons

$$\begin{aligned} f_1: A^c &\rightarrow \bar{\mathbb{R}} \\ x &\mapsto 0 \end{aligned} \quad (7.259)$$

et

$$\begin{aligned} f_2: A &\rightarrow \bar{\mathbb{R}} \\ x &\mapsto f(x). \end{aligned} \quad (7.260)$$

Alors nous avons

$$(\mathbb{1}_A f)(x) = \begin{cases} f_1(x) & \text{si } x \in A^c \\ f_2(x) & \text{si } x \in A. \end{cases} \quad (7.261)$$

Les ensembles A et A^c forment une partition mesurable dénombrable de S . La fonction f_1 est mesurable; pour prouver que f_2 est mesurable, nous l'écrivons $f_2 = f \circ j_A$ où $j_A: A \rightarrow S$ est l'injection canonique. L'application

$$j_A: (A, \mathcal{F}_A) \rightarrow (S, \mathcal{F}) \quad (7.262)$$

est mesurable parce que si $B \in \mathcal{F}$ alors $j_A^{-1}(B) = A \cap B \in \mathcal{F}_A$. D'autre part l'application

$$f: (S, \mathcal{F}) \rightarrow (\bar{\mathbb{R}}, \mathcal{B}(\bar{\mathbb{R}})) \quad (7.263)$$

est mesurable par hypothèse. La composée $f_2 = f \circ j_A$ est alors mesurable par la proposition 7.66. Le lemme de recollement 7.95 nous donne alors la mesurabilité de $f\mathbb{1}_A$.

Le produit fg est mesurable Nous posons

$$F = \{x \in S \text{ tel que } |f(x)| < +\infty, |g(x)| < \infty\}. \quad (7.264)$$

En tant qu'intersection de deux ensembles mesurables, F est mesurable. Par la partie précédente, les applications $f_1 = g\mathbb{1}_F$ et $g_1 = f\mathbb{1}_F$ sont mesurables. L'application $f_1 + g_1: S \rightarrow \bar{\mathbb{R}}$ est encore mesurable. Par conséquent l'application

$$f_1 g_1 = \frac{1}{2}((f_1 + g_1)^2 - f_1^2 - g_1^2) \quad (7.265)$$

est mesurable.

Voyons maintenant ce qui se passe en dehors de F . Nous allons utiliser le lemme de recollement sur la fonction

$$(fg)(x) = \begin{cases} (f_1 f_2)(x) & \text{si } x \in F \\ -\infty & \text{si } x \in \mathcal{U} \\ 0 & \text{si } x \in \mathcal{V} \\ +\infty & \text{si } x \in \mathcal{W} \end{cases} \quad (7.266)$$

où $F, \mathcal{U}, \mathcal{V}, \mathcal{W}$ forment une partition mesurable dénombrable²² de S . Pour le sport nous montrons que $\mathcal{U}$ est mesurable :

$$\mathcal{U} = (\{f = -\infty\} \cap \{g > 0\}) \quad (7.267a)$$

$$\cup (\{f = +\infty\} \cap \{g < 0\}) \quad (7.267b)$$

$$\cup (\{g = -\infty\} \cap \{f > 0\}) \quad (7.267c)$$

$$\cup (\{g = +\infty\} \cap \{f < 0\}). \quad (7.267d)$$

□

Proposition 7.97.

Si $f_n: S \rightarrow \bar{\mathbb{R}}$ est une suite de fonctions mesurables, alors les fonctions $\inf_n f_n$ et $\sup_n f_n$ sont mesurables.

Démonstration. Nous avons les découpages

$$\{\inf_n f_n < a\} = \bigcup_n \{f_n < a\} \in \mathcal{F} \quad (7.268)$$

et

$$\{\sup_n f_n \leq a\} = \bigcap_n \{f_n \leq a\} \in \mathcal{F}. \quad (7.269)$$

Le théorème 7.90 permet de conclure. □

Note que pour (7.269) nous ne pouvions pas utiliser les inégalités strictes parce que $\{\sup_n f_n < a\}$ n'est pas spécialement égal à $\bigcap_n \{f_n < a\}$.

7.98.

La proposition 7.97 nous permet de définir les parties positives et négatives de f par $f^+ = \sup(f, 0)$ et $f^- = \sup(-f, 0)$. Ce sont des applications mesurables. Nous avons les décompositions

$$f = f^+ - f^- \quad (7.270a)$$

$$|f| = f^+ + f^-. \quad (7.270b)$$

Corollaire 7.99.

Si $f: S \rightarrow \bar{\mathbb{R}}$ est mesurable alors les applications f^+ , f^- et $|f|$ sont mesurables en tant qu'applications $S \rightarrow \bar{\mathbb{R}}^+$.

Démonstration. Nous faisons la preuve pour f^+ . Nous savons que $f^+: S \rightarrow \bar{\mathbb{R}}$ est mesurable par la proposition 7.97. Nous considérons l'injection canonique $f: \bar{\mathbb{R}}^+ \rightarrow \bar{\mathbb{R}}$ et

$$\begin{aligned} f_1^+ : S &\rightarrow \bar{\mathbb{R}}^+ \\ x &\mapsto f^+(x). \end{aligned} \quad (7.271)$$

Alors $f_1^+ = j \circ f^+$ est mesurable. Et c'est bien cela que nous voulions. □

Note : f^+ et f_1^+ sont exactement les mêmes fonctions. Elles ne diffèrent que par la tribu que nous considérons sur l'espace d'arrivée. Nous allons à partir de maintenant les noter toutes deux f^+ .

Remarque 7.100.

L'application $|f|$ peut être mesurable sans que f le soit. Soit en effet une partie $A \notin \mathcal{F}$, et posons

$$f(x) = \begin{cases} 1 & \text{si } x \in A \\ -1 & \text{si } x \in A^c. \end{cases} \quad (7.272)$$

Alors $f^{-1}(\{1\}) = A$ n'est pas mesurable alors que $|f|(x) = 1$ pour tout x .

22. Définition 7.94.

Il est temps d'aller relire les définitions 7.86.

Proposition 7.101.

Si les fonctions $f_n: S \rightarrow \bar{\mathbb{R}}$ sont mesurables alors les fonctions $\limsup f_n$ et $\liminf f_n$ sont mesurables.

Démonstration. Par le lemme 7.88 nous écrivons $\limsup_n f_n(x) = \inf_{n \geq 1} \sup_{k \geq n} f_k(x)$. Pour chaque k nous considérons la fonction $g_k = \sup_{n \geq k} f_n$. Par la proposition 7.97, les fonctions g_k sont mesurables. En utilisant encore la même proposition, $\inf_{n \geq 1} g_k$ est encore mesurable. $\square$

Proposition 7.102 ([126]).

Si $f_n: S \rightarrow \bar{\mathbb{R}}$ est une suite de fonctions mesurables telle dont la limite ponctuelle existe, alors la limite est mesurable.

Démonstration. Si la limite existe, elle est égale à la limite supérieure par le lemme 7.89. Or la limite supérieure est mesurable par la proposition 7.101. $\square$

7.4.4 Fonction étagée

Définition 7.103 ([127]).

Soit $(S, \mathcal{F})$ un espace mesurable et une fonction $f: S \rightarrow (\bar{\mathbb{R}}, \mathcal{B}(\bar{\mathbb{R}}))$. Il serait dommage de confondre les trois concepts suivants.

- Une **fonction simple** est une fonction dont l'image est constituée d'un nombre fini de valeurs.
- Une **fonction étagée** est une fonction simple qui est elle-même une fonction mesurable.
- Une **fonction en escalier** est une fonction étagée dont les valeurs sont constantes sur des intervalles : ce sont donc des fonctions constantes par morceaux.

Dans les trois cas, la fonction f peut être écrite comme somme de fonctions caractéristiques :

$$f(x) = \sum_{j=1}^p \alpha_j \mathbb{1}_{A_j}(x) \quad (7.273)$$

où $A_j = f^{-1}(\alpha_j)$. Ce qui change est la nature des A_j .

- Si f est simple, les A_j sont quelconques.
- Si f est étagée, les A_i peuvent être choisis mesurables parce que $\{\alpha_i\}$ est un borélien, ce qui fait que $A_i = f^{-1}(\alpha_i)$ un choix mesurable.
- Si f est en escalier, les A_i sont des intervalles.

La **forme canonique** d'une fonction simple f est la suivante. Soit $\{\alpha_i\}_{i=1,\dots,l}$ les valeurs distinctes prises par f et $A_i = f^{-1}(\alpha_i)$. La forme canonique de f est alors

$$f = \sum_{i=1}^l \alpha_i \mathbb{1}_{A_i}. \quad (7.274)$$

Notons que nous avons $S = \bigcup_i A_i$, et que cette union est disjointe dans le cas d'une représentation canonique.

Problèmes et choses à faire

Le lemme 7.104 et le théorème 7.107 disent la même chose alors que la preuve du théorème 7.107 est beaucoup plus compliquée. La démonstration du lemme serait fautive ?

M'est avis que ce que le théorème donne en plus est la convergence uniforme en cas de fonction bornée. La suite (7.275) ne va pas converger uniformément.

Lemme 7.104 (Limite croissante de fonctions étagées[8]).

Soit $f: (S, \mathcal{F}) \rightarrow \bar{\mathbb{R}}$ une fonction positive mesurable. Il existe une suite $f_n: S \rightarrow \mathbb{R}$ de fonctions étagées positives telles que $f_n \rightarrow f$ ponctuellement et $f_n \leq f$.

Démonstration. Nous considérons (q_n) une suite parcourant tous les rationnels positifs²³ avec $q_0 = 0$ pour être sûr. Pour $n \in \mathbb{N}$ nous définissons la fonction

$$f_n(x) = \max\{q_i \text{ tel que } i \leq n, q_i \leq f(x)\}. \quad (7.275)$$

L'ensemble sur lequel le maximum est pris n'est pas vide parce que $q_0 = 0$. La fonction f_n est simple parce qu'elle ne prend que n valeurs différentes. Nous avons aussi par construction que $f_n(x) \leq f(x)$. Nous avons aussi pour tout $x \in S$ que $f_n(x) \rightarrow f(x)$ parce que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

En ce qui concerne le fait que f_n est mesurable, nous notons $\{r_0, \dots, r_n\}$ l'ensemble des $\{q_0, \dots, q_n\}$ classés dans l'ordre croissant. Nous posons en plus $r_{n+1} = +\infty$. Nous avons alors

$$f_n^{-1}(r_k) = \{x \in S \text{ tel que } f(x) \geq r_k, f(x) < r_{k+1}\} = \{f \geq r_k\} \cap \{f < r_{k+1}\} \quad (7.276)$$

qui est un ensemble mesurable comme intersection deux ensembles mesurables par le théorème 7.90. $\square$

Remarque 7.105.

Pour avoir $f_n < |f|$ nous pouvons poser

$$f_n(x) = \begin{cases} \max\{q_i \text{ tel que } i \leq n, q_i \leq f(x)\} & \text{si } f(x) \geq 0 \\ \min\{q_i \text{ tel que } i \leq n, q_i \geq f(x)\} & \text{si } f(x) < 0. \end{cases} \quad (7.277)$$

Proposition 7.106 ([128]).

Approximation de fonctions mesurables par des fonctions étagées.

- (1) Une fonction mesurable et positive est limite (simple) d'une suite croissante de fonctions étagées, mesurables et positives.
- (2) Si $f: \mathbb{R}^d \rightarrow \bar{\mathbb{R}}$ est mesurable, alors elle est limite (simple) de fonctions étagées f_n telles que $|f_n| \leq |f|$.

Théorème 7.107 (Théorème fondamental d'approximation[124]).

Pas à pas.

- (1) Soit une fonction mesurable $f: S \rightarrow [0, +\infty]$. Alors il existe une suite croissante de fonctions $\varphi_n: S \rightarrow [0, +\infty[$ étagées positives dont la limite ponctuelle est f .
- (2) Si de plus f est bornée, la convergence est uniforme.
- (3) Idem pour f à valeurs dans $\bar{\mathbb{R}}$ ou $\mathbb{C}$.

Démonstration. Nous découpons l'intervalle $[0, n]$ en plusieurs morceaux.

$$I_{n,k} = \begin{cases} [\frac{k}{2^n}, \frac{k+1}{2^n}[& \text{si } 0 \leq k \leq n2^n - 1 \\ [n, \infty] & \text{si } k = n2^n. \end{cases} \quad (7.278)$$

Nous posons $S_{n,k} = f^{-1}(I_{n,k})$. Ce sont des ensembles mesurables parce que f est mesurable. Et de plus pour chaque n , la suite $(S_{n,k})_{k \geq 0}$ est une partition mesurable finie de S . Nous posons

$$\varphi_n = \sum_{k=0}^{n2^n} \frac{k}{2^n} \mathbb{1}_{S_{n,k}}. \quad (7.279)$$

C'est à dire que sur chaque $S_{n,k}$ nous approximons f par le bas. La fonction φ_n est étagée et positive : $0 \leq \varphi_n(x) \leq f(x)$ par construction.

Croissance Nous allons voir que $\varphi_n \leq \varphi_{n+1}$. Soit $k \neq n2^n$. Si $x \in S_{n,k}$ alors $\varphi_n(x) = \frac{k}{2^n}$ et nous avons aussi la décomposition

$$S_{n,k} = S_{n+1,2k} \cup S_{n+1,2k+1}. \quad (7.280)$$

23. Nous rappelons que $\mathbb{Q}$ est dénombrable et dense dans $\mathbb{R}$ par la proposition 5.41.

Si $x \in S_{n+1,2k}$ alors $\varphi_{n+1}(x) = \frac{2k}{2^{n+1}} = \frac{k}{2^n} = \varphi_n(x)$. Et si $x \in S_{n+1,2k+1}$ alors

$$\varphi_{n+1}(x) = \frac{2k+1}{2^{n+1}} = \frac{k+\frac{1}{2}}{2^n} > \varphi_n(x). \quad (7.281)$$

Il reste à traiter le cas $x \in \{f \geq n\}$. Dans ce cas nous avons $\varphi_n(x) = n$. il y a encore deux cas à traiter :

$$\{f \geq n\} = \{f \in [n, n+1[\} \cup \{f \in [n+1, \infty[\}. \quad (7.282)$$

Pour plus de simplicité dans les notations, nous notons $\bar{n} = n2^n$, c'est à dire que $I_{n,\bar{n}}$ est le $I_{n,k}$ avec le k le plus grand possible. Nous avons

$$I_{n,\bar{n}} = [n, n+1[\cup [n+1, \infty[. \quad (7.283)$$

Le premier élément se décompose en $I_{n+1,k}$ avec $k < n+1$ (nous préciserons plus tard exactement les valeurs de k) tandis que le second est $[n+1, \infty[= I_{n+1,\bar{n}+1}$.

Pour $x \in S_{n+1,\bar{n}+1}$ nous avons

$$\varphi_{n+1}(x) = \frac{(n+1)2^{n+1}}{2^{n+1}} = n+1 > \varphi_n(x). \quad (7.284)$$

Si au contraire $f(x) \in [n, n+1[$ nous devons précisément voir quels sont les k qui font en sorte que $I_{n+1,k}$ recouvre $[n, n+1[$. Le plus petit k est donné par $\frac{k}{2^{n+1}} = n$, c'est à dire $k = n2^{n+1}$ et le plus grand k est donné par $\frac{k}{2^{n+1}} < n+1$, c'est à dire $k = 2^{n+1}(n+1) - 1$. Donc si $f(x) \in [n, n+1[$ alors $x \in S_{n+1,k}$ avec

$$n2^{n+1} \leq k \leq (n+1)2^{n+1} - 1 \quad (7.285)$$

Dans ce cas

$$\varphi_{n+1}(x) = \frac{k}{2^{n+1}} \geq \frac{n2^{n+1}}{2^{n+1}} = n = \varphi_n(x). \quad (7.286)$$

Convergence ponctuelle Si $f(x) < \infty$ alors il existe²⁴ $n_0 \in \mathbb{N}$ tel que $f(x) < n_0$. Pour $bn \geq n_0$ nous avons $f(x) < n$ et donc $\varphi_n(x)$ se calcule à partir d'un des intervalles de taille $1/2^n$:

$$\varphi_n(x) = \frac{k}{2^n} \leq f(x) < \frac{k+1}{2^n}. \quad (7.287)$$

Donc

$$|\varphi_n(x) - f(x)| \leq \frac{1}{2^n}, \quad (7.288)$$

ce qui signifie que $\lim_{n \rightarrow \infty} \varphi_n(x) = f(x)$.

Si $f(x) = +\infty$ alors $f(x) > n$ pour tout n . Et alors $\varphi_n(x) = n$ pour tout n , ce qui donne bien $\varphi_n(x) \rightarrow \infty$.

Convergence uniforme Soit f bornée : $0 \leq f(x) < M$ pour tout $x \in S$. Soit aussi $\epsilon > 0$. Nous prenons $n_0 > M$ tel que $\frac{1}{2^{n_0}} < \epsilon$. Alors pour tout $n \geq n_0$ nous avons

$$0 \leq f(x) - \varphi_n(x) \leq \frac{1}{2^n} \leq \frac{1}{2^{n_0}} \leq \epsilon. \quad (7.289)$$

Note qu'il n'y a pas de valeurs absolues parce que nous savons déjà que la limite est croissante.

□

24. Le vrai snob citera ici le lemme 1.38.

7.4.5 Fonctions réelle à variables réelles

Nous nous particularisons à présent au cas de fonctions

$$f: (\mathbb{R}, \mathcal{B}(\mathbb{R})) \rightarrow (\bar{\mathbb{R}}, \mathcal{B}(\bar{\mathbb{R}})). \quad (7.290)$$

Remarque 7.108.

En théorie de l'intégration il se parle souvent de fonctions mesurables au sens de la tribu de Lebesgue : $f: (\mathbb{R}, \mathcal{L}(\mathbb{R})) \rightarrow (\bar{\mathbb{R}}, \mathcal{B}(\bar{\mathbb{R}}))$ où $\mathcal{L}(\mathbb{R})$ est la tribu de Lebesgue sur $\mathbb{R}$, c'est à dire la tribu complétée de celle des boréliens (définition 7.160).

Le fait est qu'en pratique, c'est déjà assez compliqué de construire des fonctions non mesurables au sens des boréliens ; alors on va s'en contenter. Mais construire des fonctions non mesurables au sens de la tribu de Lebesgue, c'est encore plus compliqué.

Nous allons donc nous contenter de donner des conditions assurant qu'une fonction $f: (\mathbb{R}, \mathcal{B}(\mathbb{R})) \rightarrow (\bar{\mathbb{R}}, \mathcal{B}(\bar{\mathbb{R}}))$ soit mesurable. Ces fonctions seront a fortiori mesurables en les considérant comme fonctions $f: (\mathbb{R}, \mathcal{L}(\mathbb{R})) \rightarrow (\bar{\mathbb{R}}, \mathcal{B}(\bar{\mathbb{R}}))$.

Corollaire 7.109.

Si I est un intervalle de $\mathbb{R}$, alors toute application monotone $f: I \rightarrow \mathbb{R}$ est borélienne.

Démonstration. Vu que f est monotone, l'ensemble $\{f < a\}$ est un intervalle. Or tous les intervalles sont boréliens, donc f est mesurable par le théorème 7.90. $\square$

Définition 7.110.

Si I est un intervalle de $\mathbb{R}$, une fonction $f: I \rightarrow \mathbb{R}$ a une propriété (monotone, mesurable, continue, etc.) **par morceaux** si il existe une suite strictement croissante de points $(x_i)_{i \in \mathbb{Z}}$ dans I telle que f ait la propriété sur chacun des ouverts $]x_j, x_{j+1}[$.

Dans cette définition, les points sont labellés par $\mathbb{Z}$ et non par $\mathbb{N}$ parce que nous nous laissons la liberté d'avoir une infinité de points de chacun des deux côtés.

Proposition 7.111.

Soit I un intervalle de $\mathbb{R}$ et une fonction $f: I \rightarrow \mathbb{R}$. Si f est continue ou monotone par morceaux sur I alors elle y est borélienne.

Démonstration. L'ensemble $\{]x_j, x_{j+1}[\}_{j \in \mathbb{Z}} \cup \{x_i\}_{i \in \mathbb{Z}}$ forme une partition mesurable dénombrable de I (les singletons sont des boréliens). À une belle redéfinition près de la numérotation (deux fois $\mathbb{Z}$ va dans $\mathbb{N}$), nous les appelons $(I_n)_{n \in \mathbb{N}}$, et nous définissons les fonctions f_n comme étant les restrictions de f aux intervalles I_k .

Toute fonctions sur un singleton est mesurable. Toute fonctions continue sur un ouvert est mesurable (théorème 7.72). Toute fonction monotone sur un ouvert est mesurable (corollaire 7.109).

Le lemme de recollement 7.95 donne alors la mesurabilité de f . $\square$

7.112.

Toutes les fonctions que nous pouvons écrire explicitement sont mesurables ... en tout cas toutes celles que l'on trouve en pratique. En effet nous avons déjà toutes les fonctions continues par morceaux via la proposition 7.111 et ensuite toutes les limites par la proposition 7.102. Cela donne les séries, les dérivées, les primitives, etc.

7.5 Intégrale par rapport à une mesure

Nous avons besoin d'un peu de théorie de l'intégration parce que la définition de la mesure sur un espace mesurable²⁵ produit passe par une intégrale.

Une mesure μ sur un espace mesurable $(\Omega, \mathcal{A})$ permet de définir une fonctionnelle linéaire sur l'ensemble des fonctions mesurables $\Omega \rightarrow \mathbb{R}$. Cette fonctionnelle linéaire est l'intégrale que nous allons définir à présent.

25. Théorème 7.148.

Définition 7.113.

Soit $(\Omega, \mathcal{A}, \mu)$ un espace mesuré. Si $Y \in \mathcal{A}$ et si f est une fonction étagée²⁶, si sa forme canonique est $f = \sum_{i=1}^n \alpha_i \mathbb{1}_{A_i}$ alors nous définissons

$$\int_Y f d\mu = \sum_i \alpha_i \mu(Y \cap A_i). \quad (7.291)$$

Pour une fonction $\mathcal{A}$ -mesurable générale $f: \Omega \rightarrow [0, \infty]$ nous définissons l'intégrale de f sur Y par

$$\int_Y f d\mu = \sup \left\{ \int_Y h d\mu \text{ où } h \text{ est une fonction étagée telle que } 0 \leq h \leq f \right\}. \quad (7.292)$$

Si f est mesurable à valeurs dans $\bar{\mathbb{R}}$ ou $\mathbb{C}$, l'intégrale se définit séparément pour les parties positives, négatives, réelles et imaginaires.

Remarque 7.114.

Toute fonction mesurable à valeurs dans $\bar{\mathbb{R}}$ est intégrable (l'intégrale vaut éventuellement $+\infty$). Au moment où une fonction commence à prendre des valeurs positives et négatives, nous demandons à pouvoir intégrer séparément les parties positive et négative. C'est pour cela que nous disons qu'une fonction f à valeurs dans $\mathbb{R}$ est intégrable si $|f|$ l'est.

Cela est indépendant du fait que $\int_0^\infty f$ en tant que limite de $\int_0^M f$ peut très bien exister grâce à des compensations, alors que $\int_{[0, \infty[} |f|$ n'existe pas.

Lemme 7.115.

Si $(\Omega, \mathcal{A}, \mu)$ est un espace mesuré et si $B \in \mathcal{A}$ alors

$$\mu(B) = \int_B 1 d\mu = \int_\Omega \mathbb{1}_B. \quad (7.293)$$

Démonstration. La fonction caractéristique d'une partie mesurable est une fonction étagée dont la forme canonique est $\mathbb{1}_B = 1 \cdot \mathbb{1}_B + 0 \cdot \mathbb{1}_{B^c}$. Son intégrale est donc

$$\int \mathbb{1}_B d\mu = 1 \times \mu(B) + 0 \times \mu(B^c) = \mu(B) \quad (7.294)$$

parce que $0 \times \mu(B^c) = 0$, même si $\mu(B^c) = \infty$, comme nous l'avons convenu en 7.82. $\square$

Définition 7.116.

Une fonction $f: \Omega \rightarrow \mathbb{R}$ est dite **intégrable** au sens de Lebesgue si $\int_\Omega |f| < \infty$. Dans ce cas nous définissons

$$\int_\Omega f = \int_\Omega f^+ - \int_\Omega f^- \quad (7.295)$$

où f^+ et f^- sont les parties positives et négatives de f ; les deux intégrales à droite dans (7.295) sont finies dès que f est intégrable.

Nous verrons comment donner un sens à $\int_\Omega f$ dans certains cas où f n'est pas intégrable sur Ω dans la section 13.5.2 sur les intégrales impropres.

Nous définissons aussi

$$\mu(f) = \int_\Omega f \quad (7.296)$$

si f est une fonction mesurable sur Ω .

Remarque 7.117.

Dans $\mathbb{R}^d$, quasiment toutes les fonctions et ensembles sont mesurables. En effet la construction d'ensembles non mesurables demande obligatoirement l'utilisation de l'axiome du choix; de tels ensembles doivent être construits «exprès pour». Il y a très peu de chances pour que vous tombiez sur un ensemble non mesurable de $\mathbb{R}^d$ sans que vous ne vous en rendiez compte.

²⁶. Définition 7.103.

Remarque 7.118.

«Mesurable» ne signifie pas «intégrable». Par exemple la fonction

$$f: \mathbb{R} \rightarrow \bar{\mathbb{R}} \\ \omega \mapsto \begin{cases} \frac{1}{\omega} & \text{si } \omega \neq 0 \\ \infty & \omega = 0. \end{cases} \quad (7.297)$$

est mesurable, mais non intégrable.

7.5.1 Quelques propriétés**Théorème 7.119** ([119]).

Soient f, g des fonctions étagées positives sur $(S, \mathcal{F}, \mu)$. Alors si $\alpha \in [0, \infty]$ nous avons

(1)

$$\int_S (\alpha f) d\mu = \alpha \int_S f d\mu. \quad (7.298)$$

(2)

$$\int_S (f + g) d\mu = \int_S f d\mu + \int_S g d\mu. \quad (7.299)$$

(3) Si $a_k \in \mathbb{R}^+$ et si les f_k sont étagées positives,

$$\int_S \left(\sum_{k=1}^n a_k f_k \right) = \sum_{k=1}^n a_k \left(\int_S f_k d\mu \right). \quad (7.300)$$

Démonstration. En ce qui concerne le produit par un nombre, tout repose sur le fait que

$$(\alpha f)^{-1}(\alpha a_i) = f^{-1}(a_i), \quad (7.301)$$

ce qui fait que si la représentation canonique de f est $f = \sum_i a_i \mathbb{1}_{A_i}$ alors la représentation canonique de αf est $\alpha f = \sum_i (\alpha a_i) \mathbb{1}_{A_i}$. Donc

$$\int_S \alpha f d\mu = \sum_i \alpha a_i \mu(A_i) = \alpha \sum_i a_i \mu(A_i) = \alpha \int_S f d\mu. \quad (7.302)$$

Pour la somme c'est plus lourd. Soient les formes canoniques

$$f = \sum_i a_i \mathbb{1}_{A_i} \quad (7.303a)$$

$$g = \sum_j b_j \mathbb{1}_{B_j}. \quad (7.303b)$$

Vu que l'union des B_j est S nous avons l'union disjointe $A_i = \bigcup_j A_i \cap B_j$ et donc $\mu(A_i) = \sum_j \mu(A_i \cap B_j)$. Nous avons donc pour les intégrales :

$$\int_S f d\mu = \sum_i a_i \sum_j \mu(A_i \cap B_j) \quad (7.304a)$$

$$\int_S g d\mu = \sum_j b_j \sum_i \mu(B_j \cap A_i). \quad (7.304b)$$

Pour la somme :

$$\int_S f d\mu + \int_S g d\mu = \sum_{k,l} (a_k + b_l) \mu(A_k \cap B_l). \quad (7.305)$$

Nous devons maintenant évaluer $\int_S (f + g) d\mu$. Pour cela nous remarquons que si $c \in (f + g)(S)$ (l'ensemble des valeurs atteintes par $f + g$), alors nous notons

$$I_c = \{(k, l) \text{ tel que } a_k + b_l = c\} \quad (7.306)$$

et nous avons

$$\{f + g = c\} = \bigcup_{(k,l) \in I_c} (A_k \cap B_l), \quad (7.307)$$

et comme cette union est disjointe, nous pouvons faire la somme des mesures :

$$\mu(f + g = c) = \sum_{(k,l) \in I_c} \mu(A_k \cap B_l). \quad (7.308)$$

Cela nous permet de faire le calcul suivant :

$$\int_S (f + g) d\mu = \sum_{c \in (f+g)(S)} c \mu(f + g = c) \quad (7.309a)$$

$$= \sum_{c \in (f+g)(S)} c \sum_{(k,l) \in I_c} \mu(A_k \cap B_l) \quad (7.309b)$$

$$= \sum_{c \in (f+g)(S)} \sum_{(k,l) \in I_c} (a_k + b_l) \mu(A_k \cap B_l) \quad (7.309c)$$

Dans cette double somme, tous les couples (k, l) sont tirés une et une seule fois parce qu'ils sont tous dans un et un seul des I_c , donc

$$\int_S (f + g) d\mu = \sum_{c \in (f+g)(S)} \sum_{(k,l) \in I_c} (a_k + b_l) \mu(A_k \cap B_l) \quad (7.310a)$$

$$= \sum_{(k,l)} (a_k + b_l) \mu(A_k \cap B_l) \quad (7.310b)$$

$$= \int_S f d\mu + \int_S g d\mu. \quad (7.310c)$$

□

Remarque 7.120.

Si $f = \sum_k a_k \mathbb{1}_{A_k}$ n'est pas une décomposition canonique, il n'en reste pas moins que chacun des $\mathbb{1}_{A_k}$ est la forme canonique de lui-même. Donc le théorème 7.119 s'applique et nous avons quand même

$$\int_S f d\mu = \sum_k a_k \mu(A_k). \quad (7.311)$$

Proposition 7.121.

Si f, g sont des fonctions étagées et si $A, B \subset S$ sont disjoints, alors

$$(1) \int_A f d\mu = \int_S f \mathbb{1}_A d\mu$$

$$(2) \int_{A \cup B} f d\mu = \int_A f d\mu + \int_B f d\mu.$$

Démonstration. Si $f = \sum_k a_k \mathbb{1}_{B_k}$ alors d'une part

$$\int_A f d\mu = \sum_k a_k \mu(B_k \cap A) \quad (7.312)$$

et d'autre part,

$$f \mathbb{1}_A = \sum_k a_k \mathbb{1}_A \mathbb{1}_{B_k} = \sum_k a_k \mathbb{1}_{B_k \cap A}, \quad (7.313)$$

ce qui donne

$$\int f \mathbb{1}_A d\mu = \sum_k a_k \mu(B_k \cap A). \quad (7.314)$$

En ce qui concerne la seconde égalité à prouver, tout repose sur le fait que $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B$. Du coup nous avons, en utilisant le théorème 7.119 :

$$\int_{A \cup B} f d\mu = \int_S f \mathbb{1}_{A \cup B} d\mu \quad (7.315a)$$

$$= \int_S f(\mathbb{1}_A + \mathbb{1}_B) d\mu \quad (7.315b)$$

$$= \int_S f \mathbb{1}_A + \int_S f \mathbb{1}_B \quad (7.315c)$$

$$= \int_A f + \int_B f. \quad (7.315d)$$

□

Proposition 7.122.

Si $A, B \subset \Omega$ sont des ensembles disjoints et si f est intégrable sur $A \cup B$ alors

$$\int_{A \cup B} f = \int_A f + \int_B f. \quad (7.316)$$

Le lemme suivant nous aide à détecter des fonctions presque partout nulles.

Lemme 7.123.

Soit f une fonction mesurable positive ou nulle telle que

$$\int_{\Omega} f d\mu = 0. \quad (7.317)$$

Alors $f = 0$ μ -presque partout.

Démonstration. L'ensemble des points $x \in \Omega$ tels que $f(x) \neq 0$ peut s'écrire comme une union dénombrable disjointe :

$$\{x \in \Omega \text{ tel que } f(x) \neq 0\} = \bigcup_{i=0}^{\infty} E_i \quad (7.318)$$

avec

$$E_0 = \{x \in \Omega \text{ tel que } f(x) > 1\} \quad (7.319a)$$

$$E_i = \{x \in \Omega \text{ tel que } \frac{1}{i+1} \leq f(x) < \frac{1}{i}\}. \quad (7.319b)$$

Si un des ensembles E_i est de mesure non nulle, alors nous pouvons considérer la fonction simple $h(x) = \frac{1}{i+1} \mathbb{1}_{E_i}$ dont l'intégrale sur Ω est strictement positive. Par conséquent le supremum de la définition (7.292) est strictement positif.

Nous savons donc que $\mu(E_i) = 0$ pour tout i . Étant donné que la mesure d'une union disjointe dénombrable est égale à la somme des mesures, nous avons

$$\mu\{x \in \Omega \text{ tel que } f(x) \neq 0\} = 0, \quad (7.320)$$

ce qui signifie que f est nulle μ -presque partout. □

Corollaire 7.124.

Soit f une fonction mesurable sur l'espace mesuré $(\Omega, \mathcal{A}, \mu)$ telle que

$$\int_{\Omega} f \mathbb{1}_{f>0} d\mu = 0. \quad (7.321)$$

Alors $f \leq 0$ presque partout.

Démonstration. Nous avons l'égalité d'ensembles

$$\{f \mathbb{1}_{f>0} \neq 0\} = \{\mathbb{1}_{f>0} \neq 0\}. \quad (7.322)$$

Mais lemme 7.123 implique que $f \mathbb{1}_{f>0}$ est nulle presque partout, c'est à dire que la mesure de l'ensemble du membre de gauche est nulle par conséquent

$$\mu\{\mathbb{1}_{f>0} \neq 0\} = 0. \quad (7.323)$$

Cela signifie que la fonction f est presque partout négative ou nulle. $\square$

Lemme 7.125.

Soit f une fonction telle que $|f(x)| \leq g(x)$ pour tout $x \in \Omega$. Si g est intégrable, alors f est intégrable.

