Le Livre de l'Agrégation

GUIDE DE SURVIE - 2021

Florent Bréart

Université de Picardie Jules Verne

Avant-propos

I Introduction

J'ai passé l'agrégation externe de mathématiques en 2021 en étant inscrit à la préparation à l'agrégation de l'Université de Picardie Jules Verne. Ce livre regroupe toutes mes fiches pour les oraux, ainsi que des clés qui m'ont permis de préparer le concours tout au long de l'année.

Je ne donne ici que les méthodes que j'ai trouvées pertinentes lors de mon année de préparation. Il s'agit donc de conseils personnels qui ne s'appliqueront peut-être pas à tout le monde, mais qui pourraient aider certains. En aucun cas je ne me veux moralisateur.

Ce livre contient notamment :

— Tous mes plans de leçons d'analyse et d'algèbre pour la session 2021.

— Tous mes développements préparés et associés à chaque leçon.

— Des développements non utilisés dans mes leçons.

— Une bibliographie listant tous les livres sur lesquels je me suis appuyé.

— Des conseils personnels.

Tous ces documents sont de qualité relativement variable. En effet, bien que j'aie travaillé toutes les leçons individuellement, elles ont été rédigées au fur et à mesure de l'année. Les leçons écrites en septembre étant évidemment moins recommandables que celles écrites en avril. De plus, certaines fiches sont presque intégralement reprises de celles écrites par mes camarades.

Toutes les notations utilisées dans ce livre sont normalement uniformisées sur toutes les fiches. Elles sont également a priori standards. Il ne devrait donc pas y avoir de problème de compréhension des notations.

Enfin, quelques remerciements. Je remercie la promotion 2020-2021 de la préparation à l'agrégation de l'Université de Picardie Jules Verne pour la bonne ambiance apportée aux heures de cours passées ensemble. Je remercie en particulier Manon et Alexis pour l'organisation des valises de livres. Je remercie l'ensemble des enseignants intervenus dans l'année pour nous avoir apporté leurs savoirs. Je remercie ma famille pour le soutien apporté cette année.

II Conseils pour l'année

1) Conseils généraux

2) Développements

3) Livre

4) Liens Internet

Bien sûr, les livres sont des ressources qui sont importantes puisqu'ils représentent la seule aide que vous aurez lors de l'oral. Cependant, Internet regorge de ressources qui peuvent vous aider à préparer les écrits et les oraux. Voici une liste non exhaustive de telles ressources que j'ai utilisées lors de ma préparation.

Le site du jury de l'agrégation externe, à consulter régulièrement pour être au courant des actualités du concours, pour avoir les précédents rapports et sujets, et pour avoir des informations pratiques : agreg.org.

Un site de référence pour les agrégatifs, fonctionnant de manière collaborative, regroupant des plans de leçons et des développements : agreg-maths.fr.

Le profil d'Owen sur agreg-maths.fr, très complet et avec un très bon niveau, qui a partagé son travail sur presque toutes les leçons et tous ses développements. (2020)
Le profil d'Antoine Barrier sur agreg-maths.fr ainsi que son site, lui aussi très complet et très bon niveau, avec ses leçons et ses développements. (2019)
Le site Coquillages et Poincaré, dont les leçons et les développements sont accompagnés de commentaires et d'exercices, le tout agrémenté de retours d'oraux très détaillés. (2019)
Le site de Florian Lemonnier, un filon en terme de développements. (2015)

La chaîne YouTube de Philippe Caldero, pleine de bonnes choses !
Le compte Twitter AgregNancy, bot qui propose un exercice d'oral tous les jours puis toutes les heures à l'approche des oraux.

5) Conseils d'entrainement

6) Plus

III Retours et conseils pour les épreuves

IV Contenu du livre

Table des matières

Partie I

Leçons Algèbre et Géométrie

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{i=n} x_i = \frac{x_1 + x_2 + \ldots + x_n}{n}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\int_0^\infty e^{-\alpha x^2}\mathrm{d}x = \frac{1}{2}\sqrt{\int_{-\infty}^\infty e^{-\alpha x^2}\mathrm{d}x \int_{-\infty}^\infty e^{-\alpha y^2}\mathrm{d}y} = \frac{1}{2}\sqrt{\frac{\pi}{\alpha}}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\sum_{k=0}^{\infty} a_0 q^k = \lim_{n\to\infty} \sum_{k=0}^{n} a_0 q^k = \lim_{n\to\infty} a_0 \frac{1-q^{n+1}}{1-q} = \frac{a_0}{1-q}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\frac{\partial^2 \Phi}{\partial x^2} + \frac{\partial^2 \Phi}{\partial y^2} + \frac{\partial^2 \Phi}{\partial z^2} = \frac{1}{c^2} \frac{\partial^2 \Phi}{\partial t^2}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Liste des leçons d'algèbre et de géométrie

Cadre : On fixe G un groupe et X un ensemble non vide.

I Définitions et premières propriétés

1) Actions de groupes

Définition 1. Une action de groupes est la donnée d'une application $G \times X \to X$ définie par $(g, x) \mapsto g \cdot x$ telle que :

(i) $\forall\, x \in X,\ e \cdot x = x$

(ii) $\forall\, g_1, g_2 \in G,\ \forall\, x \in X,\ g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$

On dit que G agit sur X.

Proposition 2. *La donnée d'une action de groupe de G sur X est équivalente à la donnée d'un morphisme $G \to S(X)$, où $S(X)$ désigne l'ensemble des bijections de X dans X.*

Exemple 3. *G agit sur lui-même par translation et par conjugaison.*

Théorème 4 (Cayley)**.** *Si G est fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Définition 5. L'action de G sur X est dite :

(i) fidèle, si seul le neutre fixe tous les points.

(ii) libre, si tout élément non neutre agit sans point fixe.

(iii) transitive, si : $\forall\, x, y \in X, \exists\, g \in G, y = g \cdot x$.

(iv) n fois transitive, si l'action induite de G sur X^n est transitive.

Remarque 6. *Une action libre est fidèle.*

Exemple 7. *L'action du groupe linéaire sur les droites est transitive mais pas fidèle : les homothéties agissent trivialement.*

Exemple 8. *Une action induit une action fidèle du quotient du groupe par le noyau de l'action.*

Application 9. *Soit G un groupe infini et H un sous-groupe de G, distinct de G et d'indice fini. Alors G n'est pas simple.*

Définition 10. On appelle ensemble des points fixes de X sous l'action de G, ou ensemble des élément G-invariants de X, l'ensemble :

$$X^G = \{x \in X \,|\, \forall\, g \in G, g \cdot x = x\}$$

2) Stabilisateur, orbites, fixateur

Définition 11. Si $x \in X$, son stabilisateur est :

$$\mathrm{Stab}_x = \{g \in G \,|\, g \cdot x = x\}$$

Proposition 12. *Pour tout $x \in X$, Stab_x est un sous-groupe de G.*

Définition 13. Si $x \in X$, son orbite est :

$$O_x = \{g \cdot x \,|\, g \in G\}$$

Proposition 14. *Si G est fini, alors pour tout $x \in X$, $|G| = |\,\mathrm{Stab}_x\,||O_x|$.*

Proposition 15. *L'action de G sur X est dite :*

(i) fidèle, si l'intersection des stabilisateurs est triviale.

(ii) libre, si tous les stabilisateurs sont triviaux.

(iii) transitive, s'il n'y a qu'une seule orbite.

Théorème 16 (Équation aux classes)**.** *On suppose X et G finis. Soit θ une partie X contenant un unique représentant de chaque orbite. Alors :*

$$|X| = \sum_{x \in \theta} |O_x| = \sum_{x \in \theta} \frac{|G|}{|\,\mathrm{Stab}_x\,|}$$

Corollaire 17. *On note $Z(G)$ le centre de G. Si G est fini, il existe une famille finie $(H_i)_{i \in I}$ de sous-groupes stricts de G telle que :*

$$|G| = |Z(G)| + \sum_{i \in I} \frac{|G|}{|H_i|}$$

Définition 18. Si $g \in G$, son fixateur est :

$$\mathrm{Fix}_g = \{x \in X \,|\, g \cdot x = x\}$$

Théorème 19 (Burnside)**.** *On suppose G et X finis. Soit Ω l'ensemble des orbites distinctes. Alors :*

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_g\,|$$

Application 20. *Le nombre de colliers de 5 perles différents que l'on peut réaliser avec deux couleurs est 8.*

II Actions sur les groupes finis

1) Cas des p-groupes

Définition 21. Un p-groupe est un groupe d'ordre p^α, où $\alpha \in \mathbb{N}^\star$.

Exemple 22. *$|\mathbb{Z}/4\mathbb{Z}| = 2^2$, donc $\mathbb{Z}/4\mathbb{Z}$ est un 2-groupe.*

Proposition 23. *Le centre d'un p-groupe distinct n'est pas trivial.*

Théorème 24 (Cauchy)**.** *Si $p \mid |G|$, alors G a un élément d'ordre p.*

Exemple 25. *$2 \mid 4$, et $\overline{2}$ et d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$.*

Définition 26. On suppose G fini d'ordre $p^\alpha m$, où $p \nmid m$. Un p-Sylow est un sous-groupe de G d'ordre p^α.

Exemple 27. *$|GL_n(\mathbb{F}_p)| = p^\alpha m$, où $\alpha = \frac{n(n-1)}{2}$ et $p \nmid m$, et $\{(a_{i,j}) \,|\, a_{i,j} = 0 \text{ si } i > j, a_{i,i} = 1\} \subset GL_n(\mathbb{F}_p)$ est un p-Sylow.*

Lemme 28. *On suppose G fini d'ordre $p^\alpha m$, où $p \nmid m$. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Lemme 29. *Soit G un p-groupe agissant sur X. On note X^G l'ensemble des points fixes de X par G. Alors $|X| \equiv |X^G| \mod p$.*

Théorème 30 (Sylow)**.** *On suppose G fini d'ordre $n = p^\alpha m$, où $p \nmid m$.*

(i) L'ensemble $Syl_p(G)$ des p-Sylow de G est non vide.

(ii) Tous les p-Sylow sont conjugués.

(iii) $|Syl_p(G)| \equiv 1 \mod p$ et $|Syl_p(G)| \mid m$.

Corollaire 31. *Soit $S \in Syl_p(G)$, alors : $S \trianglelefteq G \Leftrightarrow |Syl_p(G)| = 1$.*

Exemple 32. *Un groupe d'ordre 63 possède un sous-groupe distingué.*

2) Groupe symétrique

Proposition 33. *Le groupe symétrique $\mathfrak{S}_n$ agit sur $[\![1, n]\!]$ par :*

$$\begin{array}{ccc} \mathfrak{S}_n \times [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ (\sigma, i) & \longmapsto & \sigma(i) \end{array}$$

Remarque 34. *Le stabilisateur d'un point est isomorphe à $\mathfrak{S}_n$.*

Application 35. *Soit $\sigma \in \mathfrak{S}_n$, alors $\langle\sigma\rangle$ agit aussi sur $[\![1, n]\!]$. Soient $F_1, \dots, F_r$ les orbites de $[\![1, n]\!]$ sur l'action de $\langle\sigma\rangle$. On pose :*

$$\sigma_i : \left| \begin{array}{ccc} [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ x & \longmapsto & \begin{cases} x & \text{si } x \notin F_i \\ \sigma(x) & \text{si } x \in F_i \end{cases} \end{array} \right.$$

Les σ_i sont des cycles à support disjoints, d'ordre $|F_i|$, qui commutent et on a $\sigma = \sigma_1 \cdots \sigma_r$.

Exemple 36. *$\mathfrak{S}_n$ agit sur $\mathbb{K}[X_1, \dots, X_n]$, avec $\mathbb{K}$ un corps, par :*

$$\begin{array}{ccc} \mathfrak{S}_n \times \mathbb{K}[X_1, \dots, X_n] & \longrightarrow & \mathbb{K}[X_1, \dots, X_n] \\ (\sigma, P) & \longmapsto & P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \end{array}$$

Remarque 37. *Ici, $\mathbb{K}[X_1, \dots, X_n]$ n'est pas fini, on ne peut donc pas utiliser l'équation de Burnside. Il y a un nombre infini d'orbites.*

Définition 38. On appelle type de $\sigma \in \mathfrak{S}_n$, notée $[l_1, \dots, l_m]$, la liste des cardinaux des orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$ dans l'ordre décroissant.

Exemple 39. *Les types possibles d'une permutation de $\mathfrak{S}_5$ sont :* $[1,1,1,1,1]$, $[2,1,1,1]$, $[2,2,1]$, $[3,1,1]$, $[3,2]$, $[4,1]$ *et* $[5]$.

Théorème 40. *Deux permutation de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles ont le même type.*

Proposition 41. *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Proposition 42. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Théorème 43. *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

III Applications

1) Théorie des représentations

Soit G un groupe d'ordre n et V un $\mathbb{C}$-espace vectoriel de dimension d.

Définition 44. Une représentation linéaire de G est un morphisme $\rho : G \to \mathcal{GL}(V)$. On appelle caractère de ρ la fonction $g \mapsto \mathrm{tr}(\rho(g))$.

Définition 45. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. On dit qu'elle est irréductible si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel non trivial de V n'est stable par G. Le caractère associé une telle représentation est dit irréductible.

Remarque 46. *Se donner une représentation de G dans V revient à se donner une action de groupes de G sur V en posant $\rho(g)(x) = g \cdot x$.*

Exemple 47. *$\rho : g \mapsto Id_V$ est une représentation de G sur V.*

Définition 48. Soient $\varphi, \psi : G \to \mathbb{C}$ deux fonctions. On pose :

$$(\varphi|\psi) = \frac{1}{|G|} \sum_{t \in G} \varphi(t)\overline{\psi(t)}$$

$(.|.)$ est un produit scalaire.

Théorème 49. *Les caractères irréductibles forment une base orthonormale de l'espace vectoriel des fonctions centrales sur G.*

Théorème 50. *Le nombre des représentations irréductibles de G (à isomorphisme près) est égal au nombre classes de conjugaison de G.*

Théorème 51. *Soit $\mathcal{T}$ un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$.*

Application 52. *La table de caractères de $\mathfrak{S}_4$ est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

2) Applications aux corps finis

Fixons $\mathbb{K}$ un corps et $n \in \mathbb{N}^\star$.

Définition 53. On pose $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \,|\, \zeta^n = 1\}$ le groupe des racines n-ièmes de l'unité.

Proposition 54. *Tout sous-groupe de $\mathbb{K}^\star$ est cyclique.*

Définition 55. On pose $\mathbb{K}_n$ un corps de décomposition de $X^n - 1 \in \mathbb{K}[X]$. Le groupe $\mu_n(\mathbb{K})$ est cyclique d'ordre n. On note $\mu_n^\star(\mathbb{K})$ l'ensemble des générateurs de $\mu_n(\mathbb{K})$, ses éléments sont les racines primitives n-ièmes de l'unité.

Remarque 56. $|\mu_n^\star(\mathbb{K}_n)| = \varphi(n)$

Définition 57. On définit le n-ième polynôme cyclotomique par :

$$\Phi_{n,\mathbb{K}} = \prod_{\zeta \in \mu_n^\star(\mathbb{K}_n)} (X - \zeta) \in \mathbb{K}[X]$$

Proposition 58. $X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{K}}$

Proposition 59. *On a $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$. De plus, pour $\sigma : \mathbb{Z} \to \mathbb{K}$ le morphisme canonique, on a $\Phi_{n,\mathbb{K}}(X) = \sigma(\Phi_{n,\mathbb{Q}}(X))$. En particulier, $\Phi_{n,\mathbb{F}_p}$ s'obtient à partir de $\Phi_{n,\mathbb{Q}}$ par réduction modulo p.*

Théorème 60 (Wedderburn)**.** *Tout corps fini est commutatif.*

Développements

- Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (41,42,43) [Per96]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (51,52) [Ser70]

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann

I Nombres complexes de module 1

1) Le groupe $\mathbb{U}$

Définition 1. On note $\mathbb{U} = \{z \in \mathbb{C} \,|\, |z| = 1\}$, l'ensemble des nombres complexes de module 1.

Exemple 2. $\pm 1, \pm i \in \mathbb{U}$.

Remarque 3. *En identifiant $\mathbb{C}$ et $\mathbb{R}^2$, $\mathbb{U}$ est identifié à $\mathbb{S}^1$.*

Théorème 4. *L'application $\mathbb{R}^{+\star} \times \mathbb{U} \to \mathbb{C}^\star$ envoyant (r, u) sur ru est un isomorphisme.*

Proposition 5. *Les groupes $\mathbb{U}$, $\mathbb{R}/2\pi\mathbb{Z}$ et $\mathcal{SO}_2(\mathbb{R})$ sont isomorphes.*

Proposition 6. *Le groupe $\mathbb{U}$ est compact et connexe.*

2) Fonctions trigonométriques

Définition 7. On définit les séries entières suivantes :

$$\exp(z) = e^z = \sum_{n\in\mathbb{N}} \frac{z^n}{n!} \quad \cos(z) = \sum_{n\in\mathbb{N}} \frac{(-1)^n z^{2n}}{(2n)!} \quad \sin(z) = \sum_{n\in\mathbb{N}} \frac{(-1)^n z^{2n+1}}{(2n+1)!}$$

Proposition 8. *(i) Pour tout $z \in \mathbb{C}$, on a $\exp(iz) = \cos(z) + i\sin(z)$.*

(ii) Pour tout $z_1, z_2 \in \mathbb{C}$, on a $e^{z_1+z_2} = e^{z_1}e^{z_2}$.

(iii) Pour tout $z \in \mathbb{C}$, on a $e^z \neq 0$, $\frac{1}{e^z} = e^{-z}$, $\overline{e^z} = e^{\overline{z}}$ et $|e^z| = e^{\mathrm{Re}\, z}$.

(iv) Pour tout $z \in \mathbb{C}$, $|\exp(z)| = 1 \Leftrightarrow z \in i\mathbb{R}$.

(v) $\exp$ est un morphisme de groupe surjectif de $(\mathbb{C}, +)$ dans $(\mathbb{C}^\star, \times)$.

(vi) $\exp$, $\sin$ et $\cos$ sont des séries entières de rayon de convergence infini, et sont donc définies et holomorphes sur $\mathbb{C}$. De plus, $\exp$ est sa propre dérivée.

(vii) Pour $\theta \in \mathbb{R}$, $\cos\theta$ et $\sin\theta$ sont réels.

Corollaire 9 (Moivre)**.** *Pour $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$, on a :*

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Corollaire 10 (Euler)**.** *Pour $\theta \in \mathbb{R}$, on a :*

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad et \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

Application 11. *On peut exprimer $\cos(n\theta)$ comme un polynôme en $\cos\theta$: ce sont les polynômes de Tchebychev.*

3) Paramétrisation du cercle unité

Proposition 12. *Dans $\mathbb{C}$, $\mathbb{U}$ est le cercle de centre 0 et de rayon 1. Il peut être paramétré, à l'exception de $(-1, 0)$ par l'application :*

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^2 \\ t & \longmapsto & \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \end{array}$$

Corollaire 13. *L'ensemble des points de $\mathbb{U}$ à coordonnées rationnelles sont denses dans $\mathbb{U}$.*

Application 14 (Triplets pythagoriciens)**.** *Soient $x, y, z \in \mathbb{N}$. Alors (x, y, z) est solution de l'équation diophantienne $x^2 + y^2 = z^2$ si, et seulement si, il existe $d \in \mathbb{Z}$ et u, v premiers entre eux tels que, à permutation près, on a $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$.*

4) Argument, rotations et angles orientés

On identifie ici $\mathbb{R}^2$ au plan complexe $\mathbb{C}$.

Définition 15. Pour $z \in \mathbb{C}^\star$, on appelle argument de z, noté $\arg z$, tout réel θ tel que $\frac{z}{|z|} = e^{i\theta}$. L'argument est donc bien défini dans $\mathbb{R}/2\pi\mathbb{Z}$.

Exemple 16. $\arg i = \frac{\pi}{2}$, $\arg x = 0$ *ou* 2π *pour* $x \in \mathbb{R}^{+\star}$.

Définition 17. La rotation autour de $a \in \mathbb{C}$ d'angle θ est l'application $r_{\theta,a}\mathbb{C} \to \mathbb{C}$ définie pour $z \in \mathbb{C}$ par $r_{\theta,a}(z) = a + (z - a)e^{i\theta}$.

Proposition 18. *Les rotations sont des isométries. En particulier, $\mathbb{U}$ est stable par toute rotation autour de 0.*

Application 19. *Les rotations du plan préservant un polygone régulier à n côtés de centre 0 est un groupe constitué des n rotations de centre 0 et d'angle $\frac{2k\pi}{n}$ pour $k \in [\![0, n-1]\!]$.*

Remarque 20. *Si on rajoute les symétries, on obtient le groupe des isométries du plan préservant le polygone régulier : le groupe diédral D_{2n}.*

Proposition 21. *Il existe une unique rotation envoyant $u \in \mathbb{U}$ sur $v \in \mathbb{U}$.*

Définition 22. On appelle angle orienté l'orbite de l'action de $\mathbb{U}$ sur $\mathbb{U} \times \mathbb{U}$ définie par $z \cdot (u, v) = (zu, zv)$.

Proposition 23. *L'application qui à un angle orienté $\overline{(u,v)}$ associe l'unique rotation envoyant u sur v est une bijection, notée Φ.*

Corollaire 24. *L'ensemble des angles orientés est un groupe s'il est muni de l'opération : $\overline{(u,v)} + \overline{(u',v')} = \Phi^{-1}\left(\Phi\left(\overline{(u,v)}\right) \circ \Phi\left(\overline{(u',v')}\right)\right)$.*

II Racines de l'unité

1) Sous-groupes des racines de l'unité

Définition 25. Soit $n \in \mathbb{N}^\star$. On appelle racine n-ième de l'unité dans $\mathbb{C}$ tout nombre complexe z tel que $z^n = 1$. On note $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité.

Définition 26. Soit $n \in \mathbb{N}^\star$. Une racine n-ième de l'unité est dite primitive si elle est d'ordre n dans $\mathbb{C}^\star$. On note μ_n l'ensemble des racines primitives n-ièmes de l'unité.

Proposition 27. *Pour $n \in \mathbb{N}^\star$, $\mathbb{U}_n$ est un groupe cyclique d'ordre n engendré par $e^{\frac{2i\pi}{n}}$. Les racines primitives sont les générateurs de $\mathbb{U}_n$.*

Corollaire 28. *Pour $n \in \mathbb{N}^\star$, on a $|\mu_n| = \varphi(n)$.*

Proposition 29. *Un sous-groupe de $\mathbb{U}$ est fini ou dense.*

Proposition 30. *On a $\mathbb{U}_d \subset \mathbb{U}_n \Leftrightarrow d \mid n$, et $\mathbb{U}_n = \bigcup_{d|n} \mu_d$.*

Application 31. *On a $n = \sum_{d|n} \varphi(d)$.*

2) Polynômes cyclotomiques

Définition 32. On définit le n-ième polynôme cyclotomique par :

$$\Phi_n(X) = \prod_{\zeta \in \mu_n} (X - \zeta) \in \mathbb{C}[X]$$

Proposition 33. *Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 34. $\forall n \in \mathbb{N}^\star, X^n - 1 = \prod_{d|n} \Phi_d(X)$

Exemple 35. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Proposition 36. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 37. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Z}[X]$.*

Lemme 38. *Soit $a \in \mathbb{Z}$ et p premier tel que $p|\Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour $d|n$ et $d < n$. Alors $p \equiv 1[n]$.*

Théorème 39 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

III Application aux représentations

Soit G un groupe d'ordre n et V un $\mathbb{C}$-espace vectoriel de dimension d.

Définition 40. Une représentation linéaire de G est un morphisme $\rho : G \to \mathcal{GL}(V)$. On appelle caractère de ρ la fonction $g \mapsto \mathrm{tr}(\rho(g))$.

Remarque 41. *Se donner une représentation de G dans V revient à se donner une action de groupes de G sur V en posant $\rho(g)(x) = g \cdot x$.*

Exemple 42. *$\rho : g \mapsto Id_V$ est une représentation de G sur V.*

Exemple 43. *On suppose que G agit sur un ensemble X de cardinal d. Soit $(e_x)_{x \in X}$ une base de V. La représentation suivante est appelée représentation de permutation associée à X :*

$$\rho : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{GL}(V) \\ s & \longmapsto & (e_x \mapsto e_{s \cdot x}) \end{array} \right.$$

Proposition 44. *Soient $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G et $g \in G$. Alors $\rho(g)$ est diagonalisable de valeurs propres dans $\mathbb{U}_n$.*

Corollaire 45. *Soient χ un caractère de G et $g \in G$. Alors $\chi(g)$ s'écrit comme somme de racines n-ièmes de l'unité.*

Théorème 46. *G est abélien si et seulement si toute représentation irréductible est de degré 1.*

Exemple 47. *La table de caractères de $\mathbb{Z}/n\mathbb{Z}$ est :*

$\mathbb{Z}/n\mathbb{Z}$	0	1	2	$\cdots$	$n-1$
χ_1	1	1	1	$\cdots$	1
χ_2	1	ω	ω^2	$\cdots$	ω^{n-1}
χ_3	1	ω^2	ω^4	$\cdots$	ω^{n-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_n	1	ω^{n-1}	ω^{n-2}	$\cdots$	ω

où $\omega = e^{\frac{2i\pi}{n}}$.

Proposition 48. *L'application $\iota : G \to \widehat{\widehat{G}}$ définie pour $g \in G$ par $\iota(g) : \chi \mapsto \chi(g)$ est un isomorphisme.*

Proposition 49. *G et $\widehat{G}$ ont même exposant.*

Théorème 50. *Il existe un unique entier ℓ et une unique suite $d_\ell | \cdots | d_2 | d_1$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G et :*

$$G \cong \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Développements

- Étude des polynômes cyclotomiques (36,37) [Per96]
- Structure des groupes abéliens finis (48,49,50) [Col09]
- Forme faible de la progression arithmétique de Dirichlet (38,39) [FGN13a]

Références

[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions*. Ellipses
[Aud06] M. Audin. *Géométrie*. EDP Sciences
[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses
[Col09] P. Colmez. *Éléments d'analyse et d'algèbre*. Les éditions de l'École Polytechnique
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1*. Cassini

Cadre : G désigne un groupe et H un sous-groupe de G.

I Action par conjugaison

1) G agit sur lui-même

Définition 1. On appelle isomorphisme intérieur tout automorphisme i_g donné, pour $g \in G$ par $i_g(h) = ghg^{-1}$ pour tout $h \in G$.

Proposition 2. *G agit sur lui-même par conjugaison en posant :*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & g \cdot h = ghg^{-1} \end{array}$$

Définition 3. L'orbite $\left\{ghg^{-1} \,\middle|\, g \in G\right\}$ de $h \in G$ sous l'action de conjugaison par G sur lui-même s'appelle la classe de conjugaison de h. Deux éléments de G qui appartiennent à la même classe de conjugaison sont dits conjugués. Le stabilisateur $Stab_G(h) = \left\{g \in G \,\middle|\, ghg^{-1} = h\right\}$ de h s'appelle le centralisateur de h dans G.

Définition 4. Le centralisateur d'une partie A de G est donnée par $C_G(A) = \{g \in G \,|\, \forall a \in A, ga = ag\}$.

Remarque 5. *On rappelle que $Z(G) = \{g \in G \,|\, \forall h \in G, gh = hg\}$ est le centre de G. On a alors en particulier $Z(G) = C_G(G)$.*

Exemple 6. *La classe de conjugaison de e est $\{e\}$ et $C_G(e) = G$.*

2) G agit sur l'ensemble de ses sous-groupes

Proposition 7. *G agit sur l'ensemble de ses sous-groupes par conjugaison par $g \cdot H = gHg^{-1}$.*

Définition 8. On dit que H et gHg^{-1} sont conjugués. Le stabilisateur de H, noté $N_G(H)$ est appelé normalisateur de H dans G : $N_G(H) = \left\{g \in G \,\middle|\, gHg^{-1} = H\right\}$.

Proposition 9. *On suppose que G agit sur un ensemble X. Les stabilisateurs des éléments d'une même orbite sont tous conjugués. Plus précisément, on a, pour tout $x \in X$ et tout $g \in G$, $Stab_G(g \cdot x) = gStab_G(x)g^{-1}$.*

II Sous-groupe distingué et groupe quotient

1) Sous-groupe distingué

Définition 10. On dit que H est distingué dans G, noté $H \trianglelefteq G$, s'il est invariant par conjugaison, c'est-à-dire si :

$$\forall\, g \in G,\ \forall\, h \in H,\ ghg^{-1} \in H$$

Exemple 11. *On a toujours : $\{e\} \trianglelefteq G$, $G \trianglelefteq G$ et $Z(G) \trianglelefteq G$.*

Exemple 12. *Soit $n \in \mathbb{N}$, alors $\mathcal{SL}_n(\mathbb{R}) \trianglelefteq \mathcal{GL}_n(\mathbb{R})$.*

Définition 13. Un groupe G est dit simple s'il est non trivial et ne possède pas de sous-groupe distingué autre que $\{e\}$ et lui-même.

Proposition 14. *Soit I un ensemble et soient $H_i \trianglelefteq G$ pour tout $i \in I$. Alors $\bigcap_{i\in I} H_i \trianglelefteq G$.*

Proposition 15. *Soient $K \leqslant H \leqslant G$. Si $K \trianglelefteq G$, alors $K \trianglelefteq H$.*

Proposition 16. *Soit G' un groupe, H' un sous-groupe de G' et $\varphi : G \to G'$ un morphisme de groupes.*

(i) Si $H \trianglelefteq G$, alors $\varphi(H) \trianglelefteq \varphi(G)$.

(ii) Si φ est surjectif, alors $\varphi(H) \trianglelefteq G'$.

(iii) Si $H' \trianglelefteq G'$, alors $\varphi^{-1}(H') \trianglelefteq G$.

Proposition 17. *$H \trianglelefteq G$ si, et seulement si, H est un point fixe de l'action de G sur l'ensemble de ses sous-groupes par conjugaison. En particulier, $H \trianglelefteq G$ si, et seulement si, pour tout $g \in G$ on a $gHg^{-1} = H$.*

2) Classes d'équivalences

Théorème 18. *La relation "$g_1 \sim_H g_2 \ \Leftrightarrow\ \exists\, h \in H,\ g_1 = g_2 h$" définit une relation d'équivalence sur G dont les classes d'équivalences sont les sous-ensembles $gH = \{gh \,|\, h \in H\}$ où $g \in G$.*

Définition 19. Ces classes sont appelées classes à gauche de G modulo H. On appelle ensemble quotient de G par $\sim_H$, et on note G/H, l'ensemble des classes à gauche de G modulo H.

Définition 20. La quantité $[G : H] = |G/H|$ est l'indice de H dans G.

Théorème 21 (Lagrange)**.** *Si G est fini, $|G| = |H||G/H| = |H|[G : H]$. En particulier, l'ordre d'un élément $g \in G$ divise l'ordre de G*

Proposition 22. *Un sous-groupe d'indice 2 est toujours distingué.*

3) Groupe quotient

Théorème 23. *On a $H \trianglelefteq G$ si, et seulement si, $(g_1H)*(g_2H) = (g_1g_2)H$ définit une loi de groupe $*$ sur G/H telle que l'application canonique $\pi : G \to G/H$ définit par $\pi(g) = gH$ soit un morphisme de groupes.*

Définition 24. Le groupe $(G/H, *)$ est le groupe quotient de G par H.