Démonstration. Nous décomposons f en parties positives et négatives :

$$A_+ = \{x \in \Omega \text{ tel que } f(x) > 0\} \quad (7.324a)$$

$$A_- = \{x \in \Omega \text{ tel que } f(x) < 0\}. \quad (7.324b)$$

Nous posons $f_+(x) = f(x) \mathbb{1}_{A_+}$ et $f_-(x) = f(x) \mathbb{1}_{A_-}$. Nous avons $f = f_+ - f_-$ et

$$\int_{\Omega} f = \int_{A_+} f + \int_{A_-} f \quad (7.325)$$

parce que $\Omega = A_+ \cup A_- \cup \{x \in \Omega \text{ tel que } f(x) = 0\}$. Si φ est une fonction simple qui majore f_+ nous avons

$$\varphi(x) = \sum_k a_k \mathbb{1}_{E_k}(x) \leq f(x) \mathbb{1}_{A_+}(x) \leq g(x). \quad (7.326)$$

Par conséquent le supremum qui définit $\int f_+$ est inférieur au supremum qui définit $\int g$. La fonction f_+ est donc intégrable. La même chose est valable pour la fonction f_- . $\square$

7.5.2 Permuter limite et intégrale

7.5.2.1 Convergence uniforme

Proposition 7.126 (Permuter limite et intégrale).

Soit $f_n \rightarrow f$ uniformément sur un ensemble mesuré A de mesure finie. Alors si les fonctions f_n et f sont intégrables sur A , nous avons

$$\lim_{n \rightarrow \infty} \int_A f_n = \int_A \lim_{n \rightarrow \infty} f_n. \quad (7.327)$$

Démonstration. Notons f la limite de la suite (f_n) . Pour tout n nous avons les majorations

$$\left| \int_A f_n d\mu - \int_A f d\mu \right| \leq \int_A |f_n - f| d\mu \quad (7.328a)$$

$$\leq \int_A \|f_n - f\|_{\infty} d\mu \quad (7.328b)$$

$$= \mu(A) \|f_n - f\|_{\infty} \quad (7.328c)$$

où $\mu(A)$ est la mesure de A . Le résultat découle maintenant du fait que $\|f_n - f\|_{\infty} \rightarrow 0$. $\square$

Il existe un résultat considérablement plus intéressant que cette proposition. En effet, l'intégrabilité de f n'est pas nécessaire. Cette hypothèse peut être remplacée soit par l'uniforme convergence de la suite (théorème 7.127), soit par le fait que les normes des f_n sont uniformément bornées (théorème de la convergence dominée de Lebesgue 7.134).

Théorème 7.127 ([129]).

La limite uniforme d'une suite de fonctions intégrables sur un borné est intégrable, et on peut permuter la limite et l'intégrale.

Plus précisément, soit A un ensemble de μ -mesure finie et $f_n: A \rightarrow \mathbb{R}$ des fonctions intégrables sur A . Si la limite $f_n \rightarrow f$ est uniforme, alors f est intégrable sur A et nous pouvons inverser la limite et l'intégrale :

$$\lim_{n \rightarrow \infty} \int_A f_n = \int_A \lim_{n \rightarrow \infty} f_n. \quad (7.329)$$

Démonstration. Soit $\epsilon > 0$ et n tel que $\|f_n - f\|_\infty \leq \epsilon$ (ici la norme uniforme est prise sur A). Étant donné que f_n est intégrable sur A , il existe une fonction simple φ_n qui minore f_n telle que

$$\left| \int_A \varphi_n - \int_A f_n \right| < \epsilon. \quad (7.330)$$

La fonction $\varphi_n + \epsilon$ est une fonction simple qui majore la fonction f . Si ψ est une fonction simple qui minore f , alors

$$\int_A \psi \leq \int_A \varphi_n + \epsilon \leq \int_A f_n + \epsilon \mu(A). \quad (7.331)$$

Par conséquent le supremum qui définit $\int_A f$ existe, ce qui montre que f est intégrable. Le fait qu'on puisse inverser la limite et l'intégrale est maintenant une conséquence de la proposition 7.126. $\square$

Remarque 7.128.

L'hypothèse sur le fait que A soit de mesure finie est importante. Il n'est pas vrai qu'une suite uniformément convergente de fonctions intégrables est intégrables. En effet nous avons par exemple la suite

$$f_n(x) = \begin{cases} 1/x & \text{si } x < n \\ 0 & \text{sinon} \end{cases} \quad (7.332)$$

qui converge uniformément vers $f(x) = 1/x$ sur $A = [1, \infty[$. Le limite n'est cependant guerre intégrable sur A .

7.5.2.2 Convergence monotone**Théorème 7.129** (Théorème de la convergence monotone ou de Beppo-Levi[130]).

Soit un espace mesuré $(\Omega, \mathcal{A}, \mu)$ et (f_n) une suite croissante de fonctions mesurables à valeurs dans $[0, \infty]$. Alors la limite ponctuelle $\lim_{n \rightarrow \infty} f_n$ existe, est mesurable et

$$\lim_{n \rightarrow \infty} \int_\Omega f_n d\mu = \int_\Omega \lim_{n \rightarrow \infty} f_n d\mu, \quad (7.333)$$

cette intégrable valant éventuellement ∞ .

Démonstration. La limite ponctuelle de la suite est la fonction à valeurs dans $[0, \infty]$ donnée par

$$f(x) = \lim_{n \rightarrow \infty} f_n(x). \quad (7.334)$$

Ces limites existent parce que pour chaque x la suite $f_n(x)$ est une suite numérique croissante. Nous notons

$$I_0 = \int_\Omega f d\mu. \quad (7.335)$$

Nous posons par ailleurs

$$I_n = \int_\Omega f_n. \quad (7.336)$$

Cela est une suite numérique croissante qui a par conséquent une limite que nous notons $I = \lim_{n \rightarrow \infty} I_n$. Notre objectif est de montrer que $I = I_0$. D'abord par croissance de la suite, pour tous n nous avons $I_n \leq I_0$, par conséquent $I \leq I_0$.

Nous prouvons maintenant l'inégalité dans l'autre sens en nous servant de la définition (7.292). Soit une fonction simple h telle que $h \leq f$, et une constante $0 < C < 1$. Nous considérons les ensembles

$$E_n = \{x \in \Omega \text{ tel que } f_n(x) \geq Ch(x)\}. \quad (7.337)$$

Ces ensembles vérifient les propriétés $E_n \subset E_{n+1}$ et $\bigcup_{n=1}^{\infty} E_n = \Omega$. Pour chaque n nous avons les inégalités

$$\int_{\Omega} f_n \geq \int_{E_n} f_n \geq C \int_{E_n} h. \quad (7.338)$$

Si nous prenons la limite $n \rightarrow \infty$ dans ces inégalités,

$$\lim_{n \rightarrow \infty} \int_{\Omega} f_n \geq C \lim_{n \rightarrow \infty} \int_{E_n} h = C \int_{\Omega} h. \quad (7.339)$$

Par conséquent $\lim_{n \rightarrow \infty} \int_{\Omega} f_n \geq C \int_{\Omega} h$. Mais étant donné que cette inégalité est valable pour tout C entre 0 et 1, nous pouvons l'écrire sans le C :

$$\lim_{n \rightarrow \infty} \int_{\Omega} f_n \geq \int_{\Omega} h. \quad (7.340)$$

Par définition, l'intégrale de f est donné par le supremum des intégrales de h où h est une fonction simple dominée par f . En prenant le supremum sur h dans l'équation (7.340) nous avons

$$\lim_{n \rightarrow \infty} \int_{\Omega} f_n \geq \int_{\Omega} f, \quad (7.341)$$

ce qu'il nous fallait. □

Remarque 7.130.

La proposition 7.107 ainsi que le lemme 7.104 montrent qu'une fonction mesurable peut-être écrite comme limite croissante de fonctions simples. Cela permet de démontrer des théorèmes en commençant par prouver sur les fonctions simples et en utilisant Beppo-Levi pour généraliser.

Remarque 7.131.

Une des raisons de demander la positivité des fonctions f_n est de n'avoir pas d'ambiguïté à parler d'intégrales qui valent ∞ . Si par exemple nous prenons $\Omega = [0, 1]$ et que nous considérons

$$f_n(x) = \begin{cases} 0 & \text{si } x \leq \frac{1}{n} \\ \frac{1}{x} & \text{sinon.} \end{cases} \quad (7.342)$$

Ce sont des fonctions intégrables, mais la limite étant la fonction $1/x$, l'égalité (7.333) est une égalité entre deux intégrales valant ∞ .

Corollaire 7.132 (Inversion de somme et intégrales).

Si (u_n) est une suite de fonctions mesurables positives ou nulles, alors

$$\sum_{i=0}^{\infty} \int u_i = \int \sum_{i=0}^{\infty} u_i. \quad (7.343)$$

Démonstration. Nous considérons la suite des sommes partielles de (u_n) : $f_n(x) = \sum_{i=0}^n u_i(x)$. Le théorème de la convergence monotone (théorème 7.129) implique que

$$\lim_{n \rightarrow \infty} \int f_n = \int \lim_{n \rightarrow \infty} f_n. \quad (7.344)$$

Nous remplaçons maintenant f_n par sa valeur en termes des u_i et dans le membre de gauche nous permutons l'intégrale avec la somme finie :

$$\lim_{n \rightarrow \infty} \sum_{i=0}^{\infty} \int u_n = \int \sum_{i=0}^{\infty} u_n, \quad (7.345)$$

ce qu'il fallait démontrer. $\square$

Lemme 7.133 (Lemme de Fatou).

Soit $(\Omega, \mathcal{A}, \mu)$ un espace mesuré et $f_n: \Omega \rightarrow [0, \infty]$ une suite de fonctions mesurables. Alors la fonction $f(x) = \liminf f_n(x)$ est mesurable et

$$\int_{\Omega} \liminf f_n d\mu \leq \liminf \int_{\Omega} f_n d\mu. \quad (7.346)$$

Démonstration. Nous posons

$$g_n(x) = \inf_{i \geq n} f_i(x). \quad (7.347)$$

Cela est une suite croissance de fonctions positives mesurables telles que, par définition,

$$\lim_{n \rightarrow \infty} g_n(x) = \liminf f_n(x). \quad (7.348)$$

Nous pouvons y appliquer le théorème de la convergence monotone,

$$\lim_{n \rightarrow \infty} \int g_n(x) = \int \liminf f_n(x). \quad (7.349)$$

Par ailleurs, pour chaque $i \geq n$ nous avons

$$\int g_n \leq \int f_i, \quad (7.350)$$

en passant à l'infimum nous avons

$$\int g_n \leq \inf_{i \geq n} \int f_i, \quad (7.351)$$

et en passant à la limite nous avons

$$\int \liminf f_n = \lim_{n \rightarrow \infty} \int g_n \leq \lim_{n \rightarrow \infty} \inf_{i \geq n} \int f_i = \liminf_{i \rightarrow \infty} \int f_i. \quad (7.352)$$

$\square$

L'inégalité donnée dans ce lemme n'est en général pas une égalité, comme le montre l'exemple suivant :

$$f_i = \begin{cases} \mathbb{1}_{[0,1]} & \text{si } i \text{ est pair} \\ \mathbb{1}_{[1,2]} & \text{si } i \text{ est impair.} \end{cases} \quad (7.353)$$

Nous avons évidemment $g_n(x) = 0$ tandis que $\int_{[0,2]} f_i = 1$ pour tout i .

7.5.2.3 Convergence dominée de Lebesgue

Théorème 7.134 (Convergence dominée de Lebesgue).

Soit $(f_n)_{n \in \mathbb{N}}$ une suite de fonctions intégrables sur $(\Omega, \mathcal{A}, \mu)$ à valeurs dans $\mathbb{C}$ ou $\mathbb{R}$. Nous supposons que $f_n \rightarrow f$ simplement sur Ω presque partout et qu'il existe une fonction intégrable g telle que

$$|f_n(x)| \leq g(x) \quad (7.354)$$

pour presque²⁷ tout $x \in \Omega$ et pour tout $n \in \mathbb{N}$. Alors

²⁷. S'il n'y avait pas le «presque» ici, ce théorème serait à peu près inutilisable en probabilité ou en théorie des espaces L^p , comme dans la démonstration du théorème de Fischer-Riesz 18.27 par exemple.

- (1) f est intégrable,
- (2) $\lim_{n \rightarrow \infty} \int_{\Omega} f_n = \int_{\Omega} f$,
- (3) $\lim_{n \rightarrow \infty} \int_{\Omega} |f_n - f| = 0$.

Démonstration. La fonction limite f est intégrable parce que $|f| \leq g$ et g est intégrable (lemme 7.125). Par hypothèse nous avons

$$-g(x) \leq f_n(x) \leq g(x). \quad (7.355)$$

En particulier la fonction $g_n = f_n + g$ est positive et mesurable si bien que le lemme de Fatou (lemme 7.133) implique

$$\int_{\Omega} \liminf g_n \leq \liminf \int_{\Omega} g_n. \quad (7.356)$$

Évidemment nous avons $\liminf g_n = f + g$, de telle sorte que

$$\int f + \int g \leq \liminf \int g_n = \liminf \int f_n + \int g, \quad (7.357)$$

et le nombre $\int g$ étant fini, nous pouvons le retrancher des deux côtés de l'inégalité :

$$\int f \leq \liminf \int f_n. \quad (7.358)$$

Afin d'obtenir une minoration de $\int f$ nous refaisons exactement le même raisonnement en utilisant la suite de fonctions $k_n = -f_n \rightarrow k = -f$. Nous obtenons que

$$\int k \geq \liminf \int k_n = -\limsup \int f_n, \quad (7.359)$$

et par conséquent

$$\liminf \int f_n \leq \int f \leq \limsup \int f_n. \quad (7.360)$$

La limite supérieure étant plus grande ou égale à la limite inférieure, les trois quantités dans les inégalités (7.360) sont égales.

Nous prouvons maintenant le troisième point. Soit la suite de fonctions

$$h_n(x) = |f_n(x) - f(x)| \quad (7.361)$$

qui tend ponctuellement vers zéro. De plus

$$h_n(x) \leq |f_n(x)| + |f(x)| \leq 2g(x), \quad (7.362)$$

ce qui prouve que les h_n majorés par une fonction intégrable. Donc

$$\lim_{n \rightarrow \infty} \int_{\Omega} |f_n - f| = \lim_{n \rightarrow \infty} \int_{\Omega} h_n(x) dx = \int_{\Omega} \lim_{n \rightarrow \infty} |f_n(x) - f(x)| = 0 \quad (7.363)$$

□

Remarque 7.135.

Lorsque nous travaillons sur des problèmes de probabilités, la fonction g peut être une constante parce que les constantes sont intégrables sur un espace de probabilité.

Corollaire 7.136.

Soit $(a_i)_{i \in \mathbb{N}}$ une suite numérique absolument convergente. Alors elle est convergente. Il en est de même pour les séries de fonctions si on considère la convergence ponctuelle.

Démonstration. L'hypothèse est la convergence de l'intégrale $\sum_{\mathbb{N}} |a_i| dm(i)$ où dm est la mesure de comptage. Étant donné que $|a_i| \leq |a_i|$, la fonction a_i (fonction de i) peut jouer le rôle de g dans le théorème de la convergence dominée de Lebesgue (théorème 7.134). □

7.5.3 Produit d'une mesure par une fonction (mesure à densité)

Proposition-définition 7.137 ([8, 131]).

Soit un espace mesuré $(S, \mathcal{F}, \mu)$ et une fonction mesurable positive $w: S \rightarrow \bar{\mathbb{R}}^+$. Alors la formule

$$(w \cdot \mu)(A) = \int_A w d\mu \quad (7.364)$$

pour tout $A \in \mathcal{F}$ définit une mesure positive sur $(S, \mathcal{F})$ appelée **produit** de la mesure μ par la fonction w . La fonction w est la **densité** de la mesure $w \cdot \mu$ par rapport à la mesure μ .

Démonstration. D'abord $(w \cdot \mu)(\emptyset) = 0$ parce que

$$(w \cdot \mu)\emptyset = \int_S w \mathbb{1}_{\emptyset} d\mu = \int_S 0 d\mu = 0 \times \mu(S) = 0 \quad (7.365)$$

où nous avons (éventuellement) utilisé deux fois la convention $0 \times \infty = 0$.

Ensuite si les ensembles A_i sont des éléments deux à deux disjoints de $\mathcal{F}$ alors nous avons $\mathbb{1}_{\bigcup_{i=1}^{\infty} A_i} = \sum_{i=1}^{\infty} \mathbb{1}_{A_i}$, et donc

$$(w \cdot \mu)\left(\bigcup_i A_i\right) = \int_S w \mathbb{1}_{\bigcup_i A_i} d\mu = \int_S \left(\sum_{i=1}^{\infty} w \mathbb{1}_{A_i}\right) d\mu = \sum_i \int_S w \mathbb{1}_{A_i} d\mu = \sum_i (w \cdot \mu)(A_i). \quad (7.366)$$

Dans ce calcul nous avons utilisé le fait que f était positive pour justifier l'application du théorème de la convergence monotone 7.129. $\square$

Proposition 7.138 ([131]).

Soit une fonction mesurable $w: (S, \mathcal{F}, \mu) \rightarrow \bar{\mathbb{R}}^+$.

- (1) Si $f: S \rightarrow \bar{\mathbb{R}}^+$ est mesurable, alors $f \cdot (w \cdot \mu) = (fg) \cdot \mu$.
- (2) Si $f: S \rightarrow \bar{\mathbb{R}}$ ou $\mathbb{C}$ est mesurable, elle est $w \cdot \mu$ -intégrable si et seulement si fw est μ -intégrable. Dans ce cas, nous avons encore $f \cdot (w \cdot \mu) = (fg) \cdot \mu$.

Attention : dans le cas où f est à valeurs dans $\mathbb{C}$, alors il faut que w soit à valeurs finies dans $\mathbb{R}$ parce que nous n'avons pas défini $\infty \times z$ lorsque $z \in \mathbb{C}$.

Démonstration. Nous commençons par prouver le résultat pour la fonction caractéristique de l'ensemble mesurable A . Nous avons : $\mathbb{1}_A \cdot (w \cdot \mu)(B) = \int_B \mathbb{1}_A d(w \cdot \mu)$. Mais par définition, l'intégrale d'une fonction indicatrice est la mesure de l'ensemble indiqué. En passant sur le fait que $\mathbb{1}_A \mathbb{1}_B = \mathbb{1}_{A \cap B}$,

$$\int_B \mathbb{1}_A d(w \cdot \mu) = (w \cdot \mu)(A \cap B) = \int_S \mathbb{1}_{A \cap B} w d\mu = \int_S \mathbb{1}_A \mathbb{1}_B w d\mu = \int_B \mathbb{1}_A w d\mu = (\mathbb{1}_A w) \cdot \mu(B). \quad (7.367)$$

Supposons maintenant que f soit une fonction étagée qui s'écrit $f = \sum_k a_k \mathbb{1}_{A_k}$ où les A_k sont des ensembles mesurables disjoints. Alors le calcul est le suivant, en utilisant le fait que sur A_k , on a $a_k = f(x)$:

$$f \cdot (g \cdot \mu)B = \int_B f d(g \cdot \mu) \quad (7.368a)$$

$$= \sum_k a_k (g \cdot \mu)(A_k \cap B) \quad (7.368b)$$

$$= \sum_k a_k \int_{A_k \cap B} g f d\mu \quad (7.368c)$$

$$= \int_{A_k \cap B} f(x) g(x) d\mu(x) \quad (7.368d)$$

$$= \sum_k (fg \cdot \mu)(A_k \cap B) \quad (7.368e)$$

$$= (fg \cdot \mu)(B) \quad (7.368f)$$

parce que les $A_k \cap B$ forment une partition de l'ensemble B (voir le point (2) de la définition 7.23).

Si $f: S \rightarrow \mathbb{R}^+$ est mesurable, le théorème 7.107 donne une suite croissante f_n de fonctions étagées positives convergeant (ponctuellement) vers f . Vu que la fonction w est positive, nous avons aussi la limite positive et croissante $wf_n \rightarrow wf$. Ainsi l'utilisation du théorème de la convergence monotone est justifié dans le calcul suivant :

$$\int_S f d(w \cdot \mu) = \lim_{n \rightarrow \infty} \int_S f_n d(w \cdot \mu) = \lim_{n \rightarrow \infty} \int_S (wf_n) d\mu = \int_S wf d\mu. \quad (7.369)$$

Nous passons maintenant au cas général où f est une fonction à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$ (avec w finie dans ce dernier cas). Nous avons la chaîne d'équivalences

$$\begin{aligned} &\Leftrightarrow f \text{ est } (w \cdot \mu) \text{ intégrable} \\ &\Leftrightarrow |f| \text{ est } (w \cdot \mu)\text{-intégrable} \\ &\Leftrightarrow |f|w \text{ est } \mu\text{-intégrable} \\ &\Leftrightarrow |fw| \text{ est } \mu\text{-intégrable.} \end{aligned}$$

Si cela est le cas, la formule se démontre en se ramenant au cas déjà prouvé des fonctions positives en utilisant les $(fw)^+ = f^+w$, $(fw)^- = f^-w$ etc. $\square$

7.6 Tribu produit, mesure produit

7.6.1 Produit d'espaces mesurables

Définition 7.139.

Si $\mathcal{A}_1$ et $\mathcal{A}_2$ sont deux tribus sur deux ensembles Ω_1 et Ω_2 , nous définissons la **tribu produit** $\mathcal{A}_1 \otimes \mathcal{A}_2$ comme étant la tribu engendrée par

$$\{X \times Y \text{ tel que } X \in \mathcal{A}_1, Y \in \mathcal{A}_2\}. \quad (7.370)$$

Ces ensembles sont appelés **rectangles** de $(\Omega_1, \mathcal{A}_1) \otimes (\Omega_2, \mathcal{A}_2)$.

Proposition 7.140 ([132]).

Soient deux espaces mesurables $(S_1, \mathcal{F}_1)$ et $(S_2, \mathcal{F}_2)$. Si $\mathcal{C}_i$ est une classe de parties de S_i avec $\mathcal{F}_i = \sigma(\mathcal{C}_i)$ et $S_i \in \mathcal{C}_i$. Alors

$$\mathcal{F}_1 \otimes \mathcal{F}_2 = \sigma(\mathcal{C}_1 \times \mathcal{C}_2). \quad (7.371)$$

Démonstration. Nous notons p_1 et p_2 les projections de $S_1 \times S_2$ vers S_1 et S_2 . Nous commençons par prouver que

$$\mathcal{F}_1 \otimes \mathcal{F}_2 = \sigma(p_1^{-1}(\mathcal{F}_1) \cup p_2^{-1}(\mathcal{F}_2)). \quad (7.372)$$

En effet cette union est dans $\mathcal{F}_1 \otimes \mathcal{F}_2$ parce que ce sont tous des produits de la forme $A_1 \times S_2$ et $S_1 \times A_2$ où $A_i \in \mathcal{F}_i$. Inversement, tous les produits de la forme $A_1 \times A_2$ sont dans la tribu engendrée par l'union parce que

$$A_1 \cup A_2 = (A_1 \times S_2) \cap (S_1 \times A_2). \quad (7.373)$$

Par conséquent, la partie $p_1^{-1}(\mathcal{F}_1) \cup p_2^{-1}(\mathcal{F}_2)$ engendre tous les produits qui engendrent la tribu $\mathcal{F}_1 \otimes \mathcal{F}_2$. L'égalité (7.372) est donc correcte.

Si $C_1 \in \mathcal{C}_1$ alors

$$p_1^{-1}(C_1) = C_1 \times S_2 \in \mathcal{C}_1 \times \mathcal{C}_2 \quad (7.374)$$

et donc $p_1^{-1}(C_1) \subset \mathcal{C}_1 \times \mathcal{C}_2$. En utilisant le lemme de transfert 7.70 nous avons alors

$$p_1^{-1}(\mathcal{F}_1) = p_1^{-1}(\sigma(\mathcal{C}_1)) = \sigma(p_1^{-1}\mathcal{C}_1) \subset \sigma(\mathcal{C}_1 \times \mathcal{C}_1) \quad (7.375)$$

et au bout de la même façon,

$$p_2^{-1}(\mathcal{F}_1) \subset \sigma(\mathcal{C}_1 \times \mathcal{C}_2). \quad (7.376)$$

Vu les relations (7.375), (7.376) et (7.372) nous avons

$$\mathcal{F}_1 \otimes \mathcal{F}_2 = \sigma(p_1^{-1}(\mathcal{F}_1) \cup p_2^{-1}(\mathcal{F}_2)) \subset \sigma(\mathcal{C}_1 \times \mathcal{C}_2). \quad (7.377)$$

Réciproquement, si $C_1 \in \mathcal{C}_1$ et $C_2 \in \mathcal{C}_2$ alors

$$C_1 \times C_2 = (C_1 \times S_1) \cap (S_1 \times C_2) = p_1^{-1}(C_1) \cap p_2^{-1}(C_2) \in \mathcal{F}_1 \otimes \mathcal{F}_2. \quad (7.378)$$

□

7.6.2 Le cas des boréliens

Si X_1 et X_2 sont des espaces topologiques et si nous notons $\mathcal{O}_i$ l'ensemble de leurs ouverts, par définition $\mathcal{B}or(X_i) = \sigma(\mathcal{O}_i)$. De plus par la proposition 7.140 nous savons que

$$\sigma(\mathcal{O}_1 \times \mathcal{O}_2) = \mathcal{B}or(X_1) \otimes \mathcal{B}or(X_2). \quad (7.379)$$

Lemme 7.141.

Si $(X_i, \mathcal{O}_i)$ sont des espaces topologiques, alors

$$\mathcal{B}or(X_1) \otimes \mathcal{B}or(X_2) \subset \mathcal{B}or(X_1 \times X_2) \quad (7.380)$$

Démonstration. Si $A_i \in \mathcal{O}_i$ alors $A_1 \times A_2$ est un ouvert de $X_1 \times X_2$ (voir la définition 5.5). Par conséquent, $\mathcal{O}_1 \times \mathcal{O}_2$ est contenu dans l'ensemble des ouverts de $X_1 \times X_2$ ou encore

$$\mathcal{O}_1 \times \mathcal{O}_2 \subset \mathcal{B}or(X_1 \times X_2), \quad (7.381)$$

et donc

$$\sigma(\mathcal{O}_1 \times \mathcal{O}_2) \subset \sigma(\mathcal{B}or(X_1 \times X_2)) \quad (7.382)$$

finalement, par (7.379)

$$\mathcal{B}or(X_1) \otimes \mathcal{B}or(X_2) \subset \mathcal{B}or(X_1 \times X_2). \quad (7.383)$$

□

Il n'y a en général pas égalité, mais nous allons immédiatement voir que dans (presque) tous les cas raisonnables, les boréliens sur un produit sont le produit des boréliens.

Proposition 7.142 ([132]).

Soient (X_1, d_1) et (X_2, d_2) des espace métriques séparables. Alors

$$\mathcal{B}or(X_1 \times X_2) = \mathcal{B}or(X_1) \otimes \mathcal{B}or(X_2). \quad (7.384)$$

Démonstration. Nous savons par le lemme 5.45 que tout ouvert de $X_1 \times X_2$ est une réunion dénombrable d'éléments de $\mathcal{O}_1 \times \mathcal{O}_2$. Donc tout ouvert de $X_1 \times X_2$ est dans $\mathcal{B}or(X_1) \otimes \mathcal{B}or(X_2)$. Par conséquent

$$\mathcal{B}or(X_1 \times X_2) \subset \mathcal{B}or(X_1) \otimes \mathcal{B}or(X_2). \quad (7.385)$$

L'inclusion inverse étant déjà acquise par le lemme 7.141, nous avons l'égalité. □

Proposition 7.143.

Les boréliens sur $\mathbb{R}^N$ sont ceux qu'on croit.

$$(1) \mathcal{B}or(\mathbb{R}^2) = \mathcal{B}or(\mathbb{R}) \otimes \mathcal{B}or(\mathbb{R})$$

$$(2) \mathcal{B}or(\mathbb{R}^{N+1}) = \mathcal{B}or(\mathbb{R}^N) \otimes \mathcal{B}or(\mathbb{R})$$

Démonstration. Cela n'est rien d'autre que la proposition 7.142. □

Proposition 7.144.

Soit un espace mesurable $(S, \mathcal{F})$ et des applications $f_k: S \rightarrow \mathbb{R}$ ($k = 1, \dots, N$). Alors l'application

$$\begin{aligned} f: (S, \mathcal{F}) &\rightarrow (\mathbb{R}^n, \mathcal{B}or(\mathbb{R}^N)) \\ x &\mapsto (f_1(x), \dots, f_N(x)) \end{aligned} \quad (7.386)$$

est mesurable si et seulement si chacun des f_i est mesurable.

Démonstration. Division en deux.

Condition nécessaire Nous supposons que les f_i sont mesurables. Nous avons

$$f^{-1}\left(\prod_{k=1}^N]a_k, b_k[\right) = \{x \in S \text{ tel que } f_1(x) \in]a_1, b_1[, \dots, f_N(x) \in]a_N, b_N[\} \quad (7.387a)$$

$$= \bigcap_{k=1}^N f_k^{-1}(]a_k, b_k[). \quad (7.387b)$$

Cela est une intersection finie d'éléments de $\mathcal{F}$ et est donc un élément de $\mathcal{F}$. Mais les pavés ouverts engendrent $\mathcal{Bor}(\mathbb{R}^N)$ parce qu'ils sont une base dénombrable de la topologie (proposition 7.9). Le théorème 7.71 nous assure alors que f est mesurable parce que l'image inverse d'une base de la tribu est mesurable.

Condition suffisante Si f est mesurable alors en particulier

$$f_k^{-1}(]a, b[) = f^{-1}(\mathbb{R} \times \dots \times]a, b[\times \mathbb{R} \times \dots \times \mathbb{R}) \in \mathcal{F}. \quad (7.388)$$

Pour cela nous avons utilisé la proposition 7.143 qui nous indique que le produit dans la parenthèse est un borélien de $\mathbb{R}^N$ en tant que produit de boréliens de $\mathbb{R}$.

Encore une fois f_k^{-1} tombe dans $\mathcal{F}$ pour une base dénombrable de la topologie de $\mathbb{R}$ et est donc mesurable. □

7.6.3 Produit de mesures

Lemme 7.145 (Propriété des sections[125]).

Soient $\mathcal{A}_1$ et $\mathcal{A}_2$ des tribus sur les ensembles Ω_1 et Ω_2 . Si $A \in \mathcal{A}_1 \otimes \mathcal{A}_2$ alors pour tout $x \in \Omega_1$ et $y \in \Omega_2$, les ensembles

$$A_1(y) = \{x \in \Omega_1 \text{ tel que } (x, y) \in A\} \quad (7.389a)$$

$$A_2(x) = \{y \in \Omega_2 \text{ tel que } (x, y) \in A\} \quad (7.389b)$$

sont mesurables.

Démonstration. Soit $y \in \Omega_2$; nous allons prouver le résultat pour $A_1(y)$. Pour cela nous notons

$$S = \{A \in \mathcal{A}_1 \otimes \mathcal{A}_2 \text{ tel que } \forall y \in \Omega_2, A_1(y) \in \mathcal{A}_1\}, \quad (7.390)$$

et nous allons noter que S est une tribu contenant les rectangles. Par conséquent, S sera égal à $\mathcal{A}_1 \otimes \mathcal{A}_2$.

Les rectangles Considérons le rectangle $A = X \times Y$ et si $y \in \Omega_2$ alors

$$A_1(y) = \{x \in \Omega_1 \text{ tel que } (x, y) \in X \times Y\}. \quad (7.391)$$

Donc soit $y \in Y$ alors $A_1(y) = X \in \mathcal{A}_1$, soit $y \notin Y$ et alors $A_1(y) = \emptyset \in \mathcal{A}_1$.

Tribu : ensemble complet Nous avons $\Omega_1 \times \Omega_2 \in S$ parce que c'est un rectangle.

Tribu : complémentaire Soit $A \in S$ et montrons que $A^c \in S$. Nous avons d'abord

$$(A^c)_1(y) = \{x \in \Omega_1 \text{ tel que } (x, y) \in A^c\}. \quad (7.392)$$

D'autre part

$$A_1(y)^c = \{x \in \Omega_1 \text{ tel que } (x, y) \notin A\} = \{x \in \Omega_1 \text{ tel que } (x, y) \in A^c\} = (A^c)_1(y). \quad (7.393)$$

Vu que $\mathcal{A}_1$ est une tribu et que par hypothèse $A_1(y) \in \mathcal{A}_1$, nous avons aussi $A_1(y)^c \in S$, et donc $(A^c)_1(y) \in \mathcal{A}_1$, ce qui prouve que $A^c \in S$.

Tribu : union dénombrable Soit une suite $A_n \in S$. Nous avons

$$\left(\bigcup_n A_n\right)_1(y) = \{x \in \Omega_1 \text{ tel que } (x, y) \in \bigcup_n A_n\} = \bigcup_n \{x \in \Omega_1 \text{ tel que } (x, y) \in A_n\} = \bigcup_n (A_n)_1(y), \quad (7.394)$$

et ce dernier ensemble est dans $\mathcal{A}_1$ parce que c'est une union dénombrable d'éléments de $\mathcal{A}_1$.

Nous avons donc prouvé que S est une tribu contenant les rectangles, donc S contient au moins $\mathcal{A}_1 \otimes \mathcal{A}_2$. $\square$

Corollaire 7.146.

Si $f: \Omega_1 \times \Omega_2 \rightarrow \mathbb{R}$ est une fonction mesurable²⁸ sur $X \times Y$ alors pour chaque y dans Ω_2 , la fonction

$$\begin{aligned} f_y: X &\rightarrow \mathbb{R} \\ x &\mapsto f(x, y) \end{aligned} \quad (7.395)$$

est mesurable.

Démonstration. Soit $\mathcal{O}$ un ensemble mesurable de $\mathbb{R}$ (i.e. un borélien), et $y \in \Omega_2$. Nous avons

$$f_y^{-1}(\mathcal{O}) = \{x \in X \text{ tel que } f(x, y) \in \mathcal{O}\} = A_1(y) \quad (7.396)$$

où

$$A = \{(x, y) \in \Omega_1 \times \Omega_2 \text{ tel que } f(x, y) \in \mathcal{O}\} = f^{-1}(\mathcal{O}). \quad (7.397)$$

Ce dernier est mesurable parce que f l'est. $\square$

Théorème 7.147 ([125]²⁹).