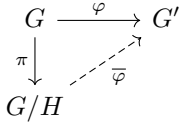
Exemple 25. *Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ est un groupe.*

Corollaire 26. *$H \trianglelefteq G$ si, et seulement si, H est le noyau d'un morphisme de groupe.*

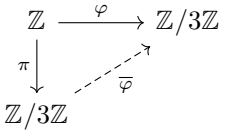
Théorème 27 (Propriété universelle du quotient)**.** *On suppose que $H \trianglelefteq G$. Soient $\pi : G \to G/H$ le morphisme canonique et $\varphi : G \to G'$ un morphisme de groupe. Les assertions suivantes sont équivalentes :*

(i) $H \subseteq \mathrm{Ker}(\varphi)$

(ii) Il existe un unique morphisme de groupe $\overline{\varphi} : G/H \to G'$ tel que le diagramme ci-contre soit commutatif.



Exemple 28. *En prenant $G = \mathbb{Z}$, $H = 6\mathbb{Z}$, $G' = \mathbb{Z}/3\mathbb{Z}$ et $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ le morphisme canonique, on a le diagramme commutatif ci-contre, car $6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathrm{Ker}(\varphi)$.*



Théorème 29 (Premier théorème d'isomorphie)**.** *Soit $\varphi : G \to G'$ un morphisme de groupe. Alors $G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.*

Exemple 30. *Le morphisme de groupe* det : $\mathcal{GL}_n(\mathbb{C}) \to \mathbb{C}^\star$ *donne* $\mathcal{GL}_n(\mathbb{C})/\mathcal{SL}_n(\mathbb{C}) \cong \mathbb{C}^\star$.

Application 31. *Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

4) Théorèmes de Sylow

Définition 32. On suppose G fini d'ordre $p^\alpha m$, où $p \nmid m$. Un p-Sylow est un sous-groupe de G d'ordre p^α.

Exemple 33. $|GL_n(\mathbb{F}_p)| = p^\alpha m$, *où* $\alpha = \frac{n(n-1)}{2}$ *et* $p \nmid m$, *et* $\{(a_{i,j}) \,|\, a_{i,j} = 0 \text{ si } i > j, a_{i,i} = 1\} \subset GL_n(\mathbb{F}_p)$ *est un p-Sylow.*

Lemme 34. *On suppose G fini d'ordre $p^\alpha m$, où $p \nmid m$. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Lemme 35. *Soit G un p-groupe agissant sur X. On note X^G l'ensemble des points fixes de X par G. Alors $|X| \equiv |X^G| \mod p$.*

Théorème 36 (Sylow)**.** *On suppose G fini d'ordre $n = p^\alpha m$, où $p \nmid m$.*

(i) L'ensemble $Syl_p(G)$ des p-Sylow de G est non vide.

(ii) Tous les p-Sylow sont conjugués.

(iii) $|Syl_p(G)| \equiv 1 \mod p$ *et* $|Syl_p(G)| \mid m$.

Corollaire 37. *Soit $S \in Syl_p(G)$, alors : $S \trianglelefteq G \Leftrightarrow |Syl_p(G)| = 1$.*

Exemple 38. *Un groupe d'ordre 63 possède un sous-groupe distingué.*

III Exemples de sous-groupes distingués et de groupes quotients

1) Groupe symétrique

Classes de conjugaison

Théorème 39. *Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit de cycles à supports disjoints. Ils correspondent aux orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$.*

Définition 40. On appelle type de $\sigma \in \mathfrak{S}_n$, notée $[l_1, \ldots, l_m]$, la liste des cardinaux des orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$ dans l'ordre décroissant.

Exemple 41. *Les types possibles d'une permutation de $\mathfrak{S}_5$ sont :* $[1,1,1,1,1]$, $[2,1,1,1]$, $[2,2,1]$, $[3,1,1]$, $[3,2]$, $[4,1]$ *et* $[5]$.

Théorème 42. *Deux permutation de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles ont le même type.*

Groupe alterné

Proposition 43. *$\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$. De plus, $\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}$.*

Lemme 44. *$\mathfrak{A}_n$ est $n-2$ fois transitif sur $[\![1, n]\!]$: si on a $a_1, \ldots, a_{n-2} \in [\![1, n]\!]$ distincts et $b_1, \ldots, b_{n-2} \in [\![1, n]\!]$ distincts, il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $i \in [\![1, n-2]\!]$.*

Proposition 45. *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Proposition 46. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Théorème 47. *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

2) Sous-groupe dérivé, groupe résoluble

Définition 48. Soient $g_1, g_2 \in G$. On appelle commutateur de g_1 et g_2 la quantité $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$. On appelle groupe dérivé de G, noté $D(G)$, le sous-groupe de G engendré par les commutateurs.

Exemple 49. *Si G est abélien, on a $D(G) = \{e\}$.*

Proposition 50. *Pour $g_1, g_2, h \in G$, on a :*

$$[g_1, g_2]^{-1} = [g_2, g_1] \quad et \quad h[g_1, g_2]h^{-1} = [hg_1h^{-1}, hg_2h^{-1}]$$

Proposition 51. $D(G) \trianglelefteq G$

Théorème 52. *$G/D(G)$ est abélien. De plus, $D(G) \subseteq H$ si, et seulement si, $H \trianglelefteq G$ et G/H est abélien.*

Définition 53. $G/D(G)$ est appelé l'abélianisé de G.

Définition 54. On définit la suite dérivée de G par :

$$G^{(0)} = G \quad \text{et} \quad \forall i \in \mathbb{N},\ G^{(i+1)} = D(G^{(i)}) = D^{i+1}(G)$$

S'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{e\}$, G est dit résoluble.

Remarque 55. *G est résoluble si, et seulement si, la suite $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots$ est stationnaire en $\{e\}$. Le quotient de deux termes consécutifs est toujours abélien.*

Exemple 56. *(i) Tout groupe abélien est résoluble.*
(ii) Un groupe simple non abélien n'est jamais résoluble.

IV Théorie des représentations

Soit G un groupe d'ordre n et V un $\mathbb{C}$-espace vectoriel de dimension d.

Définition 57. Une représentation linéaire de G est un morphisme $\rho : G \to \mathcal{GL}(V)$. On appelle caractère de ρ la fonction $g \mapsto \mathrm{tr}(\rho(g))$.

Définition 58. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. On dit qu'elle est irréductible si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel non trivial de V n'est stable par G. Le caractère associé une telle représentation est dit irréductible.

Remarque 59. *Se donner une représentation de G dans V revient à se donner une action de groupes de G sur V en posant $\rho(g)(x) = g \cdot x$.*

Exemple 60. *$\rho : g \mapsto Id_V$ est une représentation de G sur V.*

Définition 61. Soient $\varphi, \psi : G \to \mathbb{C}$ deux fonctions. On pose :

$$(\varphi|\psi) = \frac{1}{|G|} \sum_{t \in G} \varphi(t)\overline{\psi(t)}$$

$(.|.)$ est un produit scalaire.

Théorème 62. *Les caractères irréductibles forment une base orthonormale de l'espace vectoriel des fonctions centrales sur G.*

Théorème 63. *Le nombre des représentations irréductibles de G (à isomorphisme près) est égal au nombre classes de conjugaison de G.*

Théorème 64. *Soit $\mathcal{T}$ un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$.*

Application 65. *La table de caractères de $\mathfrak{S}_4$ est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

Développements

- Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (45,47) [Per96]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (64,65) [Ser70]

Références

[Ulm12] F. Ulmer. *Théorie des groupes.* Ellipses
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann

Cadre : G est un groupe, H un sous-groupe de G, et X un ensemble.

I Définitions et premières propriétés

1) Ordre d'un groupe

Définition 1. G est fini si son cardinal est fini. On appelle ordre de G son cardinal, noté $|G| = \mathrm{Card}(G)$.

Théorème 2 (Lagrange)**.** *L'ordre de H est fini et divise $|G|$.*

Définition 3. Si G est fini, l'indice de H dans G est $|G/H|$, noté $[G : H]$.

Remarque 4. *$|G| = [G : H]|H|$, un sous-groupe d'indice 2 est distingué.*

Proposition 5. *Deux groupes finis isomorphes ont même ordre.*

Exemple 6. *Soit $f : G \to G'$ un morphisme, alors $|G| = |\operatorname{Ker} f||\operatorname{Im} f|$.*

Proposition 7. *L'intersection de sous-groupes est un sous-groupe.*

Définition 8. Pour $A \subset G$, le sous-groupe engendré par A, noté $\langle A \rangle$ est le plus petit sous-groupe de G contenant A. C'est l'intersection de tous les sous-groupes de G contenant A.

Définition 9. L'ordre de $a \in G$ est l'ordre de $\langle a \rangle$.

Exemple 10. *$\overline{2}$ est d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$.*

Proposition 11. *Soit $a \in G$ d'ordre p, alors $a^q = e \Leftrightarrow p \mid q$.*

Proposition 12. *L'ordre de tout élément de G divise n.*

Corollaire 13. $\forall\, a \in G,\ a^n = e$

Remarque 14. *L'ordre de $a \in G$ est le plus petit $k \in \mathbb{N}^\star$ tel que $a^k = e$.*

2) Action de groupe

Définition 15. Une action de groupes est la donnée d'une application $G \times X \to X$ définie par $(g, x) \mapsto g \cdot x$ telle que :

(i) $\forall\, x \in X,\ e \cdot x = x$

(ii) $\forall\, g_1, g_2 \in G,\ \forall\, x \in X,\ g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$

On dit que G agit sur X.

Proposition 16. *La donnée d'une action de groupe de G sur X est équivalente à la donnée d'un morphisme $G \to S(X)$, où $S(X)$ désigne l'ensemble des bijections de X dans X.*

Exemple 17. *G agit sur lui-même par conjugaison.*

Théorème 18 (Cayley)**.** *Si G est fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Définition 19. Si $x \in X$, son orbite est $O_x = \{g \cdot x \,|\, g \in G\}$.

Définition 20. Si $x \in X$, son stabilisateur est $S_x = \{g \in G \,|\, g \cdot x = x\}$.

Proposition 21. *Pour tout $x \in X$, S_x est un sous-groupe de G.*

Proposition 22. *Si G est fini, alors, pour tout $x \in X$, $|G| = |S_x||O_x|$.*

Théorème 23 (Équation aux classes)**.** *On suppose X et G finis. Soit θ une partie X contenant un unique représentant de chaque orbite. Alors :*

$$|X| = \sum_{x \in \theta} |O_x| = \sum_{x \in \theta} \frac{|G|}{|S_x|}$$

Corollaire 24. *Si G est fini, il existe une famille finie $(H_i)_{i \in I}$ de sous-groupes stricts de G telle que :*

$$|G| = |Z(G)| + \sum_{i \in I} \frac{|G|}{|H_i|}$$

où $Z(G)$ est le centre de G.

3) Notion de p-groupe, pour p premier

Définition 25. Un p-groupe est un groupe d'ordre p^α, où $\alpha \in \mathbb{N}^\star$.

Exemple 26. *$|\mathbb{Z}/4\mathbb{Z}| = 2^2$, donc $\mathbb{Z}/4\mathbb{Z}$ est un 2-groupe.*

Proposition 27. *Le centre d'un p-groupe distinct n'est pas trivial.*

Théorème 28 (Cauchy)**.** *Si $p \mid |G|$, alors G a un élément d'ordre p.*

Exemple 29. *$2 \mid 4$, et $\overline{2}$ et d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$.*

Définition 30. On suppose G fini d'ordre $p^\alpha m$, où $p \nmid m$. Un p-Sylow est un sous-groupe de G d'ordre p^α.

Exemple 31. $|GL_n(\mathbb{F}_p)| = p^\alpha m$, *où* $\alpha = \frac{n(n-1)}{2}$ *et* $p \nmid m$, *et* $\{(a_{i,j}) \,|\, a_{i,j} = 0 \text{ si } i > j, a_{i,i} = 1\} \subset GL_n(\mathbb{F}_p)$ *est un p-Sylow.*

Lemme 32. *On suppose G fini d'ordre* $p^\alpha m$, *où* $p \nmid m$. *Soit S un p-Sylow de G. Alors il existe* $a \in G$ *tel que* $aSa^{-1} \cap H$ *est un p-Sylow de H.*

Lemme 33. *Soit G un p-groupe agissant sur X. On note* X^G *l'ensemble des points fixes de X par G. Alors* $|X| \equiv |X^G| \mod p$.

Théorème 34 (Sylow)**.** *On suppose G fini d'ordre* $n = p^\alpha m$, *où* $p \nmid m$.

(i) L'ensemble $Syl_p(G)$ *des p-Sylow de G est non vide.*

(ii) Tous les p-Sylow sont conjugués.

(iii) $|Syl_p(G)| \equiv 1 \mod p$ *et* $|Syl_p(G)| \mid m$.

Corollaire 35. *Soit* $S \in Syl_p(G)$, *alors :* $S \trianglelefteq G \Leftrightarrow |Syl_p(G)| = 1$.

Exemple 36. *Un groupe d'ordre 63 possède un sous-groupe distingué.*

II Groupes remarquables

1) Groupes cycliques

Définition 37. G est monogène s'il existe $a \in G$ tel que $G = \langle a \rangle$.

Définition 38. G est cyclique s'il est monogène et fini.

Proposition 39. *Tout groupe cyclique est abélien.*

Exemple 40. $\mathbb{Z}/n\mathbb{Z}$ *est cyclique.*

Proposition 41. *Si G est cyclique d'ordre n, alors* $G \cong \mathbb{Z}/n\mathbb{Z}$.

Proposition 42. *L'ensemble des racines n-ièmes de l'unité est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$.

Proposition 43. *Si* $|G|$ *est premier, alors G est cyclique, engendré par n'importe quel élément non neutre.*

Proposition 44. *Si G est cyclique, d'ordre n, et engendré par* $a \in G$, *alors :* $G = \langle a^k \rangle \Leftrightarrow k \wedge n = 1$.

Exemple 45. $\overline{1}$, $\overline{5}$, $\overline{7}$ *et* $\overline{12}$ *sont générateurs de* $\mathbb{Z}/12\mathbb{Z}$.

Proposition 46. *Tout sous-groupe d'un groupe cyclique est cyclique.*

2) Groupe symétrique $\mathfrak{S}_n$

Définition 47. On note $\mathfrak{S}_n$ l'ensemble des bijections de $[\![1, n]\!]$ dans $[\![1, n]\!]$. Ses éléments sont appelés permutations.

Proposition 48. $|\mathfrak{S}_n| = n!$

Définition 49. Une transposition est une permutation échangeant deux éléments i et j de $[\![1, n]\!]$ distincts et fixant les autres. On la note $(i\ j)$.

Théorème 50. *Les transpositions engendrent* $\mathfrak{S}_n$.

Définition 51. Un cycle de longueur k est une permutation, notée $\sigma = (a_1\ a_2\ \dots\ a_k)$, où $\sigma(a_i) = \sigma(a_{i+1})$ pour $i \in [\![1, k-1]\!]$, $\sigma(a_k) = a_1$ et qui fixe les autres éléments de $[\![1, n]\!]$.

Corollaire 52. *On a les engendrements suivants :*

(i) $(1\ 2)$, $(1\ 3)$, $\dots$, $(1\ n)$ *engendrent* $\mathfrak{S}_n$.

(ii) $(1\ 2)$, $(2\ 3)$, $\dots$, $((n-1)\ n)$ *engendrent* $\mathfrak{S}_n$.

(iii) $(1\ 2)$ *et* $(1\ 2\ \dots\ n)$ *engendrent* $\mathfrak{S}_n$.

Définition 53. On appelle support d'une permutation σ, noté $\text{supp}(\sigma)$, l'ensemble des éléments de $[\![1, n]\!]$ qui ne sont pas fixés par σ.

Proposition 54. *Deux permutations à support disjoints commutent.*

Proposition 55. *Si* σ *est un cycle de longueur k, alors* $\sigma^k = Id$.

Théorème 56. *Toute permutation se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près.*

Exemple 57. $\left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right) = (1\ 2)(3\ 4) = (3\ 4)(1\ 2)$

Proposition 58. *Soient* $\sigma = (a_1\ a_2\ \dots\ a_k)$ *un cycle d'ordre k et* $\tau \in \mathfrak{S}_n$. *Alors* $\tau\sigma\tau^{-1} = (\tau(a_1)\ \dots\ \tau(a_k))$.

Définition 59. Soit $\sigma \in \mathfrak{S}_n$. On définit la signature de σ par :

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Proposition 60. *La signature possède les propriétés suivantes :*

(i) $\forall\, \sigma \in \mathfrak{S}_n,\ \varepsilon(\sigma) \in \{\pm 1\}$

(ii) $\forall\, \sigma, \sigma' \in \mathfrak{S}_n,\ \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$

(iii) Si σ *est un cycle d'ordre k, alors* $\varepsilon(\sigma) = (-1)^{k-1}$.

Définition 61. $\mathfrak{A}_n = \varepsilon^{-1}(\{1\})$ est le groupe alterné.

Définition 62. Un groupe est dit simple si ses seuls sous-groupes distingués sont le sous-groupe trivial et lui-même.

Définition 63. On appelle type de $\sigma \in \mathfrak{S}_n$, notée $[l_1, \dots, l_m]$, la liste des cardinaux des orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$ dans l'ordre décroissant.

Exemple 64. *Les types possibles d'une permutation de* $\mathfrak{S}_5$ *sont :* $[1,1,1,1,1]$, $[2,1,1,1]$, $[2,2,1]$, $[3,1,1]$, $[3,2]$, $[4,1]$ *et* $[5]$.

Proposition 65. $\mathfrak{A}_n$ *est engendré par les 3-cycles de* $\mathfrak{S}_n$.

Proposition 66. *Les cycles d'ordre 3 sont conjugués dans* $\mathfrak{A}_n$ *pour* $n \geqslant 5$.

Théorème 67. $\mathfrak{A}_n$ *est simple pour* $n \geqslant 5$.

Remarque 68. *Pour* $n = 4$, $\{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq \mathfrak{A}_n$.

III Théorie des représentations

Soit G un groupe d'ordre n et V un $\mathbb{C}$-espace vectoriel de dimension d.

Définition 69. Une représentation linéaire de G est un morphisme $\rho : G \to \mathcal{GL}(V)$. On appelle caractère de ρ la fonction $g \mapsto \mathrm{tr}(\rho(g))$.

Définition 70. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. On dit qu'elle est irréductible si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel non trivial de V n'est stable par G. Le caractère associé une telle représentation est dit irréductible.

Remarque 71. *Se donner une représentation de* G *dans* V *revient à se donner une action de groupes de* G *sur* V *en posant* $\rho(g)(x) = g \cdot x$.

Exemple 72. $\rho : g \mapsto Id_V$ *est une représentation de* G *sur* V.

Définition 73. Soient $\varphi, \psi : G \to \mathbb{C}$ deux fonctions. On pose :

$$(\varphi|\psi) = \frac{1}{|G|} \sum_{t \in G} \varphi(t)\overline{\psi(t)}$$

$(.|.)$ est un produit scalaire.

Théorème 74. *Les caractères irréductibles forment une base orthonormale de l'espace vectoriel des fonctions centrales sur* G.

Théorème 75. *Le nombre des représentations irréductibles de* G *(à isomorphisme près) est égal au nombre classes de conjugaison de* G.

Théorème 76. *Soit* $\mathcal{T}$ *un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant* $\mathcal{T}$ *est isomorphe à* $\mathfrak{S}_4$.

Application 77. *La table de caractères de* $\mathfrak{S}_4$ *est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

Proposition 78. *L'application* $\iota : G \to \widehat{\widehat{G}}$ *définie pour* $g \in G$ *par* $\iota(g) : \chi \mapsto \chi(g)$ *est un isomorphisme.*

Proposition 79. G *et* $\widehat{G}$ *ont même exposant.*

Théorème 80. *Il existe un unique entier* ℓ *et une unique suite* $d_\ell | \cdots | d_2 | d_1$ *d'entiers supérieurs à 2 tels que* d_1 *est l'exposant de* G *et :*

$$G \cong \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Développements

- Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (65,67) [Per96]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (76,77) [Ser70]
- Structure des groupes abéliens finis (78,79,80) [Col09]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann
[Col09] P. Colmez. *Éléments d'analyse et d'algèbre.* Les éditions de l'École Polytechnique

Cadre : Soient E un ensemble et $n \in \mathbb{N}^\star$.

I Généralités sur le groupe symétrique

1) Définitions et premières propriétés

Définition 1. L'ensemble $\mathfrak{S}(E)$ des bijections de E dans E, muni de la composition des applications, est un groupe qu'on appelle groupe symétrique de E. On note simplement $\mathfrak{S}_n$ le groupe $\mathfrak{S}(\llbracket 1, n \rrbracket)$. On appelle permutation les éléments de $\mathfrak{S}(E)$.

Proposition 2. *On a une bijection entre les actions d'un groupe G sur E et les morphismes $\varphi : G \to \mathfrak{S}(E)$.*

Proposition 3. *Si E est de cardinal fini n, alors les groupes $\mathfrak{S}(E)$ est $\mathfrak{S}_n$ sont isomorphes. De plus, $|\mathfrak{S}_n| = n!$.*

Corollaire 4. *On suppose E de cardinal fini n. À toute numérotation des éléments de E correspond une bijection entre les actions d'un groupe G sur E et les morphismes $\varphi : G \to \mathfrak{S}_n$.*

Définition 5. Soit $\sigma \in \mathfrak{S}_n$. On note :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Exemple 6. *Soient $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ et $\rho = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$ dans $\mathfrak{S}_3$. On a alors $\sigma \circ \rho = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)$ et $\rho \circ \sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$. Ainsi $\mathfrak{S}_n$ n'est en général pas abélien.*

Théorème 7 (Cayley)**.** *Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

2) Orbites et cycles

Définition 8. Soit $\sigma \in \mathfrak{S}_n$.

(i) Les éléments i de $\llbracket 1, n \rrbracket$ qui vérifient $\sigma(i) = i$ sont appelés points fixes de la permutation σ.

(ii) L'ensemble $\llbracket 1, n \rrbracket$ privé des points fixes de la permutation σ est appelé support de σ et noté $\mathrm{supp}(\sigma)$.

Proposition 9. *Les permutations à supports disjoints commutent.*

Définition 10. Soient $\ell \in \mathbb{N}^\star$ et $i_1, \ldots, i_\ell \in \llbracket 1, n \rrbracket$. On considère la permutation $\gamma \in \mathfrak{S}_n$ définie pour $j \in \llbracket 1, n \rrbracket$ par :

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \ldots, i_\ell\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < \ell \\ i_1 & \text{si } j = i_\ell \end{cases}$$

On dit que γ est un cycle de longueur ℓ, noté $\gamma = (i_1\ i_2\ \cdots\ i_\ell)$. Un cycle de longueur 2 est appelé une transposition.

Exemple 11. *Avec la notation générale des permutations, le cycle $(1\ 4\ 2\ 5) \in \mathfrak{S}_5$ s'écrit $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{smallmatrix}\right)$.*

Proposition 12. *Le groupe $\mathfrak{S}_n$ agit naturellement sur $\llbracket 1, n \rrbracket$ par permutations. Cette action est donnée pour $\sigma \in \mathfrak{S}_n$ et $i \in \llbracket 1, n \rrbracket$ par $\sigma \cdot i = \sigma(i)$.*

Théorème 13. *Toute permutation s'écrit comme produit de cycles à supports disjoints. Ils correspondent aux orbites de l'action de $\langle \sigma \rangle$ sur $\llbracket 1, n \rrbracket$. Cette décomposition est unique à l'ordre près.*

Exemple 14. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4) = (3\ 4)(1\ 2)$

Définition 15. On appelle type de $\sigma \in \mathfrak{S}_n$, notée $[l_1, \ldots, l_m]$, la liste des cardinaux des orbites de l'action de $\langle \sigma \rangle$ sur $\llbracket 1, n \rrbracket$ dans l'ordre décroissant.

Exemple 16. *Les types possibles d'une permutation de $\mathfrak{S}_5$ sont : $[1,1,1,1,1]$, $[2,1,1,1]$, $[2,2,1]$, $[3,1,1]$, $[3,2]$, $[4,1]$ et $[5]$.*

Théorème 17. *Deux permutation de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles ont le même type.*

3) Générateurs

Lemme 18. *Tout cycle d'ordre ℓ est produit de $\ell - 1$ transpositions. On a en fait $(i_1\ i_2\ \cdots\ i_\ell) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{\ell-1}\ i_\ell)$.*

Exemple 19. *Pour $\sigma = (3\ 1\ 5\ 2) \in \mathfrak{S}_5$, on a $\sigma = (3\ 1)(1\ 5)(5\ 2)$.*

Corollaire 20. *Les familles suivantes engendrent $\mathfrak{S}_n$:*

(i) $\{(1\ i)\,|\,1 < i \leqslant n\}$

(ii) $\{(i\ i+1)\,|\,1 \leqslant i < n\}$

(iii) $\{(1\ 2), (1\ 2\ \ldots\ n)\}$

Remarque 21. *Quel que soit n, deux éléments suffisent à engendrer $\mathfrak{S}_n$.*

II Signature et groupe alterné

1) Signature

Définition 22. Soit $\sigma \in \mathfrak{S}_n$. On définit la signature de σ par :

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Exemple 23. $\varepsilon((1\ 2)) = -1$

Proposition 24. *La signature possède les propriétés suivantes :*

(i) $\forall \sigma \in \mathfrak{S}_n,\ \varepsilon(\sigma) \in \{\pm 1\}$

(ii) $\forall \sigma, \sigma' \in \mathfrak{S}_n,\ \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$

(iii) Si σ est un cycle d'ordre k, alors $\varepsilon(\sigma) = (-1)^{k-1}$.

2) Groupe alterné

Définition 25. Le noyau du morphisme ε est un sous-groupe de $\mathfrak{S}_n$, noté $\mathfrak{A}_n$ et appelé groupe alterné.

Proposition 26. $\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$. *De plus,* $\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}$.

Lemme 27. $\mathfrak{A}_n$ *est $n-2$ fois transitif sur $[\![1, n]\!]$: si on a $a_1, \ldots, a_{n-2} \in [\![1, n]\!]$ distincts et $b_1, \ldots, b_{n-2} \in [\![1, n]\!]$ distincts, il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $i \in [\![1, n-2]\!]$.*

Proposition 28. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Proposition 29. $\mathfrak{A}_n$ *est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Définition 30. Un groupe non trivial est dit simple si ses sous-groupes distingués sont le groupe trivial et lui-même.

Exemple 31. $\mathfrak{A}_4$ *n'est pas simple.*

Théorème 32. $\mathfrak{A}_n$ *est simple pour $n \geqslant 5$.*

Corollaire 33. *Pour $n \geqslant 5$, le groupe dérivé de $\mathfrak{A}_n$ est $\mathfrak{A}_n$.*

Corollaire 34. *Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathfrak{A}_n$ et $\{Id\}$.*

III Applications

1) Déterminants

$\mathbb{K}$ est un corps, E est un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^\star$ et $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E.

Définition 35. Soient $E_1, \ldots, E_p$ et F des $\mathbb{K}$-espaces vectoriels. Une application $f : \left| \begin{array}{ccc} E_1 \times \ldots \times E_p & \longrightarrow & F \\ (x_1, \ldots, x_n) & \longmapsto & f(x_1, \ldots, x_n) \end{array} \right.$ est dite p-linéaire si, en tout point, les p applications partielles sont linéaires. On note $f \in \mathscr{L}_p(E_1 \times \ldots \times E_p, F)$. On parle de formes p-linéaires sur E si $E_1 = \ldots = E_p = E$ et $F = \mathbb{K}$, l'ensemble des formes p-linéaires sur E est noté $\mathscr{L}_p(E, \mathbb{K})$.

Exemple 36. *Soient $\varphi_1, \ldots, \varphi_p \in \mathcal{L}(E, \mathbb{K})$. Alors $\varphi = (\varphi_1, \ldots, \varphi_p)$ est dans $\mathscr{L}_p(E, \mathbb{K})$.*

Définition 37. Soit $f \in \mathscr{L}_p(E, \mathbb{K})$.

(i) f est dite alternée si $f(x_1, \ldots, x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux.

(ii) f est dite antisymétrique si l'échange de deux vecteurs dans la suite $(x_1, \ldots, x_p)$ donne à f des valeurs opposées.

Remarque 38. *Soit $f \in \mathscr{L}_p(E, \mathbb{K})$, f est antisymétrique si, et seulement si, pour tout $\sigma \in \mathfrak{S}_p$ et pour tout $(x_1, \ldots, x_p) \in E^p$, on a :*

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(p)}) = \varepsilon(\sigma) f(x_1, \ldots, x_p)$$

Théorème 39. *Soit $f \in \mathscr{L}_p(E, \mathbb{K})$. Si $\mathrm{car}(\mathbb{K}) \neq 2$, alors f est antisymétrique si, et seulement si, f est alternée.*

Théorème 40. *L'ensemble des formes n-linéaires alternées sur E est un $\mathbb{K}$-espace vectoriel de dimension 1. De plus, si x_j s'écrit $(x_{1,j}, \ldots, x_{n,j})$ dans la base $\mathcal{B}$, les formes n-linéaires alternées sur E sont les applications qui sont de la forme :*

$$f(x_1, \ldots, x_n) = \lambda \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \ldots x_{n,\sigma(n)},\ \text{avec } \lambda \in \mathbb{K}$$

Définition 41. On appelle déterminant dans la base $\mathcal{B}$ l'unique forme n-linéaire alternée sur E prenant la valeur 1 sur la base $\mathcal{B}$:

$$\det_{\mathcal{B}}(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \ldots x_{n,\sigma(n)}$$

2) Groupe symétrique et géométrie

On considère E un $\mathbb{R}$-espace affine euclidien.

Définition 42. Soit X une partie de E. On note $\mathrm{Isom}(X)$ le sous-ensemble de $\mathcal{O}_n(\mathbb{R})$ des isométries qui stabilisent X.

Définition 43. Un polygone convexe de $\mathbb{R}^2$ est dit régulier si tous ses côtés sont de même longueur, et si les angles entre deux côtés sont égaux.

Définition 44. On appelle groupe diédral le groupe D_n formé des isométries du polygone régulier à n cotés.

Proposition 45. *D_n est engendré par une symétrie et une rotation.*

Théorème 46. *Soit $\mathcal{T}$ un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$.*

Application 47. *La table de caractères de $\mathfrak{S}_4$ est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

Développements

— Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (29,32) [Per96]

— Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (46,47) [Ser70]

Références

[Ulm12] F. Ulmer. *Théorie des groupes.* Ellipses
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[CG15] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 2.* Calvage et Mounet
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann

Cadre : Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^\star$, où $\mathbb{K}$ est un corps commutatif.

I Le groupe linéaire $\mathcal{GL}(E)$

1) Définition et premières propriétés

Définition 1. Le groupe linéaire $\mathcal{GL}(E)$ de E est l'ensemble des $\mathbb{K}$-automorphismes de E, c'est-à-dire des applications $\mathbb{K}$-linéaires bijectives de E dans E. C'est un groupe pour la composition des applications.