Soient $(\Omega_i, \mathcal{A}_i, \mu_i)$ ($i = 1, 2$) deux espaces mesurés σ -finie. Soit $A \in \mathcal{A}_1 \otimes \mathcal{A}_2$. Alors les fonctions³⁰

$$x \mapsto \mu_2(A_2(x)) \quad (7.398a)$$

$$y \mapsto \mu_1(A_1(y)) \quad (7.398b)$$

sont mesurables et

$$\int_{\Omega_1} \mu_2(A_2(x)) d\mu_1(x) = \int_{\Omega_2} \mu_1(A_1(y)) d\mu_2(y). \quad (7.399)$$

Démonstration. Nous supposons d'abord que μ_1 et μ_2 sont finies et nous notons $\mathcal{D}$ le sous-ensemble de $\mathcal{A}_1 \otimes \mathcal{A}_2$ sur lequel le théorème est correct. Nous allons commencer par prouver que $\mathcal{D}$ est un λ -système.

λ -système : différence ensembliste Soient $A, B \in \mathcal{D}$ avec $A \subset B$. Nous avons

$$(B \setminus A)_1(y) = \{x \in \Omega_1 \text{ tel que } (x, y) \in B \setminus A\} \quad (7.400a)$$

$$= \{x \in \Omega_1 \text{ tel que } (x, y) \in B\} \setminus \{x \in \Omega_1 \text{ tel que } (x, y) \in A\} \quad (7.400b)$$

$$= B_1(y) \setminus A_1(y). \quad (7.400c)$$

Vu que $A_1(y) \subset B_1(y)$ et que les mesures sont finies le lemme 7.26 nous donne

$$\mu_1((B \setminus A)_1(y)) = \mu_1(B_1(y)) - \mu_1(A_1(y)), \quad (7.401)$$

et similairement pour $1 \leftrightarrow 2$. Les deux fonctions (de y) à droite étant mesurables, nous avons la mesurabilité de la fonction $y \mapsto \mu_1((B \setminus A)_1(y))$.

28. Définition 7.63.

29. Modèle non contractuel : des notations et la définition de λ -système peuvent varier entre la référence et le présent texte.

30. Voir la notation du lemme 7.389.

Prouvons la formule intégrale en nous rappelant que la formule (7.399) est supposée correcte pour A et B séparément :

$$\int_{\Omega_2} \mu_1((B \setminus A)_1(y)) d\mu_2(y) = \int_{\Omega_2} \mu_1(B_1(y)) d\mu_2(y) - \int_{\Omega_2} \mu_1(A_1(y)) d\mu_2(y) \quad (7.402a)$$

$$= \int_{\Omega_1} \mu_2(B_2(x)) d\mu_1(x) - \int_{\Omega_1} \mu_2(A_2(x)) d\mu_1(x) \quad (7.402b)$$

$$= \int_{\Omega_1} \mu_2((B \setminus A)_2(x)) d\mu_1(x). \quad (7.402c)$$

λ -système : limite de suite croissante Soit (A_n) une suite croissante dans $\mathcal{D}$; nous posons $B_n = A_n \setminus A_{n-1}$ et $A_0 = \emptyset$ de telle sorte à travailler avec une suite d'ensembles disjoints qui satisfait $\bigcup_n A_n = \bigcup_n B_n$. Vu que la suite est croissante nous avons $A_{n-1} \subset A_n$ et donc $B_n \in \mathcal{D}$ par le point déjà fait sur la différence ensembliste. Nous avons :

$$\mu_1((\bigcup_n B_n)_1(y)) = \{x \in \Omega_1 \text{ tel que } (x, y) \in \bigcup_n B_n\} \quad (7.403a)$$

$$= \bigcup_n \{x \in \Omega_1 \text{ tel que } (x, y) \in B_n\} \quad (7.403b)$$

$$= \bigcup_n (B_n)_1(y). \quad (7.403c)$$

Par conséquent, par la propriété (2) d'une mesure nous avons

$$\mu_1((\bigcup_n B_n)_1(y)) = \sum_n \mu_1((B_n)_1(y)). \quad (7.404)$$

En tant que somme de fonctions positives et mesurables, la fonction

$$y \mapsto \sum_n \mu_1((B_n)_1(y)) \quad (7.405)$$

est mesurable par la proposition 7.93. Il faut encore vérifier la formule intégrale. Le gros du boulot est de permuter une somme et une intégrale par le corollaire 7.132 :

$$\int_{\Omega_2} \sum_n \mu_1((B_n)_1(y)) d\mu_2(y) = \sum_n \int_{\Omega_2} \mu_1((B_n)_1(y)) d\mu_2(y) \quad (7.406a)$$

$$= \sum_n \int_{\Omega_1} \mu_2((B_n)_2(x)) d\mu_1(x) \quad (7.406b)$$

$$= \int_{\Omega_1} \sum_n \mu_2((B_n)_2(x)) d\mu_1(x) \quad (7.406c)$$

$$= \int_{\Omega_1} \mu_2((\bigcup_n B_n)_1(y)) d\mu_1(x). \quad (7.406d)$$

Maintenant que $\mathcal{D}$ est un λ -système contenant les rectangles, le lemme 7.39 dit que la tribu engendrée par $\mathcal{D}$ (c'est à dire $\mathcal{A}_1 \otimes \mathcal{A}_2$) est le λ -système $\mathcal{D}$ lui-même.

La preuve est finie dans le cas de mesures finies. Nous commençons maintenant à prouver dans le cas où les mesures μ_1 et μ_2 sont seulement σ -finies. Nous considérons des suites croissantes $\Omega_{i,n} \rightarrow \Omega_i$ d'ensembles mesurables et de mesure finie : $\mu_i(\Omega_{i,n}) < \infty$. D'abord remarquons que

$$\mu_2((A \cap \Omega_{1,j} \times E_{2,j})_2(x)) = \mu_2(A_2(x) \cap \Omega_{2,j}) \mathbb{1}_{\Omega_{1,j}}. \quad (7.407)$$

En effet,

$$\heartsuit = (A \cap \Omega_{1,j} \times E_{2,j})_2(x) \quad (7.408a)$$

$$= \{y \in \Omega_2 \text{ tel que } (x, y) \in A \cap \Omega_{1,j} \times E_{2,j}\} \quad (7.408b)$$

$$= \{y \in \Omega_2 \text{ tel que } (x, y) \in A \times \Omega_{2,j}\} \cap \{y \in \Omega_2 \text{ tel que } (x, y) \in \Omega_{1,j} \times \Omega_{2,j}\}. \quad (7.408c)$$

Si $y \in \Omega_{1,j}$ alors $\{y \in \Omega_2 \text{ tel que } (x, y) \in \Omega_{1,j} \times \Omega_{2,j}\} = \Omega_{2,j}$ et dans ce cas

$$\heartsuit = \{y \in \Omega_2 \text{ tel que } (x, y) \in A \times \Omega_{2,j}\} \cap \Omega_{2,j} = A_2(x) \cap E_{2,j}. \quad (7.409)$$

Et inversement, si $x \notin \Omega_{1,j}$ alors $\heartsuit = \emptyset$. Dans les deux cas nous avons (7.407).

Les ensembles $A \cap \Omega_{1,j} \times \Omega_{2,j}$ étant de mesure finie, nous pouvons leur appliquer la première partie :

$$\int_{\Omega_1} \mu_2((A \cap \Omega_{1,j} \times \Omega_{2,j})_2(x)) d\mu_1(x) = \int_{\Omega_2} \mu_1((A \cap \Omega_{1,j} \times \Omega_{2,j})_1(y)) d\mu_2(y), \quad (7.410)$$

ou encore

$$\int_{\Omega_1} \mu_2(A_2(x) \cap \Omega_{2,j}) \mathbb{1}_{\Omega_{1,j}}(x) d\mu_1(x) = \int_{\Omega_2} \mu_1(A_1(y) \cap \Omega_{1,j}) \mathbb{1}_{\Omega_{2,j}}(y) d\mu_2(y). \quad (7.411)$$

Ce que nous avons dans ces intégrales sont (par rapport à j) des suites croissantes de fonction positives ; nous pouvons donc permuter une limite et une intégrale. En sachant que si $k \rightarrow \infty$, alors

$$\mathbb{1}_{1,j}(x) \rightarrow 1 \quad (7.412a)$$

$$\mu_2(A_2(x) \cap \Omega_{2,j}) \rightarrow \mu_2(A_2(x)), \quad (7.412b)$$

nous trouvons le résultat demandé. $\square$

Théorème 7.148 ([133, 134]).

Soient μ_i des mesures σ -finies sur $(\Omega_i, \mathcal{A}_i)$ ($i = 1, 2$).

(1) Il existe une et une seule mesure, notée $\mu_1 \otimes \mu_2$, sur $(\Omega_1 \times \Omega_2, \mathcal{A}_1 \otimes \mathcal{A}_2)$ telle que

$$(\mu_1 \otimes \mu_2)(A_1 \times A_2) = \mu_1(A_1)\mu_2(A_2) \quad (7.413)$$

pour tout $A_1 \in \mathcal{A}_1$ et $A_2 \in \mathcal{A}_2$.

(2) Cette mesure est donnée par la formule³¹

$$(\mu_1 \otimes \mu_2)(A) = \int_{\Omega_1} \mu_2(A_2(x)) d\mu_1(x) = \int_{\Omega_2} \mu_1(A_1(y)) d\mu_2(y). \quad (7.414)$$

Cette mesure est la **mesure produit** de μ_1 par μ_2 .

(3) La mesure $\mu_1 \otimes \mu_2$ ainsi définie est σ -finie.

Démonstration. La partie «existence» sera divisée en deux parties : l'une pour prouver que les formules (7.414) donnent une mesure et une pour montrer que cette mesure vérifie la condition (7.413).

Unicité L'ensemble des rectangles de $\Omega_1 \times \Omega_2$ engendre la tribu $\mathcal{A}_1 \otimes \mathcal{A}_2$, est fermé par intersection et contient une suite croissante d'ensembles $P_n \times R_n$ de mesure finie ($\mu(P_n \times R_n) < \infty$) telle que $P_n \times R_n \rightarrow \Omega_1 \times \Omega_2$. Cette suite est donnée par le fait que μ_1 et μ_2 sont σ -finies. En effet si (X_n) et (Y_n) sont des recouvrements dénombrables de Ω_1 et Ω_2 par des ensembles de mesure finie, en posant $P_n = \bigcup_{k=1}^n X_k$ et $R_n = \bigcup_{k=1}^n Y_k$ nous avons bien une suite croissante de rectangles qui tendent vers $\Omega_1 \times \Omega_2$. Avec ces rectangles en main, le théorème 7.40 donne l'unicité.

Les formules définissent une mesure Le théorème 7.147 dit que ces formules ont un sens et que l'égalité entre les deux intégrales est correcte. Nous prouvons à présent qu'elles déterminent effectivement une mesure sur $(\Omega_1 \times \Omega_2, \mathcal{A}_1 \otimes \mathcal{A}_2)$.

Pour tout $A \in \mathcal{A}_1 \otimes \mathcal{A}_2$, $\mu(A) \geq 0$ parce que μ est donnée par l'intégrale d'une fonction positive.

31. Voir les notations du lemme 7.145.

En ce qui concerne la condition d'unions dénombrable disjointe, soient A^i des éléments disjoints de $\mathcal{A}_1 \otimes \mathcal{A}_2$; nous commençons par remarquer que

$$\left(\bigcup_{i=1}^{\infty} A^{(i)} \right)_2 (x) = \{y \in \Omega_2 \text{ tel que } (x, y) \in \bigcup_{i=1}^{\infty} A^{(i)}\} \quad (7.415a)$$

$$= \bigcup_{i=1}^{\infty} \{y \in \Omega_2 \text{ tel que } (x, y) \in A^{(i)}\} \quad (7.415b)$$

$$= \bigcup_{i=1}^{\infty} A_2^{(i)}(x). \quad (7.415c)$$

Par conséquent,

$$\mu \left(\bigcup_{i=1}^{\infty} A^{(i)} \right) = \int_{\Omega_1} \mu_2 \left(\left(\bigcup_{i=1}^{\infty} A^{(i)} \right)_2 (x) \right) d\mu_1(x) \quad (7.416a)$$

$$= \int_{\Omega_1} \sum_{i=1}^{\infty} \mu_2(A_2^{(i)}(x)) d\mu_1(x) \quad (7.416b)$$

$$= \int_{\Omega_1} \lim_{n \rightarrow \infty} \sum_{i=1}^n \mu_2(A_2^{(i)}(x)) d\mu_1(x). \quad (7.416c)$$

où nous avons utilisé l'additivité de la mesure μ_2 . À ce niveau, il serait commode de permuter la somme et l'intégrale. Pour ce faire nous considérons la suite (croissante) de fonctions

$$f_n(x) = \sum_{i=1}^n \mu_2(A_2^{(i)}(x)). \quad (7.417)$$

Nous pouvons permuter la limite et l'intégrale grâce au théorème de la convergence monotone 7.129 ; ensuite la somme se permute avec l'intégrale en tant que somme finie :

$$\mu \left(\bigcup_{i=1}^{\infty} A^{(i)} \right) = \lim_{n \rightarrow \infty} \sum_{i=1}^n \int_{\Omega_1} (A_2^{(i)}(x)) d\mu_1(x) \quad (7.418a)$$

$$= \lim_{n \rightarrow \infty} \sum_{i=1}^n \mu(A^{(i)}) \quad (7.418b)$$

$$= \sum_{i=1}^{\infty} \mu(A^{(i)}). \quad (7.418c)$$

Elles vérifient la condition Prouvons que les formules (7.414) se réduisent à (7.413) dans le cas des rectangles. Soit donc $A = X_1 \times X_2$ avec $X_i \in \mathcal{A}_i$. Alors

$$A_1(y) = \{x \in \Omega_1 \text{ tel que } (x, y) \in X_1 \times X_2\} \quad (7.419)$$

et

$$\mu_1(A_1(y)) = \mathbb{1}_{X_2}(y) \mu_1(X_1), \quad (7.420)$$

donc

$$(\mu_1 \otimes \mu_2)(A) = \int_{\Omega_2} \mu_1(A_1(y)) d\mu_2(y) \quad (7.421a)$$

$$= \int_{\Omega_2} \mu_1(X_1) \mathbb{1}_{X_2}(y) d\mu_2(y) \quad (7.421b)$$

$$= \mu_1(X_1) \int_{\Omega_2} \mathbb{1}_{X_2}(y) d\mu_2(y) \quad (7.421c)$$

$$= \mu_1(X_1) \mu_2(X_2). \quad (7.421d)$$

Pour cela nous avons utilisé le fait que l'intégrale de la fonction caractéristique d'un ensemble mesurable est la mesure de cet ensemble.

□

Définition 7.149 (Produit d'espaces mesurés).

Si $(\Omega_i, \mathcal{A}_i, \mu_i)$ sont deux espaces mesurés, l'**espace produit** est l'ensemble $\Omega_1 \times \Omega_2$ muni de la tribu produit $\mathcal{A}_1 \otimes \mathcal{A}_2$ de la définition 7.139 et de la mesure produit $\mu_1 \otimes \mu_2$ définie par le théorème 7.148.

Remarque 7.150.

Il n'est pas garanti que la tribu $\mathcal{A}_1 \otimes \mathcal{A}_2$ soit la tribu la plus adaptée à l'ensemble $S_1 \times S_2$. Dans le cas de $\mathbb{R}^N$, il se fait que c'est le cas : en prenant des produits des boréliens sur $\mathbb{R}$ on obtient bien les boréliens sur $\mathbb{R}^N$, voir proposition 7.143.

7.7 Mesure de Lebesgue sur $\mathbb{R}$

Nous notons $\mathcal{S}$ l'ensemble des intervalles³² de $\mathbb{R}$.

Proposition 7.151.

L'ensemble réunions finies d'éléments de $\mathcal{S}$ est une algèbre de parties de $\mathbb{R}$.

Cette algèbre de parties de $\mathbb{R}$ est notée $\mathcal{A}_{\mathcal{S}}$.

Démonstration. Nous devons vérifier la définition 7.18. Les ensembles $\mathbb{R}$ et $\emptyset$ sont des intervalles et font donc partie de $\mathcal{A}_{\mathcal{S}}$.

Si $A \in \mathcal{A}_{\mathcal{S}}$ se décompose en union d'intervalles de la forme (a_k, b_k) avec $k = 1, \dots, n$ (ici nous mettons des parenthèses au lieu de crochets parce qu'a priori nous ne savons pas). Alors

$$A^c = \bigcup_{k=0}^k (b_k, a_{k+1}) \quad (7.422)$$

où nous avons posé $b_0 = -\infty$ et $a_{n+1} = +\infty$. Ici encore les parenthèses sont soit fermées soit ouvertes en fonction de ce qu'étaient celles dans la décomposition de A . Quoi qu'il en soit, cette décomposition de A^c montre que $A^c \in \mathcal{A}_{\mathcal{S}}$.

Enfin si $A, B \in \mathcal{A}_{\mathcal{S}}$ alors $A \cup B \in \mathcal{A}_{\mathcal{S}}$. □

Lemme 7.152.

Tout élément de $\mathcal{A}_{\mathcal{S}}$ admet une décomposition minimale unique en réunion finie d'intervalles. Cette décomposition est formée d'intervalles deux à deux disjoints.

Démonstration. Nous allons montrer que si $A \in \mathcal{A}_{\mathcal{S}}$, alors la décomposition minimale consiste en les composantes connexes de A . Pour cela nous rappelons que la proposition 5.103 dit qu'une partie de $\mathbb{R}$ est connexe si et seulement si elle est un intervalle. D'abord cela nous dit immédiatement que les composantes connexes de A forment une décomposition de A en intervalles. Nous devons prouver qu'elle est minimale.

Soit $\{C_k\}_{k=1, \dots, n}$ les composantes connexes de A . Aucun connexe de $\mathbb{R}$ contenu dans A ne peut intersecter plus d'un des C_k , et par conséquent nous ne pouvons pas décomposer A en moins de n intervalles.

Pour l'unicité, soit $\{I_k\}_{k=1, \dots, n}$ un ensemble de n intervalles tels que $\bigcup_{k=1}^n I_k = A$. Chacun des I_k intersecte un et un seul des C_k . En effet si $x \in I_k \cap C_i$ et $y \in I_k \cap C_j$, alors $[x, y] \subset I_k$ parce que I_k est un intervalle. Mais C_i étant le plus grand connexe contenant x , $[x, y] \subset C_i$ et de la même façon, $[x, y] \subset C_j$. Par conséquent C_i et C_j sont tous deux la composante connexe de x et y . Nous en déduisons que $C_i = C_j$, c'est à dire $i = j$.

Par ailleurs nous avons $I_k \cap I_l = \emptyset$ dès que $k \neq l$ parce que sinon l'ensemble $I_k \cap I_l$ serait connexe et la décomposition des $\{I_k\}_{k=1, \dots, n}$ ne serait pas minimale : en remplaçant I_k et I_l par $I_k \cup I_l$ on aurait eu une décomposition contenant moins d'éléments. Donc à renumérotation près nous pouvons supposer que I_k intersecte C_l si et seulement si $k = l$.

32. Définition 5.101.

Dans ce cas nous devons avoir $I_k = C_k$, sinon les éléments de $C_k \setminus I_k$ ne seraient pas dans $\bigcup_{i=1}^n I_i$. $\square$

Définition 7.153 (longueur d'intervalle[119]).

Si I est un intervalle d'extrémités a et b avec $-\infty \leq a \leq b \leq +\infty$ alors nous définissons la **longueur** de I par

$$\ell(I) = \begin{cases} b - a & \text{si } -\infty < a \leq b < +\infty \\ \infty & \text{si } a \text{ ou } b \text{ est infini} \end{cases} \quad (7.423)$$

Si $A \in \mathcal{A}_S$ et si sa décomposition minimale est $A = \bigcup_{k=1}^n I_k$, alors on définit

$$\ell(A) = \sum_{k=1}^n \ell(I_k). \quad (7.424)$$

Le lemme suivant nous indique que nous pouvons calculer la longueur d'un élément de $\mathcal{A}_S$ sans savoir la décomposition minimale, pourvu que l'on connaisse une décomposition disjointe.

Lemme 7.154 ([119]).

Si

$$B = \bigcup_{r=1}^p J_r \quad (7.425)$$

est une décomposition de $B \in \mathcal{A}_S$ en intervalles deux à deux disjoints alors

$$\ell(B) = \sum_{r=1}^p \ell(J_r). \quad (7.426)$$

Démonstration. Nous prouvons dans un premier temps le résultat dans le cas où $B = I$ est un intervalle. Soit I un intervalle et une décomposition en intervalles disjoints $I = \bigcup_{r=1}^p J_r$. Nous montrons qu'alors $\ell(I) = \sum_{r=1}^p \ell(J_r)$. Nous verrons ensuite comment passer au cas où B est un élément générique de $\mathcal{A}_S$.

Si $B = I$ est un intervalle infini Si I est infini alors un des J_r soit l'être et donc $\sum_{r=1}^p \ell(J_r) = \infty = \ell(I)$.

Si $B = I$ est un intervalle ininfini Pour chaque $r = 1, \dots, p$ nous notons a_r et b_r les extrémités de J_r . Vu que les J_r sont connexes et disjoints, si $a_k \leq a_l$ alors $b_k \leq a_l$, sinon l'ensemble (non vide) $]a_l, b_k[$ serait dans l'intersection $I_k \cap I_l$ qui, elle, est vide. Plus généralement, si $x \in J_k$ et $y \in J_l$ avec $x < y$ alors pour tout $x' \in J_k$ et tout $y' \in J_l$ nous avons $x' < y'$. Vu qu'il y a un nombre fini d'ensembles J_r , nous pouvons les classer dans l'ordre croissant :

$$a_1 \leq b_1 \leq a_2 \leq b_2 \leq \dots \leq b_{p-1} \leq a_p \leq b_p. \quad (7.427)$$

Vu que les J_r sont disjoints et que leur union est connexe nous avons en réalité

$$a = a_1 \leq b_1 = a_2 \leq b_2 = a_3 \leq \dots \leq b_{p-1} = a_p \leq b_p, \quad (7.428)$$

donc une somme télescopique donne

$$\ell(I) = b - a = \sum_{r=1}^p (b_r - a_r) = \sum_{r=1}^p \ell(J_r). \quad (7.429)$$

Si B n'est pas un intervalle Soit $\{I_k\}_{k=1, \dots, n}$ la décomposition minimale de B . Alors

$$\spadesuit = \ell(B) = \sum_{k=1}^n \ell(I_k) = \sum_{k=1}^n \ell\left(\bigcup_{r=1}^p (I_k \cap J_r)\right). \quad (7.430)$$

Mais I_k est un intervalle et s'écrit comme union disjointe $I_k = \bigcup_{r=1}^p (I_k \cap J_r)$, donc par la première partie

$$\spadesuit = \sum_{k=1}^n \sum_{r=1}^p \ell(I_k \cap J_r) = \sum_{r=1}^p \sum_{k=1}^n \ell(I_k \cap J_r). \quad (7.431)$$

Ici J_r est un intervalle qui se décompose en $J_r = \bigcup_{k=1}^n (I_k \cap J_r)$, donc nous pouvons encore utiliser la première partie :

$$\spadesuit = \sum_{r=1}^p \ell(J_r), \quad (7.432)$$

ce qu'il fallait. □

Lemme 7.155.

Si $A, B \in \mathcal{A}_S$ avec $A \subset B$ alors $\ell(A) \leq \ell(B)$.

Démonstration. Nous avons évidemment $B = A \cup B \setminus A$. Notons que $B \setminus A \in \mathcal{A}_S$ par le lemme 7.19. Si $\{I_k\}$ est une décomposition disjointe de A et $\{J_i\}$ une de $B \setminus A$ alors $\{I_k\} \cup \{J_i\}$ est une décomposition disjointe de $A \cup B \setminus A$ et le lemme 7.154 nous dit que

$$\ell(B) = \ell(A \cup B \setminus A) = \ell(A) + \ell(B \setminus A). \quad (7.433)$$

Par conséquent $\ell(B) \geq \ell(A)$. □

Lemme 7.156.

Si I est un intervalle et si il se décompose en

$$I = \bigcup_{n \in \mathbb{N}} I_n \quad (7.434)$$

où les I_n sont des intervalles disjoints, alors

$$\ell(I) = \sum_{n=1}^{\infty} \ell(I_n). \quad (7.435)$$

Démonstration. Nous allons encore diviser la preuve en deux parties suivant que I soit de longueur finie ou pas.

Si I est de longueur finie Soient a et b les extrémités de I : $-\infty < a \leq b < +\infty$. Pour tout $N \geq 1$ nous avons

$$\sum_{n=1}^N \ell(I_n) = \ell\left(\bigcup_{n=1}^N I_n\right) \leq \ell(I). \quad (7.436)$$

La première égalité est le lemme dans le cas d'une union finie 7.154. L'inégalité est le lemme 7.155. Cela étant vrai pour tout N , à la limite $N \rightarrow \infty$ nous conservons l'inégalité :

$$\sum_{n=1}^{\infty} \ell(I_n) \leq \ell(I). \quad (7.437)$$

Nous devons encore voir l'inégalité inverse. Pour cela nous supposons que $a < b$. Sinon $\ell(I) = 0$ et tous les I_n doivent être vide sauf un qui contiendra seulement $\{a\}$ (si I le contient).

Soit $\epsilon > 0$ avec $\epsilon < b - a$ et l'intervalle

$$\left[a + \frac{\epsilon}{4}, b - \frac{\epsilon}{4}\right] = [a', b'] \subset I. \quad (7.438)$$

Si les a_n et le b_n sont les extrémités des I_n alors

$$[a', b'] \subset I = \bigcup_{n \geq 1} I_n \subset \bigcup_{n \geq 1} \left[a_n - \frac{\epsilon}{2^{n+2}}, b_n + \frac{\epsilon}{2^{n+2}}\right] = \bigcup_{n \geq 1} [a'_n, b'_n] \quad (7.439)$$

où nous avons posé $a'_n = a_n - \epsilon/2^{n+2}$ et $b'_n = b_n + \epsilon/2^{n+2}$. Nous avons donc recouvert le compact³³ $[a', b']$ par des ouverts. Nous pouvons donc en extraire un sous-recouvrement fini (c'est la définition de la compacité), c'est à dire une partie finie F de $\mathbb{N}$ telle que

$$[a', b'] \subset \bigcup_{n \in F}]a'_n, b'_n[. \quad (7.440)$$

Le lemme 7.155 nous dit alors que

$$\heartsuit = b' - a' \leq \ell\left(\bigcup_{n \in F}]a'_n, b'_n[\right) \leq \sum_{n \in F} (b'_n - a'_n). \quad (7.441)$$

La seconde inégalité se prouve en recopiant³⁴ la preuve de 7.21. Nous continuons le calcul :

$$\heartsuit \leq \sum_{n \in F} (b_n - a_n) + \sum_{n \in F} \frac{\epsilon}{2^{n+1}} \leq \sum_{n \in F} (b_n - a_n) + \frac{\epsilon}{2}. \quad (7.442)$$

Mais $b' - a' = (b - a) - \frac{\epsilon}{2}$, donc

$$b - a - \frac{\epsilon}{2} \leq \sum_{n \in F} (b_n - a_n) + \frac{\epsilon}{2}. \quad (7.443)$$

D'où nous déduisons que

$$\ell(I) = b - a \leq \sum_{n \in F} (b_n - a_n) + \epsilon \leq \sum_{n \in \mathbb{N}} (b_n - a_n) + \epsilon = \sum_{n \in \mathbb{N}} \ell(I_n) + \epsilon. \quad (7.444)$$

Cela étant valable pour tout ϵ nous déduisons que

$$\ell(I) \leq \sum_{n \in \mathbb{N}} \ell(I_n). \quad (7.445)$$

Si I est de longueur infinie Étant donné que I est un intervalle de longueur infinie, il contient au moins un ensemble du type $]-\infty, a]$ ou $[a, +\infty[$; donc pour tout $M > 0$, il existe $N \geq 1$ tel que

$$\ell(I \cap [-N, N]) \geq M. \quad (7.446)$$

Mais $I \cap [-N, N]$ est un intervalle et

$$I \cap [-N, N] = \bigcup_{n \in \mathbb{N}} I_n \cap [-N, N] \quad (7.447)$$

qui est une union disjointe. Par conséquent,

$$M \leq \ell(I \cap [-N, N]) = \sum_n \ell(I_n \cap [-N, N]) \leq \sum_n \ell(I_n). \quad (7.448)$$

Cela étant vrai pour tout $M > 0$, nous concluons que

$$\sum_{n \in \mathbb{N}} \ell(I_n) = \infty. \quad (7.449)$$

□

Remarque 7.157.

Pour la preuve de 7.156 nous ne pouvons pas classer les I_n en ordre croissant comme nous l'avons fait dans la preuve de 7.154. En effet si $I = [0, 1]$ et que nous recouvrons $[0, \frac{1}{2}[$ et $]\frac{1}{2}, 1]$ par une infinité d'intervalles chacun, nous ne pouvons plus les classer par ordre croissant.

33. Lemme 5.105.

34. Nous ne pouvons pas invoquer directement le lemme 7.21 parce que nous n'avons pas encore prouvé que ℓ était une mesure sur $(\mathbb{R}, \mathcal{A}_S)$.

Proposition 7.158 ([119]).

La fonction ℓ ainsi définie est une mesure σ -finie sur l'algèbre de parties $\mathcal{A}_{\mathcal{S}}$.

Démonstration. Le fait que ℓ soit σ -finie provient par exemple du fait que $\ell(]-n, n[) = 2n$ tandis que $\bigcup_n]-n, n[= \mathbb{R}$.

Nous devons à présent prouver que ℓ est additive. Soient $(A_i)_{i \in \mathbb{N}}$ des éléments disjoints de $\mathcal{A}_{\mathcal{S}}$, avec leurs décomposition minimales

$$A_i = \bigcup_{k=1}^n I_k^{(i)}. \quad (7.450)$$

Pour chaque $i \in \mathbb{N}$, le lemme 7.156 nous indique que

$$\ell(A_i) = \sum_{k \in \mathbb{N}} \ell(I_k^{(i)}). \quad (7.451)$$

L'ensemble $\mathbb{N} \times \mathbb{N}$ est dénombrable et nous pouvons considérer la décomposition

$$\bigcup_{i \in \mathbb{N}} A_i = \bigcup_{(i,k) \in \mathbb{N} \times \mathbb{N}} I_k^{(i)}. \quad (7.452)$$

Cette décomposition n'est pas spécialement minimale³⁵ mais elle est disjointe. Le lemme 7.156 donne

$$\ell\left(\bigcup_i A_i\right) = \sum_{(i,k) \in \mathbb{N} \times \mathbb{N}} \ell(I_k^{(i)}) = \sum_{i \in \mathbb{N}} \left(\sum_{k \in \mathbb{N}} \ell(I_k^{(i)}) \right) = \sum_{i \in \mathbb{N}} \ell(A_i). \quad (7.453)$$

La décomposition de la somme sur $\mathbb{N}^2$ en deux sommes sur $\mathbb{N}$ est faite en vertu de la proposition 6.190. □

7.7.1 Mesure et tribu de Lebesgue**Théorème 7.159.**

Il existe une unique mesure λ sur $(\mathbb{R}, \mathcal{B}or(\mathbb{R}))$ telle que

$$\lambda(]a, b[) = b - a \quad (7.454)$$

pour tout $a \leq b$ dans $\mathbb{R}$.

Démonstration. L'existence provient du théorème de prolongement de Hahn 7.60 : la mesure ℓ sur $(\mathcal{A}_{\mathcal{S}})$ se prolonge à $\sigma(\mathcal{A}_{\mathcal{S}}) = \mathcal{B}or(\mathbb{R})$.

Nous ne pouvons pas prouver l'unicité en invoquant la partie unicité de Hahn (c'est tentant parce que ℓ est σ -finie) parce que dans ce théorème nous ne fixons la valeur de λ que sur une toute petite partie de $\mathcal{A}_{\mathcal{S}}$. Nous allons cependant voir que cette petite partie suffit à garantir l'unicité.

La classe

$$\mathcal{D} = \{]a, b[\text{ tel que } -\infty < a \leq b < +\infty\} \quad (7.455)$$

est stable par intersection finie et engendre la tribu borélienne. En effet $\mathcal{D}$ contient toutes les boules et donc une base dénombrable de la topologie de $\mathbb{R}$ (proposition 5.43). Donc tous les ouverts de $\mathbb{R}$ sont dans $\sigma(\mathcal{D})$ et $\sigma(\mathcal{D}) = \mathcal{B}or(\mathbb{R})$. Nous pouvons donc dire grâce au théorème 7.40 qu'il y a unicité de la mesure sur $\mathcal{B}or(\mathbb{R})$ lorsque les valeurs sur $\mathcal{D}$ sont fixées. □

Définition 7.160.

La mesure de l'espace mesuré $(\mathbb{R}, \mathcal{B}or(\mathbb{R}), \lambda)$ donné par le théorème 7.159 est la **mesure de Lebesgue** sur $(\mathbb{R}, \mathcal{B}or(\mathbb{R}))$.

Nous définissons aussi la **tribu de Lebesgue** par la proposition 7.59 : $(\mathbb{R}, \mathcal{L}eb(\mathbb{R}), \lambda)$ est l'espace mesuré complété de $(\mathbb{R}, \mathcal{B}or(\mathbb{R}), \lambda)$.

^{35.} A_1 pourrait contenir $[0, 1]$ et A_2 contenir $]1, 2]$.

Remarque 7.161.

Il n'est pas évident que la tribu de Lebesgue soit plus grande que celle des boréliens, ni que la tribu des parties soit plus grande que celle de Lebesgue. Nous mentionnons cependant les faits suivants.

- (1) Il existe des ensembles mesurables non-boréliens, et cela ne nécessite pas l'axiome du choix. Un argument classique de cardinalité est donné dans [118]. La construction la plus explicite que j'aie trouvée est dans [6], mais ça a l'air de demander des connaissances précises sur les ordinaux.
- (2) Vu que l'ensemble de Cantor C est mesurable de mesure nulle, tout sous-ensemble de Cantor est mesurable de mesure nulle parce que la tribu de Lebesgue est complète par définition. Le cardinal de $\mathcal{P}(C)$ est strictement supérieur à la puissance du continu, alors que le cardinal de l'ensemble des boréliens est au plus égal à la puissance du continu. Donc il existe des non boréliens contenus dans Cantor ; de tels non boréliens sont alors mesurables au sens de Lebesgue.
Pour savoir des choses sur la cardinalité de l'ensemble des parties, on peut aller voir dans [10].
- (3) Si nous admettons l'axiome du choix alors il existe des ensembles non mesurables au sens de Lebesgue. Nous en verrons un dans l'exemple 7.178.