Exemple 2. *Les homothéties et les rotations sont dans $\mathcal{GL}(E)$.*

Proposition 3. *Soit $u \in \mathcal{L}(E)$. Alors la surjectivité de u, son injectivité et sa bijectivité sont équivalentes.*

Proposition 4. *Pour une base $\mathcal{B}$ donnée de E, on a un isomorphisme de $\mathcal{GL}(E)$ sur $\mathcal{GL}_n(\mathbb{K})$.*

Proposition 5. *Soit $u \in \mathcal{L}(E)$. $u \in \mathcal{GL}(E)$ si, et seulement si,* $\det u \neq 0$.

Définition 6. Le déterminant $\det : \mathcal{GL}(E) \to \mathbb{K}^\star$ est un morphisme de groupes. On appelle groupe spécial linéaire, noté $\mathcal{SL}(E)$, son noyau.

Proposition 7. *$\mathcal{SL}(E)$ est un sous-groupe distingué de $\mathcal{GL}(E)$, et $\mathcal{GL}(E)/\mathcal{SL}(E) \cong \mathbb{K}^\star$.*

2) Quelques éléments de $\mathcal{GL}(E)$

Dilatations

Proposition 8. *Soient H un hyperplan de E et $u \in \mathcal{GL}(E)$ tel que $u|_H = Id_H$. Les assertions suivantes sont équivalentes.*

(i) $\det(u) = \lambda \neq 1$

(ii) *λ est valeur propre de u et u est diagonalisable.*

(iii) $D = \mathrm{Im}(u - Id_E) \not\subset H$

(iv) *La matrice de u dans une certaine base est $D_i(\lambda)$.*

u est alors une dilatation d'hyperplan H de droite D et de rapport λ.

Proposition 9. *Deux dilatations de même rapport sont conjuguées.*

Transvections

Proposition 10. *Soient $H = \mathrm{Ker}(f)$ un hyperplan de E et $u \in \mathcal{GL}(E)$ tel que $u \neq Id_E$ et $u|_H = Id_H$. On note $D = \mathrm{Im}(u - Id_E)$. Les assertions suivantes sont équivalentes.*

(i) $\det(u) = 1$

(ii) *u n'est pas diagonalisable.*

(iii) *$D \subset H$*

(iv) *$\overline{u} : E/H \to E/H$ définie par $\overline{u}(\overline{x}) = \overline{u(x)}$ est l'identité.*

(v) *Il existe $a \in H \setminus \{0\}$ tel que $u = Id_E + fa$.*

(vi) *La matrice de u dans une certaine base est $T_{i,j}(\lambda)$.*

u est alors une transvection d'hyperplan H de droite D.

Corollaire 11. *Soit $u \in \mathcal{GL}(E)$ tel que $u \neq Id_E$. Les assertions suivantes sont équivalentes :*

(i) *u est une transvection de droite D.*

(ii) *$\overline{u} : E/D \to E/D$ définie par $\overline{u}(\overline{x}) = \overline{u(x)}$ est l'identité et $u|_D = Id_D$.*

Homothéties

Définition 12. Soit $u \in \mathcal{GL}(E)$. On dit que u est une homothétie de rapport $\lambda \in \mathbb{K}^\star$ si $u = \lambda Id_E$.

Proposition 13. *Soit u une homothétie de rapport λ. Alors* $\det u = \lambda^n$.

Proposition 14. *Soit $u \in \mathcal{GL}(E)$. Alors u est une homothétie si, et seulement si, u stabilise toutes les droites.*

3) Générateurs

Lemme 15. *On suppose E de dimension $n \geqslant 2$. Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u ou un produit de deux transvections uv, tel que $u(x) = y$ ou $uv(x) = y$.*

Théorème 16. *Les transvections engendrent $\mathcal{SL}(E)$.*

Théorème 17. *Les transvections et les dilatations engendrent $\mathcal{GL}(E)$.*

II Sous-groupes de $\mathcal{GL}(E)$

1) Centres

Théorème 18. *Le centre de $\mathcal{GL}(E)$ est $Z(\mathcal{GL}(E)) = \{\lambda Id_E \,|\, \lambda \in \mathbb{K}^\star\}$. Le centre de $\mathcal{SL}(E)$ est $Z(\mathcal{SL}(E)) = Z(\mathcal{GL}(E)) \cap \mathcal{SL}(E)$.*

Exemple 19. *On considère $\mathbb{K} = \mathbb{R}$ Alors $Z(\mathcal{GL}(E)) = \{\pm Id_E\}$. De plus, $Z(\mathcal{SL}(E)) = \{Id_E\}$ si n est impair, et $Z(\mathcal{SL}(E)) = \{\pm Id_E\}$ si n est pair.*

Exemple 20. *On considère $\mathbb{K} = \mathbb{C}$ Alors $Z(\mathcal{SL}(E)) \cong \mathbb{Z}/n\mathbb{Z}$.*

Définition 21. Le quotient de $\mathcal{GL}(E)$ (resp. $\mathcal{SL}(E)$) par son centre est appelé groupe projectif (spécial) linéaire, noté $\mathcal{PGL}(\mathcal{E})$ (resp. $\mathcal{PSL}(\mathcal{E})$).

2) Groupe orthogonal $\mathcal{O}(E)$

On suppose ici que $\mathrm{car}(\mathbb{K}) \neq 2$. Soit q une forme quadratique sur E de forme polaire f.

Définition 22. On appelle groupe orthogonal l'ensemble $\mathcal{O}(q)$ défini par :

$$\mathcal{O}(q) = \{u \in \mathcal{GL}(E) \,|\, \forall x \in E,\, q(u(x)) = q(x)\}$$

Les éléments de $\mathcal{O}(q)$ sont appelés les isométries de E relativement à q. On note $\mathcal{SO}(q)$ les isométries de déterminant 1.

Proposition 23. *$\mathcal{O}(q)$ est un sous-groupe de $\mathcal{GL}(E)$.*

Proposition 24. *Si $u \in \mathcal{GL}(E)$ est tel que $u^2 = Id_E$, il existe une décomposition $E = E^+ \oplus E^-$ telle que $u|_{E^+} = Id_E$ et $u|_{E^-} = -Id_E$. Si $E^- = \{0\}$, on dit que u est une involution. Si $\dim E^- = 1$ (resp. 2), on dit que u est une réflexion (resp. un renversement).*

Proposition 25. *Si $u \in \mathcal{GL}(E)$ est tel que $u^2 = Id_E$, alors u est une isométrie pour q si, et seulement si, E^+ et E^- sont orthogonaux.*

Théorème 26. *Si f est le produit scalaire usuel sur $\mathbb{R}^n$, alors $\mathcal{O}(q)$ est engendré par les réflexions, et $\mathcal{SO}(q)$ par les renversements si $n \geqslant 3$.*

Théorème 27. *Soit $M \in \mathcal{O}_n(\mathbb{R})$, alors M est semblable à :*

$$\begin{pmatrix} I_r & & & & 0 \\ & -I_m & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_s} \end{pmatrix} \text{ avec } \begin{cases} \theta_i \in]0; 2\pi[\setminus \{\pi\} \\ R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \end{cases}$$

III Actions de $\mathcal{GL}(E)$ et de ses sous-groupes

1) Action sur les sous-espaces de E

Le groupe $\mathcal{GL}(E)$ agit sur E par $u \cdot x = u(x)$, et sur l'ensemble des sous-espaces vectoriels de E de même dimension par $f \cdot V = f(V)$.

Remarque 28. *Ces actions de groupes sont transitives.*

Proposition 29. *La restriction à $\mathcal{SL}(E)$ de ces actions est encore transitive. De même, si E est euclidien, la restriction à $\mathcal{SO}(E)$ est transitive.*

2) Action sur les espaces de matrices

Action par translation

Le groupe $\mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_n(\mathbb{K})$ par multiplication à gauche.

Proposition 30. *Les orbites sont en bijections avec les sous-espaces vectoriels de $\mathbb{K}^n$: $A \sim B \Leftrightarrow \mathrm{Ker}\, A = \mathrm{Ker}\, B$.*

Proposition 31. *Toute matrice est dans l'orbite d'une unique matrice échelonnée.*

Action par conjugaison

Le groupe $\mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_n(\mathbb{K})$ par $P \cdot M = PMP^{-1}$. Cette action traduit le changement de base. La réduction des endomorphismes consiste à trouver des représentants élémentaires des orbites de cette action.

Théorème 32. *Soit $A \in \mathcal{M}_n(\mathbb{C})$. On note O_A l'orbite de A pour cette action. Alors O_A est fermé dans $\mathcal{M}_n(\mathbb{C})$ si, et seulement si, A est diagonalisable. De plus, $O \in \overline{O_A}$ si, et seulement si, A est nilpotente.*

Proposition 33. *Deux matrices A, B de $\mathcal{M}_n(\mathbb{R})$ sont semblables dans $\mathcal{M}_n(\mathbb{C})$ si, et seulement si, elles le sont dans $\mathcal{M}_n(\mathbb{R})$.*

Action par équivalence

Le groupe $\mathcal{GL}_n(\mathbb{K}) \times \mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_{n,m}(\mathbb{K})$ par $(P, T) \cdot M = PMT^{-1}$. Deux matrices de la même orbites sont dites équivalentes. On peut définir le rang d'une matrice comme sa classe de conjugaison pour cette action.

Proposition 34. *Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. En notant O_r l'orbite des matrices de rang r, on a que, pour tout $r \leqslant \min(n, m)$, $\overline{O_r} = \bigcup_{k \leqslant r} O_k$.*

IV Éléments de topologie

On se place dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On munit $\mathcal{M}_n(\mathbb{K})$ d'une norme quelconque.

Proposition 35. *L'ensemble $\mathcal{GL}_n(\mathbb{K})$ est dense dans $\mathcal{M}_n(\mathbb{K})$.*

Proposition 36. *L'ensemble $\mathcal{GL}_n(\mathbb{C})$ est connexe dans $\mathcal{M}_n(\mathbb{C})$, cependant $\mathcal{GL}_n(\mathbb{R})$ n'est pas connexe et admet deux composantes connexes.*

Proposition 37. *L'ensemble $\mathcal{SL}_n(\mathbb{K})$ est connexe dans $\mathcal{M}_n(\mathbb{K})$.*

Proposition 38. *L'ensemble $\mathcal{SO}_n(\mathbb{K})$ est connexe par arcs, et $\mathcal{O}_n(\mathbb{R})$ a deux composantes connexes homéomorphes.*

Proposition 39. *Le groupe $\mathcal{O}_n(\mathbb{R})$ est compact.*

Théorème 40 (Décomposition polaire)**.** *On a les homéomorphismes :*

$$\begin{array}{ccccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) & \mathcal{U}_n(\mathbb{R}) \times \mathcal{H}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O,S) & \longmapsto & OS & (U,H) & \longmapsto & UH \end{array}$$

Corollaire 41. *Tout sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ qui contient le groupe orthogonal $\mathcal{O}_n(\mathbb{R})$ est le groupe $\mathcal{O}_n(\mathbb{R})$ lui-même.*

Développements

- Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$ (15,16,17) [Per96]
- Réduction des endomorphismes normaux (27) [Gou94, CG13]
- Décomposition polaire (40) [CG13]

Références

[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck
[Ulm12] F. Ulmer. *Théorie des groupes.* Ellipses

Cadre : G est un groupe fini de cardinal n, V est un $\mathbb{C}$-espace vectoriel de dimension finie d.

I Représentation d'un groupe fini

1) Définitions et premiers exemples

Définition 1. Une représentation linéaire de G dans V est un morphisme $\rho : G \to \mathcal{GL}(V)$. On notera souvent ρ_s au lieu de $\rho(s)$. On dit que V est un espace de représentation de G. Le degré de ρ est $d = \dim V$.

Exemple 2. *La représentation triviale la représentation de degré 1 :*

$$\rho : \left| \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ s & \longmapsto & 1 \end{array} \right.$$

Exemple 3. *On suppose que G agit sur un ensemble X de cardinal d. Soit $(e_x)_{x\in X}$ une base de V. La représentation suivante est appelée représentation de permutation associée à X :*

$$\rho : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{GL}(V) \\ s & \longmapsto & (e_x \mapsto e_{s\cdot x}) \end{array} \right.$$

Exemple 4. *On suppose que $d = n$. Soit $(e_t)_{t\in G}$ une base de V. La représentation suivante est appelée représentation régulière :*

$$R : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{GL}(V) \\ s & \longmapsto & (e_t \mapsto e_{st}) \end{array} \right.$$

Définition 5. Soient $\rho : G \to \mathcal{GL}(V)$ et $\rho' : G \to \mathcal{GL}(V')$ deux représentations linéaires de G. On dit que ces représentations sont isomorphes (ou semblables) s'il existe un isomorphisme $\tau : V \to V'$ qui vérifie $\tau \circ \rho_s = \rho'_s \circ \tau$ pour tout $s \in G$.

Remarque 6. *Deux représentations isomorphes ont même degré.*

Exemple 7. *Soit ρ une représentation de G. On suppose qu'il existe $w \in W$ tel que $(\rho_s(w))_{s\in G}$ soit une base de V. Alors ρ est isomorphe à la représentation régulière par $e_s \mapsto \rho_s(w)$.*

2) Sous-représentations

Définition 8. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire, et soit W un sous-espace vectoriel de V stable par G (donc stable par ρ_s pour tout $s \in G$). On définit alors une sous-représentation de ρ par :

$$\rho|_W : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{GL}(W) \\ s & \longmapsto & p_s|_W \end{array} \right.$$

Exemple 9. *Soit $R : G \to \mathcal{GL}(V)$ la représentation régulière de G. Soient $x = \sum_{s\in G} e_s$ et $W = \mathrm{Vect}(x)$. Alors, pour tout $s \in G$, on a $R_s(x) = x$. Ainsi, $\tau|_W$ est une sous-représentation de τ, qui est isomorphe à la représentation unité par $\lambda \mapsto \lambda x$.*

Théorème 10 (Théorème de Maschke)**.** *Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire, et soit W un sous-espace vectoriel de V stable par G. Il existe alors un supplémentaire W_0 de W dans V qui est stable par G.*

3) Représentations irréductibles

Définition 11. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. Si $V = \bigoplus_{i=1}^{r} V_i$, on dit alors que ρ est la somme directe des $\rho_i = \rho|_{V_i}$, que l'on note $\rho = \bigoplus_{i=1}^{r} \rho_i$.

Définition 12. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. On dit qu'elle est irréductible si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel non trivial de V n'est stable par G.

Remarque 13. *Toute représentation de degré 1 est irréductible.*

Théorème 14. *Toute représentation linéaire est somme directe de représentations irréductibles.*

Remarque 15. *Cette décomposition n'est pas unique en général. En effet, si, pour tout $s \in G$, $\rho_s = Id_V$, ρ peut se décomposer de bien des façons en écrivant V comme somme directe de droites vectorielles.*

II Caractère d'un groupe fini

1) Définitions et premières propriétés

Définition 16. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. On appelle caractère de ρ la fonction :

$$\chi : \left| \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ s & \longmapsto & \mathrm{tr}(\rho_s) \end{array} \right.$$

Proposition 17. *Soit χ le caractère d'un représentation de degré n.*

(i) $\chi(e) = n$

(ii) $\forall\, s \in G,\ \chi(s^{-1}) = \overline{\chi(s)}$

(iii) χ *est central :* $\forall\, s, t \in G,\ \chi(tst^{-1}) = \chi(s)$

Proposition 18. *Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G de caractère χ. On suppose que ρ est somme directe de représentations $\rho_i : G \to \mathcal{GL}(V_i)$ de caractères χ_i pour $i \in [\![1, r]\!]$. Alors $\chi = \sum_{i=1}^{r} \chi_r$.*

Exemple 19. *On suppose que G agit sur un ensemble X. Soit ρ la représentation de permutation correspondante. Alors :*

$$\forall\, s \in G,\ \chi(s) = \mathrm{Card}\left(\{x \in X \mid s \cdot x = x\}\right)$$

2) Lemme de Schur, premières applications

Proposition 20 (Lemme de Schur)**.** *Soient $\rho^1 : G \to \mathcal{GL}(V_1)$ et $\rho^2 : G \to \mathcal{GL}(V_2)$ deux représentations irréductibles de G. Soit $f : V_1 \to V_2$ une application linéaire telle que, pour tout $s \in G$, $\rho^2_s \circ f = f \circ \rho^1_s$. Alors :*

(i) Si ρ^1 et ρ^2 ne sont pas isomorphes, alors $f = 0$.

(ii) Si $V_1 = V_2$ et $\rho^1 = \rho^2$, alors f est une homothétie.

Corollaire 21. *Soient $\rho^1 : G \to \mathcal{GL}(V_1)$ et $\rho^2 : G \to \mathcal{GL}(V_2)$ deux représentations irréductibles de G. Soit h une application linéaire de V_1 dans V_2, et posons pour tout $t \in G$:*

$$h^0 = \frac{1}{|G|} \sum_{t \in G} (\rho^2_t)^{-1} h \rho^1_t$$

(i) Si ρ^1 et ρ^2 ne sont pas isomorphes, alors $h^0 = 0$.

(ii) Si $V_1 = V_2$ et $\rho^1 = \rho^2$, alors h^0 est une homothétie de rapport $\frac{\mathrm{tr}(h)}{\dim V_1}$.

Définition 22. Soient $\varphi, \psi : G \to \mathbb{C}$ deux fonctions. On pose :

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{t \in G} \varphi(t) \psi(t^{-1})$$

Théorème 23. *Soient $\rho^1 : G \to \mathcal{GL}(V_1)$ et $\rho^2 : G \to \mathcal{GL}(V_2)$ deux représentations irréductibles de G. Pour $t \in G$, on écrit $(r_{i,j}(t))_{1 \leqslant i,j \leqslant n_1}$ la matrice de ρ^1_t dans une base de V_1 et $(u_{i,j}(t))_{1 \leqslant i,j \leqslant n_2}$ la matrice de ρ^2_t dans une base de V_2. Soient $i_1, j_1 \in [\![1, n_1]\!]$ et $i_2, j_2 \in [\![1, n_2]\!]$, alors :*

(i) Si ρ^1 et ρ^2 ne sont pas isomorphes, alors on a $\langle u_{i_2,j_2}, r_{i_1,j_1} \rangle = 0$.

(ii) Si $V_1 = V_2$ et $\rho^1 = \rho^2$, alors on a $\langle u_{i_2,j_2}, r_{i_1,j_1} \rangle = \frac{1}{n} \delta_{i_2,i_1} \delta_{j_2,j_1}$.

3) Orthogonalité des caractères

Définition 24. Soient $\varphi, \psi : G \to \mathbb{C}$ deux fonctions. On pose :

$$(\varphi | \psi) = \frac{1}{|G|} \sum_{t \in G} \varphi(t) \overline{\psi(t)}$$

$(.|.)$ est un produit scalaire.

Remarque 25. *Si χ est un caractère, alors $\langle \varphi, \chi \rangle = (\varphi | \chi)$.*

Théorème 26. *(i) Si χ est le caractère d'une représentation irréductible, on a $(\chi | \chi) = 1$.*

(ii) Si χ et χ' sont les caractères de deux représentations irréductibles non isomorphes, on a $(\chi | \chi') = 0$.

Remarque 27. *Les caractères irréductibles sont un système orthogonal.*

Théorème 28. *Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G, de caractère χ, et supposons ρ décomposée en somme directe de représentations irréductibles : $\rho = \bigoplus_{i=1}^{r} \rho_i$. Alors, si ρ_0 est une représentation irréductible de caractère χ_0, le nombre de ρ_i isomorphes à ρ_0 est égal au produit scalaire $(\chi | \chi_0) = \langle \chi, \chi_0 \rangle$.*

Remarque 29. *Le nombre des ρ_i isomorphes à représentation irréductible donnée ne dépend pas de la décomposition.*

Corollaire 30. *Deux représentations de même caractère sont isomorphes.*

Théorème 31. *Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G, de caractère χ. Alors $(\chi | \chi) = \sum_{i=1}^{r} m_i^2$, où l'on a écrit $\rho = \bigoplus_{i=1}^{r} m_i \rho_i$.*

Corollaire 32. *Si χ est un caractère, alors $(\chi | \chi)$ est un entier positif, et vaut 1 si, et seulement si, il est irréductible.*

4) Nombre de représentations irréductibles

Proposition 33. *Soit f une fonction centrale sur G, et soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. Soit ρ l'application linéaire de V dans lui-même définie par $\rho_f = \sum_{t\in G} f(t)\rho_t$. Si ρ est irréductible de degré n et de caractère χ, alors ρ_f est une homothétie de rapport $\lambda = \frac{|G|}{n}(f|\overline{\chi})$.*

Théorème 34. *Les caractères irréductibles forment une base orthonormale de l'espace vectoriel des fonctions centrales sur G.*

Théorème 35. *Le nombre des représentations irréductibles de G (à isomorphisme près) est égal au nombre classes de conjugaison de G.*

Proposition 36. *Soit $s \in G$ et soit $c(s)$ le nombre d'éléments de la classe de conjugaison de s. Soient $\chi_1, \dots, \chi_k$ les caractères irréductibles de G.*

(i) $\sum_{i=1}^{k} \overline{\chi_i(s)}\chi_i(s) = \frac{|G|}{c(s)}$

(ii) Si $t \in G$ n'est pas conjugué à s, on a $\sum_{i=1}^{k} \overline{\chi_i(s)}\chi_i(t) = 0$.

III Tables de caractères

1) Généralités

Définition 37. On note $C_1, \dots, C_r$ les classes de conjugaison de G et $\chi_1, \dots, \chi_r$ les caractères irréductibles de G. On appelle table de caractères de G le tableau de taille $r \times r$ dont la valeur à la ligne i et à la colonne j vaut $\chi_i(C_j)$.

Exemple 38. *Table de D_8 et de $\mathbb{H}_8$ (voir Annexe). Ces groupes ont même table de caractères mais ne sont pas isomorphes.*

2) Groupes cycliques et abéliens

Supposons que G est abélien.

Théorème 39. *G est abélien si et seulement si toute représentation irréductible est de degré 1.*

Exemple 40. *Table de $\mathbb{Z}/n\mathbb{Z}$ (voir Annexe).*

Définition 41. L'exposant de G est le ppcm des ordres de ses éléments.

Définition 42. On pose $\widehat{G}$ l'ensemble des caractères de G. C'est un groupe, appelé groupe dual de G.

Proposition 43. *L'application $\iota : G \to \widehat{\widehat{G}}$ définie pour $g \in G$ par $\iota(g) : \chi \mapsto \chi(g)$ est un isomorphisme.*

Lemme 44. *Il existe un élément de G d'ordre l'exposant de G.*

Proposition 45. *G et $\widehat{G}$ ont même exposant.*

Théorème 46. *Il existe un unique entier ℓ et une unique suite $d_\ell | \cdots | d_2 | d_1$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G et :*

$$G \cong \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Corollaire 47. *G et $\widehat{G}$ sont isomorphes.*

3) Tables et simplicités

Lemme 48. *Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G de caractère χ. Alors* $\mathrm{Ker}(\rho) = \mathrm{Ker}(\chi) = \{g \in G \,|\, \chi(g) = \chi(e)\}$.

Proposition 49. *Soient $\chi_1, \dots, \chi_k$ les caractères irréductibles de G. Les sous-groupes distingués de G sont les $\bigcap_{i\in I} \mathrm{Ker}(\chi_i)$ où $I \subset [\![1, k]\!]$.*

Corollaire 50. *G est simple si, et seulement si, pour tout caractère irréductible non trivial de G et tout $g \in G \setminus \{e\}$ on a $\chi(g) \neq \chi(e)$.*

Exemple 51. *Tables de $\mathfrak{S}_3$ et $\mathfrak{S}_4$ (voir Annexe).*

Remarque 52. *Grâce à leurs tables de caractères, on voit que $\mathfrak{S}_3$ est simple, mais $\mathfrak{S}_4$ ne l'est pas car le sous-groupe $\mathrm{Ker}(\theta)$ des doubles transpositions et $\mathfrak{A}_4 = \mathrm{Ker}(\varepsilon)$ sont distingués et non triviaux.*

Développements

- Structure des groupes abéliens finis (43,44,45,46) [Col09]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (51) [Ser70]

Références

[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann
[Col09] P. Colmez. *Éléments d'analyse et d'algèbre.* Les éditions de l'École Polytechnique
[Pey08] G. Peyré. *L'algèbre discrète de la transformée de Fourier.* Ellipses

Annexes

D_8	$\{id\}$	$\{r^2\}$	$\{r, r^3\}$	$\{s, r^2s\}$	$\{rs, r^3s\}$
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

FIGURE 1 – Table de caractères de D_8

$\mathbb{H}_8$	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

FIGURE 2 – Table de caractères de $\mathbb{H}_8$

$\mathbb{Z}/n\mathbb{Z}$	0	1	2	$\cdots$	$n-1$
χ_1	1	1	1	$\cdots$	1
χ_2	1	ω	ω^2	$\cdots$	ω^{n-1}
χ_3	1	ω^2	ω^4	$\cdots$	ω^{n-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_n	1	ω^{n-1}	ω^{n-2}	$\cdots$	ω

où $\omega = e^{\frac{2i\pi}{n}}$.

FIGURE 3 – Table de caractères de $\mathbb{Z}/n\mathbb{Z}$

$\mathfrak{S}_3$	Id	(ab)	(abc)
1	1	1	1
ε	1	-1	1
θ	2	0	-1

FIGURE 4 – Table de caractères de $\mathfrak{S}_3$

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

FIGURE 5 – Table de caractères de $\mathfrak{S}_4$

$\mathfrak{A}_4$	Id	$C \setminus \{Id\}$	tC	t^2C
1	1	1	1	1
χ_1	1	1	j	j^2
χ_2	1	1	j^2	j
χ_3	3	-1	0	0

FIGURE 6 – Table de caractères de $\mathfrak{A}_4$

Cadre : G est un groupe.

I Génération d'un groupe

1) Sous-groupe engendré

Définition 1. Soit X une partie de G. L'intersection des sous-groupes de G qui contiennent X est un sous-groupe de G, qu'on appelle sous-groupe engendré par X et qu'on note $\langle X \rangle$. Si $G = \langle X \rangle$, alors on dit que X est une partie génératrice de G.

Exemple 2. *(i)* $\forall\, a \in G,\ \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$

(ii) Si a et b commutent dans G, $\langle a, b \rangle = \{a^m b^n \mid m, n \in \mathbb{Z}\}$. On peut généraliser pour tout nombre fini d'élément.

Définition 3. (i) G est monogène s'il est engendré par un élément.

(ii) G est cyclique s'il est monogène et fini.

(iii) G est de type fini s'il est engendré par une partie finie.

Exemple 4. $(n\mathbb{Z}, +)$ *est monogène car engendré par n.*

Définition 5. On appelle groupe dérivé de G le sous-groupe de G engendré par ses commutateurs.

Remarque 6. *Si G est abélien, son groupe dérivé est trivial.*

2) Ordre d'un élément

Définition 7. Un élément a de G est dit d'ordre $p \in \mathbb{N}^\star$ si $\langle a \rangle$ est fini de cardinal p. On a alors $\langle a \rangle = \{e, a, a^2, \ldots, a^{p-1}\}$. Si cet ensemble n'est pas fini, a est dit d'ordre infini.

Exemple 8. *(i) e est d'ordre 1 dans G.*

(ii) 1 est d'ordre infini dans $\mathbb{Z}$.

(iii) Dans $\mathfrak{S}_n$, un cycle de longueur ℓ est d'ordre ℓ.

Théorème 9. *Si G est fini d'ordre n, l'ordre de tout élément divise n.*

Proposition 10. *Soit $a \in G$ d'ordre p. Alors $a^q = e \Leftrightarrow p \mid q$.*

Proposition 11. *Soit G d'ordre fini. Soient $g, h \in G$ qui commutent d'ordre p et q.*

(i) gh est d'ordre fini qui divise $\mathrm{ppcm}(p, q)$.

(ii) Si $\langle g \rangle \cap \langle h \rangle = \{e\}$, alors gh est d'ordre $\mathrm{ppcm}(p, q)$.

(iii) Si p et q sont premiers entre eux, alors gh est d'ordre pq.

Théorème 12. *Soit G un groupe abélien fini. Il existe un élément d'ordre le* ppcm *de tous ses éléments. Cet entier est l'exposant de G.*

II Cas des groupes abéliens

1) Groupes cycliques

Exemple 13. *Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et le groupe des racines n-ièmes de l'unité sont cycliques d'ordre n.*

Théorème 14. *Un groupe cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Proposition 15. *Soit $G = \langle a \rangle$ cyclique à n éléments. Alors $G = \langle g \rangle$ si, et seulement si, k et n sont premiers entre eux.*

Corollaire 16. *Un groupe cyclique d'ordre n possède $\varphi(n)$ générateurs.*

Corollaire 17. *Un groupe de cardinal premier est cyclique et tout élément non trivial est générateur.*

Théorème 18. *Soit $G = \langle a \rangle$ cyclique à n éléments.*

(i) Les sous-groupes de G sont cycliques d'ordre divisant n.

(ii) Soit d un diviseur de n. Il existe un unique sous-groupe de G d'ordre d qui est $\left\langle a^{\frac{n}{d}} \right\rangle$. Ces générateurs sont les éléments d'ordre d.

Application 19. *Soit $n \in \mathbb{N}^\star$, alors $n = \sum_{d \mid n} \varphi(d)$.*

Application 20. *Soit $\mathbb{K}$ un corps. Tout sous-groupe du groupe multiplicatif est cyclique.*

2) Groupes abéliens finis

Théorème 21. *Soit G un groupe abélien fini, alors :*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z} \quad \text{où} \quad \forall\, i \in [\![1, n-1]\!],\ d_i \mid d_{i+1}$$

De plus, les d_i sont uniques. Ce sont les facteurs invariants.

Corollaire 22. *Si $d \mid |G|$, G admet un sous-groupe cyclique d'ordre d.*

III Groupe symétrique

1) Générateurs

Proposition 23. *Toute permutation se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près.*

Exemple 24. $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\3&10&2&4&7&9&8&5&6&1\end{smallmatrix}\right) = (1\ 3\ 2\ 10)(4)(5\ 7\ 8)(6\ 9)$

Proposition 25. *Toute permutation de $\mathfrak{S}_n$ se décompose en produit de (au plus $n-1$) transpositions.*

Exemple 26. $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9&10\\3&10&2&4&7&9&8&5&6&1\end{smallmatrix}\right) = (1\ 10)(1\ 2)(1\ 3)(5\ 8)(5\ 7)(6\ 9)$

Corollaire 27. *La signature d'une permutation est déterminée par la parité du nombre de transpositions la composant.*

Proposition 28. *Les familles suivantes engendrent $\mathfrak{S}_n$:*

(i) $\{(1\ i)\,|\,1 < i \leqslant n\}$

(ii) $\{(i\ i+1)\,|\,1 \leqslant i < n\}$

(iii) $\{(1\ 2), (1\ 2\ \ldots\ n)\}$

Remarque 29. *Quel que soit n, deux éléments suffisent à engendrer $\mathfrak{S}_n$.*

2) Groupe alterné

Proposition 30. *$\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$. De plus, $\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}$.*

Lemme 31. *$\mathfrak{A}_n$ est $n-2$ fois transitif sur $[\![1,n]\!]$: si on a $a_1,\ldots,a_{n-2} \in [\![1,n]\!]$ distincts et $b_1,\ldots,b_{n-2} \in [\![1,n]\!]$ distincts, il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $i \in [\![1,n-2]\!]$.*

Proposition 32. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Proposition 33. *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Théorème 34. *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

Corollaire 35. *Pour $n \geqslant 5$, le groupe dérivé de $\mathfrak{A}_n$ est $\mathfrak{A}_n$.*

Corollaire 36. *Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathfrak{A}_n$ et $\{Id\}$.*

IV Applications en algèbre linéaire

On considère E un $\mathbb{K}$-espace vectoriel de dimension finie n.