Exemple 7.162(Un ouvert contenant tous les rationnel et de mesure arbitrairement petite)

Il est possible de construire un ouvert de $\mathbb{R}$ contenant $\mathbb{Q}$ et de mesure de Lebesgue plus petite que ϵ . Pour cela si (q_i) est une énumération des rationnels, il suffit de prendre

$$\mathcal{O} = \bigcup_{n=1}^{\infty} B(q_n, \frac{\epsilon}{2^{n+1}}). \quad (7.456)$$

Cela est un ouvert comme union d'ouverts, ça contient tous les rationnels, et sa mesure se majore. En effet le théorème 7.159 donne $\lambda(B(q_n, \frac{\epsilon}{2^n})) = \frac{\epsilon}{2^n}$. Vu que ces boules ne sont a priori pas disjointes, le lemme 7.26 donne

$$\lambda(\mathcal{O}) \leq \sum_{n=1}^{\infty} \frac{\epsilon}{2^n} = \epsilon \quad (7.457)$$

par (6.349) avec $q = \frac{1}{2}$.

Par complémentarité, nous pouvons construire un ensemble fermé de mesure non nulle et ne contenant aucun rationnel. Et même un fermé dans $[0, 1]$, de mesure $1 - \epsilon$ ne contenant aucun rationnel.

Cela peut surprendre parce qu'il existe des tonnes de suites d'irrationnels qui convergent vers des rationnels³⁶, et il semble difficile de créer un ensemble contenant beaucoup d'irrationnels tout en préservant la propriété de fermeture vis à vis des suites convergentes. $\triangle$

7.7.2 Propriétés de la mesure de Lebesgue**Proposition 7.163.**

Tout ensemble dénombrable de $\mathbb{R}$ est mesurable de mesure nulle.

Démonstration. Un point de $\mathbb{R}$ est un intervalle de mesure nulle. Si D est dénombrable, il est union disjointes et dénombrable de points. Le lemme 7.156 nous dit alors que sa mesure est $\lambda(D) = \sum_{i=1}^{\infty} \lambda(\{a_i\}) = 0$. $\square$

Remarque 7.164.

Il existe cependant des ensembles non dénombrables et tout de même de mesure nulle. Par exemple l'ensemble de Cantor (voir la proposition 7.177).

36. Si $q \in \mathbb{Q}$ et $r \in \mathbb{R} \setminus \mathbb{Q}$ alors la suite $(q + r/10^k)_k$ est une suite d'irrationnels convergente vers le rationnel q

Proposition 7.165.

La mesure de Lebesgue est invariante par translation, c'est à dire que si A est mesurable alors $\lambda(A) = \lambda(A + \alpha)$ pour tout réel α .

Démonstration. Nous commençons par les intervalles ouverts :

$$\lambda([a, b[+ \alpha) = \lambda([a + \alpha, b + \alpha[) = (b + \alpha) - (a + \alpha) = b - a = \lambda([a, b[). \quad (7.458)$$

D'après ce qui est dit dans l'exemple 7.41, la mesure de Lebesgue sur les boréliens est invariante par translation.

Si A est mesurable alors il existe un borélien B et un ensemble négligeable N tels que $A = B \cup N$ par la caractérisation 7.97b de la complétion. Alors $A + \alpha = B + \alpha \cup N + \alpha$ et $N + \alpha$ est encore un ensemble négligeable. Donc $\lambda(A + \alpha) = \lambda(B + \alpha) = \lambda(B)$. $\square$

Le mesure ℓ définie sur l'algèbre de parties $\mathcal{A}_S$ (voir proposition 7.158). La proposition 7.22 nous donne donc une mesure extérieure par

$$\lambda^*(X) = \inf \left\{ \sum_n \ell(A_n); A_n \in \mathcal{A}_S, X \subset \bigcup_n A_n \right\}. \quad (7.459)$$

La proposition suivante montre que cette mesure extérieure peut être exprimée seulement avec des intervalles ouverts.

Proposition 7.166.

Nous avons

$$\lambda^*(X) = \inf \left\{ \sum_{n \geq 1} \ell(I_n); I_n \text{ sont des intervalles ouverts et } X \subset \bigcup_n I_n \right\}. \quad (7.460)$$

Démonstration. Nous savons que dans la définition (7.459), chacun des A_n est une réunion disjointe d'intervalles (pas spécialement ouverts) deux à deux disjoints; donc

$$\lambda^*(X) = \inf \left\{ \sum_n \ell(I_n); I_n \in \mathcal{S}, X \subset \bigcup_n I_n \right\}. \quad (7.461)$$

Soit $\epsilon > 0$. Si $A \subset \bigcup_n I_n$, pour chaque $n \geq 1$ nous considérons un intervalle ouvert J_n tel que $I_n \subset J_n$ et $\ell(I_n) + \frac{\epsilon}{2^n} \leq \ell(J_n)$. Faisant cela pour chacun des découpages de X en intervalles nous trouvons

$$\lambda^*(X) \leq \inf \left\{ \sum_n \ell(J_n) \mid J_n \text{ est ouvert et } X \subset \bigcup_n J_n \right\} + \epsilon. \quad (7.462)$$

Étant donné que ϵ est arbitraire nous avons l'égalité. $\square$

Proposition 7.167 ([119]).

Si $X \subset \mathbb{R}$ est tel que $\lambda^*(X) < \infty$ alors

(1) Pour tout $\epsilon > 0$ il existe un ouvert Ω_ϵ tel que

$$\begin{cases} X \subset \Omega_\epsilon \\ \lambda(\Omega_\epsilon) \leq \lambda^*(X) + \epsilon. \end{cases} \quad (7.463a)$$

$$\lambda(\Omega_\epsilon) \leq \lambda^*(X) + \epsilon. \quad (7.463b)$$

(2) Il existe une intersection dénombrable d'ouverts G telle que

$$\begin{cases} X \subset G \\ \lambda(G) = \lambda^*(X). \end{cases} \quad (7.464a)$$

$$\lambda(G) = \lambda^*(X). \quad (7.464b)$$

Démonstration. Pour (1), la proposition 7.166 nous a déjà dit que

$$\lambda^*(X) = \inf \left\{ \sum_n \ell(I_n) \mid I_n \text{ est un intervalle ouvert, } X \subset \bigcup_n I_n \right\}, \quad (7.465)$$

donc si $\epsilon > 0$, il existe des intervalles ouverts I_n tels que

$$\left\{ \begin{array}{l} X \subset \bigcup_n I_n \end{array} \right. \quad (7.466a)$$

$$\left\{ \begin{array}{l} \sum_n \ell(I_n) \leq \lambda^*(X) + \epsilon. \end{array} \right. \quad (7.466b)$$

Si nous posons $\Omega_\epsilon = \bigcup_n I_n$, alors nous avons bien

$$\left\{ \begin{array}{l} X \subset \Omega_\epsilon \end{array} \right. \quad (7.467a)$$

$$\left\{ \begin{array}{l} \lambda(\Omega_\epsilon) \leq \sum_n \ell(I_n) \leq \lambda^*(X) + \epsilon. \end{array} \right. \quad (7.467b)$$

En ce qui concerne (2), pour chaque $k \geq 1$ nous considérons l'ensemble $\Omega_{1/k}$ obtenu comme précédemment avec $\epsilon = 1/k$ et nous posons $G = \bigcap_{k \geq 1} \Omega_{1/k}$. Cela est une intersection dénombrable d'ouverts vérifiant $X \subset G$ (parce que $X \subset \Omega_{1/k}$ pour tout k) et donc $\lambda^*(X) \leq \lambda^*(G) = \lambda(G)$. De plus pour tout k nous avons

$$\lambda(G) \leq (\Omega_{1/k}) \leq \lambda^*(X) + \frac{1}{k} \quad (7.468)$$

pour tout k . En faisant $k \rightarrow \infty$ nous avons

$$\lambda(G) \leq \lambda^*(X). \quad (7.469)$$

Au final

$$\lambda(G) \leq \lambda^*(X) \leq \lambda(G), \quad (7.470)$$

d'où l'égalité. $\square$

Corollaire 7.168.

Une partie $N \subset \mathbb{R}$ est négligeable³⁷ si et seulement si $\lambda^*(N) = 0$.

Démonstration. Nous savons que si N est négligeable il existe un borélien Y tel que $N \subset Y$ avec $\lambda(Y) = 0$. Par conséquent³⁸

$$\lambda^*(N) \leq \lambda^*(Y) = \lambda(Y) = 0. \quad (7.471)$$

Pour l'implication inverse nous supposons que $\lambda^*(N) = 0$ et nous prenons l'ensemble G défini par la proposition 7.167(2) : c'est un borélien contenant N et tel que $\lambda(G) = \lambda^*(N) = 0$. L'ensemble N est donc négligeable. $\square$

Théorème 7.169 (Régularité extérieure de la mesure de Lebesgue).

Pour tout mesurable $A \subset \mathbb{R}$ nous avons

$$\lambda(A) = \inf\{\lambda(\Omega); \Omega \text{ ouvert contenant } A\}. \quad (7.472)$$

Démonstration. Nous commençons par le cas où B est un borélien.

Si B borélien, $\lambda(B) < \infty$ Soit $\epsilon > 0$; par la proposition 7.167(1) il existe un ouvert Ω_ϵ contenant B tel que $\lambda(\Omega_\epsilon) \leq \lambda^*(B) + \epsilon$. Vu qu'ici B est borélien, $\lambda^*(B) = \lambda(B)$ et nous concluons que pour tout ϵ il existe un ouvert Ω_ϵ tel que

$$\left\{ \begin{array}{l} B \subset \Omega_\epsilon \end{array} \right. \quad (7.473a)$$

$$\left\{ \begin{array}{l} \lambda(\Omega_\epsilon) \leq \lambda(B) + \epsilon, \end{array} \right. \quad (7.473b)$$

et donc

$$\lambda(B) = \inf\{\lambda(\Omega); \Omega \text{ ouvert contenant } B\}. \quad (7.474)$$

Si B borélien, $\lambda(B) = +\infty$ Dans ce cas l'infimum est pris uniquement sur des ouverts Ω tels que $\lambda(\Omega) = \infty$.

³⁷. Définition 7.48.

³⁸. Au péril d'être lourd nous rappelons que λ^* est défini sur toutes les parties de $\mathbb{R}$.

Si A est mesurable non borélien Nous passons maintenant au cas où A est mesurable sans être borélien. Il s'écrit donc $A = B \cup N$ avec B borélien et N négligeable par la proposition 7.51, et par définition $\lambda(A) = \lambda(B)$. Si Y est un borélien tel que $N \subset Y$ et $\lambda(Y) = 0$ alors

$$\lambda(A) = \lambda(B) = \inf\{\lambda(\Omega) \text{ tel que } \Omega \text{ ouvert, } B \subset \Omega\} \quad (7.475a)$$

$$\leq \inf\{\lambda(\Omega) \text{ tel que } \Omega \text{ ouvert, } B \cup N \subset \Omega\} \quad (7.475b)$$

$$\leq \inf_{\Omega', Y'}\{\lambda(\Omega' \cup Y') \text{ tel que } \Omega', Y' \text{ ouverts, } B \subset \Omega', Y \subset Y'\} \quad (7.475c)$$

$$\leq \inf_{\Omega', Y'}\{\lambda(\Omega') + \lambda(Y') \text{ tel que } \Omega', Y' \text{ ouverts, } B \subset \Omega', Y \subset Y'\} \quad (7.475d)$$

$$\leq \inf_{\Omega'}\{\lambda(\Omega') \text{ tel que } \Omega' \text{ ouvert, } B \subset \Omega'\} \quad (7.475e)$$

$$= \lambda(B). \quad (7.475f)$$

Justifications :

- (7.475a) Le cas borélien déjà fait.
- (7.475b) Les ouverts Ω tels que $B \cup N \subset \Omega$ vérifient a fortiori $B \subset \Omega$; nous avons donc agrandi l'ensemble sur lequel l'infimum est pris.
- (7.475c) Parmi les ouverts Ω qui recouvrent $B \cup N$, il y a ceux de la forme $\Omega' \cup Y'$ où Ω' recouvre B et Y' est un ouvert contenant Y . Donc nous avons rétréci l'ensemble sur lequel l'infimum est pris et par conséquent agrandi l'infimum.
- (7.475d) Mesure d'une union majorée par la somme des mesures.
- (7.475e) Vu que Y est borélien, $\lambda(Y) = \inf_{Y' \text{ ouvert}}\{\lambda(Y') \text{ tel que } Y \subset Y'\} = 0$. Donc pour tout Ω' et tout $\epsilon > 0$, nous pouvons trouver un Y' vérifiant les conditions tel que $\lambda(\Omega') + \lambda(Y') \leq \lambda(\Omega') + \epsilon$.

Toutes les inégalités sont des égalités en particulier (7.475b) donne

$$\lambda(A) = \inf\{\lambda(\Omega) \text{ tel que } \Omega \text{ ouvert, } B \cup N \subset \Omega\}, \quad (7.476)$$

ce qu'il fallait. □

Proposition 7.170 ([119]).

Si A est mesurable dans $\mathbb{R}$ et si $\epsilon > 0$ alors il existe un ouvert Ω_ϵ et un fermé F_ϵ tels que

$$\left\{ \begin{array}{l} F_\epsilon \subset A \subset \Omega_\epsilon \\ \lambda(\Omega_\epsilon \setminus F_\epsilon) \leq \epsilon. \end{array} \right. \quad (7.477a)$$

$$\quad (7.477b)$$

Démonstration. Nous commençons par le cas d'un borélien B .

Première étape Montrons qu'il existe un ouvert U_ϵ tel que

$$\left\{ \begin{array}{l} B \subset U_\epsilon \\ \lambda(U_\epsilon \setminus B) \leq \frac{\epsilon}{2}. \end{array} \right. \quad (7.478a)$$

$$\quad (7.478b)$$

Si $\lambda(B) < \infty$ alors le théorème 7.169 nous donne un ouvert U_ϵ tel que $B \subset U_\epsilon$ et $\lambda(U_\epsilon) \leq \lambda(B) + \frac{\epsilon}{2}$. Nous avons alors

$$\lambda(\Omega_\epsilon \setminus B) = \lambda(\Omega_\epsilon) - \lambda(B) \leq \frac{\epsilon}{2}. \quad (7.479)$$

Si par contre $\lambda(B) = \infty$, nous posons $B_n = B \cap [-n, n]$ et $\epsilon_n = \epsilon/2^{n+1}$. Pour chaque n nous avons un ouvert Ω_n tel que

$$\left\{ \begin{array}{l} B_n \subset \Omega_n \\ \lambda(\Omega_n \setminus B_n) \leq \frac{\epsilon}{2^{n+1}} \end{array} \right. \quad (7.480a)$$

$$\quad (7.480b)$$

Par conséquent en posant $\Omega = \bigcup_{n \geq 1} \Omega_n$ nous avons³⁹

$$\begin{cases} B \subset \Omega \\ \lambda(\Omega \setminus B) \leq \lambda\left(\bigcup_n (\Omega_n \setminus B_n)\right) \leq \sum_{n \geq 1} \lambda(\Omega_n \setminus B_n) = \frac{\epsilon}{2}. \end{cases} \quad \begin{matrix} (7.481a) \\ (7.481b) \end{matrix}$$

La première étape est terminée.

Deuxième étape Nous prouvons à présent qu'il existe un ouvert Ω_ϵ et un fermé F_ϵ tels que

$$\begin{cases} F_\epsilon \subset B \subset \Omega_\epsilon \\ \lambda(\Omega_\epsilon \setminus B) \leq \frac{\epsilon}{2} \\ \lambda(B \setminus F_\epsilon) \leq \frac{\epsilon}{2}. \end{cases} \quad \begin{matrix} (7.482a) \\ (7.482b) \\ (7.482c) \end{matrix}$$

L'ouvert Ω_ϵ , nous l'avons déjà de l'étape précédente. Pour le fermé, nous appliquons la première étape au borélien B^c ; ce qui nous trouvons est un ouvert G_ϵ tel que

$$\begin{cases} B^c \subset G_\epsilon \\ \lambda(G_\epsilon \setminus B^c) \leq \frac{\epsilon}{2}. \end{cases} \quad \begin{matrix} (7.483a) \\ (7.483b) \end{matrix}$$

En posant $F_\epsilon = G_\epsilon^c$ nous avons un fermé tel que $F_\epsilon \subset B$ et

$$\lambda(B \setminus F_\epsilon) = \lambda(F_\epsilon^c \setminus B^c) = \lambda(G_\epsilon \setminus B^c) \leq \frac{\epsilon}{2}. \quad (7.484)$$

Dernière étape Les ensembles F_ϵ et Ω_ϵ trouvés à la deuxième étape donnent bien les relations (7.477). En effet $\Omega_\epsilon \setminus F_\epsilon = (\Omega_\epsilon \setminus B) \cup (B \setminus F_\epsilon)$, donc

$$\lambda(\Omega_\epsilon \setminus F_\epsilon) \leq \lambda(\Omega_\epsilon \setminus B) + \lambda(B \setminus F_\epsilon) = \epsilon. \quad (7.485)$$

Nous passons au cas où $A = B \cup N$ est mesurable. Nous commençons par prendre les Ω_ϵ et F_ϵ qui correspondent à B :

$$\begin{cases} F_\epsilon \subset B \subset \Omega_\epsilon \\ \lambda(\Omega_\epsilon \setminus F_\epsilon) \leq \epsilon. \end{cases} \quad \begin{matrix} (7.486a) \\ (7.486b) \end{matrix}$$

Soit Y un borélien tel que $N \subset Y$ et $\lambda(Y)$ puis un ouvert Y' tel que $\lambda(Y') \leq \epsilon$ et $Y \subset Y'$. L'existence d'un tel Y' est assurée par la proposition 7.169 appliquée à Y . Nous vérifions que les ensembles F_ϵ et $\Omega_\epsilon \cup Y'$ fonctionnent. En effet $\Omega_\epsilon \cup Y' \setminus F_\epsilon \subset (\Omega_\epsilon \setminus F_\epsilon) \cup Y'$, donc

$$\begin{cases} F_\epsilon \subset B \cup N \subset \Omega_\epsilon \cup Y' \\ \lambda((\Omega_\epsilon \setminus F_\epsilon) \cup Y') \leq \lambda(\Omega_\epsilon \setminus F_\epsilon) + \lambda(Y') \leq 2\epsilon. \end{cases} \quad \begin{matrix} (7.487a) \\ (7.487b) \end{matrix}$$

Donc en réalité il faut choisir $\Omega_{\epsilon/2}$, $F_{\epsilon/2}$ et $\lambda(Y') \leq \epsilon/2$. □

Théorème 7.171 (Régularité intérieure de la mesure de Lebesgue).

Si A est mesurable dans $\mathbb{R}$ alors

$$\lambda(A) = \sup\{\lambda(K); K \text{ compact contenu dans } A\}. \quad (7.488)$$

Démonstration. Par la proposition 7.170 nous avons

$$\lambda(A) = \sup_{F \text{ fermé dans } A} \lambda(F). \quad (7.489)$$

39. Nous utilisons la petite relation ensembliste $(\bigcup_n A_n) \setminus (\bigcup_n B_n) \subset \bigcup_n (A_n \setminus B_n)$.

Pour un tel F nous posons $K_n = F \cap [-n, n]$ qui est compact⁴⁰ et contenu dans B . De plus le lemme 7.27(2) nous dit que

$$\lambda(F) = \lim_{n \rightarrow \infty} \lambda(K_n) \quad (7.490)$$

Donc tous les $\lambda(F)$ peuvent être arbitrairement approchés par un $\lambda(K)$ avec K compact dans A , et le supremum (7.489) n'est pas affecté en nous restreignant à prendre des compacts contenus dans B :

$$\lambda(A) = \sup_{F \text{ fermé dans } A} \lambda(F) = \sup_{K \text{ compact dans } A} \lambda(K). \quad (7.491)$$

□

7.7.3 Ensemble de Cantor

Nous considérons la fonction donnant l'écriture décimale des nombres définie en (6.359).

Définition 7.172 (Ensemble de Cantor).

Soit $K_0 = [0, 1[$ et les ensembles K_n définis par la récurrence

$$K_{n+1} = \left(\frac{1}{3}K_n\right) \cup \left(\frac{1}{3}(K_n + 2)\right). \quad (7.492)$$

L'ensemble

$$K = \bigcup_{n \geq 0} K_n \quad (7.493)$$

est l'ensemble triadique de Cantor.

Les principales propriétés de l'ensemble de Cantor sont qu'il est non dénombrable (proposition 7.176) et borélien de mesure nulle (proposition 7.177).

7.173.

L'idée de base pour prouver que l'ensemble K est non dénombrable est que ses éléments sont les nombres qui s'écrivent en base 3 sans utiliser le chiffre 1. En prenant un nombre sans 1 écrit en base 3, en changeant tous les 2 en 1 et en lisant le résultat en base 2, nous obtenons tous les nombres possibles en base 2 et donc une quantité non dénombrable. L'idée est donc simple et astucieuse. La mise en musique est un peu plus délicate parce qu'il faut faire attention aux queues de suites ; c'est pour cela que nous avons construit l'ensemble de Cantor en partant de $[0, 1[$ et non de $[0, 1]$.

Le lemme suivant dit précisément ce que nous entendons en disant que les éléments de l'ensemble de Cantor sont les nombres qui s'écrivent en base 3 sans utiliser le chiffre 1.

Lemme 7.174.

Soit $n \in \mathbb{N}$ et $x \in \mathbb{D}_3$; nous avons $\varphi_3(x) \in K_n$ si et seulement si $x_1, \dots, x_n \in \{0, 2\}$.

Démonstration. Nous procédons par récurrence en commençant avec $n = 1$. Si $x_1 = 1$ alors

$$\varphi_3(x) = \frac{1}{3} + \sum_{k=2}^{\infty} \frac{x_k}{3^k} \in \left[\frac{1}{3}, \frac{2}{3}\right]. \quad (7.494)$$

Notons que $\varphi_3(x) = \frac{2}{3}$ est impossible parce que ça demanderait une queue de suite de 2. Par conséquent $\varphi_3(x) \in [0, 1[\setminus [\frac{1}{3}, \frac{2}{3}] = K_1$.

Nous passons à la récurrence.

Sens direct Nous supposons que $x_1, \dots, x_{n+1} \in \{0, 2\}$ et nous montrons que $\varphi_3(x) \in K_{n+1}$. La chose surprenante est que nous n'allons pas considérer deux cas suivant que x_{n+1} vaut 0 ou

40. parce que fermé et borné, théorème de Borel-Lebesgue 5.107.

1 ; nous allons considérer deux cas suivant ⁴¹ que x_1 vaut 0 ou 1. Écrivons encore $\varphi_3(x)$:

$$\varphi_3(x) = \sum_{k=1}^{n+1} \frac{x_k}{3^k} + \sum_{k=n+2}^{\infty} \frac{x_k}{3^k}. \quad (7.495)$$

Si $x_1 = 0$ Alors nous avons

$$3\varphi_3(x) = \sum_{k=2}^{\infty} \frac{x_k}{3^{k-1}} = \sum_{k=1}^{\infty} \frac{x_{k+1}}{3^k} = \varphi_3(x_2, \dots, x_n, x_{n+1}, \dots) \quad (7.496)$$

Vu que par hypothèse $x_2, \dots, x_{n+1}$ sont dans $\{0, 2\}$ nous avons $3\varphi_3(x) \in K_n$ par hypothèse de récurrence. Cela implique que $\varphi_3(x) \in K_{n+1}$.

Si $x_1 = 2$ Alors

$$\varphi_3(x) = \frac{2}{3} + \sum_{k=2}^{\infty} \frac{x_k}{3^k}, \quad (7.497)$$

et

$$3\varphi_3(x) - 2 = \sum_{k=1}^{\infty} \frac{x_{k+1}}{3^k} = \varphi_3(x_2, \dots, x_{n+1}, \dots), \quad (7.498)$$

et donc là nous avons $3\varphi_3(x) - 2 \in K_n$, ce qui implique encore $\varphi_3(x) \in K_{n+1}$.

Sens réciproque Nous devons maintenant prouver que $\varphi_3(x) \in K_{n+1}$ implique $x_1, \dots, x_{n+1} \in \{0, 2\}$. Par le même calcul que précédemment nous avons soit

$$3\varphi_3(x) = \varphi_3(x_2, \dots, x_{n+1}, \dots), \quad (7.499)$$

si $x_1 = 0$, soit

$$3\varphi_3(x) - 2 = \varphi_3(x_2, \dots, x_{n+1}, \dots), \quad (7.500)$$

si $x_1 = 2$. Dans les deux cas, si $x_l = 1$ pour un certain $2 \leq l \leq n+1$, alors l'hypothèse de récurrence donne que ces éléments ne sont pas dans K_n et donc $\varphi_3(x)$ pas dans K_{n+1} . □

Corollaire 7.175.

En posant $\mathbb{E} = \{x \in \mathbb{D}_3 \text{ tel que } x_i \neq 1 \forall i\}$ nous avons $K = \varphi_3(\mathbb{E})$. Et plus précisément, $\varphi_3: \mathbb{E} \rightarrow K$ est une bijection.

Démonstration. Nous divisons la preuve en trois étapes.

Image contenue dans K Si $x \in \mathbb{E}$ et $n \in \mathbb{N}$ nous avons $x_1, \dots, x_n \in \{0, 2\}$ et donc $\varphi_3(x) \in K_n$ par la proposition 7.174. Donc

$$\varphi_3(x) \in \bigcup_{n \geq 1} K_n = K. \quad (7.501)$$

Injective L'application $\varphi_3: \mathbb{E} \rightarrow K$ est injective parce qu'elle est déjà injective depuis $\mathbb{D}_3$.

Surjective Soit $p \in K \subset [0, 1[$. Vu que $\varphi_3: \mathbb{D}_3 \rightarrow [0, 1[$ est surjective (théorème 6.174), il existe $x \in \mathbb{D}_3$ tel que $\varphi_3(x) = p$. Pour tout n nous avons $\varphi_3(x) \in K_n$ et donc $x_1, \dots, x_n \in \{0, 2\}$ et donc au final $x \in \mathbb{E}$. □

Proposition 7.176.

L'ensemble de Cantor est non dénombrable.

⁴¹. Pour comprendre pourquoi, faire un dessin de comment K_n se transforme en K_{n+1} et remarquer dans K_2 , les deux premiers segments ne sont pas une division du premier segment de K_1 , mais bien une copie des deux segments de K_1 .

Démonstration. Nous avons prouvé à la proposition 6.175 que l'ensemble $\mathbb{D}_2$ n'était pas dénombrable. Nous allons à présent prouver que l'application

$$\begin{aligned}\psi: \mathbb{D}_2 &\rightarrow K \\ c &\mapsto \varphi_3(c \text{ en remplaçant les } 1 \text{ par des } 2)\end{aligned}\tag{7.502}$$

est une bijection. Le fait que ψ soit injective est une conséquence du fait que ce soit la composition de deux applications injectives (le remplacement et φ_3). Il faut par contre montrer que l'image est égale à K , en notant qu'il n'est pas évident a priori que l'image soit contenue dans K .

L'opération qui consiste à remplacer les 1 par des 2 est une bijection $\mathbb{D}_2 \rightarrow \mathbb{E}$. Le corollaire 7.175 nous dit aussi que $\varphi_3: \mathbb{E} \rightarrow K$ est une bijection. En tant que composée de bijections, ψ est une bijection.

Étant en bijection avec $\mathbb{D}_2$ qui n'est pas dénombrable par la proposition 6.175, l'ensemble de Cantor n'est pas dénombrable. $\square$

Proposition 7.177 (Ensemble de Cantor).

L'ensemble de Cantor⁴² est borélien, non dénombrable et de mesure nulle.

Démonstration. Nous reprenons les notations de la définition 7.172. Le fait que l'ensemble de Cantor soit non dénombrable a été prouvé dans la proposition 7.176.

L'ensemble de Cantor étant une intersection dénombrable de boréliens, il est borélien par le lemme 7.3. Vu que $K_n \subset [0, 1[$ nous avons $\frac{1}{3}K_n \leq \frac{1}{3}$ et $\frac{1}{3}(K_n + 2) \geq \frac{2}{3}$, donc K_n est une union disjointe de 2^n intervalles de mesure $2/3^n$. Nous avons donc

$$\lambda(K_n) = \left(\frac{2}{3}\right)^n.\tag{7.503}$$

L'ensemble de Cantor étant contenu dans chacun des K_n , sa mesure est plus petite que la mesure de chacun des K_n (lemme 7.26) et donc $\lambda(K) \leq \left(\frac{2}{3}\right)^n$ pour tout n ; ergo $\lambda(K) = 0$. $\square$

7.7.4 Ensemble de Vitali (non mesurable)

Exemple 7.178(Un ensemble non mesurable au sens de Lebesgue)

Nous considérons[135] l'ensemble quotient $\mathbb{R}/\mathbb{Q}$; chaque classe intersecte l'intervalle $[0, 1]$. Grâce à l'axiome du choix (voir 1.2) nous pouvons construire un ensemble V contenant un représentant dans $[0, 1]$ de chaque classe. Un tel ensemble est un **ensemble de Vitali**. Nous allons prouver que V n'est pas mesurable.

Supposons que V soit mesurable. Alors tous les ensembles de la forme $V + q$ ($q \in \mathbb{Q}$) sont mesurables et ont même mesure par la proposition 7.165. Nous posons

$$A = \bigcup_{\substack{q \in \mathbb{Q} \\ -1 \leq q \leq 1}} (V + q) \subset [-1, 2].\tag{7.504}$$

Cela est une union disjointe d'ensembles mesurables. Donc

$$\lambda(A) = \sum_{\substack{q \in \mathbb{Q} \\ -1 \leq q \leq 1}} \lambda(V + q).\tag{7.505}$$

Vu que $A \subset [-1, 2]$ nous avons $\lambda(A) \leq 3$ et donc tous les termes de la somme doivent être nuls. Nous avons donc $\lambda(A) = 0$.

Prouvons toutefois que $[0, 1] \subset A$, ce qui serait une contradiction. Soit $x \in [0, 1]$; il est dans une des classes de $\mathbb{R}/\mathbb{Q}$ et donc il existe $v \in V$ tel que $x - v \in \mathbb{Q}$. De plus $x, v \in [0, 1]$, donc

$$-1 \leq x - v \leq 1.\tag{7.506}$$

Cela fait que $x \in V + (x - v) \subset A$. Nous avons donc $x \in A$ et donc $[0, 1] \subset A$. En conséquence de quoi nous aurions $\lambda(A) \geq 1$. $\triangle$

42. Définition 7.172

7.8 Tribu et mesure de Lebesgue sur $\mathbb{R}^d$

Quelques liens internes :

- Le produit de tribus est donné par la définition 7.139,
- le produit d'espaces mesurés est donné par la définition 7.149.

La mesure de Lebesgue sur $\mathbb{R}^d$, notée λ_N est d'abord la mesure définie sur

$$(\mathbb{R}^d, \mathcal{B}(\mathbb{R}) \otimes \dots \otimes \mathcal{B}(\mathbb{R})) \quad (7.507)$$

comme le produit $\lambda \otimes \dots \otimes \lambda$. Ensuite nous nous souvenons du corollaire 7.143 qui donne λ_N comme une mesure sur

$$(\mathbb{R}^N, \mathcal{B}(\mathbb{R}^N)). \quad (7.508)$$

Et enfin λ_N est la complétion de cette mesure.

Proposition 7.179 ([136]).

Tout ouvert de $\mathbb{R}^n$ est une union dénombrable et disjointe de cubes semi-ouverts.

Démonstration. Nous allons même montrer que ces cubes peuvent être choisis sur un quadrillage.

Soit G un ouvert de $\mathbb{R}^n$. Soit $\{Q_i^1\}_{i \in \mathbb{N}}$ un découpage de $\mathbb{R}^n$ en cubes semi-ouverts de côté 1 et dont les sommets sont en les coordonnées entières. Ils sont de la forme

$$\prod_{i=1}^n [n_i, n_i + 1[\quad (7.509)$$

où les n_i sont des entiers. Ce sont des cubes disjoints. Nous considérons ensuite pour chaque $k > 1$ le découpage $\{Q_i^{(k)}\}_{i \in \mathbb{N}}$ de $\mathbb{R}^n$ en cubes de côtés 2^{-k} qui consiste à découper en 2 les côtés des cubes du découpage $Q^{(k-1)}$. Ces cubes forment encore un découpage dénombrable de $\mathbb{R}^n$ en des cubes disjoints. Ils sont de la forme

$$\prod_{i=1}^n \left[\frac{n_i}{2^k}, \frac{n_i + 1}{2^k} \right[\quad (7.510)$$

où les n_i sont encore entiers. Ensuite nous considérons $\mathcal{E}$ l'union de tous les $Q_i^{(k)}$ contenus dans G .

Montrons que $\mathcal{E} = G$. D'abord $\mathcal{E} \subset G$ parce que $\mathcal{E}$ est une union d'ensembles contenus dans G . Ensuite si $x \in G$, il existe une boule de rayon r autour de x contenue dans G ; alors un des ensembles $Q_i^{(k)}$ avec $2^{-j} < \frac{r}{2}$ est contenue dans $B(x, r)$ et donc dans $\mathcal{E}$.

Bien entendu l'union qui donne $\mathcal{E}$ n'est pas satisfaisante par ce que les $Q_i^{(k+1)}$ sont contenus dans les $Q_i^{(k)}$; les intersections sont donc loin d'être vides.

Nous faisons ceci :

$$R^{(0)} = \{Q_i^{(1)} \text{ contenu dans } G\} \quad (7.511a)$$

$$R^{(k+1)} = \{Q_i^{(k+1)} \text{ contenus dans } G \text{ et pas dans } R^{(k)}\}. \quad (7.511b)$$

En fin de compte l'union de tous les ensembles contenus dans les $R^{(k)}$ forment encore $\mathbb{R}^n$, mais sont d'intersection vide. $\square$

Les cubes dont il est question dans cette preuve, de côtés 2^{-k} sont souvent appelés des cubes **dyadiques**.

Corollaire 7.180 ([136]).

Tout ouvert de $\mathbb{R}^n$ est une union dénombrable de cubes presque disjoints⁴³.