1) Groupe linéaire

Proposition 37. *Soient $H = \mathrm{Ker}(f)$ un hyperplan de E et $u \in \mathcal{GL}(E)$ tel que $u \neq Id_E$ et $u|_H = Id_H$. On note $D = \mathrm{Im}(u - Id_E)$. Les assertions suivantes sont équivalentes.*

(i) $\det(u) = 1$

(ii) *u n'est pas diagonalisable.*

(iii) $D \subset H$

(iv) *$\overline{u} : E/H \to E/H$ définie par $\overline{u}(\overline{x}) = \overline{u(x)}$ est l'identité.*

(v) *Il existe $a \in H \setminus \{0\}$ tel que $u = Id_E + fa$.*

(vi) *La matrice de u dans une certaine base est $T_{i,j}(\lambda)$.*

u est alors une transvection d'hyperplan H de droite D.

Corollaire 38. *Soit $u \in \mathcal{GL}(E)$ tel que $u \neq Id_E$. Les assertions suivantes sont équivalentes :*

(i) *u est une transvection de droite D.*

(ii) *$\overline{u} : E/D \to E/D$ définie par $\overline{u}(\overline{x}) = \overline{u(x)}$ est l'identité et $u|_D = Id_D$.*

Proposition 39. *Soient H un hyperplan de E et $u \in \mathcal{GL}(E)$ tel que $u|_H = Id_H$. Les assertions suivantes sont équivalentes.*

(i) $\det(u) = \lambda \neq 1$

(ii) *λ est valeur propre de u et u est diagonalisable.*

(iii) $D = \mathrm{Im}(u - Id_E) \not\subset H$

(iv) *La matrice de u dans une certaine base est $D_i(\lambda)$.*

u est alors une dilatation d'hyperplan H de droite D et de rapport λ.

Lemme 40. *On suppose E de dimension $n \geqslant 2$. Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u ou un produit de deux transvections uv, tel que $u(x) = y$ ou $uv(x) = y$.*

Théorème 41. *Les transvections engendrent $\mathcal{SL}(E)$.*

Théorème 42. *Les transvections et les dilatations engendrent $\mathcal{GL}(E)$.*

2) Groupe orthogonal

Définition 43. Soit F un sous-espace vectoriel de E. Pour tout $x \in E$, il existe une unique décomposition $x = x_1 + x_2$ avec $x_1 \in F$ et $x_2 \in F^\perp$. On appelle symétrie orthogonale par rapport à F l'application :

$$s : \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x_1 - x_2 \end{array} \right.$$

Définition 44. Une réflexion est une symétrie orthogonale par rapport à un hyperplan. Un retournement est une symétrie par rapport à un hyperplan de dimension $n-2$.

Théorème 45. *Tout élément de $\mathcal{O}(E)$ s'écrit comme produit de r réflexions, où $r = \mathrm{rg}(u - Id_E)$.*

Corollaire 46. *Si $n \geqslant 3$, $\mathcal{SO}(E)$ est engendré par les retournements.*

Théorème 47. *Soit $M \in \mathcal{O}_n(\mathbb{R})$, alors M est semblable à :*

$$\begin{pmatrix} I_r & & & & 0 \\ & -I_m & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_s} \end{pmatrix} \quad \text{avec} \quad \left\{ \begin{array}{l} \theta_i \in]0; 2\pi[\setminus \{\pi\} \\ R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \end{array} \right.$$

Application 48. *$S\mathcal{O}_n(\mathbb{R})$ est connexe par arcs.*

Développements

— Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (33,34) [Per96]
— Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$ (40,41,42) [Per96]

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck

Cadre : Soient n et m des entiers naturels non nuls.

I Structures

1) Structure de groupe

Rappel. *Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, ce sont aussi ses idéaux.*

Définition 1. $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}, +)$ est muni d'une structure de groupe par : $\overline{x} + \overline{y} = \overline{x+y}$.

Proposition 2. *$(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.*

Proposition 3. *Tout groupe monogène est isomorphe soit à $(\mathbb{Z}, +)$ soit à $(\mathbb{Z}/n\mathbb{Z}, +)$ pour un certain entier n, selon son cardinal.*

Exemple 4. *Groupe des racines n-ième de l'unité isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 5. *(i) Un sous-groupe d'un groupe cyclique est cyclique.*

(ii) Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est engendré par la classe d'un diviseur b de n, ce sous-groupe est d'ordre $a = \frac{n}{b}$.

(iii) Réciproquement, si $a|n$ et $b = \frac{n}{a}$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre a, engendré par la classe b modulo n.

Exemple 6. *Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont engendrés par les classes de 1, 2, 3, 6 : $\langle 1\rangle \cong \mathbb{Z}/6\mathbb{Z}$, $\langle 2\rangle \cong \mathbb{Z}/3\mathbb{Z}$, $\langle 3\rangle \cong \mathbb{Z}/2\mathbb{Z}$ et $\langle 6\rangle \cong \{0\}$.*

Définition 7. On appelle indicatrice d'Euler de $n \geqslant 1$ l'entier :

$$\varphi(n) = \text{Card}\left(\{k \in [\![1, n]\!] \mid k \wedge n = 1\}\right)$$

Proposition 8. *Soit $k \in \mathbb{N}$. $\overline{k}$ est inversible $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, $k \wedge n = 1$. En particulier, $\varphi(n)$ est le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 9. *Les générateurs sont exactement les inversibles.*

Exemple 10. *$\varphi(6) = 2$ et les générateurs de $\mathbb{Z}/6\mathbb{Z}$ sont 1 et 5.*

Proposition 11. *(i) Pour $d|n$, $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(d)$ éléments d'ordre d.*

(ii) (Formule de Möbius) $n = \sum_{d|n} \varphi(n)$

Proposition 12. *Les automorphismes de groupe de $\mathbb{Z}/n\mathbb{Z}$ sont les applications $\psi_k : \overline{x} \mapsto k\overline{x}$ pour $1 \leqslant k \leqslant n$ avec $k \wedge n = 1$. On a ainsi $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Exemple 13. $\text{Aut}(\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ *(groupe à deux éléments)*

2) Structure d'anneau

Définition 14. $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est muni d'une structure d'anneau par : $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \cdot \overline{y} = \overline{xy}$.

Proposition 15. *Soit $n > 1$ et $a \in \mathbb{Z}$. Alors $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

Corollaire 16. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier. On note alors $\mathbb{Z}/n\mathbb{Z} = \mathbb{F}_n$.*

Proposition 17 (Euler)**.** *Soient a et n deux entiers non nuls premiers entre eux. Alors $a^{\varphi(n)} \equiv 1[n]$.*

Corollaire 18 (Fermat)**.** *Soient p un nombre premier et $a \in \mathbb{N}^\star$ non divisible par p. Alors $a^{p-1} \equiv 1[p]$.*

Proposition 19 (Wilson)**.** *Soit $p \in \mathbb{N}^\star$, alors p est premier si, et seulement si, $(p-1)! \equiv -1[p]$.*

Théorème 20 (Bézout)**.** *Soient a et b deux entiers non nuls, alors a et b sont premiers entre eux si, et seulement si, il existe deux entiers u et v tels que $au + bv = 1$.*

Théorème 21 (Restes chinois)**.** *Soit $n = m_1 m_2$ avec $m_1 \wedge m_2 = 1$. Alors l'application définie par :*

$$\Phi : \left| \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z} \\ \overline{n}^m & \longmapsto & (\overline{n}^{m_1}, \ldots, \overline{n}^{m_k}) \end{array} \right.$$

est un isomorphisme d'anneaux.

Généralisation 22. *Le théorème des restes chinois se généralise à tout produit d'entiers premiers entre eux deux à deux.*

Exemple 23. *Résolution de systèmes de congruences :*

$$\begin{cases} x &\equiv 1[3] \\ x &\equiv 2[4] \\ x &\equiv 0[5] \end{cases} \Leftrightarrow x = 10 + 60k,\ k \in \mathbb{Z}$$

Corollaire 24. *Soient $m, n \in \mathbb{N}$ premiers entre eux. On a alors $(\mathbb{Z}/nm\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, et donc $\varphi(nm) = \varphi(n)\varphi(m)$.*

Corollaire 25. *Soit $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Alors :*

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/(p_1^{\alpha_1})\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/(p_k^{\alpha_k})\mathbb{Z})^\times$$

II Arithmétique dans $\mathbb{Z}$

1) Équations diophantiennes

Définition 26. Un équation diophantienne est une équation de la forme $P(x_1, \dots, x_n) = 0$, où P est un polynôme à n variables et à coefficients entiers, et dont on cherche les solutions parmi les entiers.

Exemple 27. *(i) Triplets pythagoriciens : $x^2 + y^2 = z^2$*
(ii) Équation de Pell-Fermat : $x^2 - ny^2 = 1$
(iii) Somme de carrés : $n = x^2 + y^2$

Proposition 28. *Soit a, b et c des entiers. On note (E) l'équation $ax + by = c$. L'équation (E) admet des solution si, et seulement si, le* pgcd *de a et b divise c. Dans ce cas, il y a une infinité de solutions.*

Théorème 29 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

2) Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 30. Si $q = p^n$ avec p premier, on note $\mathbb{F}_q$ le corps à q éléments.

Définition 31. On pose $(\mathbb{F}_q)^2 = \left\{x^2 \in \mathbb{F}_q \,\middle|\, x \in \mathbb{F}_q\right\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{\star 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$.

Proposition 32. *Si $q = p^n$, on a :*
(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$
(ii) Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\star 2}| = \frac{q-1}{2}$

Proposition 33. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 34. *Si $q = p^n$ et $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, q est congru à 1 modulo 4.*

Corollaire 35. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 36. Soit p un premier impair et $a \in \mathbb{N}$. On définit le symbole de Legendre de a par p par $\left(\frac{a}{p}\right) = \begin{cases} 1 & si\ \overline{a} \in \mathbb{F}_p^{\star 2} \\ -1 & si\ \overline{a} \notin \mathbb{F}_p^{\star 2} \\ 0 & si\ \overline{a} = 0 \end{cases}$.

Proposition 37. *Pour $x, y \in \mathbb{F}_p^\star$, on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.*
Le symbole de Legendre donne un morphisme $\mathbb{F}_q^\star \to \{\pm 1\}$.

Proposition 38. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$*

Théorème 39 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$.*

Proposition 40. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 41. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 42. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

III Applications aux polynômes

1) Irréductibilité des polynômes de $\mathbb{Z}[X]$

Proposition 43. *Soient $P, Q \in \mathbb{F}_p[X]$. Alors :*

$$(P + Q)^p = P^p + Q^p \text{ et } (P(X))^p = P(X^p)$$

Définition 44. On définit le contenu de $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ par $c(P) = \text{pgcd}(a_0, \dots, a_n)$. Un polynôme P est dit primitif si $c(P) = 1$.

Proposition 45. *Soient $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.*

Proposition 46. *Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :*
(i) Les polynômes constants, irréductibles dans $\mathbb{Z}$ (premiers).
(ii) Les polynômes non constants, primitifs et irréductibles dans $\mathbb{Q}[X]$.

Théorème 47 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.*
Soit un nombre premier p tel que $p \nmid a_n$, $\forall i < n, p | a_i$ et $p^2 \nmid a_0$.
Alors P est irréductible dans $\mathbb{Z}[X]$.

2) Polynômes cyclotomiques

Définition 48. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 49. *Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 50. $\forall n \in \mathbb{N}^\star, X^n - 1 = \prod_{d|n} \Phi_d(n)$

Exemple 51. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Proposition 52. *Pour $n \in \mathbb{N}^\star$, Φ_n est à coefficients entiers, et est irréductible dans $\mathbb{Z}[X]$.*

Lemme 53. *Soit $a \in \mathbb{Z}$ et p premier tel que $p|\Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour $d|n$ et $d < n$. Alors $p \equiv 1[n]$.*

Théorème 54 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

Développements

- Théorème de Sophie Germain (29) [FGN13a]
- Loi de réciprocité quadratique (39) [Ser13]
- Forme faible de la progression arithmétique de Dirichlet (53,54) [FGN13a]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[Ser13] J.-P. Serre. *Cours d'Arithmétique.* PUF

I Arithmétique dans $\mathbb{Z}$

1) Définitions et premières propriétés

Définition 1. Un entier naturel est un nombre premier s'il est supérieur ou égal à 2 et si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et lui-même. Un entier qui n'est pas premier est appelé composé. On notera $\mathbb{P}$ l'ensemble des nombres premiers.

Proposition 2. *Soit $n \geqslant 2$ un entier composé, alors il existe $p \in \mathbb{P}$ tel que p divise n et $p^2 \leqslant n$.*

Application 3 (Crible d'Erathostène)**.** *C'est un algorithme qui permet de déterminer dans $\mathbb{N}$ la suite des nombres premiers inférieurs à un nombre donné N. Il consiste à rayer dans la liste $A, \dots, N$ les multiples de 2, puis de 3, et ainsi de suite. Quand on rencontre un entier qui n'est pas encore rayé, il est premier. On supprime ses multiples de la liste et alors apparaît, non rayé, le nombre premier suivant.*

Exemple 4. *401 est premier, mais 403 est composé.*

Théorème 5 (Euclide)**.** *Il existe une infinité de nombres premiers.*

Théorème 6 (admis)**.** *Si on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x, on a $\pi(x) \underset{x\to\infty}{\sim} \frac{x}{\ln x}$.*

Théorème 7 (Théorème fondamental de l'arithmétique)**.** *Soit n un entier strictement supérieur à 1. Alors ou bien n est premier, ou bien n se décompose de manière unique en un produit de facteurs premiers.*

Application 8. $780 \wedge 1001 = 13$, $780 \vee 1001 = 60060$, *780 a 24 diviseurs.*

2) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 9. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.*

Proposition 10. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si, et seulement si, n est premier.*

Proposition 11. *Si $p \in \mathbb{P}$, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.*

Théorème 12 (Wilson)**.** *Un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-1)!$ est congru à -1 modulo p.*

Théorème 13 (Petit théorème de Fermat)**.** *Si p est un entier naturel premier, pour tout entier relatif n, on a alors $n^p \equiv n[p]$, et dans le cas où n est premier avec p, on a $n^{p-1} \equiv 1[p]$.*

Contre-exemple 14 (Nombres de Carmichael)**.** *La réciproque du petit théorème de Fermat est rendue fausse par les nombres de Carmichael, comme 561.*

Lemme 15. *Soit p un nombre premier, alors , pour tout entier k compris entre 1 et $p-1$, on a $\binom{p}{k} \equiv 0[p]$ et $\binom{p-1}{k} \equiv (-1)^k[p]$.*

Définition 16. Pour tout $n \in \mathbb{N}$, on note $\varphi(n)$ le nombre d'entiers premiers à n. Alors, $\varphi(n)$ est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Théorème 17 (Euler-Fermat)**.** *Si n est un entier naturel non nul, pour tout entier relatif a, on a alors $a^{\varphi(n)} \equiv a[n]$.*

Théorème 18 (Restes chinois)**.** *Soient m et n deux entiers naturels premiers entre eux. Alors $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Corollaire 19. *φ est multiplicative.*

II Applications de la réduction modulo p

1) Irréductibilité des polynômes de $\mathbb{Z}[X]$

Proposition 20. *Soient $P, Q \in \mathbb{F}_p[X]$. Alors :*

$$(P+Q)^p = P^p + Q^p \text{ et } (P(X))^p = P(X^p)$$

Définition 21. On définit le contenu de $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ par $c(P) = \text{pgcd}(a_0, \dots, a_n)$. Un polynôme P est dit primitif si $c(P) = 1$.

Proposition 22. *Soient $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.*

Proposition 23. *Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :*

(i) Les polynômes constants, irréductibles dans $\mathbb{Z}$ (premiers).

(ii) Les polynômes non constants, primitifs et irréductibles dans $\mathbb{Q}[X]$.

Théorème 24 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.*
Soit un nombre premier p tel que $p \nmid a_n$, $\forall i < n, p | a_i$ et $p^2 \nmid a_0$.
Alors P est irréductible dans $\mathbb{Z}[X]$.

2) Résolution d'équations diophantiennes

Définition 25. Un équation diophantienne est une équation de la forme $P(x_1, \dots, x_n) = 0$, où P est un polynôme à n variables et à coefficients entiers, et dont on cherche les solutions parmi les entiers.

Exemple 26. *(i) Triplets pythagoriciens : $x^2 + y^2 = z^2$*
(ii) Équation de Pell-Fermat : $x^2 - ny^2 = 1$
(iii) Somme de carrés : $n = x^2 + y^2$

Proposition 27. *Soit a, b et c des entiers. On note (E) l'équation $ax + by = c$. L'équation (E) admet des solution si, et seulement si, le* pgcd *de a et b divise c. Dans ce cas, il y a une infinité de solutions.*

Théorème 28 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

III Les corps finis

1) Propriétés des corps finis

Définition 29. Soit $\mathbb{K}$ un corps, on appelle sous-corps premier de $\mathbb{K}$ l'intersection de tous ses sous-corps non nuls.

Exemple 30. *Le sous-corps premier de $\mathbb{R}$ et $\mathbb{C}$ est $\mathbb{Q}$.*

Définition 31. Soit A un anneau unitaire, il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$. Le générateur positif de $\operatorname{Ker}\varphi$ est appelé caractéristique de A, notée $\operatorname{car}(A)$.

Proposition 32. *Si $A = \mathbb{K}$ est un corps, sa caractéristique est nulle ou est un nombre premier.*

Corollaire 33. *Si $\operatorname{car}(K) = 0$, alors $\mathbb{K}$ est infini, mais la réciproque est fausse.*

Théorème 34. *Soit $\mathbb{L}$ une extension de corps de $\mathbb{K}$, alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.*

Corollaire 35. *Soit $\mathbb{L}$ une extension de corps de $\mathbb{K}$ avec $\mathbb{K}$ et $\mathbb{L}$ finis, alors $\mathbb{L} \cong \mathbb{K}^n$.*

Théorème 36. *Si $\mathbb{K}$ est un corps fini de caractéristique p, son sous-corps premier de $\mathbb{K}$ est $\mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathbb{K}$ a pour cardinal une puissance de p.*

Théorème 37. *À $\mathbb{F}_p$-isomorphisme près, il existe un unique corps de cardinal p^n, noté $\mathbb{F}_{p^n}$.*

2) Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 38. Si $q = p^n$ avec p premier, on note $\mathbb{F}_q$ le corps à q éléments.

Définition 39. On pose $(\mathbb{F}_q)^2 = \left\{x^2 \in \mathbb{F}_q \,\middle|\, x \in \mathbb{F}_q\right\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{\star 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$.

Proposition 40. *Si $q = p^n$, on a :*
(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$
(ii) Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\star 2}| = \frac{q-1}{2}$

Proposition 41. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 42. *Si $q = p^n$ et $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, q est congru à 1 modulo 4.*

Corollaire 43. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 44. Soit p un premier impair et $a \in \mathbb{N}$. On définit le symbole de Legendre de a par p par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si \quad \overline{a} \in \mathbb{F}_p^{\star 2} \\ -1 & si \quad \overline{a} \notin \mathbb{F}_p^{\star 2} \\ 0 & si \quad \overline{a} = 0 \end{cases}$$

Proposition 45. *Pour $x, y \in \mathbb{F}_p^\star$, on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.*
Le symbole de Legendre donne un morphisme $\mathbb{F}_q^\star \to \{\pm 1\}$.

Proposition 46. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$*

Théorème 47 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$.*

Proposition 48. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 49. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 50. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

3) Polynômes cyclotomiques

Définition 51. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 52. *Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 53. $\forall n \in \mathbb{N}^\star, X^n - 1 = \prod_{d|n} \Phi_d(n)$

Exemple 54. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Proposition 55. *Pour $n \in \mathbb{N}^\star$, Φ_n est à coefficients entiers, et est irréductible dans $\mathbb{Z}[X]$.*

Lemme 56. *Soit $a \in \mathbb{Z}$ et p premier tel que $p|\Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour $d|n$ et $d < n$. Alors $p \equiv 1[n]$.*

Théorème 57 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

Développements

- Théorème de Sophie Germain (28) [FGN13a]
- Loi de réciprocité quadratique (47) [Ser13]
- Forme faible de la progression arithmétique de Dirichlet (56,57) [FGN13a]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[Ser13] J.-P. Serre. *Cours d'Arithmétique.* PUF

Cadre : A un anneau commutatif unitaire, $\mathbb{K}$ un corps.

I Notion de principalité

1) Idéaux

Définition 1. Un idéal I de A es un sous-groupe de $(A,+)$ tel que pour tout $i \in I$ et tout $a \in A$, $ai \in I$.

Définition 2. Un idéal I de A est dit principal s'il est monogène, i.e. engendré par un élément $x \in A$. On note $I = (x) = xA$.

Exemple 3. *Tout idéal de $\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}$ pour p premier est principal.*

Exemple 4. *Dans $\mathbb{Z}[X]$, $(2,X)$ n'est pas principal*

Définition 5. Un idéal I de A est dit premier si $A \neq I$ et pour tous $a,b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.

Proposition 6. *I est idéal premier si, et seulement si, A/I est intègre.*

Exemple 7. *L'idéal $n\mathbb{Z}$ de $\mathbb{Z}$ est premier ssi $n = 0$ ou n est premier.*

Définition 8. Un idéal I de A est dit maximal si $A \neq I$ et pour tout J idéal de A, $I \subset J \subset A \Rightarrow J = I$ ou $J = A$.

Proposition 9. *I est idéal maximal si, et seulement si, A/I est un corps.*

Exemple 10. *Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ pour p premier.*

Remarque 11. *Tout idéal maximal est premier. La réciproque est fausse. En effet, dans $\mathbb{Z}[X]$, (X) est premier, mais non maximal ($\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ est intègre mais ce n'est pas un corps).*

2) Anneaux principaux

Définition 12. Un anneau est dit principal s'il est intègre et si tous ses idéaux sont principaux.

Exemple 13. *L'anneau $\mathbb{Z}$ est principal, ainsi que $\mathbb{K}[X]$, mais pas $\mathbb{Z}[X]$. $\mathbb{Z}/n\mathbb{Z}$ est principal si, et seulement si, n est premier.*

Application 14. *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, et soit $u \in \mathcal{L}(E)$. On note ϕ_u l'évaluation en u. L'anneau $\mathbb{K}[X]$ étant principal, $\operatorname{Ker}\phi_u$ est monogène. On appelle polynôme minimal de u l'unique générateur unitaire de $\operatorname{Ker}\phi_u$.*

Application 15. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps, et soit $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Un même raisonnement avec l'évaluation des polynômes en α donne l'existence du polynôme minimal en α.*

Définition 16. Soit $p \in A$, p est dit irréductible si $p \notin A^\times$ et si $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Exemple 17. *Les irréductibles de $\mathbb{Z}$ sont les nombres premiers.*

Proposition 18. *Si A est principal, alors :*

$$p \text{ est irréductible} \Leftrightarrow (p) \text{ est premier} \Leftrightarrow (p) \text{ est maximal}$$

Proposition 19. *Si A est un corps, alors $A[X]$ est principal.*

3) Cas des anneaux euclidiens

Définition 20. Un stathme d'un anneau intègre est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que pour tous $a,b \in A \setminus \{0\}$, il existe $q,r \in A$ avec $a = bq + r$ et ($r = 0$ ou $\nu(r) < \nu(b)$).
Un anneau intègre possédant un stathme est dit euclidien.

Exemple 21. *$\mathbb{Z}$ muni de la valeur absolue est euclidien.*

Théorème 22. *Un anneau euclidien est principal.*

Proposition 23. *Soit $P \in A[X] \setminus \{0\}$ de coefficient dominant inversible, et $F \in A[X]$. Alors il existe $Q,R \in A[X]$ tels que $F = PQ + R$ et ($R = 0$ ou $\deg R < \deg P$).*

Corollaire 24. *Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est euclidien.*

Proposition 25. *A corps $\Leftrightarrow$ $A[X]$ euclidien $\Leftrightarrow$ $A[X]$ principal*

Exemple 26. *$\mathbb{Z}[i] = \{z = a + ib \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$ est un anneau euclidien.*

Lemme 27. *Soit A un anneau euclidien. Il existe $x \in A \setminus A^\times$ tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective.*

Exemple 28. *L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal et non-euclidien.*

II Arithmétique et anneaux principaux

1) Divisibilité

Définition 29. Soient $a, b \in A$. On dit que a divise b, noté $a|b$, s'il existe $c \in A$ tel que $b = ac$.

Remarque 30. $a|b \Leftrightarrow (b) \subseteq (a)$

Définition 31. a et b sont dits associés si $(a) = (b)$.

Proposition 32. *Si A est intègre, a et b sont associés si, et seulement si, il existe $u \in A^\times$ tel que $b = au$.*

Définition 33. On dit que a et b sont premiers entre eux, noté $a \wedge b = 1$, si $(d|a$ et $d|b) \Rightarrow d \in A^\times$.

Définition 34. $p \in A \setminus \{0\}$ est premier si $p \notin A^\times$ et si $p|ab \Rightarrow p|a$ ou $p|b$.

Définition 35. Si A est principal, pour $a, b \in A$, on pose :

(i) $\text{pgcd}(a, b)$ tout générateur de l'idéal $((a) \cup (b))$.

(ii) $\text{ppcm}(a, b)$ tout générateur de l'idéal $(a) \cap (b)$

On note $\text{pgcd}(a, b) = a \wedge b$ et $\text{ppcm}(a, b) = a \vee b$.

Exemple 36. *Dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2 + i\sqrt{5}$ n'ont pas de* ppcm*, et 9 et $6 + 3i\sqrt{5}$ n'ont pas de* pgcd*.*

Théorème 37 (Bézout)**.** *Soit A principal, alors pour tous $a, b \in A \setminus \{0\}$, il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = a \wedge b$.*

Lemme 38 (Gauss)**.** *Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.*

Lemme 39 (Euclide)**.** *Soit $p \in A$ irréductible, et soit $a, b \in A$, alors $p|ab \Rightarrow p|a$ ou $p|b$.*

Proposition 40. *Si A est principal, et $a, b, c, d \in A$, alors :*

(i) $(a|c$ *et* $b|c) \Leftrightarrow a \vee b|c$

(ii) $(d|a$ *et* $d|b) \Leftrightarrow d|a \wedge b$

Proposition 41. *Les éléments iréductibles d'un anneau principal sont exactement les éléments premiers.*

2) Factorialité

On suppose que A est intègre.

Définition 42. On appelle système de représentants des irréductibles de A un ensemble P d'irréductibles tel que tout irréductible de A admette un unique associé dans P.

Exemple 43. *Les nombres premiers sont un système de représentants des irréductibles de $\mathbb{Z}$.*

Définition 44. Un anneau A est dit factoriel si tout $a \in A \setminus \{0\}$ se décompose sous la forme $a = u \prod_{p \in P} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ presque tous nuls et P un système de représentants des irréductibles.

Exemple 45. *$\mathbb{Z}$ est factoriel, $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas.*

Proposition 46. *Tout anneau principal est factoriel.*

Proposition 47. *Dans un anneau factoriel, les* pgcd *et* ppcm *existent.*

3) Théorème des restes chinois

Lemme 48. *Soient I et J des idéaux de A tels que $A = (I, J)$. On a alors $A/(IJ) \cong A/I \times A/J$.*

Corollaire 49. *Soit A un anneau principal, et soient $a_1, \ldots, a_n \in A \setminus \{0\}$ non-inversibles et premiers entre eux deux à deux. Alors $A/(a_1 \ldots a_n)$ est isomorphe à $A/(a_1) \times \ldots \times A/(a_n)$.*

Application 50. $\begin{cases} x \equiv 2 \ [4] \\ x \equiv 3 \ [5] \\ x \equiv 1 \ [9] \end{cases} \Leftrightarrow x = 118 + 180k$ *pour* $k \in \mathbb{Z}$.

III Entiers de corps quadratiques

1) Généralités

Définition 51. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ et sans facteur carré, et soit $\sqrt{d}$ une racine carrée de d dans $\mathbb{C}$. $\mathbb{Q}[\sqrt{d}] = \left\{ a + b\sqrt{d} \,\middle|\, a, b \in \mathbb{Q} \right\}$ est un sous-corps de $\mathbb{C}$, appelé corps quadratique. On note $\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} \,\middle|\, a, b \in \mathbb{Z} \right\}$. C'est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$.

Définition 52. Soit $z = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. On définit :

(i) son conjugué par $\overline{z} = a - b\sqrt{d}$.

(ii) sa trace par $\mathrm{tr}(z) = z + \overline{z} = 2a$.

(iii) sa norme par $N(z) = z\overline{z} = a^2 - db^2$.

Définition 53. On dit que $z = a + b\sqrt{d}$ est un entier de $\mathbb{Q}[\sqrt{d}]$ si a et b sont des entiers. On note A_d l'ensemble des entiers de $\mathbb{Q}[\sqrt{d}]$.

Définition 54. z est entier si, et seulement si, $\mathrm{tr}(z)$ et $N(z)$ sont entiers.

Proposition 55. *A_d est un anneau intègre.*

Théorème 56. $A_d = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *si* $d \equiv 1[4]$.
$A_d = \mathbb{Z}[\sqrt{d}]$ *si* $d \equiv 2[4]$ *ou* $d \equiv 3[4]$.

2) L'anneau $\mathbb{Z}[i]$ des entiers de Gauss

Proposition 57. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Proposition 58. $\mathbb{Z}[i]$ *est un anneau euclidien.*

Définition 59. On note $\Sigma = \left\{n = a^2 + b^2 \,\middle|\, a, b \in \mathbb{N}\right\}$.

Lemme 60. *Soit p premier impair. Alors $p \in \Sigma$ si, et seulement si, p est réductible dans $\mathbb{Z}[i]$.*

Lemme 61. Σ *est stable par multiplication.*

Théorème 62. *Soit p premier impair. Alors $p \in \Sigma$ ssi $p \equiv 1[4]$.*

Corollaire 63 (Théorème des deux carrés)**.** *Soit $n \in \mathbb{N}*$. On le décompose en produit de facteurs premiers : $n = \prod_{p\in\mathbb{P}} p^{v_p n}$. Alors :*

$$n \in \Sigma \Leftrightarrow (\forall p \in \mathbb{P}, p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2])$$

IV Irréductibilité des polynômes de $\mathbb{Z}[X]$

On suppose que A est factoriel. On considère $\mathbb{K} = \mathrm{Frac}(A)$.

Définition 64. Soit $P \in A[X]$ non nul. On appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. Si $c(P) = 1$, on dit que P est primitif.

Lemme 65. *Le produit de deux polynômes primitifs est primitif.*

Lemme 66. *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Théorème 67. *Soit $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

Théorème 68 (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_k sauf a_n et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{K}[X]$.*

Application 69. *Si p est premier, $\sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.*

Développements

— Théorème des deux carrés (57,58,60,61,62,63) [Per96]

— Critère d'Eisenstein (65,66,67,68) [FGN13a]

Références

[Com98] F. Combes. *Algèbre et géométrie.* Bréal
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Cadre : Sauf indication contraire, $\mathbb{k}$, $\mathbb{K}$ et $\mathbb{L}$ sont des corps. Tous les corps seront commutatifs, sauf dans le Théorème 35.

I Généralités sur les corps finis

1) Caractéristiques, sous-corps premier

Définition 1. Soit $\mathbb{K}$ un corps, on appelle sous-corps premier de $\mathbb{K}$ l'intersection de tous ses sous-corps non nuls.

Exemple 2. *Le sous-corps premier de $\mathbb{R}$ et $\mathbb{C}$ est $\mathbb{Q}$.*

Définition 3. Soit A un anneau unitaire, il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$. Le générateur positif de $\operatorname{Ker}\varphi$ est appelé caractéristique de A, notée $\operatorname{car}(A)$.

Proposition 4. *La caractéristique est soit nulle soit un nombre premier.*

Corollaire 5. *Si $\operatorname{car}(K) = 0$, $\mathbb{K}$ est infini, mais la réciproque est fausse.*

Théorème 6. *Soient $\mathbb{k} \subseteq \mathbb{K} \subseteq \mathbb{L}$ des extensions de corps. Alors $\mathbb{L}$ (resp. $\mathbb{K}$) est un espace vectoriel sur $\mathbb{K}$ (resp. $\mathbb{k}$). Si $(b_i)_{i\in I}$ est une $\mathbb{k}$-base de $\mathbb{K}$ et $(a_j)_{j\in J}$ est une $\mathbb{K}$-base de $\mathbb{L}$, alors $(a_j b_i)_{(i,j)\in I\times J}$ est une $\mathbb{k}$-base de $\mathbb{L}$.*

Corollaire 7. *Soit $\mathbb{k} \subseteq \mathbb{K}$ une extension finie. Alors $\mathbb{L} \cong \mathbb{K}^{[\mathbb{K}:\mathbb{k}]}$.*

Théorème 8. *Si $\mathbb{K}$ est un corps fini de caractéristique p, alors le sous-corps premier de $\mathbb{K}$ est $\mathbb{Z}/p\mathbb{Z}$. Ainsi $|\mathbb{K}|$ est une puissance de p.*

Exemple 9. *Il n'existe pas de corps de cardinal 57.*

Proposition 10. *Si $\operatorname{car}(\mathbb{K}) = p$, alors l'application $F : \mathbb{K} \to \mathbb{K}$ définie par $F(x) = x^p$ est un morphisme de corps, dit morphisme de Frobenius. Si $\mathbb{K}$ est fini, c'est un automorphisme, qui est l'identité si $\mathbb{K} = \mathbb{F}_q$.*

Corollaire 11 (Fermat)**.** *Soient $p \in \mathbb{Z}$ premier et $a \in \mathbb{Z}$, alors $a^p \equiv a\ [p]$.*

2) Existence et unicité des corps finis

Définition 12. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si P est scindé sur $\mathbb{L}[X]$, et si $\mathbb{L}$ est minimal pour cette propriété.

Théorème 13. *Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^\star$. Il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près.*

Théorème 14. *Soit p un nombre premier et soit $n \in \mathbb{N}^\star$. On pose $q = p^n$.*

(i) Il existe un corps $\mathbb{K}$ à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$.

(ii) De plus, $\mathbb{K}$ est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Proposition 15. *Soient $m, n \in \mathbb{N}^\star$, alors $(\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}) \Leftrightarrow n \mid m$.*

Exemple 16. *Les sous-corps de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$ et $\mathbb{F}_{16}$.*

3) Structure de $\mathbb{F}_q^\times$

Théorème 17. *Tout sous-groupe fini de $\mathbb{K}^\star$ est cyclique. En particulier, le groupe $\mathbb{F}_p^\times$ est cyclique.*

Remarque 18. *On ne sait pas en général trouver un générateur de $\mathbb{F}_q^\times$.*

Exemple 19. *$\mathbb{F}_8^\times \cong \mathbb{Z}/7\mathbb{Z}$, tout élément non neutre de $\mathbb{F}_8^\times$ est générateur.*

Théorème 20. *On considère l'extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$. Il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} \cong \mathbb{F}_q(\alpha)$.*

II Polynômes sur un corps fini

1) Polynômes irréductibles

Théorème 21. *Soient $\mathbb{F}_p \subset \mathbb{K}$ une extension finie de degré $n \geqslant 1$ et $\xi \in \mathbb{K}$. Les assertions suivantes sont équivalentes :*

(i) $\mathbb{K} = \mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$

(ii) $(1, \xi, \xi^2, \ldots, \xi^{n-1})$ *est une base du $\mathbb{F}_p$-espace vectoriel $\mathbb{K}$.*

(iii) $(1, \xi, \xi^2, \ldots, \xi^{n-1})$ *est une famille libre sur $\mathbb{F}_p$.*

(iv) Le polynôme minimal de ξ sur $\mathbb{K}$ est de degré n.

Proposition 22. *Soient p premier, $n \in \mathbb{N}^\star$ et $q = p^n$. Soit $P \in \mathbb{F}_p[X]$ unitaire et irréductible de degré n. Alors $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_q$.*

Corollaire 23. *Soient p premier, $n \in \mathbb{N}^\star$ et $P \in \mathbb{F}_p[X]$ de degré n.*

(i) Il existe des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p[X]$.

(ii) Si P est unitaire et irréductible, $\mathbb{F}_{p^n}$ est un corps de rupture de P.

(iii) Si P est unitaire et irréductible, P divise $X^{p^n} - X$.

Lemme 24. *Soient $d, n \in \mathbb{N}^\star$ et $q = p^n$. Soit $P \in \mathbb{F}_p[X]$ unitaire et irréductible de degré d. Si P divise $X^q - X$, alors d divise n.*

Théorème 25. *Soient p premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Proposition 26 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall\, n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Corollaire 27. *Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

$$I(q,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{+\infty}{\sim} \frac{q^n}{n}$$

2) Cyclotomie

Définition 28. On pose $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \,|\, \zeta^n = 1\}$ le groupe des racines n-ièmes de l'unité.

Proposition 29. *Tout sous-groupe de $\mathbb{K}^\star$ est cyclique.*

Définition 30. On pose $\mathbb{K}_n$ un corps de décomposition de $X^n - 1 \in \mathbb{K}[X]$. Le groupe $\mu_n(\mathbb{K})$ est cyclique d'ordre n. On note $\mu_n^\star(\mathbb{K})$ l'ensemble des générateurs de $\mu_n(\mathbb{K})$, ses éléments sont les racines primitives n-ièmes de l'unité.

Remarque 31. $|\mu_n^\star(\mathbb{K}_n)| = \varphi(n)$

Définition 32. On définit le n-ième polynôme cyclotomique par :

$$\Phi_{n,\mathbb{K}} = \prod_{\zeta \in \mu_n^\star(\mathbb{K}_n)} (X - \zeta) \in \mathbb{K}[X]$$

Proposition 33. $X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{K}}$

Proposition 34. *On a $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$. De plus, pour $\sigma : \mathbb{Z} \to \mathbb{K}$ le morphisme canonique, on a $\Phi_{n,\mathbb{K}}(X) = \sigma(\Phi_{n,\mathbb{Q}}(X))$. En particulier, $\Phi_{n,\mathbb{F}_p}$ s'obtient à partir de $\Phi_{n,\mathbb{Q}}$ par réduction modulo p.*

Théorème 35 (Wedderburn)**.** *Tout corps fini est commutatif.*

III Applications

1) Irréductibilité des polynômes de $\mathbb{Z}[X]$

Proposition 36. *Soient $P, Q \in \mathbb{F}_p[X]$. Alors :*

$$(P+Q)^p = P^p + Q^p \quad et \quad (P(X))^p = P(X^p)$$

Définition 37. On définit le contenu de $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$ par $c(P) = \mathrm{pgcd}(a_0, \ldots, a_n)$. Un polynôme P est dit primitif si $c(P) = 1$.

Proposition 38. *Soient $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.*

Proposition 39. *Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :*

(i) Les polynômes constants, irréductibles dans $\mathbb{Z}$ (premiers).

(ii) Les polynômes non constants, primitifs et irréductibles dans $\mathbb{Q}[X]$.

Théorème 40 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$. Soit un nombre premier p tel que $p \nmid a_n$, $\forall i < n, p | a_i$ et $p^2 \nmid a_0$. Alors P est irréductible dans $\mathbb{Z}[X]$.*

Application 41. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

2) Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 42. On pose $(\mathbb{F}_q)^2 = \left\{x^2 \in \mathbb{F}_q \,\middle|\, x \in \mathbb{F}_q\right\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{\star 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$.

Proposition 43. *Si $q = p^n$, on a :*

(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

(ii) Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\star 2}| = \frac{q-1}{2}$

Proposition 44. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 45. *Si $q = p^n$ et $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, q est congru à 1 modulo 4.*

Corollaire 46. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 47. Soit p un premier impair et $a \in \mathbb{N}$. On définit le symbole de Legendre de a par p par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si \quad \overline{a} \in \mathbb{F}_p^{\star 2} \\ -1 & si \quad \overline{a} \notin \mathbb{F}_p^{\star 2} \\ 0 & si \quad \overline{a} = 0 \end{cases}$$

Proposition 48. *Pour $x, y \in \mathbb{F}_p^\star$, on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.*
Le symbole de Legendre donne un morphisme $\mathbb{F}_q^\star \to \{\pm 1\}$.

Proposition 49. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$*

Théorème 50 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$.*

Proposition 51. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 52. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 53. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

Développements

- Polynômes irréductibles unitaires sur $\mathbb{F}_q$ (25,26,27) [Tau08]
- Étude des polynômes cyclotomiques (41) [Per96]
- Loi de réciprocité quadratique (50) [Ser13]

Références

[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses
[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois*. Calvage et Mounet
[Ser13] J.-P. Serre. *Cours d'Arithmétique*. PUF

Cadre : Sauf indication contraire, $\mathbb{k}$, $\mathbb{K}$ et $\mathbb{L}$ sont des corps.

I Extensions de corps

1) Définitions et premières propriétés

Définition 1. Soit $\mathbb{K}$ un corps. On appelle extension de $\mathbb{K}$ un corps $\mathbb{L}$ tel qu'il existe un morphisme de corps $\mathbb{K} \to \mathbb{L}$.

Exemple 2. *On a la tour d'extensions* $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Remarque 3. *Tout morphisme de corps est injectif. Quitte à identifier* $\mathbb{K}$ *et son image dans* $\mathbb{L}$*, on peut supposer que* $\mathbb{K}$ *est un sous-corps de* $\mathbb{L}$.

Définition 4. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. Alors $\mathbb{L}$ est muni d'une structure de $\mathbb{K}$-espace vectoriel. Sa dimension est appelée degré de $\mathbb{L}$ sur $\mathbb{K}$, notée $[\mathbb{L} : \mathbb{K}]$.

Exemple 5. $[\mathbb{C} : \mathbb{R}] = 2$ *et* $[\mathbb{R} : \mathbb{Q}] = \infty$.

Définition 6. Soit $\mathbb{K}$ un corps. Il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$. Le générateur positif de $\operatorname{Ker}\varphi$ est appelé caractéristique de A, notée $\operatorname{car}(A)$.

Proposition 7. *Soit* $\mathbb{K}$ *un corps, et soit* $p = \operatorname{car}(\mathbb{K})$.

(i) Si $p = 0$*, alors* $\mathbb{K}$ *est une extension de* $\mathbb{Q}$.

(ii) Si $p \neq 0$*, alors* p *est premier et* $\mathbb{K}$ *est une extension de* $\mathbb{Z}/p\mathbb{Z}$.

Exemple 8. *Si* $\operatorname{car}(\mathbb{K}) = 0$*,* $\mathbb{Q}$ *est le plus petit sous-corps de* $\mathbb{K}$*. Si* $\operatorname{car}(\mathbb{K}) \neq 0$*, c'est* $\mathbb{Z}/p\mathbb{Z}$.

Théorème 9 (Base téléscopique)**.** *Soit* $\mathbb{k} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *une tour d'extension. Soient* $(\alpha_j)_{j\in J}$ *une* $\mathbb{K}$*-base de* $\mathbb{L}$ *et* $(\beta_i)_{i\in I}$ *une* $\mathbb{k}$*-base de* $\mathbb{K}$*. Alors* $(\alpha_j\beta_i)_{(i,j)\in I\times J}$ *forme une* $\mathbb{k}$*-base de* $\mathbb{L}$.

Corollaire 10 (Extensions emboîtées)**.** *Soit* $\mathbb{k} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *une tour d'extension, où* $\mathbb{k}$*,* $\mathbb{K}$ *et* $\mathbb{L}$ *sont finis. Alors* $[\mathbb{L} : \mathbb{K}]\,[\mathbb{K} : \mathbb{k}] = [\mathbb{L} : \mathbb{k}]$.

Remarque 11. *On a* $[\mathbb{K} : \mathbb{k}] = 1$ *si, et seulement si,* $\mathbb{K} = \mathbb{k}$.

2) Extensions algébriques

Définition 12. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit S une partie de $\mathbb{L}$. Le plus petit sous-corps de $\mathbb{L}$ contenant S est noté $\mathbb{K}(S)$ et est appelé sous-corps de $\mathbb{L}$ engendré par S dans $\mathbb{K}$. Si $S = \{\alpha_1, \ldots, \alpha_n\}$, on notera $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$.

Définition 13. Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$. On considère l'application $\varphi : \mathbb{K}[X] \to \mathbb{L}$ définie par $\varphi|_{\mathbb{K}} = Id_{\mathbb{K}}$ et $\varphi(X) = \alpha$.

(i) S'il existe $P \in \mathbb{K}[X]$ tel que $P(\alpha) = 0$, on dit que α est algébrique.

(ii) Sinon, φ est injective, et on dit que α est transcendant sur $\mathbb{K}$.

Exemple 14. $\sqrt{2}$ *et* $e^{\frac{2i\pi}{n}}$ *sont algébriques sur* $\mathbb{Q}$*,* e *et* π *y sont algébriques.*

Définition 15. Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ et $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. L'ensemble des polynômes de $\mathbb{K}[X]$ qui annulent α est un idéal non nul de $\mathbb{K}[X]$. On appelle polynôme minimal de α sur $\mathbb{K}$, noté π_α, l'unique polynôme unitaire non nul qui engendre cet idéal.

Théorème 16. *Soient* $\mathbb{L}$ *une extension d'un corps* $\mathbb{K}$ *et* $\alpha \in \mathbb{L}$*. Alors :*

(i) Si α *est algébrique sur* $\mathbb{K}$*, alors* $\mathbb{K}(\alpha) \cong \mathbb{K}[X]/(\pi_\alpha)$.

(ii) Si α *est transcendant sur* $\mathbb{K}$*, alors* $\mathbb{K}(\alpha) \cong \mathbb{K}[X]$.

Corollaire 17. *Soient* $\mathbb{L}$ *une extension d'un corps* $\mathbb{K}$ *et* $\alpha \in \mathbb{L}$*. Alors* α *est algébrique sur* $\mathbb{K}$ *si, et seulement si,* $[\mathbb{K}(\alpha) : \mathbb{K}]$ *est fini. Dans ce cas, on a* $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg \pi_\alpha$.

Définition 18. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. On dit qu'elle est finie si son degré est fini. On dit qu'elle est algébrique si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Proposition 19. *Toute extension finie est algébrique.*

Théorème 20. *Soit* $\mathbb{k} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *des extensions. Alors* $\mathbb{k} \subseteq \mathbb{L}$ *est algébrique si, et seulement si,* $\mathbb{K} \subseteq \mathbb{L}$ *et* $\mathbb{k} \subseteq \mathbb{K}$ *sont algébriques.*

Définition 21. Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. On appelle fermeture algébrique, notée $\overline{\mathbb{K}}$, le sous-corps de $\mathbb{L}$ des éléments algébriques sur $\mathbb{K}$. C'est une extension algébrique sur $\mathbb{K}$.

II Corps de rupture, de décomposition

1) Corps de rupture

Définition 22. Soit $P \in \mathbb{K}[X]$ irréductible. Une extension monogène $\mathbb{L}$ de $\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si elle est engendré par $\mathbb{K}$ et par une racine α de P.

Remarque 23. *$\mathbb{L}$ est alors une extension de $\mathbb{K}$ de degré le degré de P.*

Exemple 24. *Si P est de degré 1, $\mathbb{K}$ est un corps de rupture de P.*

Théorème 25. *Tout polynôme irréductible sur $\mathbb{K}$ admet un corps de rupture, qui est unique à $\mathbb{K}$-isomorphisme près.*

Exemple 26. *$\mathbb{C}$ est le corps de rupture de X^2+1 sur $\mathbb{R}$.*

Exemple 27. *Le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$ a 4 éléments.*

Corollaire 28. *Pour tout polynôme sur $\mathbb{K}$, il existe une extension de $\mathbb{K}$ dans laquelle il admet au moins une racine.*

2) Corps de décomposition

Définition 29. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si P est scindé sur $\mathbb{L}[X]$, et si $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$ avec $\alpha_k \in \mathbb{L}$ des racines de P.

Remarque 30. *Un corps de décomposition est une extension finie.*

Exemple 31. *$\mathbb{Q}[\sqrt{2}]$ est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.*

Théorème 32. *Soit $P \in \mathbb{K}[X]$ non constant. Alors P admet un corps de décomposition, unique à isomorphisme près, de degré au plus* $(\deg P)!$.

Exemple 33. *$\mathbb{Q}[\sqrt[3]{2}]$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$, mais ce n'est pas un corps de décomposition.*

Théorème 34. *Soit $\mathbb{K}$ un corps de caractéristique nulle, et soit $P \in \mathbb{K}[X]$ irréductible. Si $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$, alors P est à racines simples dans $\mathbb{L}$.*

Théorème 35 (Élément primitif en caractéristique nulle)**.** *Toute extension finie d'un corps de caractéristique nulle est monogène.*

Application 36. *Soient p, q premiers. Alors $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p}+\sqrt{q})$.*

Exemple 37. *$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est une extension de degré 4 de $\mathbb{Q}$ engendrée par $\sqrt{2}+\sqrt{3}$.*

III Corps finis

Proposition 38. *Soit $\mathbb{K}$ un corps fini de caractéristique p non nulle. Alors il existe $n \in \mathbb{N}^\star$ tel que $|\mathbb{K}| = p^n$.*

Définition 39. Soient p premier, $n \in \mathbb{N}^\star$ et $q = p^n$. Le corps de décomposition de $X^q - X$ est de cardinal q. On note $\mathbb{F}_q$ ce corps.

Proposition 40. *Soient p premier et $d, n \in \mathbb{N}^\star$. Alors $\mathbb{F}_{p^n}$ est une extension de $\mathbb{F}_{p^d}$ si, et seulement si, d divise n.*

Théorème 41. *Le groupe multiplicatif $\mathbb{F}_q^\times$ est cyclique.*

Corollaire 42. *Soit $\mathbb{F}_{q^n}$ une extension de $\mathbb{F}_q$, alors il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. En particulier, pour $n \in \mathbb{N}^\star$, il existe un polynôme irréductible dans $\mathbb{F}_q[X]$ de degré d.*

IV Applications

1) Polynômes cyclotomiques

Définition 43. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 44. *Pour $n \in \mathbb{N}^\star$, Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 45. *Pour $n \in \mathbb{N}^\star$, $X^n - 1 = \prod_{d|n} \Phi_d(n)$*

Exemple 46. $\Phi_1(X) = X-1$, $\Phi_2(X) = X+1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Lemme 47. *Soient $A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P = AB \in \mathbb{Z}[X]$. Si A et P sont unitaires, alors A et B sont à coefficients entiers.*

Proposition 48. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 49. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

2) Polynômes irréductibles

Théorème 50. *Soient $\mathbb{F}_p \subset \mathbb{K}$ une extension finie de degré $n \geqslant 1$ et $\xi \in \mathbb{K}$. Les assertions suivantes sont équivalentes :*

(i) $\mathbb{K} = \mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$

(ii) $(1, \xi, \xi^2, \dots, \xi^{n-1})$ *est une base du $\mathbb{F}_p$-espace vectoriel $\mathbb{K}$.*

(iii) $(1, \xi, \xi^2, \dots, \xi^{n-1})$ *est une famille libre sur $\mathbb{F}_p$.*

(iv) Le polynôme minimal de ξ sur $\mathbb{K}$ est de degré n.

Proposition 51. *Soient p premier, $n \in \mathbb{N}^\star$ et $q = p^n$. Soit $P \in \mathbb{F}_p[X]$ unitaire et irréductible de degré n. Alors $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_q$.*

Corollaire 52. *Soient p premier, $n \in \mathbb{N}^\star$ et $P \in \mathbb{F}_p[X]$ de degré n.*

(i) Il existe des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p[X]$.

(ii) Si P est unitaire et irréductible, $\mathbb{F}_{p^n}$ est un corps de rupture de P.

(iii) Si P est unitaire et irréductible, P divise $X^{p^n} - X$.

Lemme 53. *Soient $d, n \in \mathbb{N}^\star$ et $q = p^n$. Soit $P \in \mathbb{F}_p[X]$ unitaire et irréductible de degré d. Si P divise $X^q - X$, alors d divise n.*

Théorème 54. *Soient p premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Proposition 55 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall\, n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Corollaire 56. *Si $I(q, d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

$$I(q, n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{+\infty}{\sim} \frac{q^n}{n}$$

3) Nombres constructibles

Définition 57. Soient $A \subset \mathbb{R}^2$ et $M \in \mathbb{R}^2$. On dit que M est constructible en un pas à partir de A s'il existe deux éléments distincts, droites ou cercles, tels que M est un point d'intersection de ces éléments.

Définition 58. Soit $M \in \mathbb{R}^2$. On dit que M est constructible s'il existe $A_0 \subset A_1 \subset \dots \subset A_n$ des parties de $\mathbb{R}^2$, avec $A_0 = \{(0,0), (1,0)\}$, $M \in A_n$ et $A_i = A_{i-1} \cup \{M_i\}$ où M_i est constructible en un pas à partir de A_{i-1}.

Définition 59. Un réel x est dit constructible si $(x, 0)$ est constructible.

Proposition 60. *Tout rationnel est constructible.*

Proposition 61. *Si $x > 0$ est constructible, alors $\sqrt{x}$ est constructible.*

Théorème 62. *Soit $x \in \mathbb{R}$ constructible. Alors x est algébrique sur $\mathbb{Q}$, et $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2.*

Application 63. *La duplication du cube, la trisection de l'angle et la quadrature du cercle sont impossibles à la règle et au compas. Autrement dit, $\sqrt[3]{2}$, $\sqrt{\pi}$ et $\cos\left(\frac{\pi}{9}\right)$ ne sont pas constructibles.*

Développements

— Étude des polynômes cyclotomiques (48,49) [Per96]

— Polynômes irréductibles unitaires sur $\mathbb{F}_q$ (54,55,56) [Tau08]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet

Définition 1. Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$. On appelle équation diophantienne toute équation de la forme $P(x_1, \dots, x_n) = 0$, dont on cherche les solutions sur $\mathbb{Z}^n$.

I Équations diophantiennes linéaires

1) Arithmétique dans $\mathbb{Z}$

Proposition 2. *Soient $a, b \in \mathbb{Z}$ non nuls simultanément. L'équation $ax = b$ possède une unique solution si, et seulement si $a \mid b$. Dans ce cas, cette unique solution est $x = \frac{b}{a} \in \mathbb{Z}$.*

Proposition 3 (Bézout)**.** *Soient $a_1, \dots, a_n \in \mathbb{Z}$ et $d = \text{pgcd}(a_1, \dots, a_n)$. Alors il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que $a_1u_1 + \dots + a_nu_n = d$.*

Définition 4. Soient $a_1, \dots, a_n \in \mathbb{Z}$. On dit que $a_1, \dots, a_n$ sont premiers entre eux si $\text{pgcd}(a_1, \dots, a_n) = 1$.

Théorème 5 (Bézout)**.** *$a_1, \dots, a_n \in \mathbb{Z}$ sont premiers entre eux si, et seulement si, il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que $a_1u_1 + \dots + a_nu_n = 1$.*

Lemme 6 (Gauss)**.** *Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.*

Lemme 7 (Euclide)**.** *Soit p premier. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.*

2) Équations diophantiennes de degré 1

On s'intéresse à l'équation de la forme $ax + by = c$, avec $a, b, c \in \mathbb{Z}$.

Méthode 8. *On effectue l'algorithme d'Euclide pour trouver le* pgcd *de a et b, noté d. En remontant les étapes de l'algorithme, trouver une solution de $au' + bv' = d$ puis de $au + bv = c$. Si (x_0, y_0) est une solution générale, on obtient $a(x - u_0) = b(v - y_0)$ et par le lemme de Gauss, $a \mid v - y_0$ et $b \mid u - x_0$, donc $v = y_0 + ak$ et $u = x_0 - bk$.*

Théorème 9. *Soient $a, b \in \mathbb{Z}$. L'équation $ax + by = c$ admet des solutions si, et seulement si, $d = \text{pgcd}(a, b) \mid c$. Dans ce cas, soit (x_0, y_0) une solution particulière donnée par l'identité de Bézout. L'ensemble des solutions est donné par :*

$$\left\{ \left(x_0 + k \times \frac{b}{d}, y_0 - k \times \frac{a}{d} \right) \middle| \, k \in \mathbb{Z} \right\}$$

Exemple 10. *(i) $42x + 66y = 10$ n'admet pas de solutions.*
(ii) $112x + 70y = 14$ a pour solutions les $(2 + 5k, -3 - 8k)$ pour $k \in \mathbb{Z}$.

Proposition 11. *L'équation $a_1x_1 + \dots + a_nx_n = b$ admet une solution si, et seulement si,* $\text{pgcd}(a_1, \dots, a_n) \mid b$.

II Équations modulaires

On fixe $n \geqslant 2$ et p premier. On travaille par défaut dans $\mathbb{Z}/n\mathbb{Z}$.

1) Systèmes de congruences

Méthode 12. *Pour résoudre l'équation $ax \equiv b\,[n]$, on peut résoudre dans $\mathbb{Z}$ l'équation $ax = b + kn, k \in \mathbb{Z}$, reformulée en $ax - nk = b$. On retrouve alors une équation vue dans la première partie.*

Proposition 13. *L'équation $ax \equiv b\,[n]$ admet des solutions si, et seulement si,* $\text{pgcd}(a, b) \mid b$. *En particulier, $a \in \mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement si, $a \wedge n = 1$.*

Corollaire 14. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.*

Théorème 15 (Restes chinois)**.** *Soient $m_1, \dots, m_k$ des entiers premiers entre eux deux à deux, et $m = m_1 \dots m_k$. Alors l'application définie par :*

$$\Phi : \left| \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \\ \overline{n}^m & \longmapsto & (\overline{n}^{m_1}, \dots, \overline{n}^{m_k}) \end{array} \right.$$

est un isomorphisme d'anneaux.

Exemple 16. *Résolution de systèmes de congruences :*

$$\begin{cases} x & \equiv & 2 & [3] \\ x & \equiv & 4 & [5] \end{cases} \Leftrightarrow x = 14 + 15k,\ k \in \mathbb{Z}$$

2) Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 17. On pose $(\mathbb{F}_q)^2 = \left\{ x^2 \in \mathbb{F}_q \,\middle|\, x \in \mathbb{F}_q \right\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{\star 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$.

Proposition 18. *Si $q = p^n$, on a :*
(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$
(ii) Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\star 2}| = \frac{q-1}{2}$

Proposition 19. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 20. *Si $q = p^n$ et $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, q est congru à 1 modulo 4.*

Corollaire 21. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 22. Soit p un premier impair et $a \in \mathbb{N}$. On définit le symbole de Legendre de a par p par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si \ \overline{a} \in \mathbb{F}_p^{\star 2} \\ -1 & si \ \overline{a} \notin \mathbb{F}_p^{\star 2} \\ 0 & si \ \overline{a} = 0 \end{cases}$$

Proposition 23. *Pour $x, y \in \mathbb{F}_p^\star$, on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.*
Le symbole de Legendre donne un morphisme $\mathbb{F}_q^\star \to \{\pm 1\}$.

Proposition 24. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$*

Théorème 25 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$.*

Proposition 26. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 27. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 28. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

III Équations diophantiennes non linéaires

1) Premiers exemples

Méthode 29 (Descente infinie)**.**

(i) On suppose par l'absurde qu'il existe une solution non triviale.

(ii) On construit à partir de cette solution une autre solution plus petite.

(iii) Par récurrence, on obtient une suite décroissante infinie de solutions non triviales. Ce qui est impossible car toute suite décroissante de $\mathbb{N}$ est stationnaire.

Théorème 30. *L'équation $x^4+y^4+z^2$ n'as pas de solutions entières non triviales*

Théorème 31. *Soit (x, y, z) un triplet pythagoricien, c'est-à-dire solution de $x^2 + y^2 = z^2$. Il existe $d \in \mathbb{Z}$ et u, v premiers entre eux tels que, à permutation près, on a $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$.*

Théorème 32. *L'équation de Fermat $x^n + y^n = z^n$ n'a pas de solutions pour $n = 4$.*

Remarque 33. *Cette équation n'a en fait pas de solution non triviale pour tout $n \geqslant 3$. Conjecture de Pierre de Fermat, prouvée par Andrew Wiles en 1995.*

Théorème 34 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

2) Réduction modulaire

Méthode 35. *On peut réduire une équation à une équation modulaire dans $\mathbb{Z}/n\mathbb{Z}$ pour trouver (ou pas) une solution.*

Exemple 36. *La résolution de $x^2 + py = z$ nous ramène à la recherche d'une racine carrée de z modulo p.*

Exemple 37. *L'équation $x^3 + 5 = 117y^3$ n'a pas de solution.*

Exemple 38. *Les équations $x^3 + y^3 + z^3 = 4$ et $x^3 + y^3 + z^3 = 5$ n'ont pas de solutions entières.*

3) L'anneau $\mathbb{Z}[i]$ des entiers de Gauss

Définition 39. On définit $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss.

Proposition 40. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Proposition 41. $\mathbb{Z}[i]$ *est un anneau euclidien.*

Définition 42. On note $\Sigma = \left\{n = a^2 + b^2 \,\middle|\, a, b \in \mathbb{N}\right\}$.

Lemme 43. *Soit p premier impair. Alors $p \in \Sigma$ si, et seulement si, p est réductible dans $\mathbb{Z}[i]$.*

Lemme 44. Σ *est stable par multiplication.*

Théorème 45. *Soit p premier impair. Alors $p \in \Sigma$ ssi $p \equiv 1[4]$.*

Corollaire 46 (Théorème des deux carrés)**.** *Soit $n \in \mathbb{N}*$. On le décompose en produit de facteurs premiers : $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$. Alors :*

$$n \in \Sigma \Leftrightarrow (\forall p \in \mathbb{P}, p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2])$$

Développements

— Théorème des deux carrés (40,41,43,44,45,46) [Per96]
— Loi de réciprocité quadratique (25) [Ser13]
— Théorème de Sophie Germain (34) [FGN13a]

Références

[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie*. DeBoeck
[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses
[Ser13] J.-P. Serre. *Cours d'Arithmétique*. PUF
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1*. Cassini

Cadre : A est un anneau commutatif unitaire intègre, et $\mathbb{K}$ un corps.

I Polynômes irréductibles

1) Définition et premières propriétés

Définition 1. Soit $P \in A[X]$. On dit que P est irréductible sur $A[X]$ lorsque P n'est ni nul ni inversible et si $P = QR$, avec $Q, R \in A[X]$, implique que soit Q soit R est inversible.