Démonstration. Il suffit de prendre les cubes de la proposition 7.179 et de les fermer. Ce que l'on ajoute est de mesure nulle. $\square$

43. «presque» au sens où les intersections éventuelles sont de mesure de Lebesgue nulle.

Remarque 7.181.

La proposition 7.179 est une propriété seulement de la topologie de $\mathbb{R}^n$ alors que le corollaire fait intervenir la mesure de Lebesgue parce qu'il faut bien dire que les intersections sont de mesure (de Lebesgue) nulle.

7.8.1 Ensembles négligeables**Lemme 7.182** ([137]).

L'image d'une partie négligeable de $\mathbb{R}^N$ par une application Lipschitz est négligeable.

Démonstration. Soit N une partie négligeable de $\mathbb{R}^N$ et une application Lipschitz $f: N \rightarrow \mathbb{R}^N$. Soit $Q \subset \mathbb{R}^N$ un cube borné de côté r . Pour tout $x, x' \in N \cap Q$ nous avons

$$\|f(x) - f(x')\| \leq C\|x - x'\| \leq Cr. \quad (7.512)$$

Donc $f(N \cap Q)$ est dans une boule de rayon Cr . Mais comme toutes les normes sont équivalentes⁴⁴ sur $\mathbb{R}^N$ nous pouvons tout aussi bien prendre la norme $\|\cdot\|_1$ au lieu de la norme $\|\cdot\|_2$ (qui est toujours la norme prise implicitement lorsqu'on parle de $\mathbb{R}^n$), de telle sorte que les boules soient des cubes. Quoi qu'il en soit, $f(N \cap Q)$ est contenu dans un cube de côté $2Cr$ et au niveau de la mesure extérieure,

$$m^*(f(N \cap Q)) \leq (2Cr)^N = (2C)^N r^N, \quad (7.513)$$

ou encore

$$m(f(N \cap Q)) \leq (2C)^N m(Q) \quad (7.514)$$

parce que r^N est la mesure du cube Q .

Soit maintenant $\epsilon > 0$; vu que N est négligeable, il existe un ouvert U contenant N et tel que $m(U) < \epsilon$. Ce U est une union presque disjointe de cubes dyadiques (Q_n) par le corollaire 7.180. Nous avons alors

$$m^*(f(N)) = m^*\left(f\left(\bigcup_n N \cap Q_n\right)\right) \quad (7.515a)$$

$$= m^*\left(\bigcup_n f(N \cap Q_n)\right) \quad (7.515b)$$

$$\leq \sum_n m^*(f(N \cap Q_n)) \quad (7.515c)$$

$$\leq \sum_n (2C)^N m(Q_n) \quad (7.515d)$$

$$= (2C)^N m(U) \quad (7.515e)$$

$$< (2C)^d \epsilon. \quad (7.515f)$$

Au final, $m^*(f(N)) \leq (2C)^N \epsilon$. L'ensemble N est donc négligeable parce que le lemme 7.57 le dit : $m^*(N) = 0$. $\square$

Corollaire 7.183.

Un sous-espace vectoriel strict de $\mathbb{R}^N$ est négligeable.

Démonstration. Un sous-espace vectoriel strict de $\mathbb{R}^N$ de dimension $k < N$ est l'image de

$$A = \{t_1 e_1 + \dots + t_k e_k \text{ tel que } t_i \in \mathbb{R}\} \quad (7.516)$$

par une application linéaire. Ce A est un pavé de mesure de Lebesgue nulle. Donc l'image est négligeable par le lemme 7.182. $\square$

44. Proposition 6.138

7.8.2 Parties et fonctions mesurables

Pour rappel, la notion d'application de classe C^1 est donnée par la définition 6.213.

Proposition 7.184.

Soient U et V des ouverts de $\mathbb{R}^N$ et $\phi: U \rightarrow V$ un C^1 -difféomorphisme. Si $E \subset U$ est mesurable, alors $\phi(E)$ est mesurable⁴⁵.

Démonstration. Si E est mesurable, il existe un borélien B et un ensemble négligeable N tels que $E = B \cup N$. Vu que ϕ est un homéomorphisme, l'application ϕ^{-1} est borélienne parce que continue (théorème 7.72). Nous avons

$$\phi(B) = (\phi^{-1})^{-1}(B), \quad (7.517)$$

c'est à dire que $\phi(B)$ est l'image inverse de B par ϕ^{-1} . L'ensemble $\phi(B)$ est donc borélien.

Il reste à voir que $\phi(N)$ est négligeable. Soit $Q \subset U$ une cube compact. L'application $d\phi: Q \rightarrow \mathcal{L}(\mathbb{R}^N, \mathbb{R}^N)$ est continue et donc bornée (par la remarque 6.214) sur le compact Q . Par les accroissements finis (théorème 6.231), l'application ϕ est donc Lipschitz sur Q . La partie $\phi(N \cap Q)$ est alors négligeable par le lemme 7.182. Pour conclure,

$$\phi(N) = \bigcup_i \phi(N \cap Q_i) \quad (7.518)$$

où les Q_i sont tous des cubes compacts. Donc $\phi(N)$ est une union dénombrable d'ensembles négligeables ; ergo négligeable lui-même par le lemme 7.49. $\square$

Proposition 7.185.

Soient U et V des ouverts de $\mathbb{R}^N$ et $\phi: U \rightarrow V$ un C^1 -difféomorphisme. Si $f: V \rightarrow \mathbb{C}$ est mesurable, alors $f \circ \phi: U \rightarrow \mathbb{C}$ l'est.

Démonstration. Soit A une partie mesurable de $\mathbb{C}$. Il nous faut prouver que

$$(f \circ \phi)^{-1}(A) = \phi^{-1}(f^{-1}(A)) \quad (7.519)$$

soit mesurable. Par hypothèse, $f^{-1}(A)$ est mesurable. Vu que ϕ est un C^1 -difféomorphisme, elle et son inverse sont mesurables par la proposition 7.184. Donc l'image du mesurable $f^{-1}(A)$ par ϕ^{-1} est encore mesurable. $\square$

7.8.3 Propriétés d'unicité

Corollaire 7.186.

La mesure λ_N est l'unique mesure sur $(\mathbb{R}^N, \mathcal{B}or(\mathbb{R}^N))$ à satisfaire

$$\mu\left(\prod_{i=1}^N [a_i, b_i]\right) = \prod_{i=1}^n |a_i - b_i| \quad (7.520)$$

Démonstration. Par définition de la mesure produit, λ_N est l'unique mesure sur $(\mathbb{R}^N, \mathcal{B}or(\mathbb{R}) \otimes \dots \otimes \mathcal{B}or(\mathbb{R}))$ à satisfaire la condition. La proposition 7.143 conclut. $\square$

Vu que les compacts de $\mathbb{R}^n$ sont les fermés bornés (théorème 5.107), et que tout borné est dans un tel produit d'intervalle, la mesure de Lebesgue est une mesure de Borel (définition 7.78(1)).

Théorème 7.187 ([138]).

La mesure de Lebesgue est invariante par translation. Autrement dit si A est mesurable dans $\mathbb{R}^n$ et si $a \in \mathbb{R}^n$ alors $A + a$ est mesurable et

$$\lambda_N(A + a) = \lambda_N(A). \quad (7.521)$$

45. Ici «mesurable» parle de mesurabilité au sens de la tribu de Lebesgue, c'est à dire pas seulement les boréliens.

Démonstration. Nous supposons que A est borélien ; sinon il l'est à ensemble négligeable près. Nous notons t_a la translation et nous nommons μ la mesure donnée par

$$\mu(A) = \lambda_N(A + a). \quad (7.522)$$

Vu que

$$\mu\left(\prod_{n=1}^N [r_n, s_n[\right) = \lambda_N\left(\prod_i [r_n + a_n, s_n + a_n[\right) = \prod_i |s_n - r_n|. \quad (7.523)$$

Vu qu'il y a unicité de la mesure vérifiant cette propriété (corollaire 7.186), nous avons $\mu = \lambda_N$. $\square$

Pour la suite nous notons Q_0 le cube unité de $\mathbb{R}^N$: $Q_0 = ([0, 1])^N$.

Théorème 7.188 ([138]).

Soit μ une mesure positive sur $\mathbb{R}^N$ telle que

(1) μ soit invariante par translation (des boréliens),

(2) $\mu(Q_0) = 1$.

Alors $\mu = \lambda_N$.

Démonstration. Pour simplifier l'écriture nous faisons $N = 2$. Notre but est de prouver que $\mu([0, r[\times [0, r'[) = rr'$ pour tout $r, r' \in \mathbb{R}$.

Longueur $= 1/J$ Soient J, K des entiers. Nous pouvons diviser le cube Q_0 en rectangles de cotés $1/J$ et $1/K$:

$$Q_0 = \bigcup_{\substack{1 \leq j \leq J \\ 1 \leq k \leq K}} \left[\frac{j-1}{J}, \frac{j}{J} \right[\times \left[\frac{k-1}{K}, \frac{k}{K} \right[\quad (7.524)$$

où l'union est disjointe. En ce qui concerne la mesure nous commençons par utiliser la sous-additivité :

$$\mu(Q_0) = \sum_{\substack{1 \leq j \leq J \\ 1 \leq k \leq K}} \mu\left(\left[\frac{j-1}{J}, \frac{j}{J} \right[\times \left[\frac{k-1}{K}, \frac{k}{K} \right[\right). \quad (7.525)$$

Nous utilisons ensuite, sur chacun des termes séparément l'invariance par translation selon les vecteurs $(\frac{j-1}{J}, 0)$ et $(0, \frac{k-1}{K})$:

$$1 = \mu(Q_0) = \sum_{\substack{1 \leq j \leq J \\ 1 \leq k \leq K}} \mu\left(\left[0, \frac{1}{J} \right[\times \left[0, \frac{1}{K} \right[\right) = JK \mu\left(\left[0, \frac{1}{J} \right[\times \left[0, \frac{1}{K} \right[\right), \quad (7.526)$$

et donc

$$\mu\left(\left[0, \frac{1}{J} \right[\times \left[0, \frac{1}{K} \right[\right) = \frac{1}{J} \times \frac{1}{K}. \quad (7.527)$$

Longueur L/K Soient L, M des entiers et calculons :

$$\mu\left(\left[\frac{0}{J}, \frac{L}{J} \right[\times \left[\frac{0}{K}, \frac{M}{K} \right[\right) = \sum_{\substack{0 \leq l \leq L-1 \\ 0 \leq m \leq M-1}} \mu\left(\left[\frac{l}{J}, \frac{l+1}{J} \right[\times \left[\frac{m}{K}, \frac{m+1}{K} \right[\right) \quad (7.528a)$$

$$= LM \mu\left(\left[\frac{0}{J}, \frac{1}{J} \right[\times \left[\frac{0}{K}, \frac{1}{K} \right[\right) \quad (7.528b)$$

$$= LM \times \frac{1}{J} \times \frac{1}{K}. \quad (7.528c)$$

Nous avons donc, pour tout J, K, L, M :

$$\mu\left(\left[0, \frac{L}{J} \right[\times \left[0, \frac{M}{K} \right[\right) = \frac{L}{J} \times \frac{M}{K}, \quad (7.529)$$

c'est à dire que pour tout $r, s \in \mathbb{Q}^+$ nous avons

$$\mu([0, r[\times [0, s[) = rs. \quad (7.530)$$

Longueur réelle Nous passons au cas de longueur réelle. Soit $a > 0$ et une suite croissante de rationnels $r_n \rightarrow a$. Une telle suite existe par la proposition 5.42. Nous avons $[0, a[= \bigcup_{n \geq 1} [0, r_n[$ où l'union n'est pas disjointe mais croissante, ce qui permet d'utiliser le lemme 7.27(1) pour écrire

$$\mu([0, a]) = \mu\left(\bigcup_{n \geq 1} [0, r_n[\right) = \lim_{n \rightarrow \infty} \mu([0, r_n]) = \lim_{n \rightarrow \infty} r_n = a. \quad (7.531)$$

Enfin, si $a, a' \in \mathbb{R}$, l'invariance par translation donne

$$\mu([a, a']) = \mu([0, a' - a]) = a' - a. \quad (7.532)$$

Par unicité de la mesure ayant cette propriété, nous avons $\mu = \lambda_N$. $\square$

Corollaire 7.189.

Si μ est une mesure positive sur $\mathbb{R}^N$ invariante par translation et telle que $\mu(Q_0) = C < \infty$ alors $\mu = C\lambda_N$.

Démonstration. Si $C > 0$ nous considérons la mesure $\frac{1}{C}\mu$ qui vérifie $(\frac{1}{C}\mu)(Q_0) = 1$. En conséquence du théorème 7.188, $\frac{1}{C}\mu = \lambda_N$ et $\mu = C\lambda_N$.

Si au contraire $C = 0$ alors nous pouvons paver $\mathbb{R}^N$ avec des cubes Q_i de côté 1 qui ont tous mesure 0. Par conséquent, $\mathbb{R}^N = \bigcup_{i=1}^{\infty} Q_i$, donc $\mu(\mathbb{R}^N) = \sum_i \mu(Q_i) = 0$. Par conséquent $\mu = 0$ parce que toute partie de $\mathbb{R}^N$ a une mesure au maximum égale à celle de $\mathbb{R}^N$. $\square$

7.8.4 Régularité

Les différentes notions de régularité pour une mesure sont données dans la définition 7.78. Ce sont essentiellement des questions de compatibilité entre la mesure et la topologie.

Proposition 7.190.

La mesure de Lebesgue est une mesure de Radon sur tout ouvert de $\mathbb{R}^N$.

Démonstration. Soit V un ouvert de $\mathbb{R}^N$. C'est localement compact et dénombrable à l'infini. Il suffit de prouver que λ_N est de Borel sur V pour que le théorème 7.79 conclue à la régularité de la mesure de Lebesgue.

Soit K un compact de V . Par la proposition 5.59 c'est également un compact de $\mathbb{R}^N$. Par conséquent K est dans un pavé fermé de $\mathbb{R}^N$ du type

$$K \subset \prod_{n=1}^N [a_n, b_n] \quad (7.533)$$

et donc en passant par le corollaire 7.186,

$$\lambda_N(K) \leq \prod_{i=1}^N (b_n - a_n) < \infty. \quad (7.534)$$

Nous avons démontré que λ_N reste fini sur tout compact de V . $\square$

Chapitre 8

Espaces affines

Ce chapitre provient principalement de [21].

Définition 8.1.

Soit E , un espace vectoriel. Un **espace affine** modelé sur E est un ensemble $\mathcal{E}$ sur lequel le groupe¹ $(E, +)$ agit à droite transitivement et librement.

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 .

Remarque 8.2.

Lorsque nous écrivons « $M + x$ », le symbole plus n'est pas une loi de composition interne de $\mathcal{E}$, mais une action.

Soient $N, M \in \mathcal{E}$. Par liberté et transitivité de l'action, il existe un unique $x \in E$ tel que $M + x = N$. Ce vecteur x sera noté $\overrightarrow{MN}$.

Proposition 8.3.

Si $A, B, C \in \mathcal{E}$ nous avons les égalités suivantes dans E :

- (1) $AB + BC = AC$ (relations de Chasles),
- (2) $AA = 0$,
- (3) $AB = -AB$.

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 $\mathbb{K}$.

8.1 Repères affines

Soit E un $\mathbb{K}$ -espace vectoriel de dimension n et $\mathcal{E}$ un espace affine construit sur E .

Définition 8.4.

Un **multipléte** $(A, e_1, \dots, e_n)$ où A est un point de $\mathcal{E}$ et $\{e_i\}$ est une base de E est un **repère cartésien** de $\mathcal{E}$.

Un tel repère donne une bijection

$$\begin{aligned} \phi: \mathbb{K}^n &\rightarrow \mathcal{E} \\ (x_1, \dots, x_n) &\mapsto A + \sum_i x_i e_i. \end{aligned} \tag{8.1}$$

1. Voir exemple 2.69.

Ces nombres x_i sont les **coordonnées** du point $A + \sum_i x_i e_i$ dans le repère (A, e_i) .

Soient (A, e_i) et (A', e'_i) deux repères cartésiens pour l'espace affine $\mathcal{E}$. Soit (a_{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

$$A + \sum_i x_i e_i = A' + \sum_i x'_i e'_i. \quad (8.2)$$

Nous considérons les coordonnées (a_i) de A' dans le repère (A, e_i) , c'est à dire

$$A' = A + \sum_i a_i e_i. \quad (8.3)$$

En substituant $e'_i = \sum_k a_{jk} e_k$ et (8.3) dans (8.2) nous trouvons

$$\sum_k x_k e_k = \sum_k a_k e_k + \sum_{jk} a_{jk} x'_j e_k, \quad (8.4)$$

et par conséquent

$$x_k = a_k + \sum_j a_{jk} x'_j. \quad (8.5)$$

8.2 Classification affine des conique

Soit une conique $f(x, y) = 0$ avec

$$f(x, y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f \quad (8.6)$$

dans le repère $R = (A, e_i)$. La signature de la quadratique

$$q(x, y) = ax^2 + 2bx + cy^2 \quad (8.7)$$

ne dépend pas de la base choisie et un changement de variables

$$\begin{cases} \tilde{x} = \alpha x + \beta y \\ \tilde{y} = \gamma x + \delta y \end{cases} \quad (8.8a)$$

$$\quad (8.8b)$$

peut nous amener dans trois cas :

$$q(x, y) = \begin{cases} \tilde{x}^2 + \tilde{y}^2 & \text{genre ellipse} \\ \tilde{x}^2 - \tilde{y}^2 & \text{genre hyperbole} \\ \tilde{x}^2 & \text{genre parabole.} \end{cases} \quad (8.9)$$

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

$$\begin{cases} x = x_0 + \tilde{x} \\ y = y_0 + \tilde{y}. \end{cases} \quad (8.10a)$$

$$\quad (8.10b)$$

Un peu de calcul montre qu'alors la conique s'écrit

$$f(x_0, y_0) + q(\tilde{x}, \tilde{y}) + (2ax_0 + 2by_0 + 2d)\tilde{x} + (2bx_0 + 2cy_0 + 2e)\tilde{y} = 0. \quad (8.11)$$

Le point I sera un centre de symétrie si les termes linéaires en $\tilde{x}$ et $\tilde{y}$ s'annulent, c'est à dire si

$$\begin{cases} ax_0 + by_0 + d = 0 \\ bx_0 + cy_0 + e = 0. \end{cases} \quad (8.12a)$$

$$\quad (8.12b)$$

Nous supposons que $(d, e) \neq (0, 0)$, sinon la conique de départ serait déjà centrée. Le déterminant du système (8.12) est

$$\delta = ac - b^2. \quad (8.13)$$

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 pas de 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 8.5

Soit

$$f(x, y) = x^2 + 2xy - y^2 - 6x + 2y - 1 = 0 \quad (8.14)$$

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

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (8.15)$$

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 posant $x = \tilde{x} + x_0$, $y = \tilde{y} + y_0$. Le système à résoudre est

$$\begin{cases} x_0 + y_0 - 3 = 0 \\ x_0 - y_0 + 1 = 0, \end{cases} \quad (8.16a) \quad (8.16b)$$

dont 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

$$R' = (I, \{e_i\}) \quad (8.17)$$

avec $I = A + x_0 e_1 + y_0 e_2$ où A est l'origine du repère dans lequel l'équation (8.14) était donnée.

Par construction dans ce repère nous avons la conique

$$f(x_0, y_0) + q(\tilde{x}, \tilde{y}) = 0, \quad (8.18)$$

c'est à dire

$$\tilde{x}^2 + 2\tilde{x}\tilde{y} - \tilde{y}^2 = 0. \quad (8.19)$$

Maintenant là nous avons une quadrique centrée nous voulons la mettre sous une forme plus canonique :

$$\left(\frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y})\right)^2 - \tilde{y}^2 - 1 = 0. \quad (8.20)$$

Nous posons donc

$$\begin{cases} X = \frac{1}{\sqrt{2}}(\tilde{x} + \tilde{y}) \\ Y = \tilde{y}, \end{cases} \quad (8.21a) \quad (8.21b)$$

et nous trouvons l'hyperbole

$$X^2 - Y^2 - 1 = 0. \quad (8.22)$$

Cela revient à faire le changement de base

$$\begin{cases} e'_1 = \sqrt{2}e_1 \\ e'_2 = -e_1 + e_2. \end{cases} \quad (8.23a) \quad (8.23b)$$

Pour rappel, les vecteurs de bases se transforment avec la matrice inverse des coefficients. Étant donné que

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \tilde{x} \\ \tilde{y} \end{pmatrix}, \quad (8.24)$$

nous avons

$$\begin{pmatrix} e'_1 \\ e'_2 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}. \quad (8.25)$$

C'est de là que provient le changement (8.23). $\triangle$

8.3 Applications affines

Définition 8.6.

Soient $\mathcal{E}$ et $\mathcal{E}'$ deux espaces affines sur les espaces vectoriels E et E' (sur le même corps $\mathbb{K}$). Une application $f: \mathcal{E} \rightarrow \mathcal{E}'$ est dite **affine** si il existe une application linéaire $u: E \rightarrow E'$ telle que pour tout $M \in \mathcal{E}$ on ait

$$f(M + x) = f(M) + u(x). \quad (8.26)$$

Remarque 8.7.

La condition (8.26) pour tout $M \in \mathcal{E}$ est équivalente à demander

$$f \circ t_x = t_{u(x)} \circ f \quad (8.27)$$

pour tout $x \in E$.

Proposition 8.8.

Soit f une application affine.

(1) Une application linéaire vérifiant la condition (8.26) est unique. Nous la noterons u_f .

(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.

Si $\mathcal{E}$ et $\mathcal{E}'$ ont même dimension finie, alors en plus f est injective si et seulement si f est surjective.

Remarque 8.9.

La fonction linéaire u_f qui vérifie $f(M + x) = f(M) + u_f(x)$ ne dépend pas du point M . En effet si

$$f(M + x) = f(M) + u(x) \quad (8.28a)$$

$$f(N + y) = f(N) + v(y). \quad (8.28b)$$

En effet si $N = M + a$ nous avons d'une part que

$$f(N + y) = f(M + y + a) = f(M) + u(y + a), \quad (8.29)$$

et d'autre part

$$f(N + y) = f(M + a) + v(y) = f(M) + u(a) + v(y). \quad (8.30)$$

Par conséquent $u = v$.

Proposition 8.10.

Si $f: \mathcal{E} \rightarrow \mathcal{E}'$ et $g: \mathcal{E} \rightarrow \mathcal{E}''$ sont des applications affines, alors $g \circ f: \mathcal{E} \rightarrow \mathcal{E}''$ est affine et $u_{g \circ f} = u_g \circ u_f$.

Démonstration. Si $M \in \mathcal{E}$ et $x \in E$ nous avons

$$\begin{aligned} (g \circ f)(M + x) &= g(f(M) + u_f(x)) \\ &= g(f(M)) + u_g(u_f(x)) \\ &= (g \circ f)(M) + (u_g \circ u_f)(x). \end{aligned} \quad (8.31)$$

□

Théorème 8.11.

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 $f: \mathcal{E} \rightarrow \mathcal{E}'$ 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

$$f(x) = b + ax. \quad (8.32)$$

Remarque 8.12.

L'équation (8.32) 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 $(A, \{e_i\})$.

8.4 Isomorphismes

Définition 8.13.

Un **isomorphisme** entre les espaces affines $\mathcal{E}$ et $\mathcal{E}'$ est une application affine $f: \mathcal{E} \rightarrow \mathcal{E}'$ inversible dont l'inverse est affine.

Proposition 8.14.

Une application affine bijective est un isomorphisme. Si f est un isomorphisme d'espaces affines, alors $u_{f^{-1}} = (u_f)^{-1}$.

Proposition 8.15.

Un espace affine de dimension finie n sur un corps $\mathbb{K}$ est isomorphe à l'espace affine canonique $\mathcal{E}_n(\mathbb{K})$.

Démonstration. Si nous considérons le repère $R = (A, \{e_i\})$ de l'espace affine $\mathcal{E}$ alors l'application

$$\begin{aligned} \varphi: \mathbb{K}^n &\rightarrow \mathcal{E} \\ (x_1, \dots, x_n) &\mapsto A + \sum_i x_i e_i \end{aligned} \quad (8.33)$$

est un isomorphisme. □

8.5 Sous espaces affines

Définition 8.16.

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

$$F = \{AB \text{ tel que } A, B \in \mathcal{F}\} \quad (8.34)$$

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 8.17.

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 $f: \mathcal{E} \rightarrow \mathbb{K}^{n-k}$ telle que $\mathcal{F} = f^{-1}(0)$.

Démonstration. Soit F la direction de $\mathcal{F}$ et $A \in \mathcal{F}$. Nous considérons une base $\{e_i\}$ adaptée à F au sens $\{e_1, \dots, e_k\}$ est une base de F . Nous considérons maintenant le repère cartésien $(A, \{e_i\})$

avec $A \in \mathcal{F}$ et nous construisons l'application affine

$$f: \mathcal{E} \rightarrow \mathbb{K}^{n-k}$$

$$A + \sum_{i=1}^n x_i e_i \mapsto \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}. \quad (8.35)$$

Par construction nous avons $f(M) = 0$ si et seulement si $M \in \mathcal{F}$. $\square$

Proposition 8.18 ([21]).

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

$$F = \text{Span}\{\overrightarrow{AM} \text{ tel que } M \in \sigma\}. \quad (8.36)$$

Le sous-espace affine donné par la proposition 8.18 est le sous-espace affine **engendré** par la partie σ , et il est noté $\text{eae}(\sigma)$.

Proposition 8.19.

Soit $\mathcal{E}$ un espace affine de dimension n sur $\mathbb{K}$, soit $f: \mathcal{E} \rightarrow \mathbb{K}^r$ une fonction affine. Pour tout $a = (a_1, \dots, a_r) \in \mathbb{K}^r$, l'ensemble $f^{-1}(a)$ est un sous-espace affine de dimension $\dim \ker(u_f)$.

Démonstration. Nous considérons le repère $(A, \{e_i\})$ de $\mathcal{E}$. Étant donné que f est affine nous avons

$$f\left(A + \sum_i x_i e_i\right) = f(A) + u_f\left(\sum_i x_i e_i\right). \quad (8.37)$$

Nous avons donc $f\left(A + \sum_i x_i e_i\right) = a$ lorsque

$$u_f\left(\sum_i x_i e_i\right) = a - f(A). \quad (8.38)$$

Nous avons donc

$$f^{-1}(a) = A + (u_f)^{-1}(a - f(A)), \quad (8.39)$$

dont la dimension est le rang de $(u_f)^{-1} = u_{f^{-1}}$ (proposition 8.14). Le rang de $(u_f)^{-1}$ est la dimension du noyau de u_f . $\square$

Proposition 8.20.

Soit A un ensemble convexe dans un espace vectoriel et $v_1, \dots, v_n$ des éléments de A . Alors toute combinaison

$$a_1 v_1 + \dots + a_n v_n \quad (8.40)$$

telle que $a_1 + \dots + a_n = 1$ 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

$$t_2(t_1 v_1 + (1 - t_1)v_2) + (1 - t_2)v_3 = a v_1 + b v_2 + c v_3. \quad (8.41)$$

La réponse est immédiatement donnée par

$$t_2 a = 1 - c \quad (8.42a)$$

$$t_1 = a/t_2. \quad (8.42b)$$

Étant donné que $c \in [0, 1]$ nous avons $t_2 \in [0, 1]$. En ce qui concerne t_1 nous avons

$$t_1 = \frac{a}{t_2} \leq \frac{1 - c}{1 - c} = 1. \quad (8.43)$$

$\square$

8.6 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 8.21 ([139]).

Soit une famille de points pondérés $\{(A_i, \lambda_i)\}_{i=1\dots r}$. Si $\sum_i \lambda_i \neq 0$, alors il existe un unique $G \in \mathcal{E}$ tel que

$$\sum_{i=1}^r \lambda_i \overrightarrow{GA_i} = 0. \quad (8.44)$$

Le point G donné par le lemme 8.21 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 8.22 (Combinaison convexe).

Des nombres $\lambda_1, \dots, \lambda_n$ vérifiant $\sum_i \lambda_i = 1$ forment une **combinaison convexe**.

Le théorème suivant donne quelques caractérisations équivalentes du barycentre.

Théorème 8.23 ([139]).

Soient $\{(A_i, \lambda_i)\}_{i=1,\dots,r}$ une famille de points pondérés. Les conditions suivantes sur le point $G \in \mathcal{E}$ sont équivalentes.

- (1) Le point G est 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 $(\sum_i \lambda_i) \overrightarrow{AG} = \sum_i \lambda_i \overrightarrow{AA_i}$.
- (4) Pour tout $B \in \mathcal{E}$, nous avons $(\sum_i \lambda_i) \overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}$.

Définition 8.24.

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 $(A_i, 1)$.

Proposition 8.25.

Une partie $\mathcal{F}$ des $\mathcal{E}$ est un sous-espace affine si et seulement si elle est stable par barycentrisation.

Démonstration. Soit $\mathcal{F}$ une sous-espace affine de direction F et $A_1, \dots, A_n$ 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 8.23 : pour tout $B \in \mathcal{F}$,

$$\overrightarrow{BG} = \sum_i \lambda_i \overrightarrow{BA_i}. \quad (8.45)$$

Vu que 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

$$F = \{\overrightarrow{AB} \text{ tel que } A, B \in \mathcal{F}\} \quad (8.46)$$

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

$$\overrightarrow{AV} = \overrightarrow{AX} + \overrightarrow{AY}. \quad (8.47)$$

Par les relations de Chasles,

$$\overrightarrow{AV} = \overrightarrow{AV} + \overrightarrow{VX} + \overrightarrow{AV} + \overrightarrow{VY}, \quad (8.48)$$

donc

$$0 = \overrightarrow{VX} - \overrightarrow{VA} + \overrightarrow{VY}, \quad (8.49)$$

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

$$\overrightarrow{AW} = \mu \overrightarrow{AX} = \mu(\overrightarrow{AW} + \overrightarrow{WX}), \quad (8.50)$$

ce qui signifie que

$$(1 - \mu)\overrightarrow{AW} + \mu\overrightarrow{XW} = 0 \quad (8.51)$$

et que W est un barycentre.

Afin de montrer que (8.46) 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

$$\overrightarrow{AX} + \overrightarrow{BY} = \overrightarrow{AX} + \overrightarrow{BA} + \overrightarrow{AY} \quad (8.52a)$$

$$= \overrightarrow{AV} + \overrightarrow{BA} \quad V \text{ est celui donné plus haut} \quad (8.52b)$$

$$= \overrightarrow{AV} - \overrightarrow{AB} \quad (8.52c)$$

$$= \overrightarrow{AV} + \overrightarrow{AW} \quad W \text{ est donné par } \mu = -1. \quad (8.52d)$$

$$= \overrightarrow{AV'}. \quad (8.52e)$$

□

Proposition 8.26 ([139]).

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

$$G = A_0 + \overrightarrow{A_0G} = A_0 + \sum_{i=1}^r \lambda_i \overrightarrow{A_0A_i}. \quad (8.53)$$

Notons que les vecteurs $\overrightarrow{A_0A_i}$ sont dans la direction du sous-espace affine engendré par les A_i par (8.36). Donc G est bien dans $\mathcal{F}$.

Inversement si X est dans $\mathcal{F}$, on a

$$X = A_0 + \sum_i \lambda_i \overrightarrow{A_0A_i} \quad (8.54)$$

parce que $\sum_i \lambda_i \overrightarrow{A_0A_i}$ est un élément général de la direction de $\mathcal{F}$. Du coup

$$\overrightarrow{A_0X} = \sum_i \lambda_i \overrightarrow{A_0A_i}, \quad (8.55)$$

et en utilisant la relation de Chasles sur chacun des $\overrightarrow{A_0A_i}$,

$$\overrightarrow{A_0X} = \sum_i \lambda_i (\overrightarrow{A_0X} + \overrightarrow{XA_i}). \quad (8.56)$$

De là nous concluons que

$$(1 - \sum_i \lambda_i) \overrightarrow{A_0X} + \sum_i \lambda_i \overrightarrow{XA_i} = 0, \quad (8.57)$$

ce qui signifie précisément que X est un barycentre des A_i . □

Proposition 8.27.

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

$$\text{Span}\{\overrightarrow{A_0 A_{i=1, \dots, r}}\} \quad (8.58)$$

qui est engendré par r vecteurs et donc est au plus de dimension r . $\square$

En deux mots, la proposition suivante signifie que le barycentre des barycentres est le barycentre.

Proposition 8.28 (Associativité des barycentres[140]).

Soit $I = \{0, 1, \dots, n\}$ et une partition $I = J_0 \cup \dots \cup J_r$. 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

$$0 = \sum_{k=0}^r \mu_k \overrightarrow{bb_k} \quad (8.59a)$$

$$= \sum_k \sum_{i \in J_k} \lambda_i \overrightarrow{bb_k} \quad (8.59b)$$

$$= \sum_{k=0}^r \sum_{i \in J_k} \lambda_i (\overrightarrow{ba_i} + \overrightarrow{a_i b_k}) \quad (8.59c)$$

$$= \sum_{k=0}^r \sum_{i \in J_k} \lambda_i \overrightarrow{ba_i} + \underbrace{\sum_{k=0}^r \sum_{i \in J_k} \lambda_i \overrightarrow{a_i b_k}}_{=0} \quad (8.59d)$$

$$= \sum_{i \in I} \lambda_i \overrightarrow{ba_i}. \quad (8.59e)$$

Donc b est bien barycentre des a_i avec les poids λ_i . $\square$

8.6.1 Enveloppe convexe**Définition 8.29.**

Soit A une partie d'un espace vectoriel E . L'**enveloppe convexe** de A , notée $\text{Conv}(A)$ est l'intersection de tous les convexes contenant A .

L'enveloppe convexe est un convexe. En effet soit C un convexe contenant A et $x, y \in \text{Conv}(A)$; alors x et y sont dans C et par conséquent le segment $[x, y]$ est inclus à C . Ce segment étant inclus à tout convexe contenant A , il est inclus à $\text{Conv}(A)$.

Proposition 8.30 ([141]).

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'autres termes, un convexe est stable par barycentrage à poids positifs².