Remarque 2. *On a $A[X]^\times = A^\times$.*

Proposition 3. *On se place dans $\mathbb{K}[X]$, alors :*

(i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré 2 ou plus n'a pas de racine dans $\mathbb{K}$.

Remarque 4. *$(X^2+1)^2$ est de degré 4 et n'a pas de racine dans $\mathbb{R}$ mais, n'est pas irréductible sur $\mathbb{R}$.*

Proposition 5. *Tout polynôme sur $\mathbb{K}$ de degré 2 ou 3 qui n'admet pas de racine dans $\mathbb{K}$ est irréductible.*

Proposition 6. *L'anneau $A[X]$ est principal si, et seulement si, il est euclidien et si, et seulement si A est un corps.*

Corollaire 7. *$P \in \mathbb{K}[X]$ est irréductible si, et seulement si, (P) est un idéal maximal.*

Exemple 8. *Dans $\mathbb{Z}[X]$, X^2+1 est irréductible, mais $\mathbb{Z}[X]/(X^2+1)$ est isomorphe à $\mathbb{Z}[i]$ qui n'est pas un corps.*

2) Factorialité

Définition 9. On appelle système de représentants des irréductibles de A un ensemble P d'irréductibles tel que tout irréductible de A admette un unique associé dans P.

Exemple 10. *Les nombres premiers sont un système de représentants des irréductibles de $\mathbb{Z}$.*

Définition 11. Un anneau A est dit factoriel si tout $a \in A \setminus \{0\}$ se décompose sous la forme $a = u \prod_{p \in P} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ presque tous nuls et P un système de représentants des irréductibles.

Exemple 12. *$\mathbb{Z}$ est factoriel, $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas.*

Proposition 13. *Tout anneau principal est factoriel.*

Théorème 14. *Si A est factoriel, alors $A[X]$ est factoriel.*

Théorème 15 (Lemme des noyaux)**.** *Soient $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

$$\operatorname{Ker} P(f) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(f)$$

3) Critère d'irréductibilité

On suppose que A est factoriel. On considère $\mathbb{K} = \operatorname{Frac}(A)$.

Définition 16. Soit $P \in A[X]$ non nul. On appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. Si $c(P) = 1$, on dit que P est primitif.

Lemme 17. *Le produit de deux polynômes primitifs est primitif.*

Lemme 18. *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Théorème 19. *Soit $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

Théorème 20 (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_k sauf a_n et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{K}[X]$.*

Application 21. *Si p est premier, $\sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.*

II Corps de rupture, de décomposition

1) Corps de rupture

Définition 22. Soit $P \in \mathbb{K}[X]$ irréductible. Une extension monogène $\mathbb{L}$ de $\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si elle est engendré par $\mathbb{K}$ et par une racine α de P.

Remarque 23. *$\mathbb{L}$ est alors une extension de $\mathbb{K}$ de degré le degré de P.*

Exemple 24. *Si P est de degré 1, $\mathbb{K}$ est un corps de rupture de P.*

Théorème 25. *Tout polynôme irréductible sur $\mathbb{K}$ admet un corps de rupture, qui est unique à $\mathbb{K}$-isomorphisme près.*

Exemple 26. $\mathbb{C}$ *est le corps de rupture de X^2+1 sur $\mathbb{R}$.*

Exemple 27. *Le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$ est un corps à 4 éléments.*

Corollaire 28. *Pour tout polynôme sur $\mathbb{K}$, il existe une extension de $\mathbb{K}$ dans laquelle il admet au moins une racine.*

Proposition 29. *Soit $P \in \mathbb{K}[X]$ de degré n. Alors P est irréductible sur $\mathbb{K}$ si, et seulement si, P n'a pas de racine dans les extensions $\mathbb{L}$ de $\mathbb{K}$ avec $[\mathbb{L}:\mathbb{K}] \leqslant \frac{n}{2}$.*

Remarque 30. *On retrouve le critère d'irréductibilité pour $n=2$ ou 3.*

Proposition 31. *Soit $P \in \mathbb{K}[X]$ irréductible non constant. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré premier avec le degré de P, alors P est irréductible dans $\mathbb{K}[X]$.*

2) Corps de décomposition

Définition 32. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si P est scindée sur $\mathbb{L}[X]$, et si $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$ avec $\alpha_k \in \mathbb{L}$ des racines de P.

Remarque 33. *Un corps de décomposition est une extension de degré fini.*

Exemple 34. $\mathbb{K}$ *est corps de décomposition de tout polynôme de degré 1.*

Exemple 35. $\mathbb{C}$ *est un corps de décomposition de tout polynôme réel irréductible de degré 2.*

Exemple 36. $\mathbb{Q}[\sqrt{2}]$ *est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.*

Théorème 37. *Soit $P \in \mathbb{K}[X]$ de degré $n \geqslant 1$. Alors il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près, de degré au plus $n!$.*

Exemple 38. $\mathbb{Q}[\sqrt[3]{2}]$ *est un corps de rupture de X^3-2 sur $\mathbb{Q}$, mais ce n'est pas un corps de décomposition.*

Théorème 39 (Élément primitif)**.** *Soit $\mathbb{L}$ une extension finie de $\mathbb{K}$. On suppose $\mathbb{K}$ de caractéristique nulle. Alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$.*

III Applications

1) Corps finis

Définition 40. Soit $\mathbb{K}$ un corps, on appelle sous-corps premier de $\mathbb{K}$ l'intersection de tous ses sous-corps non nuls.

Exemple 41. *Le sous-corps premier de $\mathbb{R}$ et $\mathbb{C}$ est $\mathbb{Q}$.*

Définition 42. Soit A un anneau unitaire, il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$. Le générateur positif de $\operatorname{Ker}\varphi$ est appelé caractéristique de A, notée $\operatorname{car}(A)$.

Proposition 43. *Si $A = \mathbb{K}$ est un corps, sa caractéristique est nulle ou est un nombre premier.*

Corollaire 44. *Si $\operatorname{car}(K) = 0$, alors $\mathbb{K}$ est infini, mais la réciproque est fausse.*

Théorème 45. *Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps, alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.*

Corollaire 46. *Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps avec $\mathbb{K}$ et $\mathbb{L}$ finis, alors $\mathbb{L} \cong \mathbb{K}^n$.*

Théorème 47. *Si $\mathbb{K}$ est un corps fini de caractéristique p, son sous-corps premier est $\mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathbb{K}$ a pour cardinal une puissance de p.*

Théorème 48. *À $\mathbb{F}_p$-isomorphisme près, il existe un unique corps de cardinal p^n, noté $\mathbb{F}_{p^n}$.*

2) Polynômes cyclotomiques

Définition 49. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 50. *Pour $n \in \mathbb{N}^\star$, Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 51. *Pour $n \in \mathbb{N}^\star$, $X^n - 1 = \prod_{d|n} \Phi_d(n)$*

Exemple 52. $\Phi_1(X) = X-1$, $\Phi_2(X) = X+1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Lemme 53. *Soient $A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P = AB \in \mathbb{Z}[X]$. Si A et P sont unitaires, alors A et B sont à coefficients entiers.*

Proposition 54. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 55. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

Développements

— Critère d'Eisenstein (17,18,19,20) [FGN13a]
— Étude des polynômes cyclotomiques (54,55) [Per96]

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Cadre : On considère $\mathbb{K}$ un corps commutatif et $(A, +, \times)$ un anneau unitaire commutatif intègre.

I Anneau factoriel : pgcd et ppcm

1) Notion de divisibilité

Définition 1. Soient $a, b \in A$. On dit que a divise b, noté $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. C'est équivalent à dire que $(b) \subseteq (a)$.

Définition 2. Soient $a, b \in A$. On dit que a et b sont associés si $a \mid b$ et $b \mid a$. C'est équivalent à dire que $(a) = (b)$.

Remarque 3. *C'est une relation d'équivalence. Deux éléments associés sont indiscernables du point de vue de la divisibilité.*

Proposition 4. *Soient $a, b \in A$. Alors a et b sont associés si, et seulement si, il existe $u \in A^\times$ tel que $b = au$.*

Définition 5. Soit $a \in A$ non inversible et non nul. On dit que a est irréductible si, pour tous $b, c \in A$ tels que $a = bc$, on a $b \in A^\times$ ou $c \in A^\times$.

Exemple 6. *Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.*

Définition 7. $p \in A \setminus \{0\}$ est premier si $p \notin A^\times$ et, pour tous $a, b \in A$, $p \mid ab \Rightarrow (p \mid a$ ou $p \mid b)$.

2) Notions de pgcd et de ppcm

Définition 8. Soient $a, b \in A$. Pour $d \in A$ et $m \in A$, on dit que :

(i) d est pgcd de a et b, noté $d = a \wedge b$, si : $\forall c \in A, (c|a$ et $c|b) \Rightarrow c|d$.

(ii) m est ppcm de a et b, noté $m = a \vee b$, si : $\forall c \in A, (a|c$ et $b|c) \Rightarrow m|c$.

On dit que a et b sont premiers entre eux si $a \wedge b \in A^\times$.

Remarque 9. *L'existence de* pgcd *et* ppcm *n'est pas garantie en général. S'ils existent, ils sont définis à un inversible près. On peut généraliser à une famille quelconque d'éléments.*

Proposition 10. *Deux* pgcd *(ou* ppcm*) sont associés.*

Définition 11. On appelle système de représentants des irréductibles de A un ensemble P d'irréductibles tel que tout irréductible de A admette un unique associé dans P.

Exemple 12. *Les nombres premiers sont un système de représentants des irréductibles de $\mathbb{Z}$.*

Définition 13. Un anneau A est dit factoriel si tout $a \in A\setminus\{0\}$ se décompose sous la forme $a = u\prod_{p\in P} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ presque tous nuls et P un système de représentants des irréductibles de façon unique à l'ordre des irréductibles près.

Exemple 14. *$\mathbb{Z}$ est factoriel, $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas.*

On suppose maintenant que A est un anneau factoriel.

Proposition 15. *Dans un anneau factoriel, les* pgcd *et* ppcm *existent.*

Proposition 16. *Soient $a, b \in A$, et soient $a = u\prod_{p\in P} p^{v_p(a)}$ et $b = v\prod_{p\in P} p^{v_p(b)}$ leurs décompositions en produits d'irréductibles. Alors :*

(i) $a \wedge b = \prod_{p\in P} p^{\min(v_p(a),v_p(b))}$

(ii) $a \vee b = \prod_{p\in P} p^{\max(v_p(a),v_p(b))}$

Application 17. *Dans un groupe, il existe un élément d'ordre l'exposant du groupe.*

Lemme 18 (Gauss)**.** *Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.*

Lemme 19 (Euclide)**.** *Soit $p \in A$ irréductible, et soit $a, b \in A$, alors $p|ab \Rightarrow p|a$ ou $p|b$.*

Corollaire 20. *Un élément d'un anneau factoriel est premier si, et seulement si, il est irréductible.*

Proposition 21. *Pour $a, b \in A$, $(a\wedge b)(a\vee b) = ab$ et $a\wedge(b\vee a) = a\vee(b\wedge a)$.*

3) Contenu d'un polynôme

Définition 22. Soit $P \in A[X]$ non nul. On appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. Si $c(P) = 1$, on dit que P est primitif.

Lemme 23. *Le produit de deux polynômes primitifs est primitif.*

Lemme 24. *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Théorème 25. *Soit $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

Théorème 26 (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_k sauf a_n et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{K}[X]$.*

Application 27. *Si p est premier, $\sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.*

II Anneau principal : Théorème de Bézout

Définition 28. Un idéal I de A est dit principal s'il est monogène. Un anneau A est dit principal s'il est intègre et si ses idéaux sont principaux.

Exemple 29. *L'anneau $\mathbb{Z}$ est principal, ainsi que $\mathbb{K}[X]$, mais pas $\mathbb{Z}[X]$. $\mathbb{Z}/n\mathbb{Z}$ est principal si, et seulement si, n est premier.*

On suppose maintenant que A est un anneau principal.

Proposition 30. *Soient A principal et $a, b \in A$. Alors $a \wedge b$ est un générateur de $(a) + (b)$, et $a \vee n$ est un générateur de $(a) \cap (b)$.*

Théorème 31 (Bézout)**.** *Soit A principal. Alors, pour tous $a, b \in A \setminus \{0\}$, il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = a \wedge b$.*

Corollaire 32. *Soient A principal et $a, b \in A$. Alors, a et b sont premiers si, et seulement si, il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = e$.*

Remarque 33. *Ces propriétés se généralisent à une famille quelconque d'éléments.*

Application 34 (Lemme des noyaux)**.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. Soient $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

$$\operatorname{Ker} P(f) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(f)$$

Théorème 35. *Tout anneau principal est factoriel.*

III Anneau euclidien : Algorithmes

1) Obtention du pgcd

Définition 36. Un stathme est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que pour tous $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $\nu(r) < \nu(b)$). Un anneau intègre possédant un stathme est dit euclidien.

Exemple 37. *$\mathbb{Z}$ muni de la valeur absolue et $\mathbb{K}[X]$ muni du degré sont euclidien.*

Théorème 38. *Un anneau euclidien est principal.*

Exemple 39. *L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal et non-euclidien.*

Proposition 40. *Soit $P \in A[X] \setminus \{0\}$ de coefficient dominant inversible, et $F \in A[X]$. Alors il existe $Q, R \in A[X]$ tels que $F = PQ + R$ et ($R = 0$ ou $\deg R < \deg P$).*

Corollaire 41. *Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est euclidien.*

On suppose maintenant que A est un anneau euclidien.

Lemme 42. *Soient $a, b \in A$. Soient $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $\nu(r) < \nu(b)$). Si $r = 0$, alors $a \wedge b = b$, sinon, $a \wedge b = b \wedge r$.*

Méthode 43 (Algorithme d'Euclide)**.** *Grâce au lemme précédent, on peut réitérer un calcul de* pgcd *pour obtenir des éléments de stathme strictement plus petit. Ainsi, l'algorithme se termine par stricte décroissance du stathme dans $\mathbb{N}$, et on peut calculer le* pgcd *de deux éléments.*

Exemple 44. *On va calculer le* pgcd *de* 315 *et* 307 *dans $\mathbb{Z}$:*

$$\begin{aligned} 315 &= 1 \times 307 + 8 & \qquad 3 &= 2 \times 1 + 1 \\ 307 &= 8 \times 38 + 3 & \qquad 2 &= 2 \times 1 + 0 \\ 8 &= 2 \times 3 + 2 \end{aligned}$$

Ainsi, $315 \wedge 307 = 1$.

Exemple 45. *On va calculer le* pgcd *de $X^4 - 1$ et $X^3 - 1$:*

$$\begin{aligned} (X^4 - 1) &= (X^3 - 1) \times (X) + (X - 1) \\ (X^3 - 1) &= (X - 1) \times (X^2 + X + 1) \end{aligned}$$

Ainsi, $(X^4 - 1) \wedge (X^3 - 1) = X - 1$.

2) Recherche d'une relation de Bézout

Méthode 46 (Algorithme d'Euclide étendu)**.** *En remontant l'algorithme d'Euclide, on est capable de déterminer une relation de Bézout.*

Exemple 47. *Grâce au calcul de* $315 \wedge 307$*, on a :*

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (8 - 2 \times 3) \times 1 = 3 \times 3 - 8 \\ &= (307 - 8 \times 38) \times 3 - 8 = 307 \times 3 - 8 \times 115 \\ &= 307 \times 3 - (315 - 307) \times 115 = 307 \times 118 - 315 \times 115 \end{aligned}$$

IV Applications en arithmétique

1) Équations diophantiennes

Définition 48. Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$. On appelle équation diophantienne toute équation de la forme $P(x_1, \dots, x_n) = 0$, dont on cherche les solutions sur $\mathbb{Z}^n$.

Proposition 49. *Soient $a, b \in \mathbb{Z}$ non nuls simultanément. L'équation $ax = b$ possède une unique solution si, et seulement si $a \mid b$. Dans ce cas, cette unique solution est $x = \frac{b}{a} \in \mathbb{Z}$.*

On s'intéresse à l'équation de la forme $ax + by = c$, avec $a, b, c \in \mathbb{Z}$.

Méthode 50. *On effectue l'algorithme d'Euclide pour trouver le* pgcd *de a et b, noté d. En remontant les étapes de l'algorithme, trouver une solution de $au' + bv' = d$ puis de $au + bv = c$. Si (x_0, y_0) est une solution générale, on obtient $a(x - u_0) = b(v - y_0)$ et par le lemme de Gauss, $a \mid v - y_0$ et $b \mid u - x_0$, donc $v = y_0 + ak$ et $u = x_0 - bk$.*

Théorème 51. *Soient $a, b \in \mathbb{Z}$. L'équation $ax + by = c$ admet des solutions si, et seulement si, $d = \text{pgcd}(a, b) \mid c$. Dans ce cas, soit (x_0, y_0) une solution particulière donnée par l'identité de Bézout. L'ensemble des solutions est donné par :*

$$\left\{ \left(x_0 + k \times \frac{b}{d}, y_0 - k \times \frac{a}{d} \right) \middle| k \in \mathbb{Z} \right\}$$

Exemple 52. *(i)* $42x + 66y = 10$ *n'admet pas de solutions.*

(ii) $112x + 70y = 14$ *a pour solutions les* $(2 + 5k, -3 - 8k)$ *pour* $k \in \mathbb{Z}$.

Théorème 53 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

2) Systèmes de congruence

Théorème 54 (Restes chinois)**.** *Soit $n = m_1 m_2$ avec $m_1 \wedge m_2 = 1$. Alors l'application définie par :*

$$\Phi : \left| \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \\ \overline{n}^m & \longmapsto & (\overline{n}^{m_1}, \dots, \overline{n}^{m_k}) \end{array} \right.$$

est un isomorphisme d'anneaux.

Généralisation 55. *Le théorème des restes chinois se généralise à tout produit d'entiers premiers entre eux deux à deux.*

Exemple 56. *Résolution de systèmes de congruences :*

$$\begin{cases} x & \equiv & 1[3] \\ x & \equiv & 2[4] \\ x & \equiv & 0[5] \end{cases} \Leftrightarrow x = 10 + 60k,\ k \in \mathbb{Z}$$

Corollaire 57. *Soient $m, n \in \mathbb{N}$ premiers entre eux. On a alors $(\mathbb{Z}/nm\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, et donc $\varphi(nm) = \varphi(n)\varphi(m)$.*

Corollaire 58. *Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Alors :*

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/(p_1^{\alpha_1})\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/(p_k^{\alpha_k})\mathbb{Z})^\times$$

Développements

- Critère d'Eisenstein (23,24,25,26) [FGN13a]
- Théorème de Sophie Germain (53) [FGN13a]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses

[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck

[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Cadre : $\mathbb{K}$ est un corps commutatif

I Racines d'un polynôme

1) Définitions et premières propriétés

Définition 1. Pour $P \in \mathbb{K}[X]$, on dit que $a \in \mathbb{K}$ est racine de P si $(X-a)$ divise P dans $\mathbb{K}[X]$.

Exemple 2. *1 et -1 sont racines de* $X^2 - 1$.

Proposition 3. *Les racines de* $P \in \mathbb{K}[X]$ *dans* $\mathbb{K}$ *sont exactement les éléments* $a \in \mathbb{K}$ *tels que* $P(a) = 0$.

Exemple 4. *Les racines de* $X^n - 1$ *sont les racines n-ièmes de l'unité.*

Définition 5. On dit que $a \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$ d'ordre $k \in \mathbb{N}^\star$ si $(X-a)^k$ divise P et $(X-a)^{k+1}$ ne le divise pas.

Proposition 6. *Si* $P \in \mathbb{K}[X]$ *est de degré n, alors P a au plus n racines dans* $\mathbb{K}$.

Remarque 7. *Ceci est faux si* $\mathbb{K}$ *n'est qu'un anneau : Dans* $\mathcal{M}_2(\mathbb{R})$, X^2 *admet toutes les matrices de la forme* $\left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right)$ *comme racine, soit une infinité.*

Corollaire 8. *Si* $\mathbb{K}$ *est infini, il y a bijection entre les polynômes et les fonctions polynomiales associées.*

Théorème 9. *On suppose* $\mathbb{K}$ *de caractéristique nulle. Soit* $P \in \mathbb{K}[X]$ *non nul. Alors* $a \in \mathbb{K}$ *est racine d'ordre* $k \in \mathbb{N}^\star$ *de P si, et seulement si :*

$$\forall\, i \in [\![0, k-1]\!],\ P^{(i)}(a) = 0 \quad et \quad P^{(k)}(a) \neq 0$$

Remarque 10. *Le résultat précédent est vrai en caractéristique quelconque, mais seulement pour les racines simples.*

Corollaire 11. *Soient* $a_1, \dots, a_n \in \mathbb{K}$ *deux à deux distincts. L'application suivante est un isomorphisme d'espace vectoriel :*

$$\varphi : \left| \begin{array}{ccc} \mathbb{K}_{n-1}[X] & \longrightarrow & \mathbb{K}^n \\ P & \longmapsto & (P(a_i))_{i \in [\![1,n]\!]} \end{array} \right.$$

Remarque 12. *L'antécédent d'un n-uplet est le polynôme interpolateur de Lagrange associé à ce n-uplet.*

Définition 13. On dit que $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$ si on peut écrire :

$$P(X) = \lambda \prod_{i=1}^{r} (X - a_i)^{m_i} \quad \text{avec} \quad m_i \in \mathbb{N}^\star, a_i \in \mathbb{K}, \lambda \in \mathbb{K}$$

Remarque 14. *Deux polynômes scindés sont premiers entre eux si, et seulement si, ils n'ont aucune racine commune.*

Définition 15. Soit $P \in \mathbb{K}[X]$. On dit que P est irréductible sur $\mathbb{K}[X]$ lorsque P n'est pas constant et si $P = QR$, avec $Q, R \in \mathbb{K}[X]$, implique que soit Q soit R est constant.

Proposition 16. *On se place dans* $\mathbb{K}[X]$, *alors :*

(i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré 2 ou plus n'a pas de racine dans $\mathbb{K}$.

Remarque 17. $(X^2+1)^2$ *est de degré 4 et n'a pas de racine dans* $\mathbb{R}$ *mais, n'est pas irréductible sur* $\mathbb{R}$.

Théorème 18 (D'Alembert-Gauss)**.** *Tout polynôme non constant de* $\mathbb{C}[X]$ *admet une racine dans* $\mathbb{C}$.

Application 19. *Toute matrice à coefficients complexes est trigonalisable.*

Corollaire 20. *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré 1. Ceux de* $\mathbb{R}[X]$ *sont les polynômes de degré 1 et ceux de degré 2 sans racine.*

2) Corps de rupture, de décomposition

Définition 21. Soit $P \in \mathbb{K}[X]$ irréductible. Une extension monogène $\mathbb{L}$ de $\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si elle est engendré par $\mathbb{K}$ et par une racine α de P.

Remarque 22. $\mathbb{L}$ *est alors une extension de* $\mathbb{K}$ *de degré le degré de P.*

Exemple 23. *Si P est de degré 1,* $\mathbb{K}$ *est un corps de rupture de P.*

Théorème 24. *Tout polynôme irréductible sur* $\mathbb{K}$ *admet un corps de rupture, qui est unique à* $\mathbb{K}$*-isomorphisme près.*

Exemple 25. $\mathbb{C}$ *est le corps de rupture de* $X^2 + 1$ *sur* $\mathbb{R}$.

Exemple 26. *Le corps de rupture de X^2+X+1 sur $\mathbb{F}_2$ est un corps à 4 éléments.*

Corollaire 27. *Pour tout polynôme sur $\mathbb{K}$, il existe une extension de $\mathbb{K}$ dans laquelle il admet au moins une racine.*

Définition 28. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si P est scindée sur $\mathbb{L}[X]$, et si $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$ avec $\alpha_k \in \mathbb{L}$ des racines de P.

Remarque 29. *Un corps de décomposition est une extension finie.*

Exemple 30. $\mathbb{K}$ *est corps de décomposition de tout polynôme de degré 1.*

Exemple 31. $\mathbb{C}$ *est un corps de décomposition de tout polynôme réel irréductible de degré 2.*

Exemple 32. $\mathbb{Q}[\sqrt{2}]$ *est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.*

Théorème 33. *Soit $P \in \mathbb{K}[X]$ de degré $n \geqslant 1$. Alors il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près, de degré au plus $n!$.*

Exemple 34. $\mathbb{Q}[\sqrt[3]{2}]$ *est un corps de rupture de X^3-2 sur $\mathbb{Q}$, mais ce n'est pas un corps de décomposition.*

Théorème 35. *Soient p un nombre premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Proposition 36 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall\, n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Corollaire 37. *Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

$$I(q,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{+\infty}{\sim} \frac{q^n}{n}$$

II Fonctions symétriques élémentaires

Ici, A désigne un anneau commutatif unitaire intègre, et soit $n \in \mathbb{N}^\star$.

1) Définitions et premières propriétés

Définition 38. Le groupe symétrique $\mathfrak{S}_n$ agit sur $A[X_1, \dots, X_n]$ par :

$$\begin{array}{ccc} \mathfrak{S}_n \times A[X_1, \dots, X_n] & \longrightarrow & A[X_1, \dots, X_n] \\ (\sigma, P(X_1, \dots, X_n) & \longmapsto & P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \end{array}$$

Les points fixes sous cette action, notés $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$, sont appelés polynômes symétriques à n variables.

Exemple 39. *Tout polynôme à une variable est symétrique.*

Définition 40. Pour tous $n \in \mathbb{N}^\star$ et $k \in [\![0, n-1]\!]$, les polynômes suivants sont symétriques, et sont appelés polynômes symétriques élémentaires :

$$\Sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} X_{i_1} \dots X_{i_k}$$

Théorème 41. *Soit $P(X) = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ où $a_n \neq 0$. Dans un corps de décomposition de P, $P(X) = a_n(X-\alpha_0)\dots(X-\alpha_n)$. Alors :*

$$a_k = a_n (-1)^n \Sigma_{n-k+1}(\alpha_0, \dots, \alpha_n)$$

C'est une équivalence.

Application 42. *Le déterminant d'une matrice (resp. sa trace) est un coefficient de son polynôme caractéristique, produit (resp. somme) de ses valeurs propres dans une clôture algébrique.*

Proposition 43 (Formules de Newton)**.** *On pose $S_k = \sum_{i=1}^n X_i^k$, alors :*

(i) $\forall\, k \in [\![1, n]\!],\ \sum_{i=0}^k (-1)^i \Sigma_i S_{k-i} = 0$, *avec* $\Sigma_0 = 1$.

(ii) $\forall\, k \geqslant n,\ \sum_{i=0}^n (-1)^i \Sigma_i S_{k-i} = 0$

Application 44. *Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est nilpotente d'ordre n si, et seulement si, pour tout $k \in [\![1, n]\!]$, $\mathrm{tr}(A^k) = 0$.*

2) Structure des polynômes symétriques

Définition 45. Soit $X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in A[X_1, \dots, X_n]$ un monôme. On définit son poids comme $\sum_{k=1}^{n} k\alpha_k$. On appelle poids d'un polynôme $P \in A[X_1, \dots, X_n]$ le maximum des poids des monômes dont il est la somme. Par convention, on pose que le poids de 0 est $-\infty$.

Exemple 46. *Le poids de Σ_k est $nk - \frac{k(k-1)}{2}$.*

Théorème 47. *Soit $P \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$. Il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que $P = Q(\Sigma_1, \dots, \Sigma_n)$. Autrement dit, tout polynôme symétrique est polynôme en les polynômes symétriques élémentaires. De plus, le poids de Q est le degré de P.*

Exemple 48. *Dans $A[X, Y]$, $X^2 + Y^2 = (X + Y)^2 - 2XY$.*

III Applications

1) Polynômes cyclotomiques

Définition 49. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 50. *Pour $n \in \mathbb{N}^\star$, Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 51. *Pour $n \in \mathbb{N}^\star$, $X^n - 1 = \prod_{d|n} \Phi_d(n)$*

Exemple 52. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Lemme 53. *Soient $A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P = AB \in \mathbb{Z}[X]$. Si A et P sont unitaires, alors A et B sont à coefficients entiers.*

Proposition 54. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 55. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

2) Localisation des racines

Lemme 56. *Une matrice à coefficients complexes à diagonale dominante est inversible.*

Définition 57. Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{C})$. Le i-ième disque de Gerschgorin est le disque fermé de centre $a_{i,j}$ et de rayon $r_i = \sum_{j=1}^{n} \sum_{i \neq j} |a_{i,j}|$.

Théorème 58. *Les valeurs propres d'une matrice complexe sont situées dans la réunion des disques de Gerschgorin.*

Théorème 59 (Gauss-Lucas)**.** *Soit P un polynôme à coefficients complexes de degré au moins 2. Les racines de P' sont contenues dans l'enveloppe convexe de celles de P.*

Développements

- Étude des polynômes cyclotomiques (54,55) [Per96]
- Polynômes irréductibles unitaires sur $\mathbb{F}_q$ (35,36,37) [Tau08]

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet

Cadre : Soit $\mathbb{K}$ un corps commutatif. Soient $n, p \in \mathbb{N}^\star$.

I Action par translation : pivot de Gauss

1) Généralités

Définition 1. $\mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_n(\mathbb{K})$ par multiplication à gauche.

Définition 2. On appelle matrice de transvection toute matrice qui est de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$, où $\lambda \in \mathbb{K}$ et $i, j \in [\![1, n]\!]$ avec $i \neq j$.

Définition 3. On appelle matrice de dilatation toute matrice qui est de la forme $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$, où $\lambda \in \mathbb{K}$ et $i \in [\![1, n]\!]$.

Définition 4. On appelle matrice de permutation toute matrice qui est de la forme $P_{i,j} = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$, où $i, j \in [\![1, n]\!]$ avec $i \neq j$.

Remarque 5. *Ces matrices représentent également des transformations élémentaires dans l'algorithme du pivot de Gauss. Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$:*

Opération	$T_{i,j}(\lambda)A$	$D_i(\lambda)A$	$P_{i,j}A$
Résultat	$L_i \leftarrow L_i + \lambda L_j$	$L_i \leftarrow \lambda L_i$	$L_i \leftrightarrow L_j$

On a les opérations analogues sur les colonnes en multipliant à droite.

Exemple 6. $T_{3,2}(1) \times T_{3,1}(-3) \times T_{2,1}(-1) \times \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & -2 \\ 3 & 5 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & -4 \\ 0 & 0 & -2 \end{pmatrix}$

Définition 7. On appelle :

(i) pivot d'une ligne son coefficient non nul le plus à gauche.

(ii) matrice échelonnée en lignes une matrice telle que dès qu'une ligne est nulle, les suivantes sont nulles, et pour les lignes non nulles le pivot d'une ligne est strictement à droite du pivot de la ligne précédente. On dit qu'une matrice échelonnée est réduite si ses pivots valent 1.

On a la définition similaire de matrice échelonnée (réduite) en colonnes.

Proposition 8. *Les orbites sont en bijections avec les sous-espaces vectoriels de $\mathbb{K}^n$: $A \sim B \Leftrightarrow \operatorname{Ker} A = \operatorname{Ker} B$.*

Proposition 9. *Toute matrice est dans l'orbite d'une unique matrice échelonnée.*

Lemme 10. *On suppose E de dimension $n \geqslant 2$. Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u ou un produit de deux transvections uv, tel que $u(x) = y$ ou $uv(x) = y$.*

Théorème 11. *Les transvections engendrent $\mathcal{SL}(E)$.*

Théorème 12. *Les transvections et les dilatations engendrent $\mathcal{GL}(E)$.*

Application 13. *L'algorithme du pivot de Gauss permet de se ramener à la matrice réduite associée à une matrice via des opérations élémentaires sur les lignes.*

2) Application à la décomposition polaire

Pour $\mathbb{K} = \mathbb{R}$ et $n = p$, on considère l'action par translation de $\mathcal{O}_n(\mathbb{R})$.

Théorème 14 (Décomposition polaire)**.** *On a les homéomorphismes :*

$$\begin{array}{ccccccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) & \quad & \mathcal{U}_n(\mathbb{R}) \times \mathcal{H}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O, S) & \longmapsto & OS & & (U, H) & \longmapsto & UH \end{array}$$

Corollaire 15. *Pour $A \in \mathcal{GL}_n(\mathbb{R})$, on a $|||A|||_2 = \sqrt{\rho({}^{\mathrm{t}}AA)}$*

Corollaire 16. *Tout sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ qui contient le groupe orthogonal $\mathcal{O}_n(\mathbb{R})$ est le groupe $\mathcal{O}_n(\mathbb{R})$ lui-même.*

II Action de Steinitz : équivalence

Définition 17. Le groupe $\mathcal{GL}_n(\mathbb{K}) \times \mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_{n,m}(\mathbb{K})$ par $(P, T) \cdot M = PMT^{-1}$. Deux matrices de la même orbites sont dites équivalentes.

Théorème 18. *Si $M \in \mathcal{M}_{n,p}(\mathbb{K})$ est de rang r, alors M est équivalente à $J_r = \left(\begin{smallmatrix} I_r & 0 \\ 0 & 0 \end{smallmatrix}\right) \in \mathcal{M}_{n,p}(\mathbb{K})$.*

Remarque 19. *L'algorithme du pivot total permet d'obtenir J_r.*

Corollaire 20. *Deux matrices sont équivalentes si, et seulement si, elles ont même rang.*

Corollaire 21. $\operatorname{rg}({}^{\mathrm{t}}M) = \operatorname{rg}(M)$

Proposition 22. *Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. En notant O_r l'orbite des matrices de rang r, on a que, pour tout $r \leqslant \min(n, p)$, $\overline{O_r} = \bigcup_{k \leqslant r} O_k$.*

Corollaire 23. *Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. L'unique orbite fermée est $O_0 = \{0\}$, et l'unique orbite ouverte est $O_{\min(n,p)}$. Si $n = p$, alors $O_n = \mathcal{GL}_n(\mathbb{K})$ est un ouvert dense de $\mathcal{M}_n(\mathbb{K})$.*

III Action par conjugaison : similitude

1) Généralités

Définition 24. Le groupe $\mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_n(\mathbb{K})$ par $P \cdot M = PMP^{-1}$. Deux matrices d'une même orbite sont dites conjuguées ou semblables.

Remarque 25. *Cette action traduit le changement de base. La réduction des endomorphismes consiste à trouver des représentants élémentaires des orbites de cette action.*

Proposition 26. *Le rang, le déterminant, la trace, les valeurs propres, le polynôme minimal et le polynôme caractéristique sont des invariants de similitude.*

Remarque 27. *Ce n'est pas une caractérisation ! Par exemple, I_2 et $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ ont même polynôme caractéristique.*

2) Trigonalisabilité et diagonalisabilté

Définition 28. On dit que $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable (resp. trigonalisable) si elle est semblable à une matrice diagonale (resp. triangulaire).

Application 29. *Calcul de puissances :* $(PAP^{-1})^n = PA^nP^{-1}$.

Théorème 30. *Une matrice est diagonalisable (resp. trigonalisable) si et seulement si son polynôme minimal est scindé à racines simples (resp. scindé).*

Corollaire 31. *Si $\mathbb{K}$ est algébriquement clos, toute matrice est trigonalisable.*

3) Action de $\mathcal{O}_n(\mathbb{R})$

Si $\mathbb{K} = \mathbb{R}$, restreignons l'action par conjugaison à $\mathcal{O}_n(\mathbb{R})$.

Remarque 32. *Cette action traduit le changement de base orthonormée.*

Proposition 33. *Les valeurs propres (complexes) d'une matrice orthogonale sont des racines de l'unité.*

Lemme 34. *Soit $u \in \mathcal{O}(E)$, et soit F un sous-espace vectoriel stable par u. Alors $F^\perp$ est stable par u.*

Lemme 35. *Pour $M \in \mathcal{O}_n(\mathbb{R})$, il existe un sous-espace vectoriel W_n de $\mathbb{R}^n$ tel que $\dim W_n \leqslant 2$ stable par M.*

Lemme 36. *Pour $u \in \mathcal{O}(E)$, il existe des sous-espaces vectoriels $W_1, \dots, W_k$ de $\mathbb{R}^n$ stables par u tels que, pour tout i, $\dim W_i \leqslant 2$, et $E = \perp_{i=1}^{k} W_i$.*

Théorème 37. *Soit $M \in \mathcal{O}_n(\mathbb{R})$, alors M est semblable à :*

$$\begin{pmatrix} I_r & & & & 0 \\ & -I_m & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_s} \end{pmatrix} \text{ avec } \begin{cases} \theta_i \in]0; 2\pi[\setminus \{\pi\} \\ R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \end{cases}$$

IV Action par congruence

On suppose ici que $\mathrm{car}(\mathbb{K}) \neq 2$.

Définition 38. Le groupe $\mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{S}_n(\mathbb{K})$ par $P \cdot S = PS\,{}^tP$. Deux matrices d'une même orbite sont dites congruentes.

Remarque 39. *Cette action traduit le changement de base pour les formes quadratiques.*

Théorème 40 (Sylvester)**.** *Soit $A \in \mathcal{S}_n(\mathbb{R})$. Il existe $s, r \in \mathbb{N}$ tels que $s + r \leqslant n$ uniquement déterminés par A tels que A soit congruente à la matrice $\left(\begin{smallmatrix} I_r & 0 & 0 \\ 0 & -I_s & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$. Les orbites sont caractérisées par les couples (s, r), appelés signatures des formes quadratiques associées.*

Proposition 41. *On a en fait :*

$$s = \max\{\dim F \mid F \in \mathcal{P}\} \quad \text{et} \quad t = \max\{\dim F \mid F \in \mathcal{N}\}$$

où $\mathcal{P}$ (resp. $\mathcal{N}$) désigne l'ensemble des sous-espaces de $\mathbb{R}^n$ sur lesquels la restriction de la forme quadratique est définie positive (resp. négative).

Corollaire 42. *Deux matrices de $\mathcal{S}_n(\mathbb{R})$ sont congruentes si et seulement si elles ont même signature.*

Théorème 43. *Si $\mathbb{K}$ est algébriquement clos, il existe $r \in [\![1, n]\!]$ et $P \in \mathcal{GL}_n(\mathbb{R})$ tel que A soit congruente à la matrice $\left(\begin{smallmatrix} I_r & 0 \\ 0 & 0 \end{smallmatrix}\right)$.*

Développements

— Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$ (10,11,12) [Per96]
— Décomposition polaire (14) [CG13]
— Réduction des matrices orthogonales (34,35,36,37) [Gou94, CG13]

Références

[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck
[Ulm12] F. Ulmer. *Théorie des groupes.* Ellipses

Cadre : On considère un $\mathbb{K}$-espace vectoriel E. Soit $n \in \mathbb{N}^\star$

I Dimension d'un espace vectoriel

1) Familles libres, familles génératrices, bases

Définition 1. Soit $(x_i)_{i\in I}$ une famille de vecteurs de E. On dit que $(x_i)_{i\in I}$ est une famille génératrice de E si $\mathrm{Vect}(x_i)_{i\in I} = E$.

Exemple 2. *Dans $\mathbb{R}^2$, la famille $\{\binom{1}{0}, \binom{0}{2}, \binom{1}{2}\}$ est génératrice.*

Définition 3. Un espace vectoriel est de dimension finie s'il admet une famille génératrice finie. Sinon, il est de dimension infinie.

Exemple 4. *$\mathbb{K}^n$ est de dimension finie. $\mathbb{R}[X]$ est de dimension infinie.*

Définition 5. Une famille $(x_i)_{i\in I}$ de E est dite libre si toute combinaison linéaire vérifiant $\sum_{i\in I} \lambda_i x_i = 0$ implique que, pour tout $i \in I$, $\lambda_i = 0$. Dans le cas contraire, la famille est dite liée.

Exemple 6. *(i) Dans $\mathbb{R}^3$, $\left\{\begin{pmatrix}1\\2\\1\end{pmatrix}, \begin{pmatrix}-1\\3\\1\end{pmatrix}, \begin{pmatrix}-1\\13\\5\end{pmatrix}\right\}$ est liée.*

(ii) Dans $\mathbb{R}^3$, $\left\{\begin{pmatrix}1\\1\\-1\end{pmatrix}, \begin{pmatrix}0\\2\\1\end{pmatrix}, \begin{pmatrix}0\\0\\5\end{pmatrix}\right\}$ est libre.

Proposition 7. *Une famille de E est libre si, et seulement si, aucun vecteur de la famille n'est combinaison linéaire des autres.*

Théorème 8. *Si E est engendré par un nombre fini n de vecteurs, toute famille libre de E a au plus n éléments.*

Définition 9. Une famille à la fois libre et génératrice est appelée base.

Exemple 10. *(i) La famille $(e_i)_{i\in I}$ (où $e_i = (\delta_{i,j})_{1\leqslant j\leqslant n}$) est une base de $\mathbb{K}^n$ (base canonique).*

(ii) La famille $(X^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$.

(iii) La famille $\{\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)\}$ est une base de $\mathcal{M}_2(\mathbb{K})$.

Proposition 11. *Soit $(e_i)_{i\in I}$ une base de E. Pour tout $x \in E$, il existe une unique famille $(\lambda_i)_{i\in I}$ telle que $x = \sum_{i\in I} \lambda_i e_i$.*

2) Théorie de la dimension

Théorème 12 (de la base incomplète)**.** *Soient E de dimension finie, $\mathcal{G}$ une famille génératrice de E finie, et $\mathcal{L}$ une famille libre dans E. Alors il existe une famille $\mathcal{F}$ de $\mathcal{G}$ telle que $\mathcal{L} \cup \mathcal{F}$ soit une base de E.*

Corollaire 13. *(i) Tout espace vectoriel de dimension finie a une base.*

(ii) Toute partie libre peut être complétée en une base.

(iii) De toute famille génératrice on peut extraire une base.

Lemme 14. *Soient E de dimension finie, $\mathcal{G}$ une famille génératrice de E finie, et $\mathcal{L}$ une famille libre dans E. Alors* $\mathrm{Card}\,\mathcal{L} \leqslant \mathrm{Card}\,\mathcal{G}$.

Théorème 15. *En dimension finie, les bases ont même cardinal.*

Définition 16. Cet entier, noté $\dim_{\mathbb{K}} E$, s'appelle dimension de E.

Proposition 17. *Supposons E de dimension finie n, alors :*

(i) Toute famille libre ou génératrice de n vecteurs est une base de E.

(ii) Toute famille de plus de n éléments est liée.

(iii) Toute famille de moins de n éléments ne peut être génératrice.

Théorème 18. *Deux $\mathbb{K}$-espaces vectoriels de dimension finie sont isomorphes si, et seulement si, ils ont même dimension.*

Corollaire 19. *Si $\dim_{\mathbb{K}} E = n$, alors $E \cong \mathbb{K}^n$.*

3) Sous-espaces et somme de sous-espaces

Soient E de dimension finie et E_1, E_2 sous-espaces vectoriels de E.

Théorème 20. *(i)* $\dim_{\mathbb{K}} E_1 \leqslant \dim_{\mathbb{K}} E < +\infty$

(ii) $\dim_{\mathbb{K}} E_1 = \dim_{\mathbb{K}} E \Leftrightarrow E_1 = E$

(iii) $\dim_{\mathbb{K}}(E_1 + E_2) = \dim_{\mathbb{K}} E_1 + \dim_{\mathbb{K}} E_2 - \dim_{\mathbb{K}}(E_1 \cap E_2)$

Théorème 21. *Les assertions suivantes sont équivalentes :*

(i) $E = E_1 \oplus E_2$

(ii) $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} E_1 + \dim_{\mathbb{K}} E_2$ *et* $E_1 \cap E_2 = \{0\}$

(iii) $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} E_1 + \dim_{\mathbb{K}} E_2$ *et* $E_1 + E_2 = E$

(iv) $E = E_1 + E_2$ *et* $E_1 \cap E_2 = \{0\}$

II Théorie du rang

1) Rang d'une application linéaire

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. Soit $f \in \mathcal{L}(E,F)$.

Définition 22. On dit que f est de rang fini si $\operatorname{Im} f$ est de dimension finie. Dans ce cas, l'entier $\dim \operatorname{Im} f$ est appelé rang de f et est noté $\operatorname{rg} f$.

Exemple 23. *$(x,y,z) \mapsto (x+y-z, 2x+y+z, 3x+2y)$ est de rang 2.*

Théorème 24 (du rang)**.** $\dim_{\mathbb{K}} E = \operatorname{rg} f + \dim_{\mathbb{K}} \operatorname{Ker} f$

Exemple 25. *En appelant f la fonction définie à l'exemple 23, on a* $\operatorname{Ker} f = \operatorname{Vect}\begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}$*, donc* $\dim_{\mathbb{K}} \operatorname{Ker} f = 1$*, et on a bien* $3 = 2+1$

Corollaire 26. *Supposons $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} F < +\infty$, alors :*

$$f \text{ est bijective} \Leftrightarrow f \text{ est injective} \Leftrightarrow f \text{ est surjective}$$

Contre-exemple 27. *En dimension infinie, la dérivation sur $\mathbb{R}[X]$ est surjective, mais non bijective.*

2) Rang d'une matrice

Définition 28. On appelle rang d'une famille de vecteurs la dimension de l'espace engendré par ces vecteurs. On appelle rang d'une matrice A le rang de la famille de ses vecteurs colonnes. On le note $\operatorname{rg} A$.

Proposition 29. *Si $A \in \mathcal{M}_n(\mathbb{K})$, A est inversible $\Leftrightarrow \operatorname{rg} A = n$.*

Exemple 30. *La matrice* $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 2 & 1 & 0 \end{pmatrix}$ *est de rang 3, donc inversible.*

Définition 31. Soit $A \in \mathcal{M}_{p,q}(\mathbb{K})$. On appelle mineur d'ordre r le déterminant d'une sous-matrice carrée de taille r.

Théorème 32. *Le rang d'une matrice $A \in \mathcal{M}_{p,q}(\mathbb{K})$ est la taille de son plus grand mineur non nul.*

Corollaire 33. *Le rang de toute matrice est égal au rang de sa transposée.*

Corollaire 34. *Le rang d'une matrice est également le rang de la famille de ses vecteurs lignes.*

Remarque 35. *Si $A \in \mathcal{M}_{p,q}(\mathbb{K})$, $\operatorname{rg} A \leqslant \min(p,q)$.*

Définition 36. Soient $A, B \in \mathcal{M}_{p,q}(\mathbb{K})$. A et B sont équivalentes s'il existe $P \in \mathcal{GL}_p(\mathbb{K})$ et $Q \in \mathcal{GL}_q(\mathbb{K})$ telles que $B = PAQ$.

Exemple 37. *Les matrices* $\begin{pmatrix} 3 & -1 & 1 \\ 0 & 2 & 0 \\ 1 & -1 & 3 \end{pmatrix}$ *et* $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ *sont équivalentes.*

Théorème 38. *Soit $A \in \mathcal{M}_{p,q}(\mathbb{K})$. Si $r = \operatorname{rg} A \geqslant 1$, A est équivalente à la matrice* $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$*, où I_r est la matrice identité de taille r.*

Corollaire 39. *Deux matrices de même taille sont équivalentes si, et seulement si, elles ont même rang.*

Corollaire 40. *On ne change pas le rang d'une matrice en multipliant une colone par un scalaire non nul, ou en ajoutant à une colonne une combinaison linéaire des autres colonnes (même chose avec les lignes).*

III Applications

Supposons E de dimension finie n.

1) Dualité

Définition 41. On note $E^\star = \mathcal{L}(E,\mathbb{K})$ l'ensemble des formes linéaires sur E, appelé espace dual de E.

Proposition 42. *Soit $f \in E^\star \setminus \{0\}$. Alors* $\operatorname{rg} f = 1$ *et* $\dim_{\mathbb{K}} \operatorname{Ker} f = n-1$.

Proposition 43. $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} E^\star$ *et* $E \cong E^\star$.

Théorème 44. *La base duale de la base $(e_1, \dots, e_n)$ de E est donnée par $(f_1, \dots, f_n)$, où $f_i(e_j) = \delta_{i,j}$.*

Proposition 45. *On a $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} E^{\star\star}$. De plus, E et $E^{\star\star}$ sont canoniquement isomorphes.*

Définition 46. Pour $A \subseteq E$ et $B \subseteq E^\star$, on note :

(i) $A^\perp = \{\varphi \in E^\star \,|\, \forall x \in A, \varphi(x) = 0\}$ l'orthogonal de A dans $E^\star$.

(ii) $B^\circ = \{x \in E \,|\, \forall \varphi \in B, \varphi(x) = 0\}$ l'orthogonal de B dans E.

Proposition 47. *(i) Si $A_1 \subset A_2 \subset E$, $A_2^\perp \subset A_1^\perp$.*

(ii) Si $B_1 \subset B_2 \subset E^\star$, $B_2^\circ \subset B_1^\circ$.

(iii) Si $A \subset E$, $A^\perp = (\operatorname{Vect} A)^\perp$.

(iv) Si $B \subset E^\star$, $B^\circ = (\operatorname{Vect} B)^\circ$.

Proposition 48. *Soit F un sous-espace vectoriel de E. Alors $F^{\perp\circ} = F$ et $\dim_{\mathbb{K}} F + \dim_{\mathbb{K}} F^{\perp} = \dim_{\mathbb{K}} E$.*

Proposition 49. *Si G un sous-espace vectoriel de $E^\star$. Alors $G^{\circ\perp} = G$ et $\dim_{\mathbb{K}} G + \dim_{\mathbb{K}} G^{\circ} = \dim_{\mathbb{K}} E^\star$.*

Définition 50. Soient E et F deux $\mathbb{K}$-espaces vectoriels, et soit $u \in \mathcal{L}(E,F)$. L'application ${}^t u : F^\star \to E^\star$ définie par ${}^t u(f) = f \circ u$ est appelée transposée de u.

Proposition 51. *Soit $u \in \mathcal{L}(E)$. Un sous-espace vectoriel F de E est stable par u si, et seulement si, $F^\perp$ est stable par ${}^t u$.*

2) Réduction de Jordan pour les nilpotents

Proposition 52. *Soit $u \in \mathcal{L}(E)$. Supposons que $\chi_u = \prod_{i=1}^{p}(X-\lambda_i)^{\alpha_i}$ et $\pi_u = \prod_{i=1}^{\rho}(X-\lambda_i)^{\beta_i}$, alors :*

(i) $E = \bigoplus_{k=1}^{\rho} N_k$, $\dim_{\mathbb{K}} N_k = \alpha_k$, $N_k = Ker(u-\lambda_k Id_E)^{\beta_k}$

(ii) $(u - Id_E)|_{N_k}$ *est nilpotent d'indice* β_k.

(iii) N_k *est stable par* u *et* λ_k *est la seule valeur propre de* $u|_{N_k}$.

Lemme 53. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Pour tout $x \in E$ tel que $u^{q-1}(x) \neq 0$, la famille $\mathcal{B}_{u,x} = (u^k(x))_{1\leqslant k\leqslant q-1}$ est une famille libre de E et l'espace vectoriel $F = \mathrm{Vect}(\mathcal{B}_{u,x})$ est u-stable.*

Théorème 54. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Alors il existe une base $\mathcal{B} = B_1 \cup \ldots \cup B_r$ de E telle que chaque s.e.v. $E_i = \mathrm{Vect}\, \mathcal{B}_i$ soit stable par u et que la matrice de $u|_{E_i}$ soit :*

$$J_i = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_{q_i}(\mathbb{K}), \text{ avec } q_i = \dim_{\mathbb{K}} E_i$$

Théorème 55. *Soit $u \in \mathcal{L}(E)$ non nul tel que $\chi_u = \prod_{i=1}^{p}(X-\lambda_i)^{\alpha_i}$ et $\Pi_u = \prod_{i=1}^{\rho}(X-\lambda_i)^{\beta_i}$. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u soit de la forme $A = \mathrm{Diag}(J_1, \ldots, J_\rho)$ avec pour tout $k \in [\![1,\rho]\!]$:*

$$J_k = \begin{pmatrix} \lambda_k & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & \lambda_k & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{k,\alpha_k-1} & \lambda_k & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}), \text{ où } \varepsilon_{k,i} \in \{0,1\}$$

3) Réduction des endomorphismes normaux

Lemme 56. *Si F est un sous-espace vectoriel de E stable par u, alors F et $F^\perp$ sont stables par u et $u^\star$.*

Lemme 57. *Supposons que $n = 2$. Alors :*

(i) Si u a une valeur propre réelle, u est diagonalisable dans une base orthonormée.

(ii) Si u n'a pas de valeur propre réelle, la matrice de u dans une base orthonormée est de la forme $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$.

Théorème 58. *Il existe une base orthonormée $\mathcal{B}$ de E telle que :*

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & 0 & & \\ & & \lambda_r & & & & \\ & & & \tau_1 & & & \\ & 0 & & & \ddots & & \\ & & & & & \tau_s & \end{pmatrix}$$

où $n = r + 2s$, $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ et $\tau_k = \left(\begin{smallmatrix} a_k & -b_k \\ b_k & a_k \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R})$ pour $k \in [\![1,s]\!]$.

Développements

- Réduction de Jordan (par la dualité) (53,54,55) [Rom20]
- Réduction des endomorphismes normaux (56,57,58) [Gou94]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Gri11] J. Grifone. *Algèbre Linéaire.* Cépaduès, 4e édition
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck

Cadre : $\mathbb{K}$ est un corps, E est un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^\star$ et $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

I Formes multilinéaires et déterminant

1) Formes multilinéaires

Définition 1. Soient $E_1, \dots, E_p$ et F des $\mathbb{K}$-espaces vectoriels. Une application $f : E_1 \times \dots \times E_p \to F$ est dite p-linéaire si, en tout point, les p applications partielles sont linéaires. On note $f \in \mathcal{L}_p(E_1 \times \dots \times E_p, F)$. On parle de forme p-linéaire sur E si $E_1 = \dots = E_p = E$ et $F = \mathbb{K}$, l'ensemble des formes p-linéaires sur E est noté $\mathcal{L}_p(E, \mathbb{K})$.

Exemple 2. *Si $\varphi_1, \dots, \varphi_p$ sont dans $\mathcal{L}(E, \mathbb{K})$, l'application*

$$\varphi : \left| \begin{array}{ccc} E^p & \longrightarrow & \mathbb{K} \\ (x_1, \dots, x_p) & \longmapsto & \varphi_1(x_1) \dots \varphi_p(x_p) \end{array} \right.$$

est dans $\mathcal{L}_p(E, \mathbb{K})$.

Définition 3. Soit $f \in \mathcal{L}_p(E, \mathbb{K})$.

(i) f est dite alternée si $f(x_1, \dots, x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux.

(ii) f est dite antisymétrique si l'échange de deux vecteurs dans la suite $(x_1, \dots, x_p)$ donne à f des valeurs opposées.

Remarque 4. *Soit $f \in \mathcal{L}_p(E, \mathbb{K})$, f est antisymétrique si, et seulement si, pour tout $\sigma \in \mathfrak{S}_p$ et pour tout $(x_1, \dots, x_p) \in E^p$, on a :*

$$f(x_{\sigma(1)}, \dots, x_{\sigma(p)}) = \varepsilon(\sigma) f(x_1, \dots, x_p)$$

Théorème 5. *Soit $f \in \mathcal{L}_p(E, \mathbb{K})$. Si $\mathrm{car}(\mathbb{K}) \neq 2$, alors f est antisymétrique si, et seulement si, f est alternée.*

Théorème 6. *L'ensemble des formes n-linéaires alternées sur E est un $\mathbb{K}$-espace vectoriel de dimension 1. De plus, si x_j s'écrit $(x_{1,j}, \dots, x_{n,j})$ dans la base $\mathcal{B}$, les formes n-linéaires alternées sur E sont les applications qui sont de la forme :*

$$f(x_1, \dots, x_n) = \lambda \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \dots x_{n,\sigma(n)}, \text{ avec } \lambda \in \mathbb{K}$$

2) Déterminant d'une famille de vecteurs

Définition 7. On appelle déterminant dans la base $\mathcal{B}$ l'unique forme n-linéaire alternée sur E prenant la valeur 1 sur la base $\mathcal{B}$:

$$\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \dots x_{n,\sigma(n)}$$

Proposition 8. *(i) Soit $f \in \mathcal{L}_n(E, \mathbb{K})$, alors on a :*

$$f(x_1, \dots, x_n) = f(e_1, \dots, e_n) \det_{\mathcal{B}}(x_1, \dots, x_n)$$

(ii) Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases de E, alors :

$$\det_{\mathcal{B}'}(x_1, \dots, x_n) = \det_{\mathcal{B}'} \mathcal{B} \cdot \det_{\mathcal{B}}(x_1, \dots, x_n) \text{ et } \det_{\mathcal{B}'} \mathcal{B} \det_{\mathcal{B}} \mathcal{B}' = 1$$

Théorème 9. *Soient $x_1, \dots, x_n \in E$, il y a équivalence entre :*

(i) La famille $(x_1, \dots, x_n)$ est liée.

(ii) Pour toute base $\mathcal{B}$ de E, $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$.

(iii) Il existe une base $\mathcal{B}$ de E telle que $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$.

3) Déterminant d'un endomorphisme, d'une matrice

Définition 10. Soit $f \in \mathcal{L}(E)$. Alors $\det_{\mathcal{B}}(f(e_1), \dots, f(e_n))$ ne dépend pas de la base choisie. On l'appelle déterminant de f et on le note $\det f$.

Proposition 11. *(i) Si $f, g \in \mathcal{L}(E)$, $\det(f \circ g) = \det(f) \det(g)$.*

(ii) $\det Id_E = 1$

(iii) $\forall f \in \mathcal{L}(E)$, $f \in \mathcal{GL}_n(E) \Leftrightarrow \det f \neq 0$, et on a $\det(f^{-1}) = \det(f)^{-1}$.

Définition 12. Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{K})$. On appelle déterminant de A le déterminant des vecteurs colonnes de A dans la base canonique de $\mathbb{K}^n$, et on le note $\det A$. On a :

$$\det A = \begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}$$

Exemple 13. *(i)* $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$

(ii) Règle de Sarrus : $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - ceg - bdi - afh$

Proposition 14. *(i) Si $f \in \mathcal{L}(E)$ alors* $\det f = \det \mathrm{Mat}_{\mathcal{B}}(f)$.
(ii) Si $A \in \mathcal{M}_n(\mathbb{K})$, alors $\det A = \det {}^{\mathrm{t}}A$.
(iii) Si $A, B \in \mathcal{M}_n(\mathbb{K})$, alors $\det(AB) = \det(A)\det(B)$.
(iv) Deux matrices semblables ont le même déterminant.

II Méthodes de calcul

1) Se ramener au cas triangulaire

Proposition 15. *On ne change pas la valeur du déterminant en ajoutant à une colonne une combinaison linéaire des autres colonnes, de même pour les lignes.*

Proposition 16. *Si $A \in \mathcal{M}_n(\mathbb{K})$ est triangulaire, alors* $\det A$ *est le produit des éléments diagonaux de A.*

Exemple 17. $\begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ -1 & -1 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix} = 1$

Proposition 18. *Si $M = \left(\begin{smallmatrix} A & C \\ 0 & B \end{smallmatrix}\right)$ avec $A \in \mathcal{M}_p(\mathbb{K})$, $B \in \mathcal{M}_{[}(n)-p]\mathbb{K}$ et $C \in \mathcal{M}_{[}(p), n-p]\mathbb{K}$, alors* $\det(M) = \det(A)\det(B)$.

2) Mineurs et cofacteurs

Définition 19. Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{K})$, pour tout (i,j) on appelle mineur de l'élément $a_{i,j}$ le déterminant $\Delta_{i,j}$ de la matrice obtenue en supprimant la i-ième ligne et la j-ième colonne de la matrice A. Le scalaire $A_{i,j} = (-1)^{i+j}\Delta_{i,j}$ s'appelle cofacteur de $a_{i,j}$.

Proposition 20. *Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{K})$, alors on peut développer le déterminant par rapport à :*
(i) la j-ième colonne : $\det A = \sum_{i=1}^{n} a_{i,j}A_{i,j}$
(ii) la i-ième ligne : $\det A = \sum_{j=1}^{n} a_{i,j}A_{i,j}$

Exemple 21. $\begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{vmatrix} = 1 \times \begin{vmatrix} 1 & 2 \\ 2 & 3 \end{vmatrix} = -1$

Définition 22. Soit $A \in \mathcal{M}_n(\mathbb{K})$, la matrice $(A_{i,j})_{1 \leqslant i,j \leqslant n}$ des cofacteurs est appellée comatrice de A et notée $\mathrm{Com}(A)$.

Proposition 23. *Soit $A \in \mathcal{M}_n(\mathbb{K})$, alors :*

$$A\,{}^{\mathrm{t}}\mathrm{Com}(A) = {}^{\mathrm{t}}\mathrm{Com}(A)A = \det(A)I_n$$

Exemple 24. *Pour* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{K})$, $A^{-1} = \frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$

3) Déterminants particuliers

Application 25 (Déterminant de Vandermonde)**.**
Soient $a_1, \ldots, a_n \in \mathbb{K}$ avec $n \geqslant 2$.

$$V(a_1, \ldots, a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i,j \leqslant n} (a_j - a_i)$$

Application 26 (Déterminant de Cauchy)**.**
Soient $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{K}$ tels que pour tout (i,j), $a_i + b_j \neq 0$:

$$\Delta_n = \begin{vmatrix} \frac{1}{a_1+b_1} & \frac{1}{a_1+b_2} & \cdots & \frac{1}{a_1+b_n} \\ \frac{1}{a_2+b_1} & \frac{1}{a_2+b_2} & \cdots & \frac{1}{a_2+b_n} \\ \vdots & \vdots & & \vdots \\ \frac{1}{a_2+b_1} & \frac{1}{a_n+b_2} & \cdots & \frac{1}{a_n+b_n} \end{vmatrix} = \frac{\prod_{i<j}(a_j - a_i)(b_j - b_i)}{\prod_{i,j}(a_i + b_j)}$$

Application 27 (Déterminant circulant)**.**
Soient $n \in \mathbb{N}^\star$, $\omega = e^{\frac{2i\pi}{n}}$ et $a_1, \ldots, a_n \in \mathbb{K}$.

$$\begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{vmatrix} = \prod_{j=1}^{n} P(\omega^j) \text{ où } P(X) = a_1 + a_2X + \ldots + a_nX^{n-1}$$

III Applications

1) Systèmes linéaires

Application 28 (Cramer)**.** *Soit $A \in \mathcal{M}_n(\mathbb{K})$, $b, X \in \mathbb{R}$. Alors $AX = B$ admet une unique solution si, et seulement si,* $\det A \neq 0$. *En notant A_j est la j-ième colonne de A, les x_i sont donnés par :*

$$x_i = \frac{\det_{(} A_1, \ldots, A_{i-1}, B, A_{i+1}, \ldots, A_n)}{\det A}$$

Exemple 29. *Si* $\begin{cases} 2x - 5y + 2z = 7 \\ x + 2y - 4z = 3 \\ 3x - 4y - 6z = 5 \end{cases}$ *, alors $x = 5, y = z = 1$.*

2) Réduction des endomorphismes

Définition 30. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle polynôme caractéristique de A l'élément de $\mathbb{K}[X]$ défini par $\chi_A(X) = \det(A - XI_n)$.