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

$$\lambda_1 \overrightarrow{ba_1} + \lambda_2 \overrightarrow{ba_2} = 0. \quad (8.60)$$

2. 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 (8.60), nous trouvons

$$\lambda_1(a_1 - b) + \lambda_2(a_2 - b) = 0 \quad (8.61)$$

et donc

$$b = \frac{\lambda_1}{\lambda_1 + \lambda_2}a_1 + \frac{\lambda_2}{\lambda_1 + \lambda_2}a_2, \quad (8.62)$$

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

$$A_r = \{(a_1, \lambda_1), \dots, (a_r, \lambda_r)\} \quad (8.63)$$

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 8.28 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. $\square$

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

$$\sum_i \lambda_i x_i = \sum_i \lambda_i g. \quad (8.64)$$

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 affin, nous allons toujours supposer $\sum_i \lambda_i = 1$ et avoir le barycentre

$$g = \sum_i \lambda_i x_i. \quad (8.65)$$

Proposition 8.31.

Soit E , un espace vectoriel et $A \subset E$. L'enveloppe convexe $\text{Conv}(A)$ 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 8.30, ces barycentres sont dans l'enveloppe convexe et donc $\mathcal{B} \subset \text{Conv}(A)$. A contrario, si nous prouvons que $\mathcal{B}$ était convexe, alors nous aurions $\text{Conv}(A) \subset \mathcal{B}$ 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

$$a = \sum_i \lambda_i a_i \quad \sum_{i=1}^n \lambda_i = 1 \quad (8.66a)$$

$$b = \sum_j \mu_j b_j \quad \sum_{j=1}^m \mu_j = 1 \quad (8.66b)$$

Un point du segment $[a, b]$ est de la forme $p = ta + (1 - t)b$ avec $t \in [0, 1]$. En développant,

$$p = \sum_{i=0}^n (t\lambda_i) a_i + \sum_{j=0}^m (1 - t)\mu_j b_j. \quad (8.67)$$

Cela est le barycentre de la famille $\{(a_i, \lambda_i), (b_j, \mu_j)\}$, parce que la somme des coefficients est bien 1 :

$$\sum_i (t\lambda_i) + \sum_j (1 - t)\mu_j = t + (1 - t) = 1. \quad (8.68)$$

$\square$

Théorème 8.32 (Carathéodory[1]).

Dans un espace affine de dimension n , l'enveloppe convexe³ de A est l'ensemble des barycentres à coefficients positifs ou nuls de familles de $n + 1$ points.

Démonstration. Soit $x \in \text{Conv}(A)$; on sait par la proposition 8.31 que x est barycentre de points de A avec des coefficients positifs :

$$x = \sum_{k=1}^p \lambda_k x_k \quad (8.69)$$

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

$$\sum_{i=2}^p \alpha_i x_i = \sum_{i=2}^p \alpha_i x_1. \quad (8.70)$$

Nous posons $\alpha_1 = -\sum_{i=2}^p \alpha_i$. Remarquons qu'alors $\sum_{i=1}^p \alpha_i x_i = 0$ parce que

$$\sum_{i=1}^p \alpha_i x_i = \alpha_1 x_1 + \sum_{i=2}^p \alpha_i x_i = \alpha_1 x_1 + \sum_{i=2}^p \alpha_i x_1 = \sum_{i=1}^p \alpha_i x_1 = 0. \quad (8.71)$$

Par conséquent ça ne coûte rien de récrire (8.69) sous la forme

$$x = \sum_{i=1}^p (\lambda_i + t\alpha_i) x_i. \quad (8.72)$$

Les α_i ne sont pas tous nuls, mais leur somme est nulle, donc il y en a au moins un négatif. Nous notons

$$\tau = \min\left\{-\frac{\lambda_i}{\alpha_i} \text{ tel que } \alpha_i < 0\right\}, \quad (8.73)$$

et J l'ensemble de i pour lesquels ce minimum est atteint. Nous considérons aussi le 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 $\mu_i \geq 0$, mais si $\alpha_i < 0$ alors

$$\lambda_i + \tau\alpha_i \geq \lambda_i + \left(-\frac{\lambda_i}{\alpha_i}\right)\alpha_i = 0 \quad (8.74)$$

donc $\mu_i \geq 0$ 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

$$\sum_{i \notin J} \mu_i x_i = \sum_{i=1}^p \mu_i x_i = x. \quad (8.75)$$

Et voila, nous avons écrit x comme un barycentre à coefficients positifs de moins de p éléments parce que J n'est pas vide. $\square$

Corollaire 8.33.

Dans un espace affine de dimension finie, l'enveloppe convexe d'un compact est compacte.

3. Définition 8.29.

Démonstration. Soit A une partie compacte de l'espace vectoriel E , et $\text{Conv}(A)$ son enveloppe convexe. Nous allons montrer que toute suite dans $\text{Conv}(A)$ admet une sous-suite convergente en écrivant un point de $\text{Conv}(A)$ comme le théorème de Carathéodory 8.32 nous le suggère. Pour cela nous considérons le simplexe

$$\Lambda = \left\{ \lambda \in \mathbb{R}^{n+1} \text{ tel que } \sum_{k=1}^{n+1} \lambda_k = 1 \text{ et } \lambda_k \geq 0 \forall k \right\}. \quad (8.76)$$

Montrons en passant que Λ est compact. Si $\lambda_k \in \Lambda$ est une suite, alors chacun des λ_k est un $(n+1)$ -uplet de nombres dans $[0, 1]$:

$$k \mapsto (\lambda_k)_i \quad (8.77)$$

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

$$f: \Lambda \times A^{n+1} \rightarrow \text{Conv}(A) \quad (8.78)$$

$$(\lambda, x) \mapsto \sum_{k=1}^{n+1} \lambda_k x_k.$$

C'est une application continue parce qu'elle est bilinéaire en dimension finie ; son image est contenue dans $\text{Conv}(A)$ par la proposition 8.30, et elle est surjective par le théorème de Carathéodory 8.32. Bref, $\text{Conv}(A) = f(\Lambda \times A^{n+1})$ est donc l'image d'un compact par une application continue ; elle est donc compacte par le théorème 5.60. $\square$

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 dû prendre une infinité de sous-suites et rien n'aurait été sûr.

8.7 Repères, coordonnées cartésiennes et barycentriques

Définition 8.34.

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 8.35 ([139]).

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 $\text{Aff}\{A_0, \dots, \hat{A}_i, \dots, A_r\}$.
- (3) Les points $A_0, \dots, A_{r-1}$ sont affinement indépendants et $A_r \notin \text{Aff}\{A_0, \dots, A_{r-1}\}$.
- (4) Il existe i tel que les vecteurs $\overrightarrow{A_k A_i}$ ($k \in i$) sont linéairement indépendants.
- (5) Pour tout $i \in \{1, \dots, r\}$, les vecteurs $\overrightarrow{A_k A_i}$ ($k \neq i$) sont linéairement indépendants.

Notons à propos de la condition (3) que l'existence d'un i tel que $A_i \notin \text{Aff}\{A_0, \dots, \hat{A}_i, \dots, A_r\}$ 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 8.36.

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 $\{A_0, \dots, A_n\}$ 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

$$M = A_0 + \overrightarrow{A_0M}. \quad (8.79)$$

Mais nous savons que les vecteurs $\overrightarrow{A_0A_i}$ forment une base de E , nous avons donc des nombres λ_i tels que

$$\overrightarrow{A_0M} = \sum_{i=1}^n \lambda_i \overrightarrow{A_0A_i}. \quad (8.80)$$

Les nombres λ_i ainsi construits sont les **coordonnées cartésiennes** du point M dans le repère $\{A_0, \dots, A_n\}$ d'origine A_0 .

À partir de ces coordonnées, le point $M \in \mathcal{E}$ se retrouve par la formule

$$M = A_0 + \sum_{i=1}^n \lambda_i \overrightarrow{A_0A_i}. \quad (8.81)$$

Les coordonnées barycentriques sont données par la proposition suivante.

Proposition 8.37 ([139]).

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 des A_i affectés de poids λ_i tels que $\sum_{i=0}^r \lambda_i = 1$.

Les nombres λ_i ainsi définis sont les **coordonnées barycentriques** de M dans le repère $(A_0, \dots, A_r)$ de $\mathcal{F}$.

Démonstration. Nous avons vu plus haut (définition 8.36) que l'afine 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 affine sont exactement les ensembles de barycentres (proposition 8.26), 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 8.23 avec $B = A_0$:

$$\overrightarrow{A_0M} = \sum_{i=1}^r \lambda_i \overrightarrow{A_0A_i} \quad (8.82)$$

où la somme à droite s'étend a 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

$$\overrightarrow{A_0M} = \sum_{i=1}^r \lambda_i \overrightarrow{A_0A_i} = \sum_{i=1}^r \mu_i \overrightarrow{A_0A_i} \quad (8.83)$$

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 8.35) et donc $\lambda_i = \mu_i$ pour $i = 1, \dots, r$. La condition de somme des points égale à 1 impose alors immédiatement $\lambda_0 = \mu_0$. $\square$

Exemple 8.38

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

$$A + \alpha \overrightarrow{AB} + \beta \overrightarrow{AC}, \quad (8.84)$$

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. $\triangle$

Exemple 8.39

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

$$\frac{1}{6} + \frac{1}{3} + \frac{1}{2} = 1. \quad (8.85)$$

Ensuite nous cherchons $X \in \mathbb{R}^2$ tel que

$$\frac{1}{6}\overrightarrow{AX} + \frac{1}{3}\overrightarrow{BX} + \frac{1}{2}\overrightarrow{CX} = 0, \quad (8.86)$$

c'est à dire

$$\frac{1}{6} \begin{pmatrix} x-3 \\ y-1 \end{pmatrix} + \frac{1}{3} \begin{pmatrix} x+1 \\ y-2 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} x \\ y+1 \end{pmatrix} = 0. \quad (8.87)$$

Nous trouvons immédiatement $x = 1/6$ et $y = 1/3$. Le point cherché est donc le point $\begin{pmatrix} 1/6 \\ 1/3 \end{pmatrix}$. $\triangle$

8.7.1 Équation de droite

Soit $\mathcal{E}$ un espace affine de dimension trois muni d'un repère barycentrique. Une droite est donnée par trois nombres : $D = D(a, b, c)$ est l'ensemble des points dont les coordonnées barycentriques (normalisées) (x, y, z) vérifient $ax + by + cz = 0$. C'est un espace de dimension un parce qu'il y a aussi la condition $x + y + z = 1$.

La droite $D(1, 1, 1)$ n'existe pas parce que ce serait $x + y + z = 0$, qui est incompatible avec $x + y + z = 1$.

Les droites $D(a, b, c)$ et $D(a', b', c')$ s'intersectent selon les solutions du système

$$\begin{cases} x + y + z = 1 & (8.88a) \\ ax + by + cz = 0 & (8.88b) \\ a'x + b'y + c'z = 0 & (8.88c) \end{cases}$$

Donc deux droites affines ont un unique point d'intersection si et seulement si

$$d = \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a' & b' & c' \end{vmatrix} \neq 0. \quad (8.89)$$

Elles seront parallèles ou confondues si et seulement si $d = 0$.

8.8 Structure du groupe des applications affines

Soit $v \in \mathbb{R}^n$; nous notons $\tau_v: \mathbb{R}^n \rightarrow \mathbb{R}^n$ la translation donnée par $\tau_v(x) = x + v$. Le groupe de toutes les translation de $\mathbb{R}^n$ est noté $T(n)$ et est isomorphe au groupe abélien $(\mathbb{R}^n, +)$.

En prenant $M = 0$ dans la définition 8.6 et en pensant à l'espace $\mathbb{R}^n$ comme espace affine, nous posons la définition suivante pour les applications de $\mathbb{R}^n$ dans $\mathbb{R}^n$ (et d'ailleurs pour n'importe quel espace vectoriel de dimension finie).

Définition 8.40.

Une application **affine** sur $\mathbb{R}^n$ est une application $\mathbb{R}^n \rightarrow \mathbb{R}^n$ pouvant être écrite sous la forme $\tau_c \circ \alpha$ où $v \in \mathbb{R}^n$ et où α est une application linéaire.

Proposition 8.41.

Soit une application affine $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$. L'ensemble des points fixes

$$\text{Fix}(f) = \{x \in \mathbb{R}^n \text{ tel que } f(x) = x\} \quad (8.90)$$

est soit vide soit un sous-espace affine de $\mathbb{R}^n$.

Démonstration. Soit $f = \tau_v \circ \alpha$; nous avons $x \in \text{Fix}(f)$ si et seulement si

$$x = \tau_v(\alpha(x)) = \alpha(x) + v, \quad (8.91)$$

autrement dit, en considérant l'application linéaire $\beta = \text{Id} - \alpha$, si et seulement si $\beta(x) = v$. Nous écrivons $\text{Fix}(f) = \beta^{-1}(v)$. Supposons que ce soit non vide et considérons $x_0 \in \beta^{-1}(v)$. Nous avons

$$\beta^{-1}(v) = \{x \in \mathbb{R}^n \text{ tel que } \beta(x) = \beta(x_0)\} \quad (8.92a)$$

$$= \{x \text{ tel que } \beta(x - x_0) = 0\} \quad (8.92b)$$

$$= \{x \text{ tel que } x - x_0 \in \ker(\beta)\} \quad (8.92c)$$

$$= \ker(\beta) + x_0 \quad (8.92d)$$

$$= \tau_{x_0}(\ker(\beta)). \quad (8.92e)$$

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. $\square$

Définition 8.42.

Le groupe $\text{Aff}(\mathbb{R}^n)$ est le groupe des applications affines bijectives de $\mathbb{R}^n$.

Remarque 8.43.

Le fait que ce soit un groupe est rapidement vu par le calcul suivant :

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta)(x) = (\alpha\beta)(x) + \alpha(w) + v = \tau_{\alpha(w)+v} \circ (\alpha\beta). \quad (8.93)$$

Proposition 8.44.

L'ensemble $\text{Aff}(\mathbb{R}^n)$ est isomorphe au produit semi-direct⁴

$$\text{Aff}(\mathbb{R}^n) \simeq T(n) \times_{\mathbf{Ad}} \text{GL}(n, \mathbb{R}) \quad (8.94)$$

où $\mathbf{Ad}$ est l'action adjointe, c'est à dire

$$\begin{aligned} \mathbf{Ad}: \text{GL}(n, \mathbb{R}) &\rightarrow \text{Aut}(T(n)) \\ \tau_v &\mapsto \alpha \circ \tau_v \circ \alpha^{-1}. \end{aligned} \quad (8.95)$$

Démonstration. L'application que nous allons montrer être un isomorphisme est ψ qui à $f = \tau_v \circ \alpha$ fait correspondre le couple $(\tau_v, \alpha) \in T(n) \times \text{GL}(n, \mathbb{R})$.

Égalité d'ensembles Il faut que $\text{Aff}(\mathbb{R}^n)$ soit en bijection avec $T(n) \times \text{GL}(n, \mathbb{R})$. En effet si $f \in \text{Aff}(\mathbb{R}^n)$, la décomposition $f = \tau_v \circ \alpha$ est unique. D'abord en appliquant à 0, $f(0) = \tau_v(\alpha(0)) = v$. Donc v est fixé par la valeur de $f(0)$. Ensuite $\alpha = f \circ \tau_v^{-1}$, donc α fixé.

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

$$\alpha \tau_v \alpha^{-1}(x) = \alpha(\alpha^{-1}(x) + v) = x + \alpha(v) = \tau_{\alpha(v)}(x). \quad (8.96)$$

Le fait que $\mathbf{Ad}(\alpha)$ soit un automorphisme est toujours correct.

4. Définition 2.85.

Morphisme Il faut vérifier que l'application ψ est un morphisme de groupe. D'abord la loi de groupe sur $\text{Aff}(\mathbb{R}^n)$ est donnée par

$$(\tau_v \circ \alpha) \circ (\tau_w \circ \beta) = \tau_{v+\alpha(w)} \circ (\alpha \circ \beta). \quad (8.97)$$

Ensuite le loi de groupe de le produit semi-direct est donnée par

$$(\tau_v, \alpha) \cdot (\tau_w, \beta) = (\tau_v \mathbf{Ad}(\alpha)\tau_w, \alpha\beta) = (\tau_v \tau_{\alpha(w)}, \alpha\beta) = (\tau_{\alpha(w)+v}, \alpha\beta). \quad (8.98)$$

Nous avons donc bien

$$\psi((\tau_v, \beta) \cdot (\tau_w, \beta)) = \psi(\tau_v, \beta) \circ \psi(\tau_w, \beta). \quad (8.99)$$

□

Chapitre 9

Géométrie hyperbolique

9.1 Inversion

Lemme-définition 9.1.

Soit un cercle C et un point A du plan $\mathbb{R}^2$. Soit une droite passant par A et coupant C en deux points P et P' (pas spécialement distincts). Alors le nombre

$$\|AP\|\|AP'\| \quad (9.1)$$

ne dépend pas du choix de la droite et est nommé la **puissance** du point A par rapport au cercle C .

9.1.1 Cercles perpendiculaires

Définition 9.2.

Deux cercles sont **perpendiculaires** lorsque leurs tangentes aux points d'intersection sont perpendiculaires.

Lemme 9.3 ([8]).

Soient deux cercles perpendiculaires C_1 et C_2 . Alors

- (1) le centre de C_1 est hors de C_2 .
- (2) Si ℓ est une droite passant par le centre de C_1 (nommé O) et si ℓ coupe C_2 en les deux points P et P' , alors P et P' sont situés du même côté de O .

Démonstration. Nous nommons O_1 le centre de C_1 ainsi que Q et Q' les points d'intersection de C_1 avec C_2 . Si ℓ_Q et $\ell_{Q'}$ sont les tangentes à C_1 en Q et Q' , alors ce sont des rayons de C_2 (parce que les cercles sont perpendiculaires). Par conséquent le centre O_2 de C_2 est le point d'intersection $Q' = \ell_Q \cap \ell_{Q'}$.

Le triangle O_1O_2Q est rectangle en Q et donc $\|O_1O_2\| > \|QO_2\|$. Or le nombre $\|QO_2\|$ est le rayon de C_2 , donc O_1 est en dehors de C_2 .

Ceci achève de prouver le point (1) ; nous démontrons le point (2). Les points P et P' sont sur le cercle C_2 , donc tous les points du segment $[PP']$ sont dans le cercle. Or le centre de C_1 doit être en dehors de C_2 ; il ne peut donc pas être dans le segment $[PP']$, ce qui prouve que P et P' ne sont pas de part et d'autre de O sur la droite (OPP') . $\square$

Proposition 9.4 ([8]).

Soit un cercle C_1 de centre O et de rayon R .

- (1) Un cercle C_2 est perpendiculaire à C_1 si et seulement si il existe une droite ℓ passant par O telle que les points d'intersection $\{P, P'\} = \ell \cap C_2$ soient situés du même côté de O et vérifient

$$\|OP\|\|OP'\| = R^2. \quad (9.2)$$

(2) Dans ce cas, toutes les droites passant par O et coupant C_2 en deux points P, P' vérifient le fait que P et P' soient du même côté de O et $\|OP\|\|OP'\| = R^2$.

Démonstration. Nous commençons par prouver le point (2). Le fait que les points P et P' soient du même côté de O est le lemme 9.3(2). Pour la relation sur les distances, soit $Q \in C_1 \cap C_2$. Vu que C_1 et C_2 sont perpendiculaires, la droite (OQ) ne coupe C_2 qu'en ce point, et la puissance de O par rapport au cercle C_2 est $\|OQ\|^2 = R^2$.

La même puissance peut être calculée via la droite ℓ :

$$\|OP\|\|OP'\|. \quad (9.3)$$

Donc $\|OP\|\|OP'\| = R^2$.

Soit un cercle C_2 passant par P et P' . Notons que P et P' ne sont pas sur C_1 parce qu'ils ne pourraient pas être alignés avec O . De plus l'un est à l'intérieur de C_1 et l'autre à l'extérieur de C_1 . Les cercles C_1 et C_2 possèdent donc deux points distincts d'intersections. La puissance de O par rapport à C_2 est :

$$\|OP\|\|OP'\| = R^2 \quad (9.4)$$

parce que (OP) est une droite coupant C_2 en les points P et P' .

Soit Q un point d'intersection de C_1 et C_2 , et Q' l'autre point d'intersection de C_2 avec la droite (OQ) . La puissance de O par rapport à C_2 peut également être calculée à partir de cette droite (lemme 9.1) et nous avons

$$\|OQ\|\|OQ'\| = R^2, \quad (9.5)$$

mais $Q \in C_1$, donc $\|OQ\| = R$ et partant $\|OQ'\| = R$. Nous en déduisons que $Q' \in C_1$ également. Or Q' ne peut pas être l'autre point d'intersection de C_1 avec C_2 (sinon O, Q, Q' ne seraient pas alignés). Donc $Q = Q'$ et nous déduisons que la droite (OQ) est tangente à C_2 .

Le rayon de C_1 est tangent à C_2 . Cela signifie que C_1 est perpendiculaire à C_2 . $\square$

9.1.2 Inversion

Proposition-définition 9.5 ([142]).

Soit un cercle C de centre O dans $\mathbb{R}^2$. Il existe une unique application

$$i_C: \mathbb{R}^2 \setminus O \rightarrow \mathbb{R}^2 \setminus O \quad (9.6)$$

telle que

- (1) $i_C(x) = x$ pour tout $x \in C$
- (2) i_C échange l'intérieur et l'extérieur de C .
- (3) i_C laisse invariants les droites et les cercles orthogonaux à C .

Cette application est l'**inversion** de cercle C .

Démonstration. Soit P à l'intérieur de C , mais différent de O . Nous notons ℓ la droite (OP) et nous considérons un cercle C_2 passant par P et perpendiculaire à C (existence par la proposition 9.4). Nous avons $\ell \perp C$ (parce que ℓ est un rayon) et $C_2 \perp C$. Donc $i_C(\ell) = \ell$ et $i_C(C_2) = C_2$ par l'exigence (3). Mais comme $P \in \ell \cap C_2$ nous avons aussi

$$i_C(P) \in \ell \cap C_2. \quad (9.7)$$

Mais ℓ et C_2 se coupent en exactement deux points. Vu que $i_C(P)$ doit être hors de C (exigence (2)), avoir $i_C(P) = P$ est impossible. Nous en concluons que $i_C(P)$ doit être l'autre intersection.

Nous avons prouvé que les conditions (2) et (3) fixent l'image d'un point situé dans l'intérieur de C .

Si P est extérieur au cercle C , la même procédure fonctionne : nous considérons la droite $\ell = (OP)$ et un cercle C_2 perpendiculaire à C et passant par P . Encore une fois, ces deux objets sont fixés par i_C , et vu que $i_C(P)$ doit être à l'intérieur de C , il est fixé.

L'unicité est montrée.

En ce qui concerne l'existence, si $P \neq O$, la procédure suivante donne P' :

- Soit la droite $\ell = (OP)$.
- Soit un cercle C_2 perpendiculaire à C et passant par P .
- Le point P' est le point de l'intersection $C_2 \cap \ell$ qui n'est pas P .

Il est aisé de vérifier que poser $i_C(P) = P'$ donne une application qui vérifie toutes les propriétés. $\square$

9.6.

Nous recopions la construction de l'inversion d'un point par rapport à un cercle. Si C_1 est un cercle de centre O et P est un point différent de O , alors la procédure suivante construit $P' = i_{C_1}(P)$:

- Soit la droite $\ell = (OP)$.
- Soit un cercle C_2 perpendiculaire à C_1 et passant par P .
- Le point P' est le point de l'intersection $C_2 \cap \ell$ qui n'est pas P .

Que se passe-t-il si ℓ et C_2 n'ont qu'une seule intersection ? Alors la droite $\ell = (OP)$ est tangente à C_2 . Or de O il n'existe que deux droites tangentes à C_2 , et ce sont les rayons passant par les intersections parce que les cercles sont perpendiculaires. En d'autres mots, cette situation se présente lorsque P est sur le cercle C_1 . Dans ce cas, $i_{C_1}(P) = P$.

Corollaire 9.7.

L'inversion i_C est une involution ($i_C^2 = \text{Id}$).

Démonstration. Soit un cercle C de centre O et un point P . Si C_2 est un cercle perpendiculaire à C passant par P , alors nous avons vu en 9.6 que $P' = i_C(P)$ est l'autre intersection entre C_2 et la droite (OP) .

Pour construire l'image de P' , il faut un cercle perpendiculaire à C passant par P' . Le cercle C_2 déjà utilisé fait l'affaire. Ensuite, la droite (OP') est la même que la droite (OP) . Donc l'image de P' est P . $\square$

Soit C_1 le cercle dans $\mathbb{C}$ de centre 0 et de rayon 1. Nous notons $\alpha: \mathbb{C} \rightarrow \mathbb{C}$ la dilatation de rapport R .

Proposition 9.8 ([8]).

Soit C le cercle de rayon R centré en 0 ($C = \alpha(C_1)$). Alors

$$i_{\alpha(C_1)} \circ \alpha = \alpha \circ i_{C_1}. \quad (9.8)$$

Démonstration. Soit $z = re^{i\theta}$; nous devons prouver que

$$i_C(\alpha(z)) = \alpha(i_{C_1}(z)). \quad (9.9)$$

Nous avons :

$$i_C(\alpha(z)) = i_C(Rre^{i\theta}) = R^2 \frac{1}{Rr} e^{i\theta} = R \frac{1}{r} e^{i\theta} = \alpha\left(\frac{1}{r} e^{i\theta}\right) = \alpha(i_{C_1}(z)). \quad (9.10)$$

$\square$

Proposition 9.9 ([8]).

Soit le cercle de rayon R et de centre $a \in \mathbb{C}$. Alors

$$i_C(z) = \frac{R^2}{\bar{z} - \bar{a}} + a. \quad (9.11)$$

De plus si t_a est la translation de vecteur a , nous avons la décomposition

$$i_{t_a(C_R)} = t_a \circ i_{C_R} \circ t_{-a} \quad (9.12)$$

où C_R est le cercle de rayon R centré en 0.

Démonstration. Si $z \in \mathbb{C}$ et z' est son image par i_C , alors non seulement

$$\|a - z'\| \|a - z\| = R^2, \quad (9.13)$$

mais en plus $a - z' = \lambda(a - z)$ pour un certain $\lambda > 0$. Cela est l'expression du fait que z' est sur la demi-droite qui joint a à z . Nous avons donc

$$\lambda \|a - z\|^2 = R^2 \quad (9.14)$$

et alors

$$\lambda = \frac{R^2}{(a - z)(\bar{a} - \bar{z})}. \quad (9.15)$$

En récrivant $a - z' = \alpha(a - z)$ avec cette valeur de λ nous trouvons

$$a - z' = \frac{R^2}{a - z}, \quad (9.16)$$

ce qu'il fallait démontrer.

La décomposition demandée est une simple vérification en utilisant $i_{C_R}(z) = \frac{R^2}{\bar{z}}$ qui découle de la proposition 9.8. $\square$

Avant d'aller plus loin, donnons l'équation d'un cercle dans $\mathbb{C}$. Si C est un cercle de centre ω et de rayon r , alors $z \in C$ si et seulement si $d(z, \omega) = r$. En développant, et en passant au carré sans perte d'information (les deux membres sont positifs), $z \in C$ si et seulement si

$$(z - \omega)(\bar{z} - \bar{\omega}) = r^2. \quad (9.17)$$

Proposition 9.10 ([142, 143]).

Soit un cercle C de centre O . L'inversion

$$i_C: \mathbb{R}^2 \setminus \{0\} \rightarrow \mathbb{R}^2 \setminus \{0\} \quad (9.18)$$

transforme

- (1) les droites passant par O sur elles-mêmes ;
- (2) les cercles passant par O en des droites ne passant pas par O ;
- (3) les droites ne passant pas par O en des cercles passant par O ;
- (4) les cercles ne passant pas par O en des cercles ne passant pas par O .

Démonstration. Point par point.

- (1) Une droite passant par O est une droite perpendiculaire à C . Par le point (3) de la définition 9.5, elle est invariante.
- (2) Nous construisons successivement :
 - Un cercle C_1 de centre O_1 et passant par O . Le but est de déterminer l'image de ce cercle.
 - Le point P de C_1 tel que $[OP]$ en soit un diamètre.
 - Le point $P' = i_C(P)$.
 - La droite ℓ perpendiculaire à (OP) et passant par P' .

Nous montrons maintenant que $i_C(C_1 \setminus \{O\}) = \ell$. Soit $Q \in C_1 \setminus \{P, O\}$. Nous posons

$$Q' = (QO) \cap \ell. \quad (9.19)$$

Vu que $[OP]$ est un diamètre de C_1 et que $Q \in C_1$, le triangle OPQ est rectangle en Q . Et étant donné que Q' est sur ℓ nous savons que $OP'Q'$ est rectangle en P' .

De plus les angles en O de ces deux triangles sont identiques (parce que c'est l'angle formé par les droites (OQ) et (OP)) ; les triangles OPQ et $QP'Q'$ sont donc semblables et nous pouvons utiliser le théorème de Thalès¹ :

$$\frac{OP}{OQ} = \frac{OQ'}{OP'}. \quad (9.20)$$

Donc

$$\|OP\| \|OP'\| = \|OQ\| \|OQ'\|, \quad (9.21)$$

mais P' est l'image de P par l'inversion du cercle C , c'est à dire $\|OP\| \|OP'\| = R^2$. Nous en déduisons que

$$\|OQ\| \|OQ'\| = R^2, \quad (9.22)$$

c'est à dire que Q' est l'image de Q par i_C , et donc que

$$i_C(C_1 \setminus \{O\}) \subset \ell. \quad (9.23)$$

Pour avoir l'inclusion inverse, il faut remarquer que ℓ est parallèle à la tangente à C_1 en O . Donc si $Q \in \ell$, la droite (OQ) intersecte le cercle C_1 en un point Q' . En refaisant le cheminement du résultat (9.23) à l'envers, il est loisible de prouver que $i_C(Q') = Q$ et donc que ℓ est bien incluse à l'image de C_1 par i_C .

- (3) Nous commençons par prouver que toutes les droites ne passant pas par O sont des images de cercles passant par O .

Nous considérons :

- une droite ℓ ne passant pas par O .
- la droite d , perpendiculaire à ℓ passant par O
- le point $P' = \ell \cap d$,
- le point $P = i_C(P')$,
- le cercle C_1 dont $[OP]$ est un diamètre.

Par tout ce que nous avons fait jusqu'à présent, la droite ℓ est l'image du cercle C_1 . Or si $\|OP\| = r$ alors

$$\|OP'\| = \frac{R^2}{r}. \quad (9.24)$$

Donc quelle que soit la valeur de $\|OP'\|$ dans $]0, \infty[$, il existera un point P tel que le cercle passant par O et P ait pour image la droite perpendiculaire à (OP) passant par $i_C(P)$.

Étant donné que i_C est une involution surjective des cercles passant par O vers les droites ne passant pas par O , elle transforme également toutes les droites ne passant pas par O en un cercle passant par O .

- (4) Pour cette partie, nous allons utiliser un peu de géométrie analytique dans $\mathbb{C}^2$.

Le cas centré Nous supposons que C est centré en 0 et de rayon, 1, ce telle sorte que $i_C(z) = \frac{1}{\bar{z}}$. Soit C_1 un cercle de centre ω et de rayon r , ne passant pas par 0, en particulier tel que $|\omega| \neq r$.

Si $z \in i(C_1)$ alors $i(z) \in C_1$ et nous avons

$$(i(z) - \omega) \overline{(i(z) - \omega)} = r^2. \quad (9.25)$$

En développant et en multipliant par $z\bar{z}$ nous trouvons

$$\bar{\omega}z + \omega\bar{z} + z\bar{z}(r^2 - \omega\bar{\omega}) = 1. \quad (9.26)$$

Nous pouvons diviser par $(r^2 - |\omega|^2)$ parce que C_1 ne passe pas par 0. En remettant en ordre, et en notant $s = r^2 - \omega\bar{\omega}$ pour plus de clarté,

$$\left(z - \frac{\omega}{s}\right) \left(\bar{z} - \frac{\bar{\omega}}{s}\right) - \frac{\omega\bar{\omega}}{s^2} = \frac{1}{s^2}, \quad (9.27)$$

1. Faites bien le dessin : ce n'est pas une situation de Thalès ultra-standard de collège.

2. Principalement parce que je ne comprends pas le raisonnement fait dans [142].

ou encore

$$\left(z - \frac{\omega}{s}\right)\left(\bar{z} - \frac{\bar{\omega}}{s}\right) = \frac{1}{s} + \frac{\omega\bar{\omega}}{s}. \quad (9.28)$$

Pour que cela soit l'équation du cercle de centre $\frac{\omega}{s}$ et de rayon $\sqrt{\frac{1}{s} + \frac{\omega\bar{\omega}}{s^2}}$, il faut vérifier que

$$\frac{1}{s} + \frac{\omega\bar{\omega}}{s^2} \geq 0. \quad (9.29)$$

En multipliant par s^2 , il s'agit de vérifier que $s + \omega\bar{\omega} \geq 0$, ce qui est correct parce que $s + \omega\bar{\omega} = r$.

En résumé, si $z \in i(C_1)$ alors z est dans le cercle C_2 de centre $\frac{\omega}{s}$ et de rayon $\frac{r}{s}$. Étant donné que $r \neq \omega$ nous savons que ce dernier cercle ne passe pas par 0.

Nous avons prouvé que $i(C_1) \subset C_2$. Pour prouver l'inclusion inverse, vu que i est une involution, il faut prouver $i(C_2) \subset C_1$. Pour cela nous écrivons l'équation qui donne $i(z) \in C_2$ et en développant nous devons conclure que $z \in C_1$. Nous ne le faisons pas ici.

Le cas de rayon non unité Pour un cercle quelconque, il faut passer par la formule (9.11).

Si $z \in i_C(C_1)$ alors $i(z) \in C_1$ et nous pouvons écrire

$$(i(z) - a)(\overline{i(z)} - \bar{a}) = R^2. \quad (9.30)$$

De là il faut déduire que z est sur un cercle ne passant pas par 0. Bons calculs...

□

Chapitre 10

Espaces projectifs

Sur les espaces projectifs : [144].

Définition 10.1.

Soit E un espace vectoriel de dimension finie sur le corps $\mathbb{K}$. Nous définissons sur $E \setminus \{0\}$ la relation d'équivalence $u \sim v$ si et seulement si $u = \lambda v$ pour un certain $\lambda \in \mathbb{K}$. Cette relation est la relation de **colinéarité**. L'ensemble des classes d'équivalence de $\sim$ est l'**espace projectif** de E et sera noté $P(E)$.

Si $\dim E = 2$, l'ensemble $P(E)$ est la **droite projective**, et si $\dim E = 3$ nous parlons du **plan projectif**.

Étant donné que tous les $\mathbb{K}$ -espaces vectoriels de dimensions $n + 1$ sont isomorphes à $\mathbb{K}^{n+1}$, nous noterons $P_n(\mathbb{K})$ ou P_n l'espace projectif $P(\mathbb{K}^{n+1})$.

Exemple 10.2

Si $n = 1$ et $\mathbb{K} = \mathbb{R}$, l'espace projectif est l'ensemble des droites vectorielles dans le plan usuel. Il y en a une pour chaque point du type $(x, 1)$ avec $x \in \mathbb{R}$ et ensuite une horizontale, passant par le point $(1, 0)$. Nous avons donc

$$P_1(\mathbb{R}) = \{(1, 0)\} \cup \{(x, 1) \text{ tel que } x \in \mathbb{R}\}. \quad (10.1)$$

Le point $(1, 0)$ est dit «point à l'infini».

△

10.1 Sous espaces projectifs

Un **sous-espace projectif** de $P(E)$ est une partie de la forme $P(F)$ où F est un sous-espace vectoriel de E .

Proposition 10.3.

Si F et G sont des sous-espaces vectoriels de E , alors

$$P(F) \cap P(G) = P(F \cap G) \quad (10.2)$$

et nous avons

$$\dim P(F) + \dim P(G) = \dim P(F + G) + \dim P(F \cap G). \quad (10.3)$$

Démonstration. Nous avons

$$P(F) = \{[v] \text{ tel que } v \in F\} \quad (10.4)$$

où les crochets signifient la classe par rapport à la relation de colinéarité. Nous avons alors

$$P(F) \cap P(G) = \{[v] \text{ tel que } v \in F \cap G\} = P(F \cap G). \quad (10.5)$$

Cela prouve le premier point.

En ce qui concerne l'équation (10.3), en considérant $\dim P(E) = \dim E - 1$ nous devons prouver l'égalité

$$\dim F + \dim G = \dim(F + G) + \dim(F \cap G) \quad (10.6)$$

concernant les dimensions des espaces vectoriels usuelles. Si nous considérons une base de E telle que $B_1 = \{e_1, \dots, e_{k_1}\}$ est une base de $F \cap G$, $B_2 = \{e_{k_1+1}, \dots, e_{k_2}\}$ complète B_1 en une base de F et $B_3 = \{e_{k_2+1}, \dots, e_n\}$ complète $B_1 \cup B_2$ en une base de G .

Nous avons alors

$$\dim F + \dim G = 2 \operatorname{Card}(B_1) + \operatorname{Card}(B_2) + \operatorname{Card}(B_3) \quad (10.7a)$$

$$\dim(F + G) = \operatorname{Card}(B_1) + \operatorname{Card}(B_2) + \operatorname{Card}(B_3) \quad (10.7b)$$

$$\dim(F \cap G) = \operatorname{Card}(B_1). \quad (10.7c)$$

De là la relation (10.3) se déduit immédiatement. $\square$

Théorème 10.4 (incidence).

Soient F et G deux sous-espaces vectoriels de E tels que

$$\dim P(F) + \dim P(G) \geq \dim P(E). \quad (10.8)$$

Alors $P(F) \cap P(G) \neq \emptyset$.

Démonstration. En utilisant les hypothèses et la proposition 10.3 nous avons

$$\dim P(E) + \dim P(G) = \dim P(F + G) + \dim P(F \cap G) \geq \dim P(E). \quad (10.9)$$

En passant aux espaces vectoriels correspondants,

$$\dim(F + G) + \dim(F \cap G) \geq \dim(E) + 1. \quad (10.10)$$

Mais nous avons aussi $\dim(F + G) \leq \dim(E)$ et par conséquent $\dim(F \cap G) \geq 1$. Au final, $\dim P(F \cap G) \geq 0$. Cela prouve que $P(F \cap G)$ contient au moins un élément (nous rappelons que lorsqu'un espace projectif contient un seul élément, sa dimension est zéro). $\square$

Exemple 10.5

Soient les plans $\Pi_1 \equiv x = 0$ et $\Pi_2 \equiv y = 0$. Nous avons

$$P(\Pi_1) = \{[0, y, 1]\} \cup \{[0, 1, 0]\} \quad (10.11a)$$

$$P(\Pi_2) = \{[x, 0, 1]\} \cup \{[1, 0, 0]\} \quad (10.11b)$$

où le crochet signifie la classe pour la colinéarité. Ces deux droites projectives ont comme point d'intersection le point $[0, 0, 1]$. $\triangle$

Définition 10.6.

Un **hyperplan projectif** est un sous-espace projectif de $P(E)$ de la forme $P(V)$ où V est un hyperplan de E .

Proposition 10.7.

Soit $H = P(V)$ un hyperplan projectif de $P(E)$ et soit m hors de H . Alors toute droite projective passant par m coupe H en un et un seul point.

Démonstration. Si $\dim E = n$ nous avons $\dim V = n - 1$. Soit $d = P(D)$ une droite projective passant par m , c'est à dire que D est de dimension 2 dans E . Si $D \subset V$ alors $m \in P(D) \subset P(V)$; or nous avons demandé que m soit hors de $P(V)$. Par conséquent D n'est pas inclus à V et en particulier $\dim(D + V) = \dim(E)$.

Nous recopions la formule (10.3) pour notre cas :

$$\underbrace{\dim d}_{=1} + \underbrace{\dim H}_{=n-2} = \underbrace{\dim P(D + V)}_{=n-1} + \dim P(D \cap V). \quad (10.12)$$

Nous avons donc $\dim P(D \cap V) = 0$, ce qui signifie que l'ensemble $P(D \cap V) = P(D) \cap P(V) = d \cap H$ contient un et un seul point. $\square$

10.2 Espace projectifs comme «complétés» d'espaces affines

Soit E un espace vectoriel de dimension 2 et $P(E)$ la droite projective correspondante, et soit $\{e_1, e_2\}$ une base de E . Nous considérons la droite affine $d \equiv y = 1$. Nous avons la bijection

$$\begin{aligned} \phi: d \cup \{\infty\} &\rightarrow P(E) \\ (x, 1) &\mapsto \text{la droite vectorielle passant par } (x, 1) \\ \infty &\mapsto \text{la droite vectorielle passant par } (1, 0). \end{aligned} \quad (10.13)$$

Lemme 10.8.

Si nous munissons l'ensemble $d \cup \{\infty\}$ de la topologie compactifiée d'Alexandroff, la bijection (10.13) est un homéomorphisme.

Soient maintenant les plans affines dans l'espace vectoriel E de dimension 3

$$\Pi_1 \equiv z = 0 \quad (10.14a)$$

$$\Pi_2 \equiv z = 1. \quad (10.14b)$$

Une droite (vectorielle) de E coupe Π_2 en un et un seul point, sauf si elle est contenue dans Π_1 . Nous avons donc une bijection

$$\begin{aligned} \phi: P(E) &\rightarrow \Pi_2 \cup P(\Pi_1) \\ d &\mapsto \begin{cases} \Pi_2 \cap d & \text{si cette intersection est non vide} \\ d & \text{sinon.} \end{cases} \end{aligned} \quad (10.15)$$

La droite projective $P(\Pi_1)$ est la droite à l'infini du plan projectif $P(E)$. Nous voyons que le plan projectif $P(E)$ peut être vu comme un plan affine (Π_2) «complété» par une droite affine $P(\Pi_1)$. Cette dernière droite est elle-même une droite affine complétée par un point à l'infini.

Nous pouvons généraliser cette démarche en considérant un espace affine $\mathcal{E}$ de direction E sur le corps $\mathbb{K}$. Nous construisons $F = E \times \mathbb{K}$ et nous considérons un repère affine sur F tel que $E \equiv x_{n+1} = 0$. Nous pouvons donc identifier $\mathcal{E}$ à l'hyperplan affine d'équation $x_{n+1} = 1$ dans F .

Une droite vectorielle de F non contenue dans E coupe $\mathcal{E}$ en un unique point ; nous avons donc une bijection

$$\mathcal{E} \cup P(E) \rightarrow P(F). \quad (10.16)$$

Dans ce cadre, $P(E)$ est l'hyperplan à l'infini et nous disons que $P(E)$ est la **complétion projective** de $\mathcal{E}$.

Définition 10.9.

Soit E un espace vectoriel de dimension 3. Nous disons que $d \subset P(E)$ est une **droite projective** de $P(E)$ si $d = P(D)$ pour une plan vectoriel $D \subset E$.

Exemple 10.10

Nous considérons les plans affines

$$\Pi_1 \equiv z = 0 \quad (10.17a)$$

$$\Pi_2 \equiv z = 1 \quad (10.17b)$$

et nous avons la bijection

$$P(E) = \Pi_2 \cup P(\Pi_1). \quad (10.18)$$

Un plan affine D a deux possibilités : soit il coupe Π_2 en une droite, soit il est égal à Π_1 . Si $D \cap \Pi_2 = d$ (d est une droite affine), alors nous avons

$$P(D) = d \cup \{\infty_D\}, \quad (10.19)$$

ce qui justifie la terminologie comme quoi $P(D)$ est une droite dans $P(E)$. $\triangle$

Soit E un espace vectoriel de dimension 3 et le plan projectif $P(E)$. Nous avons deux types de droites projectives :

- (1) D'abord nous avons la droite à l'infini, donnée¹ par $P(z = 0)$.
- (2) Ensuite nous avons toutes les droites affines du plan $z = 1$. Chacune de ces droites est complétée par un point à l'infini.

Exemple 10.11

Étudions un peu le second type de droites. D'abord si deux droites sont parallèles, leurs points à l'infini sont identiques. Prenons par exemple les droites $d = \{z = 1, x = 1\}$ et $d' = \{z = 1, x = 2\}$. Elles décrivent les directions des vecteurs

$$\begin{pmatrix} 1 \\ y \\ 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 2 \\ y \\ 1 \end{pmatrix}. \quad (10.20)$$

En normalisant, ce sont les vecteurs

$$\frac{1}{\sqrt{2+y^2}} \begin{pmatrix} 1 \\ y \\ 1 \end{pmatrix} \quad \text{et} \quad \frac{1}{\sqrt{5+y^2}} \begin{pmatrix} 2 \\ y \\ 1 \end{pmatrix}, \quad (10.21)$$

et toutes deux tendent vers le vecteur $(0, 1, 0)$ pour $y \rightarrow \infty$. $\triangle$

Lemme 10.12.

Deux droites d'un plan projectif ont toujours une intersection.

Démonstration. Si les deux droites sont des droites affines non parallèles, le résultat est évident. Si elles sont parallèles, alors l'intersection est donnée par le point à l'infini comme indiqué dans l'exemple 10.11.

Supposons que d est la droite à l'infini tandis que d' est une droite affine. Dans notre représentation usuelle du plan affine, la droite à l'infini d contient les vecteurs $(1, y, 0)$ et le point à l'infini $(0, 1, 0)$. La droite affine d' a pour équation paramétriques

$$\begin{cases} x = at + c \\ y = bt + d \\ z = 1. \end{cases} \quad \begin{array}{l} (10.22a) \\ (10.22b) \\ (10.22c) \end{array}$$

Les directions données par la droite d' sont donc

$$\frac{1}{a^2t^2 + b^2t^2 + c^2 + d^2} \begin{pmatrix} at + c \\ bt + d \\ 1 \end{pmatrix} \quad (10.23)$$

Son point à l'infini est la direction du vecteur $(a, b, 0)$, qui est bien un point de la droite à l'infini (éventuellement son point à l'infini²). $\square$

La plupart du temps nous considérons le plan projectif comme étant le plan affine $z = 1$ de l'espace affine de dimension 3 complété par la droite affine $x = 1, z = 0$, elle-même complétée par le point $(0, 1, 0)$. Ce n'est évidemment pas la seule manière. Tout plan peut être considéré comme le plan à l'infini et pour une droite projective, tout point peut être considéré comme point à l'infini.

Sur la figure 10.1(a), le point à l'infini est la direction $(1, 0)$ tandis que la direction $(1, 1)$ n'a rien de spécial. À l'inverse sur la figure 10.1(b), la direction à l'infini est $(1, 1)$ tandis que la direction $(1, 0)$ est une direction usuelle.

1. Dans notre représentation usuelle du plan projectif $z = 1$.

2. D'accord, aller chercher le point à l'infini de la droite à l'infini, c'est chercher loin, mais n'empêche que ça existe.

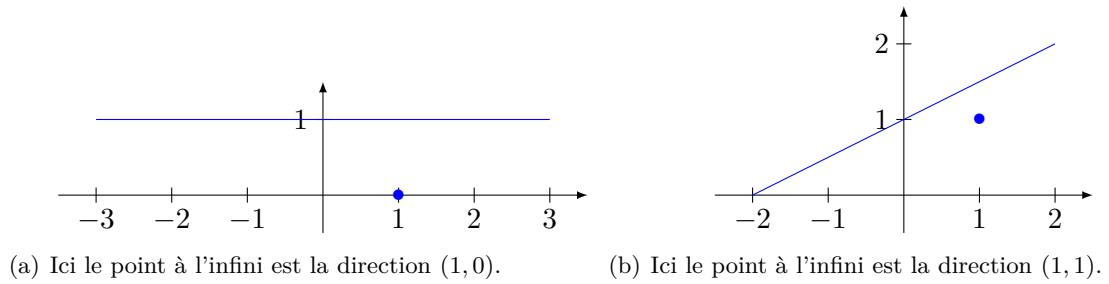


FIGURE 10.1 – Deux façons de voir la droite projective. Étant donné que les points de la droite projective doivent être interprétés comme des directions (des classes d'équivalence), en réalité les deux dessins représentent les mêmes ensembles.

Remarque 10.13.

Du point de vue de la topologie, si nous mettons celle de la compactification d'Alexandroff, tous les points de la droite projective sont équivalents.

Du point de vue de la géométrie différentielle, c'est la même chose. En effet nous pouvons mettre sur la droite projective un système de deux cartes en pensant aux angles. La première sur $] -a, a[$ avec par exemple $a < \pi/4$. La seconde carte serait $]a/2, \pi[$. Dans ce cas la direction $\theta = 0$ semble jouer un rôle spécial, mais il n'en est rien.

Nous pouvons également considérer les cartes $]\pi/4 - a, \pi/4 + a[$ et $]\pi/4 + a/2, 5\pi/4[$. Dans ces cartes, c'est plutôt le point $\theta = \pi/4$ qui semble différent (encore qu'il soit bien centré dans une carte).

10.3 Théorème de Pappus

Théorème 10.14.

Soient deux droites d et d' dans un plan affine. Soient $A, B, C \in d$ et $A', B', C' \in d'$ tels que $AB' \parallel BA'$ et $BC' \parallel B'C$. Alors $AC' \parallel A'C$.

Démonstration. Si d et d' ne sont pas parallèles nous considérons o , le point d'intersection. Les relations de parallélisme des hypothèses impliquent qu'il existe λ_1 et λ_2 tels que

$$\begin{cases} A = \lambda_1 B \\ B' = \lambda_1 A' \end{cases} \quad (10.24a)$$

$$(10.24b)$$

et

$$\begin{cases} B' = \lambda_2 C' \\ C = \lambda_2 B. \end{cases} \quad (10.25a)$$

$$(10.25b)$$

En substituant nous trouvons

$$\begin{cases} C = \frac{\lambda_2}{\lambda_1} A \\ A' = \frac{\lambda_2}{\lambda_1} C', \end{cases} \quad (10.26a)$$

$$(10.26b)$$

ce qui implique que $A'C \parallel AC'$.

Si les droites d et d' sont parallèles, alors nous avons les translations

$$\begin{cases} B = A + x \\ A' = B' + x \end{cases} \quad (10.27a)$$

$$(10.27b)$$

et

$$\begin{cases} B = C + y \\ C' = B' + y, \end{cases} \quad (10.28a)$$

$$(10.28b)$$

ce qui montre que

$$\begin{cases} C = A + x - y \\ A' = C' + x - y, \end{cases} \quad \begin{matrix} (10.29a) \\ (10.29b) \end{matrix}$$

et donc que $A'C \parallel AC'$. $\square$

Le théorème suivant est une version projective.

Théorème 10.15.

Soient d et d' deux droites projectives d'un plan projectif. Soient $A, B, C \in d$ et $A', B', C' \in d'$. Alors les points $B'C \cap C'B$, $C'A \cap A'C$ et $A'B \cap B'A$ sont alignés.

Démonstration. Soient $E = BC' \cap C'B$ et $E' = C'A \cap A'C$. Ces deux points existent parce que deux droites projectives distinctes ont toujours un unique point d'intersection. Nous allons prendre EE' comme droite à l'infini et prouver que le point $A'B \cap B'A$ est dessus. Étant donné que le point d'intersection de $B'C$ et $C'B$ est à l'infini nous avons $B'C \parallel C'B$ (cela est un exemple de la flexibilité de la notion de parallélisme en géométrie projective). De la même façon nous avons $C'A \parallel A'C$.

Par le théorème de Pappus affine nous avons alors $A'B \parallel B'A$ et par conséquent le point d'intersection est sur la droite à l'infini, c'est à dire sur la droite EE' . $\square$

10.4 Homographies

10.4.1 Homographies

Définition 10.16.

Soient E et F deux espaces vectoriels avec leurs projections naturelles

$$\pi_E: E \setminus \{0\} \rightarrow P(E) \quad (10.30a)$$

$$\pi_F: F \setminus \{0\} \rightarrow P(F). \quad (10.30b)$$

*Une application $g: P(E) \rightarrow P(F)$ est une **homographie** si il existe un isomorphisme d'espaces vectoriels $\tilde{g}: E \rightarrow F$ tel que le diagramme*

$$\begin{array}{ccc} E \setminus \{0\} & \xrightarrow{\tilde{g}} & F \setminus \{0\} \\ \pi_E \downarrow & & \downarrow \pi_F \\ P(E) & \xrightarrow{g} & P(F) \end{array} \quad (10.31)$$

commute, c'est à dire si il existe $\tilde{g}: E \rightarrow F$ telle que

$$\pi_F(\tilde{g}(v)) = g(\pi_E(v)) \quad (10.32)$$

pour tout $v \in E$.

Lemme 10.17.

Si $\tilde{g}: E \rightarrow F$ est linéaire et si $\ker \tilde{g} = \{0\}$ alors l'application g définie par

$$g(\pi_E(v)) = \pi_F(\tilde{g}(v)) \quad (10.33)$$

est une homographie.

Démonstration. Nous devons simplement vérifier que l'équation (10.33) définit bien une application. Soient $v, w \in E$ tels que $\pi_E v = \pi_E w$; nous devons montrer que

$$\pi_F \tilde{g} v = \pi_F \tilde{g} w. \quad (10.34)$$

L'équation (10.34) sera vérifiée si et seulement si il existe $\lambda \in \mathbb{R}$ tel que $\tilde{g}v = \lambda\tilde{g}w$, c'est à dire si et seulement si $\tilde{g}(v - \lambda w) = 0$. Étant donné que nous supposons que le noyau de $\tilde{g}$ est réduit à $\{0\}$, l'équation (10.34) sera vérifiée si et seulement si $v = \lambda w$, ce qui signifie exactement $\pi_E(v) = \pi_E(w)$. $\square$

La proposition suivante donne les premières propriétés des homographies.

Proposition 10.18.

Quelques propriétés des homographies.

- (1) Une homographie est bijective.
- (2) Si deux espaces projectifs sont homographes, alors ils ont même dimension.
- (3) L'ensemble des homographies $P(E) \rightarrow P(F)$ est un groupe (pour la composition).
- (4) Une homographie conserve l'alignement des points.

Démonstration. Nous considérons une homographie $g: P(E) \rightarrow P(F)$, et $\tilde{g}$ l'isomorphisme d'espaces vectoriels correspondant.

- (1) Pour l'injectivité, si $g([v]) = g([w])$ alors en utilisant la définition d'une homographie, $\pi_F \tilde{g}v = \pi_F \tilde{g}w$, ce qui implique que $\tilde{g}v = \lambda\tilde{g}w$, et donc $v = \lambda w$, ce qui signifie $[v] = [w]$.
Pour la surjectivité, un élément général de $P(F)$ prend la forme $\pi_F \tilde{g}v$ pour un certain $v \in E$. Nous avons $g(\pi_E v) = \pi_F \tilde{g}v$. Par conséquent l'élément $\pi_F \tilde{g}v$ est bien dans l'image de g .
- (2) Une homographie $P(E) \rightarrow P(F)$ n'existe que si il existe un isomorphisme $E \rightarrow F$. Les dimensions sont donc automatiquement égales.
- (3) Il suffit de vérifier que l'application

$$\begin{aligned} \varphi: P(E) &\rightarrow P(E) \\ \pi_F \tilde{g}v &\mapsto \pi_E v \end{aligned} \tag{10.35}$$

est bien définie et donne l'inverse de g .

- (4) Soient les points A, B, C alignés dans $P(E)$; ils correspondent à des directions de E qui sont données par des vecteurs situés sur la même droite affine. Autrement dit, il existe trois points $a, b, c \in E$ situés sur la même droite affine tels que $A, B, C = \pi_E(a, b, c)$. Les images par g sont données par $\pi_F \tilde{g}a, \pi_F \tilde{g}b$, et $\pi_F \tilde{g}c$.
Étant donné qu'un isomorphisme d'espaces vectoriels conserve l'alignement affine, les points $\tilde{g}a, \tilde{g}b$ et $\tilde{g}c$ sont alignés dans F . Cela implique que les projections par π_F sont alignés dans $P(F)$. $\square$

10.4.2 Le groupe projectif

Définition 10.19.

Le groupe des homographies de l'espace $P(E)$ est le **groupe projectif**, noté $\text{PGL}(E)$.

Nous avons une surjection naturelle

$$\begin{aligned} \text{GL}(E) &\rightarrow \text{PGL}(E) \\ \tilde{g} &\mapsto g \end{aligned} \tag{10.36}$$

qui s'avère être un morphisme de groupes.

Proposition 10.20.

Nous avons l'isomorphisme de groupes

$$\frac{\text{GL}(E)}{\{\text{homothéties}\}} \simeq \text{PGL}(E). \tag{10.37}$$

Démonstration. Nous devons prouver que le noyau de l'application (10.36) est constitué des homothéties. Considérons un automorphisme d'espace vectoriel $f: E \rightarrow E$ dont l'homographie associée est l'identité, et prouvons que f est une homothétie. Nous avons le diagramme commutatif suivant :

$$\begin{array}{ccc} E \setminus \{0\} & \xrightarrow{f} & E \setminus \{0\} \\ \pi_E \downarrow & & \downarrow \pi_E \\ P(E) & \xrightarrow{\text{Id}} & P(E). \end{array} \quad (10.38)$$

Pour tout vecteur $v \in E$ nous avons $\pi_E(v) = \pi_E(f(v))$. Cela implique qu'il existe $\lambda \in \mathbb{R}$ tel que $f(v) = \lambda v$. Tous les vecteurs de E sont donc des vecteurs propres de f . Cela n'est possible que si toutes les valeurs propres sont identiques, c'est à dire que f est une homothétie. $\square$

10.5 Coordonnées homogènes

Soit E un espace vectoriel de dimension $n + 1$ et une base $\{e_0, \dots, e_n\}$ de E . Soit $M \in P(E)$ et $u \in E$ un élément engendrant M . Au point M nous voudrions associer les coordonnées $(x_0, \dots, x_n)$ de u dans E . Notons que toutes les coordonnées de u ne sont jamais nulles en même temps parce que u doit indiquer une direction. Nous savons par ailleurs que les coordonnées $(x_0, \dots, x_n)$ indiquent le même point de $P(E)$ que les coordonnées $(x'_0, \dots, x'_n)$ si et seulement si $x_i = \lambda x'_i$.

Définition 10.21.

La classe d'équivalence de $(x_0, \dots, x_n)$ est la **coordonnées homogène** de M . Nous la notons $(x_0 : \dots : x_n)$.

10.5.1 Dualité

Soit E un espace vectoriel de dimension $n + 1$. Une forme linéaire non nulle est un élément de E^* , mais aussi un représentant d'un élément de $P(E^*)$.

Le noyau d'une forme linéaire ω est un hyperplan. Le noyau de la forme linéaire $\lambda\omega$ étant le même hyperplan, l'hyperplan est donné par toute la classe de ω dans $P(E^*)$. Nous avons donc une bijection

$$P(E^*) \leftrightarrow \{\text{hyperplans vectoriels de } E\}. \quad (10.39)$$

Soit E de dimension 3 et une base $\{e_1, e_2, e_3\}$. L'espace dual E^* possède la base duale $\{e_1^*, e_2^*, e_3^*\}$. À un élément $m \in P(E^*)$ nous associons la droite

$$H_m \{(X : Y : T) \text{ tel que } m(X, Y, T) = 0\} \quad (10.40)$$

dans $P(E)$. Si les coordonnées homogènes de m étaient $(u : v : w)$ alors l'équation de la droite H_m est

$$uX + vY + wT = 0. \quad (10.41)$$

En effet si $\omega \in E^*$ est un représentant de m alors $\omega = \lambda(ue_1^* + ve_2^* + we_3^*)$ et l'équation (10.41) est indépendante de λ ainsi que du choix du représentant dans E du point $(X : Y : T)$ dans $P(E)$.

Si les points m_1 et m_2 sont distincts dans $P(E^*)$, ils donnent deux droites $m_1(X, Y, T) = 0$ et $m_2(X, Y, T) = 0$. Les points de la droite qui joint m_1 à m_2 dans $P(E^*)$ sont de la forme $\lambda m_1 + \mu m_2$ et ils sont associés à l'équation

$$\lambda m_1(X, Y, T) + \mu m_2(X, Y, T) = 0 \quad (10.42)$$

qui sont encore des droites dans $P(E)$. Toutes ces droites passent par le point d'intersection des droites associées à m_1 et m_2 . Nous avons donc

$$\bigcap_{\lambda, \mu} H_{\lambda m_1 + \mu m_2} = H_{m_1} \cap H_{m_2}. \quad (10.43)$$

Lemme 10.22.*L'application*

$$\begin{aligned} P(E^*) &\rightarrow \{\text{droites dans } P(E)\} \\ m &\mapsto H_m \end{aligned} \quad (10.44)$$

est une bijection.

Démonstration. Une droite dans $P(E)$ est donnée en coordonnées homogènes par une équation $aX + bY + cT = 0$. Cette droite est décrite par le point $(a : b : c)$ dans $P(E^*)$. Ce dernier correspond à la direction de la forme $ae_1^* + be_2^* + ce_3^*$. Cela prouve que l'application est surjective.

Pour l'injectivité, si $m_1 \neq m_2$ dans $P(E^*)$, les formes ω_1 et ω_2 associées dans E^* ne sont pas multiples l'une de l'autre. Donc les équations

$$a_1X + b_1Y + z_1T = 0 \quad (10.45)$$

et

$$a_2X + b_2Y + z_2T = 0 \quad (10.46)$$

n'ont pas de solutions communes et décrivent donc des droites distinctes. $\square$ **Lemme 10.23.**

Trois points distincts m_1, m_2 et m_3 dans $P(E^*)$ sont alignés si et seulement si les droites H_{m_1}, H_{m_2} et H_{m_3} sont distinctes et concourantes.

Démonstration. Supposons avoir trois points alignés, c'est à dire

$$m_3 = m_1 + \mu(m_2 - m_1). \quad (10.47)$$

Soit $X : Y : T$ le point d'intersection de H_{m_1} avec H_{m_2} . Alors $m_1(X, Y, T) = m_2(X, Y, T) = 0$. En tenant compte de (10.47) nous avons alors évidemment $m_3(X, Y, T) = 0$.

Supposons maintenant que les trois droites H_{m_i} soient concourantes. Nous avons donc un point $(X : Y : T)$ dans $P(E)$ tel que $m_i(X, Y, T) = 0$. Si m_i est la classe de $a_ie_1^* + b_ie_2^* + c_ie_3^*$ alors nous avons le système

$$\begin{cases} a_1X + b_1Y + c_1T = 0 & (10.48a) \\ a_2X + b_2Y + c_2T = 0 & (10.48b) \\ a_3X + b_3Y + c_3T = 0. & (10.48c) \end{cases}$$

Afin que cela ait une solution non triviale nous devons avoir

$$\det \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \neq 0, \quad (10.49)$$

c'est à dire que les points (a_i, b_i, c_i) soient alignés. $\square$

En tenant compte de ce qui a été dit, une droite dans $P(E^*)$ est constituée de points qui fournissent des droites concourantes dans $P(E)$. Donc une droite de $P(E^*)$ se caractérise par un point de $P(E)$ (l'intersection) de la façon suivante. Un point $M_d \in P(E)$ donne lieu à un **faisceau de droites** passant par M_d . Chacune de ces droites donne lieu à un point de $P(E^*)$ et tous ces points sont alignés. Nous avons ainsi construit la droite d dans $P(E^*)$ correspondante au point M_d de $P(E)$.

10.5.2 Polynômes

Soit l'espace projectif de dimension n avec ses coordonnées homogènes $(X_0 : \dots : X_n)$. Nous considérons l'espace affine $H \equiv X_n = 1$ dans l'espace vectoriel E de dimension $n + 1$. Nous considérons pour H un repère affine ayant pour origine le point $(0, \dots, 0, 1)$. Considérons un polynôme homogène P sur le corps $\mathbb{K}$. L'équation

$$P(X_0, \dots, X_n) = 0 \quad (10.50)$$

sur l'espace vectoriel E descend immédiatement à l'espace projectif : étant donné que P est homogène nous avons $P(u) = 0$ si et seulement si $P(\lambda u) = 0$.

Nous essayons de décrire l'ensemble A des points de $P(E)$ satisfaisant $P(X_0, \dots, X_n) = 0$. Nous savons que les éléments de $P(E)$ ont chacun un représentant soit dans H soit sur la droite à l'infini. Ceux de A ayant un représentant dans H sont d'équation

$$Q(x_0, \dots, x_{n-1}) = 0 \quad (10.51)$$

où Q est le polynôme donné par $Q(X_0, \dots, x_{n-1}) = P(x_0, \dots, x_{n-1}, 1)$. Les points de A ayant un représentant sur la droite à l'infini s'obtiennent par l'équation

$$R(x_0, \dots, x_{n-1}) = 0 \quad (10.52)$$

où R est le polynôme donné par $R(x_0, \dots, x_{n-1}) = P(x_0, \dots, x_{n-1}, 0)$.

Exemple 10.24

Nous considérons la conique projective

$$X^2 - XT - Y^2 - T^2 = 0. \quad (10.53)$$

Elle est décomposée en deux parties : une dans l'espace affine «normale» et une à l'infini. La première s'obtient en posant $T = 1$ dans (10.53) :

$$x^2 - x - y^2 - 1 = 0. \quad (10.54)$$

L'autre est obtenue en posant $T = 0$:

$$x^2 - y^2 = 0. \quad (10.55)$$

La partie à l'infini est donc composée de deux points : $(1 : 1 : 0)$ et $(1 : -1 : 0)$.

Le graphique de l'équation (10.54) est donné à la figure 10.2. Nous y voyons que les asymptotes sont effectivement données par les directions $(1, 1)$ et $(1, -1)$ dans le plan.

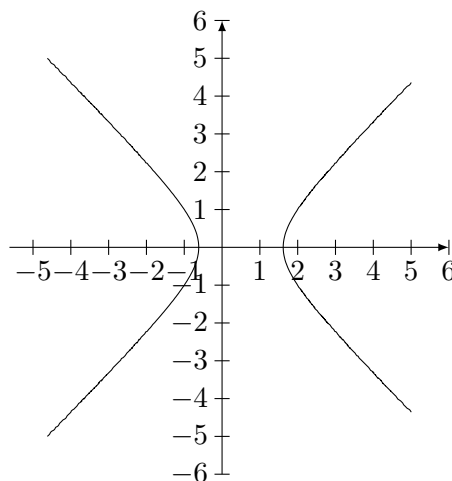


FIGURE 10.2 – Le graphique de $x^2 - x - y^2 - 1 = 0$.

△

Nous pouvons tenter de faire l'exercice inverse : considérer une conique dans $\mathbb{R}^2$, la voir comme une partie d'une conique dans l'espace projectif et trouver les points à l'infini qui la complètent.

Exemple 10.25

La droite projective usuelle est donnée par la droite affine $y - 1 = 0$. L'homogénéisation donne $y - z = 0$ et par conséquent la partie à l'infini est donnée par $y = 0$, c'est à dire la direction $(1, 0)$ comme il se doit. △

Exemple 10.26

Prenons la conique

$$x^2 + xy + y^3 - 2 = 0. \quad (10.56)$$

D'abord nous homogénéisons cette équation pour la voir dans $\mathbb{R}^3$:

$$x^2z + xyz + y^3 - 2z^3 = 0. \quad (10.57)$$

Les points à l'infini sont ceux qui correspondent à $z = 0$, c'est à dire la droite donnée en coordonnées homogènes par $(1 : 0 : 0)$. △

10.5.3 Repères projectifs

Si nous avons une base $\{e_i\}$ de $\mathbb{R}^n$ nous associons à $M \in P(E)$ les coordonnées $(X : Y : T)$. Mais si on prend la base $\{2e_1, e_2, \dots, e_n\}$, les coordonnées du même point deviennent $(X/2 : Y : T)$ alors que du point de vue de l'espace projectif, rien n'a été changé : la classe de e_1 est la même que celle de $2e_1$. Les coordonnées homogènes ne sont donc pas intrinsèques.

Définition 10.27.

Soit E un espace vectoriel de dimension $n + 1$. Un **repère projectif** de $P(E)$ est la donnée de $n + 2$ points $m_0, \dots, m_{n+1}$ tels que

- (1) les vecteurs m_i , $i \neq 0$, sont les images d'une base $\{e_i\}$ de E
- (2) $m_0 = \pi_E(e_1 + e_2 + \dots + e_{n+1})$.

Note que si $m_k = \pi_E(v_k)$ ($k = 0, \dots, n + 1$), alors tout choix de $n + 1$ vecteurs parmi les v_k est une base de E .

Lemme 10.28.

Soit $(m_0, \dots, m_{n+1})$ un repère projectif de $P(E)$. Soient $\{e_1, \dots, e_{n+1}\}$ et $\{f_1, \dots, f_{n+1}\}$ deux bases qui se projettent sur $\{m_i\}$ (c'est à dire $\pi_E(e_i) = \pi_E(f_i) = m_i$). Si $\pi_E(e_1 + \dots + e_{n+1}) = \pi_E(f_1 + \dots + f_{n+1})$ alors les deux bases sont proportionnelles : il existe un λ tel que $f_i = \lambda e_i$.

Théorème 10.29.

Soient $P(E)$ et $P(F)$ deux espaces projectifs de dimensions n .

- (1) Une homographie $P(E) \rightarrow P(E)$ envoie un repère projectif sur un repère projectif.
- (2) Si $(m_0, \dots, m_{n+1})$ est un repère projectif de $P(E)$, si $(m'_0, \dots, m'_{n+1})$ est un repère projectif de $P(F)$ alors il existe une unique homographie $g: P(E) \rightarrow P(F)$ telle que $g(m_i) = m'_i$ pour tout $i = 0, 1, \dots, n + 1$

Si nous avons une droite projective, trois points sont nécessaires pour créer un repère et donc pour construire une homographie de la droite sur elle-même. Soit E un espace vectoriel de dimension 2 et $P(E)$ la droite projective qui lui est associée. Soit une homographie $f: P(E) \rightarrow P(E)$ et $\tilde{f}: E \rightarrow E$, l'isomorphisme d'espaces vectoriels associé (par $f \circ \pi_E = \pi_E \circ \tilde{f}$). Si $\{e_1, e_2\}$ est une base de E alors l'application $\tilde{f}$ a une matrice

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathbb{M}(2, \mathbb{K}) \quad (10.58)$$

avec $\det A \neq 0$ parce que $\tilde{f}$ est un isomorphisme.

La plupart des points de $P(E)$ sont représentés par des points de la forme $(z, 1)$. Nous voudrions savoir quelle est la direction représentée par le point $\tilde{f}(z, 1)$; c'est à dire que nous voudrions savoir $f([z, 1])$ sous la forme $[z', 1]$ (si possible). Nous avons

$$\tilde{f}(z, 1) = (a_{11}z + a_{12}, a_{21}z + a_{22}). \quad (10.59)$$

Nous posons $\lambda = a_{21}z + a_{22}$ et nous avons

$$\tilde{f}(z, 1) = \lambda \left(\frac{a_{11}z + a_{12}}{\lambda}, 1 \right). \quad (10.60)$$

Il y a plusieurs possibilités suivant les valeurs de λ et de z .

- (1) Si $\lambda = 0$ c'est que nous avons $\tilde{f}(z, 1) = (a_{11}z + a_{12}, 0)$. L'application f envoie donc le point $(z : 1)$ sur le point à l'infini.
- (2) Si $\lambda \neq 0$, alors f envoie le point $(z : 1)$ vers un autre point «normal».
- (3) Si le point de départ est le point à l'infini alors $\tilde{f}(1, 0) = (a_{11}, a_{21})$. Cela peut être le point à l'infini ou non selon les valeurs des a_{ij} .

Dans tous les cas si nous posons

$$\begin{cases} \varphi_f(z) = \frac{a_{11}z + a_{12}}{a_{21}z + a_{22}} \\ \varphi_f(\infty) = \frac{a_{11}}{a_{21}} \end{cases} \quad (10.61a)$$

$$(10.61b)$$

alors nous avons

$$\tilde{f}(z, 1) = (\varphi_f(z), 1). \quad (10.62)$$

Si nous prenons la convention que $\frac{1}{0} = \infty$ et que $(\infty, 0)$ est le point à l'infini, alors cette application φ_f donne bien toutes les valeurs de f , y compris les cas à l'infini.

10.5.4 Birapport

Soit une droite projective d et trois points distincts a, b et c sur cette droite. Étant donné qu'ils forment un repère projectif, il existe une unique homographie

$$\begin{aligned} g: d &\rightarrow \mathbb{K} \cup \{\infty\} \\ a &\mapsto \infty \\ b &\mapsto 0 \\ c &\mapsto 1. \end{aligned} \quad (10.63)$$

Si x est un point de d alors nous nommons le **birapport** de x par rapport à a, b et c l'élément

$$[a, b, c, x] = g(x) \quad (10.64)$$

dans $\mathbb{K} \cup \{\infty\}$.

- (1) Les points a, b, c et x sont distincts si et seulement si $[a, b, c, x] \in \mathbb{K} \setminus \{0, 1\}$.
- (2) Étant donné que les coordonnées homogènes sont bijectives, si $k \in \mathbb{K} \cup \{\infty\}$ alors il existe un unique $x \in d$ tel que $[a, b, c, x] = k$.

Théorème 10.30.

Une bijection entre deux droites projectives est une homographie si et seulement si elle conserve le birapport.

Proposition 10.31.

Soient $a, b, c, d \in \mathbb{K} \cup \{\infty\}$. Alors

$$[a, b, c, x] = \frac{(x - b)/(x - a)}{(c - b)/(c - a)} \quad (10.65)$$

où par convention nous prenons $1/0 = \infty$.

Démonstration. Soit D une droite projective et les coordonnées $\{(1, z)\} \cup \{\infty\}$ dessus. Nous notons φ la fonction du membre de droite de (10.65). L'homographie

$$\begin{aligned} &: D \rightarrow \mathbb{K} \cup \{\infty\} \\ &z \mapsto \varphi(z) \end{aligned} \quad (10.66)$$

envoie a sur ∞ , b sur 0 et c sur 1 . C'est donc bien cette homographie que définit le birapport et $x \mapsto [a, b, c, x]$. $\square$

Lemme 10.32.

Soient a, b, c distincts sur la droite projective $D = P(E)$. Soient $x, y \in E$ tels que $\pi_E(x) = a$, $\pi_E(y) = b$, $\pi_E(x + y) = c$. Alors

$$d = \pi_E(\lambda x + \mu y) \quad (10.67)$$

si et seulement si

$$[a, b, c, d] = \pi_{\mathbb{K}^2}(\lambda, \mu). \quad (10.68)$$

Démonstration. Étant donné que a et b sont distincts, les vecteurs x et y forment une base de E . Soit $f: E \rightarrow \mathbb{K}^2$ un isomorphisme qui envoie (x, y) sur e_1, e_2 où e_i sont les vecteurs de base de $\mathbb{K}^2$. Ensuite nous considérons $g: P(E) \rightarrow P(\mathbb{K}^2)$, l'homographie associée à f . Par définition $f(\pi_E z) = \pi_{\mathbb{K}^2}(f(z))$. Par f nous avons

$$a \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad b \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (10.69)$$

Donc par g nous avons

$$a \mapsto \infty \quad b \mapsto 0. \quad (10.70)$$

Nous avons aussi $f(\lambda x + \mu y) = (\lambda, \mu)$ et

$$g(c) = g(\pi_E(x + y)) \quad (10.71a)$$

$$= \pi_F f(x + y) \quad (10.71b)$$

$$= \pi_F(f(x) + f(y)) \quad (10.71c)$$

$$= \pi_F \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (10.71d)$$

$$= 1. \quad (10.71e)$$

La dernière égalité est le fait que la direction $(1, 1)$ dans $\mathbb{R}^2$ est représentée par le point $x = 1$ sur la droite $y = 1$ qui est notre «représentation» de la droite affine. L'application g a donc toutes les propriétés qu'il faut pour être l'application qui définit le birapport. Nous avons donc bien $g(d) = [a, b, c, d]$.

D'une part si $d = \pi_E(\lambda x + \mu y)$ alors

$$g(d) = \pi_{\mathbb{K}^2} f(\lambda x + \mu y) = \pi_{\mathbb{K}^2}(\lambda, \mu). \quad (10.72)$$

Dans l'autre sens si $[a, b, c, d] = \pi_{\mathbb{K}^2}(\lambda, \mu)$ alors supposons que $g(d) = \pi_{\mathbb{K}^2}(\lambda, \mu)$ avec $d = \pi_E(v)$ alors

$$g\pi_E v = \pi_{\mathbb{K}^2} f(v), \quad (10.73)$$

ce qui implique $f(v) = \alpha(\lambda, \mu)$ pour un certain $\alpha \in \mathbb{K}$. Par conséquent $v = \alpha(\lambda x + \mu y)$ et $d = \pi_E(\lambda x + \mu y)$. $\square$

10.6 Sphère de Riemann

La **sphère de Riemann** est l'espace projectif modelé sur $\mathbb{C}^2$: en vertu des notations données à la page 531, c'est

$$P_1(\mathbb{C}) = P(\mathbb{C}^2). \quad (10.74)$$

Une homographie de cet espace est une application g qui vérifie

$$g(\pi(z_1, z_2)) = \pi(\tilde{g}(z_1, z_2)) \quad (10.75)$$

pour un certain automorphisme de $\mathbb{C}^2$. En ce qui concerne π , nous pouvons prendre la convention

$$P_1(\mathbb{C}) = \{(z, 1), z \in \mathbb{C}\} \cup \{(1, 0)\} \quad (10.76)$$

et alors avoir la projection

$$\pi \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} \frac{z_1}{z_2}, 1 \end{pmatrix} & \text{si } z_2 \neq 0 \\ (1, 0) = \infty & \text{si } z_2 = 0. \end{cases} \quad (10.77)$$

Par ailleurs un automorphisme de $\mathbb{C}^2$ est de la forme

$$\tilde{g} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \quad (10.78)$$

avec $ad - bc \neq 0$. Cela induit

$$g \left(\frac{z_1}{z_2}, 1 \right) = \pi \left(\begin{pmatrix} az_1 + bz_2 \\ cz_1 + dz_2 \end{pmatrix} \right) = \begin{cases} \left(\frac{az_1 + bz_2}{cz_1 + dz_2}, 1 \right) & \text{si } cz_1 + dz_2 \neq 0 \\ \infty & \text{sinon.} \end{cases} \quad (10.79)$$

Nous avons aussi

$$g(\infty) = \pi(\tilde{g}(1, 0)) = \pi \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \pi \begin{pmatrix} a \\ c \end{pmatrix} = \begin{cases} \frac{a}{c} & \text{si } c \neq 0 \\ \infty & \text{si } c=0. \end{cases} \quad (10.80)$$

Étant donné que les coordonnées peuvent être multipliées $((a, b) = (\lambda a, \lambda b))$ nous pouvons récrire l'homographie sous la forme

$$g(z_1, z_2) = (az_1 + bz_2, cz_1 + dz_2). \quad (10.81)$$

Nous avons aussi

$$g^{-1}(\infty) = \{\pi(z_1, z_2) \text{ tel que } cz_1 + dz_2 = 0\}. \quad (10.82)$$

10.6.1 Action du groupe modulaire

Le **demi-plan de Poincaré** est l'ensemble

$$P = \{z \in \mathbb{C} \text{ tel que } \Im(z) > 0\}. \quad (10.83)$$

Le **groupe modulaire** est le quotient de groupes

$$\text{PSL}(2, \mathbb{Z}) = \frac{\text{SL}(2, \mathbb{Z})}{\mathbb{Z}_2}. \quad (10.84)$$

Ce sont donc les matrices au signe près de la forme

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (10.85)$$

où a, b, c et d sont entiers tels que $ad - cb = 1$.

Théorème 10.33 ([145]).

Le groupe modulaire agit fidèlement (définition 2.56) sur le demi-plan de Poincaré par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * z = \frac{az + b}{cz + d}. \quad (10.86)$$

L'ensemble $D = D_1 \cup D_2$ avec

$$D_1 = \{z \in P \text{ tel que } |z| > 1, -\frac{1}{2} \leq \Re(z) < \frac{1}{2}\} \quad (10.87a)$$

$$D_2 = \{z \in P \text{ tel que } |z| = 1, -\frac{1}{2} \leq \Re(z) \leq 0\} \quad (10.87b)$$

est un domaine fondamental (définition 2.63) de cette action.

De plus si nous notons

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (10.88)$$

alors pour tout $z \in P$, il existe $A \in \text{gr}(S, T)$ telle que $A * z \in D$.

Démonstration. Nous divisons la preuve en plusieurs étapes.

Bien définie D'abord il faut remarquer que l'action (10.86) est bien définie par rapport au quotient : $A * z = (-A) * z$. La vérification est immédiate.

Interne Montrons que si $A \in \text{PSL}(2, \mathbb{Z})$ et $z \in P$ alors $A * z \in P$. Nous avons

$$A * z = \frac{az + b}{cz + d} = \frac{(az + b)(c\bar{z} + d)}{|cz + d|^2} = \frac{a|z|c + azd + bc\bar{z} + bd}{|cz + d|^2}, \quad (10.89)$$

et donc en décomposant $z = \Re(z) + i\Im(z)$,

$$\Im(A * z) = \Im\left(\frac{azd + bc\bar{z}}{|cz + d|^2}\right) = \frac{ad - bc}{|cz + d|^2} \Im(z) = \frac{\Im(z)}{|cz + d|^2} \quad (10.90)$$

où nous avons tenu compte de $ad - bc = 1$. Donc l'action respecte la (stricte) positivité de la partie imaginaire.

Action Nous vérifions maintenant que la formule donne bien une action : $A * (B * z) = (AB) * z$. Cela est un bon calcul :

$$A * (B * z) = A * \left(\frac{a'z + b'}{c'z + d'} \right) \quad (10.91a)$$

$$= \frac{a \left(\frac{a'z + b'}{c'z + d'} \right) + b}{c \left(\frac{a'z + b'}{c'z + d'} \right) + d} \quad (10.91b)$$

$$= \frac{a(a'z + b') + b(c'z + d')}{c(a'z + b') + d(c'z + d')} \quad (10.91c)$$

$$= \frac{(aa' + bc')z + (ab' + bd')}{(ca' + dc')z + (cb' + dd')} \quad (10.91d)$$

$$= \begin{pmatrix} aa' + bc' & ab' + bd' \\ a'c + dc' & cb' + dd' \end{pmatrix} * z \quad (10.91e)$$

$$= (AB) * z. \quad (10.91f)$$

Fidèle Soit $A \in \text{PSL}(2, \mathbb{Z})$ tel que pour tout $z \in P$ nous ayons

$$\frac{az + b}{cz + d} = z. \quad (10.92)$$

Alors nous avons

$$cz^2 + (d - a)z + b = 0. \quad (10.93)$$

Cela est donc un polynôme en z qui s'annule sur un ouvert³ (le demi-plan de Poincaré). Il doit donc être identiquement nul, donc $c = b = a - d = 0$. Si vous n'y croyez pas, écrivez pour $z = \epsilon i$ (avec $\epsilon > 0$) :

$$-c\epsilon^2 + \epsilon(d - a)i + b = 0 \quad (10.94)$$

pour tout ϵ . Le fait d'avoir $c\epsilon^2 = b$ pour tout ϵ implique que $c = b = 0$. Donc A est de la forme

$$A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \quad (10.95)$$

avec la contrainte supplémentaire que $ad = 1$, les nombres a et b étant entiers. Nous avons donc soit $a = d = 1$ soit $a = d = -1$. Étant donné le quotient par $\mathbb{Z}_2$, ces deux possibilités donnent le même élément de $\text{PSL}(2, \mathbb{Z})$.

Les orbites intersectent D Soit $z \in P$. Nous devons trouver $A \in \text{PSL}(2, \mathbb{Z})$ tel que $A * z \in D$. Nous savons déjà que

$$\Im(A * z) = \frac{\Im(z)}{|cz + d|^2}. \quad (10.96)$$

Nous notons $\mathcal{O}_z$ l'orbite de z sous le groupe modulaire et nous posons

$$I_z = \{\Im(u) \text{ tel que } u \in \mathcal{O}_z\} = \{\Im(A * z) \text{ tel que } A \in \text{PSL}(2, \mathbb{Z})\}, \quad (10.97)$$

l'ensemble des parties imaginaires des éléments de l'orbite de z . Nous allons montrer que cet ensemble est borné vers le haut en montrant que la quantité $|cz + d|$ ne peut, z donné, prendre qu'un nombre fini de valeurs plus grandes que $\Im(z)$ ⁴. Nous cherchons donc les couples $(c, d) \in \mathbb{Z}^2$ tels que $|cz + d| < 1$.

Nous avons $\Im(cz + d) = c\Im(z)$, donc $|cz + d| \geq |c\Im(z)|$, mais il n'y a qu'un nombre fini de $c \in \mathbb{Z}$ tels que $|c\Im(z)| < 1$. De la même façon, pour la partie réelle nous avons

$$\Re(cz + d) = c\Re(z) + d, \quad (10.98)$$

et pour chaque c , il n'y a qu'un nombre fini de $d \in \mathbb{Z}$ qui laissent cette quantité plus petite que 1 (en valeur absolue).

Donc I_z possède un maximum. Soit $A_1 \in \text{PSL}(2, \mathbb{Z})$ tel que $\Im(A_1 * z) = \max I_z$. Nous notons $z_1 = A_1 * z$, et que nous n'avons a priori pas l'unicité. Nous allons maintenant agir sur z_1 avec l'élément

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (10.99)$$

pour ramener z_1 dans le domaine D . Si $u \in P$ nous avons $T * u = u + 1$ et donc

$$T^n * u = u + n. \quad (10.100)$$

Vu que D est de largeur 1, il existe un n (éventuellement négatif) tel que

$$\Re(T^n * z_1) \in \left[-\frac{1}{2}, \frac{1}{2}\right]. \quad (10.101)$$

Notons qu'ici le fait d'être ouvert d'un côté et fermé de l'autre joue de façon essentielle (pour l'unicité aussi). Nous notons $z_2 = T^n * z_1$.

3. On ne peut pas dire que $b = 0$ simplement en justifiant qu'on l'obtient en posant $z = 0$ parce que $z = 0$ n'est pas dans le demi-plan de Poincaré.

4. Bien que cela ne soit pas indispensable pour la preuve, remarquons que I_z ne comprend qu'une quantité au plus dénombrable de valeurs. Le fait que, à z donné, la quantité $|cz + d|^2$ puisse être rendue aussi grande que l'on veut est évident. Donc I_z est borné vers le bas par zéro (qui n'est pas atteint, mais qui est une valeur d'adhérence).

Supposons un instant que $|z_2| < 1$. Nous considérons l'élément

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad (10.102)$$

qui fait

$$\Im(S * z) = \frac{\Im z}{|z|^2}. \quad (10.103)$$

Donc si $|z_2| < 1$ alors $\Im(S * z_2) > \Im(z_2)$, ce qui contredit la maximalité de $\Im(z_2)$ dans I_z . Nous en déduisons que $|z_2| \geq 1$. Nous en déduisons que $|z_2| \geq 1$.

Si $|z_2| > 1$, alors $z_2 \in D_1$ et c'est bon. Si $|z_2| = 1$, alors il faut encore un peu travailler. Si $z_2 \pm 1$ est à l'intérieur du disque, alors en agissant avec T ou T^{-1} nous retrouvons la même contradiction que précédemment. En écrivant $z_2 = e^{i\theta}$, nous devons donc avoir $2 \cos(\theta) \leq 1$ ou encore $|\Re(z_2)| \leq \frac{1}{2}$. Donc si $\Re(z_2) \leq 0$ alors $z_2 \in D_2$.

Le dernier cas à traiter est $\Re(z_2) \in]0, \frac{1}{2}]$, c'est à dire $\theta \in [\frac{\pi}{3}, \frac{\pi}{2}[$. Dans ce cas l'action avec S ramène l'angle dans la bonne zone parce que $S * z = -\frac{1}{z}$ et donc $S * (\rho e^{-i\theta}) = -\frac{1}{\rho} e^{-i\theta}$.

Unicité Nous voulons à présent montrer que si $z \in D$, alors $A * z$ n'est plus dans D (sauf si $A = \pm \mathbb{1}$). Nous supposons que $z \in D$ et $A \in \text{PSL}(2, \mathbb{Z})$ soient tels que $A * z \in D$, et nous prouvons qu'alors soit nous arrivons à une contradiction soit nous arrivons à $A = \mathbb{1}$. Pour cela nous allons décomposer en de nombreux cas.

(1) Nous commençons par $\Im(A * z) \geq \Im(z)$. Dans ce cas nous avons $|cz + d| \leq 1$ et en particulier $|c| |\Im(z)| \leq 1$. Étant donné que le point de D qui a la partie imaginaire la plus petite est $-\frac{1}{2} + \frac{2}{\sqrt{3}}i$, nous trouvons $|c| \leq 2/\sqrt{3}$. Vu que c doit être entier, nous avons trois cas : $c = -1, 0, 1$.

(a) Soit $c = 0$. Alors $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ et la condition de déterminant est $ad = 1$, ce qui signifie $a = d = 1$ (la possibilité $a = b = -1$ est «éliminée» le quotient par $\mathbb{Z}_2$ définissant $\text{PSL}(2, \mathbb{Z})$). La matrice A doit alors être de la forme

$$A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad (10.104)$$

et $A * z = z + b$. Si $z \in D$, alors le seul $z + b$ à être (peut-être) encore dans D est $b = 0$, mais alors A est l'identité.

(b) Soit $c = 1$. Alors la condition $|cz + d| \leq 1$ nous donne trois possibilités⁵ : $d = -1, 0, 1$.

i. Si $d = -1$, alors nous devons avoir $|z - 1| \leq 1$. Il est instructif de faire un dessin, mais le point d'intersection entre les cercles $|z| = 1$ et $|z - 1| = 1$ est le point $\frac{1}{2} + \frac{\sqrt{3}}{2}i$, qui n'est pas dans D . Bref, il n'y a pas de points dans D vérifiant $|z - 1| \leq 1$.

ii. Si $d = 1$, alors (et c'est maintenant que la dissymétrie de D intervient) nous avons le point

$$z = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \quad (10.105)$$

qui est dans D et qui vérifie $|z + 1| \leq 1$. Voyons à quoi ressemble la matrice A dans ce cas. Son déterminant est $a - b = 1$. Nous écrivons donc

$$A = \begin{pmatrix} b+1 & b \\ 1 & 1 \end{pmatrix}, \quad (10.106)$$

5. Je ne rigolais pas quand je disais qu'on allait avoir de nombreux cas.

et en tenant compte du fait que $z\bar{z} = |z + 1| = 1$, nous calculons

$$A * z = \frac{(b+1)z + b}{z + 1} \quad (10.107a)$$

$$= \frac{(bz + z + b)(\bar{z} + 1)}{|z + 1|^2} \quad (10.107b)$$

$$= z + b + 1. \quad (10.107c)$$

La seule façon de ne pas quitter D est d'avoir $b = -1$, mais alors nous avons

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad (10.108)$$

et $A * z = z$. Donc au final z est quand même le seul de son orbite à être dans D . Notons au passage cette très intéressante propriété du point

$$z_0 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i. \quad (10.109)$$

C'est un point de qui vérifie $z_0 = A * z_0$ pour un élément non trivial A de $\text{PSL}(2, \mathbb{Z})$. L'existence d'un tel élément est ce qui va nous coûter un peu de sueur pour prouver que $\text{PSL}(2, \mathbb{Z})$ est engendré par S et T .

iii. Le cas $d = 0$ nous fait écrire $1 = \det A = -b$, donc $b = -1$ et

$$A = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}. \quad (10.110)$$

Nous avons alors $A * z = a - \frac{1}{z}$. De plus la condition $|z| \leq 1$ revient à $|z| = 1$. Pour les nombres complexes de module 1, l'opération $z \rightarrow -1/z$ est la symétrie autour de l'axe des imaginaires purs. Le seul à ne pas sortir de D est le fameux $z = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, qui revient sur lui-même avec $a = -1$.

Nous passons à la possibilité $c = -1$. Dans ce cas la matrice est de la forme

$$A = \begin{pmatrix} a & b \\ -1 & d \end{pmatrix}, \quad (10.111)$$

et nous revenons au cas $c = 1$ en prenant $-A$ au lieu de A .

(2) Nous passons au cas $\Im(A * z) < \Im(z)$. Nous récrivons cette condition avec

$$\Im(A * z) < \Im(A^{-1} * (A * z)). \quad (10.112)$$

Si nous supposons que z et A sont tels que z et $A * z$ soient tous deux dans D , alors $z' = A * z$ est un élément de D tel que

$$\Im(z') < \Im(A^{-1} * z'). \quad (10.113)$$

Or nous avons vu qu'aucun élément de D vérifiant cette condition n'existait sans être trivial (celui qui ne bouge pas). Pour cela il suffit d'appliquer tout ce que nous venons de dire avec A^{-1} au lieu de A .

Quelques conclusions Après avoir passé tous les cas en revue, le fameux point $z_0 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ est l'unique point de D à accepter une matrice non triviale $A \in \text{PSL}(2, \mathbb{Z})$ telle que $z_0 = A * z_0$.

Nous remarquons aussi que tous les points de P sont ramenés dans D par une matrice obtenue comme produit de T , S , T^{-1} et S^{-1} .

□

Corollaire 10.34 ([146]).

Les matrices S et T génèrent le groupe modulaire au sens où toute matrice de $\mathrm{PSL}(2, \mathbb{Z})$ s'écrit comme

$$T^{m_1} S^{p_1} \dots T^{m_k} S^{p_k} \quad (10.114)$$

pour un certain k et des nombres $m_i, p_i \in \mathbb{Z}$. Autrement dit, $\mathrm{PSL}(2, \mathbb{Z}) = \mathrm{gr}(S, T)$.

Démonstration. Soit z , un point de D autre que z_0 . Alors si $A \in \mathrm{PSL}(2, \mathbb{Z})$ est non trivial nous avons $A * z$ hors de D . Du coup, comme vu dans la démonstration du théorème 10.33, il existe $B \in \mathrm{gr}(S, T)$ tel que $B * (A * z) \in D$. Vu que D ne contient qu'un seul point de chaque orbite, nous avons

$$B * A * z = z, \quad (10.115)$$

et donc $BA = \pm \mathbb{1}$, ce qui prouve que⁶ $A = B^{-1}$, c'est à dire que $A \in \mathrm{gr}(S, T)$. $\square$

6. Dans $\mathrm{PSL}(2, \mathbb{Z})$, nous n'avons pas besoin de mettre $\pm$ parce qu'il est compris dans la définition.

Liste des notations

$N \triangleleft G$ Le sous-groupe N est normal dans G , page 85

Algèbre

$\mathcal{C}^1(U, \mathbb{R}^n)$ Les applications une fois continument dérivables, page 635

$\mathcal{L}(V, W)$ Ensemble des applications linéaires de V dans W , page 272

$\mathbb{K}(A)$ corps contenant $\mathbb{K}$ et A , page 161

$\mathbb{K}[A]$ anneau contenant $\mathbb{K}$ et A , page 161

$\mathbb{N}_0$ les naturels non nuls : $\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$, page 71

$\mathcal{M}_{n \times m}$ l'ensemble des matrices $n \times m$, page 274

∇f gradient de la fonction f , page 617

proj_V projection de $V \times W$ sur V , page 346

$df_a(u)$ Application de la différentielle de f sur le vecteur u , page 607

$f^{(n)}$ La n -ième dérivée de la fonction f , page 644

$o(x)$ fonction tendant rapidement vers zéro, page 645

(p) idéal engendré par p , page 131

$[\mathbb{L} : \mathbb{K}]$ degré d'une extension de corps, page 161

$\mathbb{F}_p$ lorsque p est premier, page 151

$\mathbb{F}_{p^n}$ corps fini à p^n éléments, page 186

$\mathbb{Q}$ corps des fractions sur $\mathbb{Z}$, page 151

$\text{Frac}(\mathbb{A})$ Le corps des fractions de l'anneau $\mathbb{A}$, page 151

$\text{Fun}(X, Y)$ les applications de X vers Y , page 117

$S(E)$ Les opérateurs auto-adjoints de E , page 422

U_n Le groupe des racines n^{e} de l'unité., page 119

$\text{res}(P, Q)$ résultat des polynômes P et Q , page 293

$\sqrt{A}$ racine d'une matrice hermitienne positive, page 717

$\theta_\alpha(P)$ la multiplicité de α par rapport à P , page 145

$A[X]$ tous les polynômes de degré fini à coefficients dans A , page 141

$A_n[X]$ les polynômes à coefficients dans A et de degré inférieur à n , page 141

$B \mid A$ B divise A , page 143

$C(P)$ matrice compagnon, page 399

$E_\lambda(u)$ Espace propre de u , page 375

$mat_{\mathcal{B}}(q)$ matrice de q dans la base $\mathcal{B}$, page 894

$S^+(n, \mathbb{R})$ matrices symétriques semi-définies positives, page 384

$S^{++}(n, \mathbb{R})$ matrices symétriques strictement définies positives, page 384

$U(A)$ ensemble des inversibles, page 117

Ensembles de matrices

$O(n, \mathbb{R})$ le groupe des matrices orthogonales, page 297

$\Omega(E)$ formes quadratiques non dégénérées, page 1087

$Q(E)$ formes quadratiques réelles sur E , page 417

$Q^+(E)$ formes quadratiques positives, page 1087

$Q^{++}(E)$ formes quadratiques strictement définies positives, page 1087

$S^+(n, \mathbb{R})$ matrices symétriques définies positives, page 718

$S^{++}(n, \mathbb{R})$ matrices symétriques strictement définies positives, page 718

$S_n^{p,q}(\mathbb{R})$ matrices symétriques réelles de signature (p, q) , page 1087

$\beta(s)$ Vecteur unitaire de la binormale, page 952

$\gamma \sim g$ Équivalence d'arcs paramétrés, page 943

$\nu(s)$ Vecteur unitaire de la normale principale, page 952

$c(s)$ rayon de courbure, page 952

$t(s)$ Torsion, page 953

Géométrie

$(x_0 : \dots : x_n)$ coordonnées homogènes dans un espace projectif, page 538

$\text{Conv}(A)$ enveloppe convexe, page 517

$\mathbb{C}[G]$ combinaisons d'éléments de G à coefficients dans $\mathbb{C}$, page 773

$\text{PGL}(E)$ groupe projectif, page 537

B^o orthogonal dans le dual, page 278

$P(E)$ l'espace projectif de E , page 531

$P_1(\mathbb{C})$ sphère de Poincaré, page 544

Chaînes de Markov

$\pi(x)$ lié au temps de retour, page 1515

Probabilités et statistique

$\sigma(X)$ La tribu engendrée par la variable aléatoire X , page 1395

$a \wedge b$ $\min(a, b)$, page 1533

K_X matrice de covariance d'un vecteur gaussien, page 1439

$m(\mathcal{A})$ Ensemble des fonctions $\mathcal{A}$ -mesurables, page 454

Théorie des groupes

$(G/H)_g$ classes à gauche, page 103

$[a]_p$ ensemble des $a + kp$, page 96

$[G, G]$ groupe dérivé, page 87

- $[g, h]$ commutateur dans un groupe, page 87
- $\text{Aff}(\mathbb{R}^n)$ Le groupe des applications affines bijectives de $\mathbb{R}^n$, page 523
- gr groupe engendré, page 85
- $\hat{G}$ groupe des caractères de G , page 769
- σ_x réflexion par rapport à x , page 732
- A_n groupe alterné, page 109
- $D(G)$ groupe dérivé, page 87
- D_n groupe diédral, page 744
- G^{ab} groupe abélianisé de G , page 87
- G_x stabilisateur de x , page 102
- $N \times_{\phi} H$ produit semi-direct, page 112
- S_n le groupe symétrique, page 106

Topologie et théorie des ensembles

- $\complement A$ Le complémentaire de l'ensemble A , page 70
- $\text{Diam}(A)$ Diamètre de la partie A , page 592
- ∂A La frontière de l'ensemble A , page 320
- $A \Delta B$ différence symétrique, page 70
- A^c complémentaire de A , page 70

Analyse

- $\text{Isom}(X)$ Le groupe des isométries de X , page 222
- $\mu \ll \nu$ La mesure μ est absolument continue par rapport à la mesure ν , page 790
- $C^{\infty}(\mathbb{R}, \mathcal{S}'(\mathbb{R}^d))$ Fonctions à valeurs dans les distributions., page 1306
- $C^{\infty}(I, \mathcal{D}'(\mathbb{R}^d))$ fonctions à valeurs dans les distributions, page 1251
- $(S, \hat{\mathcal{F}}, \hat{\mu})$ complété de l'espace mesuré $(S, \hat{\mathcal{F}}, \hat{\mu})$, page 447
- $\mathcal{L}(E, F)$ Les applications linéaires de E vers F , page 351
- $\mathcal{L}^{(n)}(V, W)$ L'espace des applications n -linéaires $V^n \rightarrow W$, page 641
- L Les applications linéaires continues de E vers F , page 351
- $\mathbb{D}_b$ l'ensemble de écritures décimales en base b , page 333
- $\mathbb{R}$ l'ensemble des réels, page 78
- $\mathbb{R}^+$ les réels positifs ou nuls, page 80
- exp exponentielle, page 1019
- $\text{GL}(E, F)$ les bijections linéaires et continues, page 309
- $\mathcal{H}'$ dual, page 1109
- $\liminf a_n$ limite inférieure, page 464
- $\limsup a_n$ limite supérieure, page 464
- $\mathcal{L}^p$ espace de Lebesgue, sans les classes, page 1126
- $\mu \perp \nu$ mesures perpendiculaires, page 790

- μ^* La mesure extérieure associée à la mesure μ , page 442
- $\partial_z, \partial_{\bar{z}}$ dérivées partielles d'une fonction complexe, page 1165
- $\text{proj}_K(x)$ projection orthogonale de x sur y , page 1106
- $\sigma(\mathcal{A})$ tribu engendrée par $\mathcal{A}$, page 430
- $\mathcal{D}(\Omega)$ Les fonctions C^∞ à support compact sur Ω , page 1238
- $\mathcal{S}'(\mathbb{R}^d)$ espace des distributions tempérées, page 1244
- $A^2(\Omega)$ espace de Bergman, page 1196
- $A^\perp$ orthogonal d'une partie, page 1107
- $C_c(I)$ fonctions continues à support compact dans I , page 1108
- $f \sim g$ fonctions ayant des limites équivalentes, page 561
- $H^1(\Omega)$ espace de Sobolev sur Ω , page 1268
- $H^1(I)$ espace de Sobolev, page 1261
- $H^m(M)$ espace de Sobolev, page 1269
- $L^1_{loc}(I)$ fonctions intégrables sur les compacts de I , page 1262
- L^p espace de Lebesgue avec les classes, page 1127
- $M_i\varphi$ La fonction $x \mapsto x_i\varphi(x)$, page 1160
- S_nf somme partielle de série de Fourier, page 1138