Remarque 31. $\chi_A(0) = \det A$

Proposition 32. *λ est valeur propre de A ssi $\chi_A(\lambda) = 0$.*

Proposition 33. $\begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & & & \vdots \\ & \ddots & & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix} \Rightarrow \chi = (-1)^n \left(X^n + \sum_{i=0}^{n} a_i X i \right)$

Théorème 34 (Cayley-Hamilton)**.** *Pour $A \in \mathcal{M}_n(\mathbb{K})$, $\chi_A(A) = 0$.*

3) Matrice et déterminant de Gram

Définition 35. On appelle matrice de Gram de $(x_i)_{1 \leqslant i \leqslant n}$ la matrice $M_G(x_1, \ldots, x_n) = (\langle x_i, x_j \rangle)_{1 \leqslant i,j \leqslant n}$, et déterminant de Gram le déterminant de cette matrice, noté $G(x_1, \ldots, x_n)$.

Lemme 36. *Le déterminant de Gram d'une famille de vecteurs est nul si, et seulement si, elle est liée.*

Théorème 37. *Soit F un sous-espace vectoriel de E de dimension finie $n \in \mathbb{N}^\star$ muni d'une base $(e_i)_{1 \leqslant i \leqslant n}$. Alors, pour tout $x \in E$, on a :*

$$d(x, F)^2 = \frac{G(e_1, \ldots, e_n, x)}{G(e_1, \ldots, e_n)}$$

Théorème 38 (Hadamard)**.** *(i) Soient $x_1, \ldots, x_n$ des vecteurs de E. Alors $G(x_1, \ldots, x_n) \leqslant \prod_{i=1}^{n} \|x_i\|^2$.*

(ii) Soient $x_1, \ldots, x_n \in \mathbb{C}^n$. Alors $|\det(x_1, \ldots, x_n)| \leqslant \prod_{i=1}^{n} \|x_i\|_2$.

Dans les deux cas, on a égalité si, et seulement si, $(x_i)_{1 \leqslant i \leqslant n}$ est orthogonale ou l'un des vecteurs est nul.

4) Géométrie

Théorème 39. *Soient $v_1, \ldots, v_n \in \mathbb{K}^n$, on note $Vol(v_1, \ldots, v_n)$ le volume du parallélépipède engendré par $v_1, \ldots, v_n$, alors :*

$$Vol(v_1, \ldots, v_n) = |\det(v_1, \ldots, v_n)|$$

Lemme 40. *Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ symétriques définies positives distinctes, et $\alpha, \beta > 0$ tels que $\alpha + \beta = 1$, alors :*

$$\det(\alpha A + \beta B) > \det(A)^\alpha \det(B)^\beta$$

Application 41 (Ellipsoïde de John-Loewner)**.** *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant K.*

Développements

- Déterminant de Gram et inégalité de Hadamard (36,37,38) [Gou94]
- Ellipsoïde de John-Loewner (40,41) [FGN13c]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Gri11] J. Grifone. *Algèbre Linéaire.* Cépaduès, 4e édition
[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3.* Cassini

Cadre : $\mathbb{K}$ est un corps, E un $\mathbb{K}$-ev de dimension finie, et $u \in \mathcal{L}(E)$.

I Polynômes d'endomorphismes

1) L'algèbre $\mathbb{K}[X]$

Définition 1. Soit $P(X) = \sum_{i=0}^{p} a_i X^i \in \mathbb{K}[X]$. Pour $f \in \mathcal{L}(E)$, on note :

$$P(f) = \sum_{i=0}^{p} a_i f^i \in \mathcal{L}(E) \quad \text{où} \quad f^k = \underbrace{f \circ \ldots \circ f}_{k \text{ fois}}$$

Pour $A \in \mathcal{M}_n(\mathbb{K})$, on note $P(A) = \sum_{i=0}^{p} a_i A^i \in \mathcal{M}_n(\mathbb{K})$.

Définition 2. L'application $\varphi_u : \mathbb{K}[X] \to \mathcal{L}(E)$ définie par $\varphi_u(P) = P(u)$ est un morphisme de $\mathbb{K}$-algèbre. On note $\mathbb{K}[u]$ son image.

Remarque 3. *Comme $\mathbb{K}[X]$ est une algèbre commutative, $\mathbb{K}[u]$ aussi.*

Théorème 4 (Lemme des noyaux)**.** *Soient $f \in \mathcal{L}(E)$ et $P = P_1 \ldots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

$$\operatorname{Ker} P(f) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(f)$$

2) Polynôme minimal

Définition 5. Le morphisme φ_u possède un noyau non trivial. Comme $\mathbb{K}$ est un corps, ce noyau est un idéal monogène de $\mathbb{K}[X]$, on note π_u son générateur unitaire, qu'on appelle polynôme minimal de u. C'est aussi le polynôme unitaire annulateur de u de plus petit degré.

Remarque 6. *Tout endomorphisme annule un polynôme non nul.*

Proposition 7. $\mathbb{K}[u] \cong \mathbb{K}[X]/\operatorname{Ker}(\varphi_u)$ *au sens des $\mathbb{K}$-algèbres.*

Proposition 8. *L'algèbre $\mathbb{K}[u]$ est de dimension* $\deg \pi_u$*, avec une base donnée par* $(Id_E, u, \ldots, u^{\deg \pi_u - 1})$.

Remarque 9. *Soit $Q \in \mathbb{K}[X]$, si $Q(f) = 0$, alors $\pi_u | Q$.*

Définition 10. Soit $\lambda \in \mathbb{K}$, le scalaire λ est appelée valeur propre de u s'il existe $x \in E \setminus \{0\}$ tel que $u(x) = \lambda x$. On dit alors que x est un vecteur propre de u associé à λ.
On appelle spectre de u, noté $\operatorname{Sp}(u)$, l'ensemble des valeurs propres de u.

Remarque 11. *(i) 0 est valeur propre de u ssi* $\operatorname{Ker} u \neq \{0\}$.
(ii) Pour $A \in \mathcal{M}_n(\mathbb{K})$, on dit que $X \in \mathbb{K}^n$ est vecteur propre de A associé à la valeur propre $\lambda \in \mathbb{K}$. On note également $\operatorname{Sp}(A)$ *le spectre de A. Si A est la matrice d'un endomorphisme u,* $\operatorname{Sp}(u) = \operatorname{Sp}(A)$.

Définition 12. Soit λ une valeur propre de u. On définit E_λ par :

$$E_\lambda = \{x \in E \,|\, u(x) = \lambda x\} = \operatorname{Ker}(u - \lambda Id_E)$$

E_λ est un sous-espace vectoriel de E stable par u, appelé sous-espace propre de u associé à la valeur propre λ.

Proposition 13. *Soient $\lambda_1, \ldots, \lambda_k$ des valeurs propres distinctes de u, alors les sous-espaces propres $E_{\lambda_1}, \ldots, E_{\lambda_k}$ sont en somme directe.*

Proposition 14. *Si $f \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$, alors $\lambda \in \operatorname{Sp}(f) \Leftrightarrow \pi_f(\lambda) = 0$.*

3) Polynôme caractéristique

Définition 15. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle polynôme caractéristique de A le polynôme de $\mathbb{K}[X]$ défini par $\chi_A(X) = \det(A - XI_n)$.

Remarque 16. *(i)* $\chi_A(0) = \det A$
(ii) Une matrice a même polynôme caractéristique que a transposée.
(iii) Deux matrices semblables ont même polynôme caractéristique.

Exemple 17. *Si* $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$*, alors* $\chi_A(X) = X^2 - 5X - 2$.

Définition 18. Soit $u \in \mathcal{L}(E)$. On appelle polynôme caractéristique de u le polynôme caractéristique de la matrice de u, on le note χ_u.

Proposition 19. *λ est valeur propre de u ssi $\chi_u(\lambda) = 0$.*

Remarque 20. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. On peut écrire :*

$$\chi_A(X) = \sum_{i=0}^{n} \beta_i X^i \text{ où } \beta_0 = (-1)^n \det A,\ \beta_{n-1} = -\operatorname{tr} A,\ \beta_n = 1$$

Proposition 21. *Soit $f \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$ tel que $P(f) = 0$.*
Si λ est valeur propre de f, alors $P(\lambda) = 0$.

Remarque 22. *χ_f et π_f ont les mêmes racines.*

Exemple 23. *(i) Si f est nilpotent d'ordre n, $\pi_f(X) = X^n = \chi_f(X)$.*
(ii) Si f est l'application nulle, $\pi_f(X) = X$ et $\chi_f(X) = X^n$.

Théorème 24 (Cayley-Hamilton)**.** *Pour $f \in \mathcal{L}(E)$, $\chi_f(f) = 0$.*

II Réduction d'endomorphismes

1) Sous-espaces caractéristiques

Définition 25. Soit $f \in \mathcal{L}(E)$ tel que $\chi_f(X) = (-1)^n \prod_{i=1}^s (X-\lambda_i)^{\alpha_i}$. Pour tout i, le sous-espace vectoriel $N_i = \mathrm{Ker}(f - \lambda_i Id_E)^{\alpha_i}$ s'appelle le sous-espace caractéristique de f associé à la valeur propre λ_i.

Remarque 26. *(i) Pour tout i, N_i est stable par f et $\dim N_i = \alpha_i$.*
(ii) E est somme directe de ses sous-espaces stables.

Définition 27. Soit $f \in \mathcal{L}(E)$. Il existe un unique $r \in \mathbb{N}^\star$ tel que :

$$\{0\} = \mathrm{Ker}\, f^0 \subsetneq \mathrm{Ker}\, f \subsetneq \ldots \subsetneq \mathrm{Ker}\, f^r = \mathrm{Ker}\, f^{r+1} = \ldots = \mathrm{Ker}\, f^q = \ldots$$

r s'appelle indice de f. C'est le plus petit entier tel que $\mathrm{Ker}\, f^r = \mathrm{Ker}\, f^{r+1}$.

Remarque 28. *(i)* $\forall q < r,\ \dim \mathrm{Ker}\, f^q < \dim \mathrm{Ker}\, f^r$
(ii) $\forall q \geqslant r,\ \dim \mathrm{Ker}\, f^q = \dim \mathrm{Ker}\, f^r$
(iii) Si f est nilpotent, son indice est égal à son indice de nilpotence.
(iv) $E = \mathrm{Im}\, f^0 \supsetneq \mathrm{Im}\, f \supsetneq \ldots \supsetneq \mathrm{Im}\, f^r = \mathrm{Im}\, f^{r+1} = \ldots = \mathrm{Im}\, f^q = \ldots$

Proposition 29. *Soit $f \in \mathcal{L}(E)$ dont le polynôme caractéristique χ_f est scindé sur $\mathbb{K}$, $\chi_f(X) = (-1)^n \prod_{i=1}^s (X-\lambda_i)^{\alpha_i}$, alors :*
(i) Le polynôme minimal π_f de f est de la forme :

$$\pi_f(X) = \prod_{i=1}^{s} (X-\lambda_i)^{r_i} \text{ avec } \forall i, 0 \leqslant r_i \leqslant \alpha_i$$

(ii) r_i est l'indice de l'endomorphisme $f - \lambda_i Id_E$.

2) Diagonalisation et trigonalisation

Proposition 30. *Soient $f \in \mathcal{L}(E)$ et F un sous-espace vectoriel strict de E stable par f. En notant $g = f|_F$ la restriction de f à F, on a que g est dans $\mathcal{L}(E)$ et que χ_g divise χ_f.*

Proposition 31. *Soit $f \in \mathcal{L}(E)$, et soit $\lambda \in \mathbb{K}$ une racine de χ_f de multiplicité h, alors* $\dim E_\lambda \leqslant h$.

Théorème 32. *Soit $f \in \mathcal{L}(E)$, les assertions suivantes sont équivalentes :*
(i) f est diagonalisable
(ii) χ_f est scindé sur $\mathbb{K}$, et toute racine λ est de multiplicité $\dim E_\lambda$.
(iii) Il existe des valeurs propres $\lambda_1, \ldots, \lambda_p$ de f vérifiant $E = \bigoplus_{i=1}^p E_{\lambda_i}$.

Application 33. *Un endomorphisme est diagonalisable si, et seulement si, il admet un polynôme annulateur scindé à racines simples sur $\mathbb{K}$.*

Corollaire 34. *Soit F un sous-espace vectoriel de E stable par u. Supposons u diagonalisable (resp. trigonalisable). Alors $u|_F$ est diagonalisable (resp. trigonalisable).*

Théorème 35 (Co-réduction)**.** *Soit $(u_i)_{i\in I}$ une famille d'endomorphismes de E commutant deux à deux. Si les u_i sont diagonalisables (resp. trigonalisables), alors on peut les diagonaliser (resp. trigonaliser) dans une même base.*

3) Réduction de Jordan pour les nilpotents

Lemme 36. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Pour tout $x \in E$ tel que $u^{q-1}(x) \neq 0$, la famille $\mathcal{B}_{u,x} = (u^k(x))_{1\leqslant k\leqslant q-1}$ est une famille libre de E et l'espace vectoriel $F = \mathrm{Vect}(\mathcal{B}_{u,x})$ est u-stable.*

Théorème 37. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Alors il existe une base $\mathcal{B} = B_1 \cup \ldots \cup B_r$ de E telle que chaque s.e.v. $E_i = \mathrm{Vect}\, \mathcal{B}_i$ soit stable par u et que la matrice de $u|_{E_i}$ soit :*

$$J_i = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_{q_i}(\mathbb{K}), \text{ avec } q_i = \dim_{\mathbb{K}} E_i$$

Théorème 38. *Soit $u \in \mathcal{L}(E)$ non nul tel que $\chi_u = \prod_{i=1}^p (X-\lambda_i)^{\alpha_i}$ et $\Pi_u = \prod_{i=1}^p (X-\lambda_i)^{\beta_i}$. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u soit de la forme $A = \mathrm{Diag}(J_1, \ldots, J_\rho)$ avec pour tout $k \in [\![1, \rho]\!]$:*

$$J_k = \begin{pmatrix} \lambda_k & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & \lambda_k & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{k,\alpha_k-1} & \lambda_k & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}), \text{ où } \varepsilon_{k,i} \in \{0,1\}$$

III Applications

1) Décomposition de Dunford

Proposition 39. *Soient $f \in \mathcal{L}(E)$ et $F \in \mathbb{K}[X]$ un polynôme annulateur de f. Soit $F = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ la décomposition en facteurs irréductibles dans $\mathbb{K}[X]$ du polynôme F. Pour tout i, on note $N_i = \operatorname{Ker} M_i^{\alpha_i}(f)$. Alors :*

(i) $E = \bigoplus_{i=1}^{s} N_i$

(ii) Pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j\neq i} N_j$ est un polynôme en f.

Théorème 40 (Décomposition de Dunford)**.** *Soit $f \in \mathcal{L}(E)$ dont le polynôme caractéristique χ_f est scindé sur $\mathbb{K}$. Alors il existe un unique couple (n, d) d'endomorphismes tels que :*

(i) d est diagonalisable, n est nilpotent

(ii) $f = d + n$ et n et d commutent

De plus, d et n sont des polynômes en f

Application 41. *Soit $A \in \mathcal{M}_n(\mathbb{K})$ tel que χ_A est scindé sur $\mathbb{K}$. Soit $A = D + N$ sa décomposition de Dunford, alors la décomposition de Dunford de e^A est donnée par $e^A = e^D + e^D(e^N - I_n)$ avec e^D diagonalisable et $e^D(e^N - I)$ nilpotente.*

2) Applications en calcul matriciel

Soit $A \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique $\chi_A(X) = \sum_{i=0}^{n} \beta_i X^i$.

Proposition 42. *Soit P un polynôme annulateur de A. En effectuant la division euclidienne de X^k par P, on a $X^k = PQ + R$, donc $A^k = R(A)$. En particulier, on peut prendre $P = \chi_A$.*

Exemple 43. *Si $A = \left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, alors $A^2 - A - 2I_3 = 0$. Il vient alors que $A^k = a_k A + b_k I_3$ par la proposition. Comme -1 et 2 sont valeurs propres de A, on a $(-1)^k = -a_k + b_k$ et $2^k = 2a_k + b_k$. On en déduit que :*

$$A^k = \frac{2^k + (-1)^{k+1}}{3} A + \frac{2^k + 2(-1)^k}{3} I_3$$

Proposition 44. *Si A est inversible, alors $\det A = \beta_0 \neq 0$, et :*

$$A^{-1} = -\frac{1}{a_0}\left(\sum_{i=1}^{n} \beta_i A^{i-1}\right)$$

Exemple 45. *Si $A = \left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, alors $A^2 - A - 2I_3 = 0$, puis $A\left(\frac{1}{2}(A - I_3)\right) = I_3$. Il vient alors que $A^{-1} = \frac{1}{2}(A - I_3)$.*

Proposition 46. *Soit $A = D + N$ la décomposition de Dunford de A :*

$$\exp(A) = \exp(D)\exp(N)$$

où $\exp(D)$ est calculé par diagonalisation, et $\exp(N)$ est une somme finie.

Exemple 47. *Si $A = \left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right)$, alors :*

$$\exp(A) = \begin{pmatrix} e^3 & 0 \\ 0 & e^3 \end{pmatrix}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}\right) = \begin{pmatrix} e^3 & 2e^3 \\ 0 & e^3 \end{pmatrix}$$

Développements

- Réduction de Jordan (par la dualité) (36,37,38) [Rom20]
- Décomposition de Dunford (39,40) [Gou94]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[FGN13b] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 2.* Cassini
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck

Cadre : Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^\star$. Soit F un sous-espace vectoriel de E. Soit $u \in \mathcal{L}(E)$.

I Généralités sur les sous-espaces stables

1) Définitions et premières propriétés

Définition 1. On dit que F est stable par u si $u(F) \subset F$.

Exemple 2. *(i)* $\mathrm{Im}(u)$ *et* $\mathrm{Ker}(u)$ *sont stables par* u.
(ii) Les sous-espaces propres de u *sont stables par* u.
(iii) Si u *est une homothétie, tous les sous-espaces de* E *sont stables.*

Proposition 3. *Soient* $u, v \in \mathcal{L}(E)$ *qui commutent. Alors :*
(i) Tout sous-espace propre de u *est stable par* v.
(ii) $\mathrm{Im}(u)$ *et* $\mathrm{Ker}(u)$ *sont stables par* v.

Exemple 4. *Les sous-espaces caractéristiques de* u *sont stables par* u.

Corollaire 5. *Pour tout* $P \in \mathbb{K}[X]$, $\mathrm{Ker}(P(u))$ *et* $\mathrm{Im}(P(u))$ *sont stables par* u.

Corollaire 6. *Soit* p *un projecteur. Alors* F *est stable par* p *si, et seulement si,* F *est la somme directe d'un sous-espace de* $\mathrm{Im}(p)$ *et d'un sous-espace de* $\mathrm{Ker}(p)$.

Proposition 7. *(i) Si* F *est stable par* $u, v \in \mathcal{L}(E)$, *alors il est stable par* $u + v$ *et par* $u \circ v$.
(ii) Si F *et* G *sont deux sous-espaces vectoriels de* E *stables par* u, *alors* $F + G$ *et* $F \cap G$ *sont stables par* u.

Application 8. *Si* u *stabilise toutes les droites vectorielles de* E, *alors* u *est une homothétie.*

2) Endomorphismes induits et bases adaptées

Proposition 9. *On suppose* F *stable par* u. *Alors* u *induit deux endomorphismes* $u|_F \in \mathcal{L}(F)$ *et* $\overline{u} \in \mathcal{L}(E/F)$ *obtenu par passage au quotient :*

$$\begin{array}{ccccc} F & \hookrightarrow & E & \twoheadrightarrow & E/F \\ {\scriptstyle u|_F}\downarrow & & {\scriptstyle u}\downarrow & & {\scriptstyle \overline{u}}\downarrow \\ F & \hookrightarrow & E & \twoheadrightarrow & E/F \end{array}$$

Proposition 10. *On suppose* F *stable par* u *avec* $\dim F = r$. *Soit* $\mathcal{B} = \mathcal{B}_F \sqcup \mathcal{B}'$ *une base de* E, *dont les* r *premiers vecteurs forment une base* $\mathcal{B}_F$ *de* F. *Alors la matrice de* u *dans la base* $\mathcal{B}$ *est de la forme* $\mathrm{Mat}_{\mathcal{B}}(u) = \left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$ *avec* $A = \mathrm{Mat}_{\mathcal{B}_F}(u|_F)$ *et* $C = \mathrm{Mat}_{\pi(\mathcal{B}')}(\overline{u})$. *De plus,* $\chi_u = \chi_{u|_F}\chi_{\overline{u}}$. *Réciproquement, une matrice triangulaire par blocs fournit des sous-espaces stables.*

Proposition 11. *On suppose* F *stable par* u. *Alors :*
(i) $\chi_{u|_F}$ *divise* χ_u.
(ii) $\pi_{u|_F}$ *divise* π_u.

Proposition 12. χ_u *est irréductible si, et seulement si, les seuls sous-espaces de* E *stables par* u *sont* $\{0\}$ *et* E.

Application 13. *Soient* $u, v \in \mathcal{L}(E)$ *et* $w = uv - vu$. *Supposons que* $\mathrm{rg}(w) = 1$. *Alors* χ_u *n'est pas irréductible dans* $\mathbb{K}[X]$.

3) Dualité et sous-espaces stables

Définition 14. Pour $A \subseteq E$ et $B \subseteq E^\star$, on note :
(i) $A^\perp = \{\varphi \in E^\star \,|\, \forall x \in A, \varphi(x) = 0\}$ l'orthogonal de A dans $E^\star$.
(ii) $B^\circ = \{x \in E \,|\, \forall \varphi \in B, \varphi(x) = 0\}$ l'orthogonal de B dans E.

Proposition 15. *On a* $\dim F + \dim F^\perp = \dim E$.

Proposition 16. *(i) Si* $A_1 \subset A_2 \subset E$, $A_2^\perp \subset A_1^\perp$.
(ii) Si $B_1 \subset B_2 \subset E^\star$, $B_2^\circ \subset B_1^\circ$.
(iii) Si $A \subset E$, $A^\perp = (\mathrm{Vect}\, A)^\perp$.
(iv) Si $B \subset E^\star$, $B^\circ = (\mathrm{Vect}\, B)^\circ$.

Définition 17. Soient G un $\mathbb{K}$-espace vectoriel et $u \in \mathcal{L}(E, G)$. L'application ${}^t u : G^\star \to E^\star$ définie pour $f \in E^\star$ par ${}^t u(f) = f \circ u$ est appelée transposée de u.

Proposition 18. *Soit* $u \in \mathcal{L}(E)$. *Alors* F *est stable par* u *si, et seulement si,* $F^\perp$ *est stable par* ${}^t u$.

Application 19. u *est trigonalisable si, et seulement si,* χ_u *est scindé sur* $\mathbb{K}$.

II Application à la réduction

1) Diagonalisation et trigonalisation

Théorème 20 (Lemme des noyaux)**.** *Soient $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

$$\operatorname{Ker} P(f) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(f)$$

Corollaire 21. *(i) E est somme directe de ses sous-espaces stables.*

(ii) u est diagonalisable si, et seulement si, il existe $P \in \mathbb{K}[X]$ scindé à racines simples tel que $P(u) = 0$.

Corollaire 22. *Soit F un sous-espace vectoriel de E stable par u. Supposons u diagonalisable (resp. trigonalisable). Alors $u|_F$ est diagonalisable (resp. trigonalisable).*

Théorème 23 (Co-réduction)**.** *Soit $(u_i)_{i\in I}$ une famille d'endomorphismes de E commutant deux à deux. Si les u_i sont diagonalisables (resp. trigonalisables), alors on peut les diagonaliser (resp. trigonaliser) dans une même base.*

2) Décomposition de Dunford

Proposition 24. *Soient $f \in \mathcal{L}(E)$ et $F \in \mathbb{K}[X]$ un polynôme annulateur de f. Soit $F = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ la décomposition en facteurs irréductibles dans $\mathbb{K}[X]$ du polynôme F. Pour tout i, on note $N_i = \operatorname{Ker} M_i^{\alpha_i}(f)$. Alors :*

(i) $E = \bigoplus_{i=1}^{s} N_i$

(ii) Pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j\neq i} N_j$ est un polynôme en f.

Théorème 25 (Décomposition de Dunford)**.** *Soit $f \in \mathcal{L}(E)$ dont le polynôme caractéristique χ_f est scindé sur $\mathbb{K}$. Alors il existe un unique couple (n, d) d'endomorphismes tels que :*

(i) d est diagonalisable, n est nilpotent

(ii) $f = d + n$ et n et d commutent

De plus, d et n sont des polynômes en f

Application 26. *Soit $A \in \mathcal{M}_n(\mathbb{K})$ tel que χ_A est scindé sur $\mathbb{K}$. Soit $A = D + N$ sa décomposition de Dunford, alors la décomposition de Dunford de e^A est donnée par $e^A = e^D + e^D(e^N - I_n)$ avec e^D diagonalisable et $e^D(e^N - I)$ nilpotente.*

3) Réduction de Jordan pour les nilpotents

Lemme 27. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Pour tout $x \in E$ tel que $u^{q-1}(x) \neq 0$, la famille $\mathcal{B}_{u,x} = (u^k(x))_{1\leqslant k\leqslant q-1}$ est une famille libre de E et l'espace vectoriel $F = \operatorname{Vect}(\mathcal{B}_{u,x})$ est u-stable.*

Théorème 28. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Alors il existe une base $\mathcal{B} = B_1 \cup \ldots \cup B_r$ de E telle que chaque s.e.v. $E_i = \operatorname{Vect} \mathcal{B}_i$ soit stable par u et que la matrice de $u|_{E_i}$ soit :*

$$J_i = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_{q_i}(\mathbb{K}), \text{ avec } q_i = \dim_{\mathbb{K}} E_i$$

Théorème 29. *Soit $u \in \mathcal{L}(E)$ non nul tel que $\chi_u = \prod_{i=1}^{p}(X - \lambda_i)^{\alpha_i}$ et $\Pi_u = \prod_{i=1}^{\rho}(X - \lambda_i)^{\beta_i}$. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u soit de la forme $A = \operatorname{Diag}(J_1, \dots, J_\rho)$ avec pour tout $k \in [\![1, \rho]\!]$:*

$$J_k = \begin{pmatrix} \lambda_k & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & \lambda_k & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{k,\alpha_k-1} & \lambda_k & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}), \text{ où } \varepsilon_{k,i} \in \{0, 1\}$$

4) Réduction des endomorphismes normaux

Soit $u \in \mathcal{L}(E)$ un endomorphisme normal.

Lemme 30. *Si F est un sous-espace vectoriel de E stable par u, alors F et $F^\perp$ sont stables par u et $u^\star$.*

Lemme 31. *Si $n = 2$, alors il existe une base orthonormée telle que :*

(i) u est diagonalisable si u a une valeur propre réelle.

(ii) sa matrice est de la forme $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ sinon.

Théorème 32. *Il existe une base orthonormée $\mathcal{B}$ de E telle que :*

$$\operatorname{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & \\ & \ddots & & 0 & \\ & & \lambda_r & & \\ & & & \tau_1 & \\ & 0 & & & \ddots \\ & & & & & \tau_s \end{pmatrix} \text{ avec } \begin{cases} n = r + 2s \\ \lambda_1, \dots, \lambda_r \in \mathbb{R} \\ \tau_k = \left(\begin{smallmatrix} a_k & -b_k \\ b_k & a_k \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R}) \end{cases}$$

III Théorie des représentations

Soient G un groupe fini de cardinal n et V un $\mathbb{C}$-espace vectoriel de dimension finie d.

Définition 33. Une représentation linéaire de G dans V est un morphisme $\rho : G \to \mathcal{GL}(V)$. On notera souvent ρ_s au lieu de $\rho(s)$. On dit que V est un espace de représentation de G. Le degré de ρ est $d = \dim V$.

Exemple 34. *La représentation triviale la représentation de degré 1 :*

$$\rho : \left| \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ s & \longmapsto & 1 \end{array} \right.$$

Exemple 35. *On suppose que $d = n$. Soit $(e_t)_{t\in G}$ une base de V. La représentation suivante est appelée représentation régulière :*

$$R : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{GL}(V) \\ s & \longmapsto & (e_t \mapsto e_{st}) \end{array} \right.$$

Définition 36. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire, et soit W un sous-espace vectoriel de V stable par G (donc stable par ρ_s pour tout $s \in G$). On définit alors une sous-représentation de ρ par :

$$\rho|_W : \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{GL}(W) \\ s & \longmapsto & p_s|_W \end{array} \right.$$

Définition 37. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. Si $V = \bigoplus_{i=1}^{r} V_i$, on dit alors que ρ est la somme directe des $\rho_i = \rho|_{V_i}$, que l'on note $\rho = \bigoplus_{i=1}^{r} \rho_i$.

Définition 38. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. On dit qu'elle est irréductible si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel non trivial de V n'est stable par G.

Remarque 39. *Toute représentation de degré 1 est irréductible.*

Théorème 40. *Toute représentation linéaire est somme directe de représentations irréductibles.*

Proposition 41 (Lemme de Schur)**.** *Soient $\rho^1 : G \to \mathcal{GL}(V_1)$ et $\rho^2 : G \to \mathcal{GL}(V_2)$ deux représentations irréductibles de G. Soit $f : V_1 \to V_2$ une application linéaire telle que, pour tout $s \in G$, $\rho^2_s \circ f = f \circ \rho^1_s$. Alors :*

(i) Si ρ^1 et ρ^2 ne sont pas isomorphes, alors $f = 0$.

(ii) Si $V_1 = V_2$ et $\rho^1 = \rho^2$, alors f est une homothétie.

Développements

- Décomposition de Dunford (24,25) [Gou94]
- Réduction de Jordan (par la dualité) (27,28,29) [Rom20]
- Réduction des endomorphismes normaux (30,31,32) [Gou94]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann

Cadre : E est un $\mathbb{K}$-ev de dimension finie. $u \in \mathcal{L}(E)$ est identifié à sa matrice dans une base appropriée.

I Diagonalisation

1) Éléments propres

Définition 1. Soit $\lambda \in \mathbb{K}$, le scalaire λ est appelée valeur propre de u s'il existe $x \in E \setminus \{0\}$ tel que $u(x) = \lambda x$. On dit alors que x est un vecteur propre de u associé à λ.
On appelle spectre de u, noté $\mathrm{Sp}(u)$, l'ensemble des valeurs propres de u.

Remarque 2. *(i) 0 est valeur propre de u ssi $\operatorname{Ker} u \neq \{0\}$.*

(ii) Pour $A \in \mathcal{M}_n(\mathbb{K})$, on dit que $X \in \mathbb{K}^n$ est vecteur propre de A associé à la valeur propre $\lambda \in \mathbb{K}$. On note également $\mathrm{Sp}(A)$ le spectre de A. Si A est la matrice d'un endomorphisme u, $\mathrm{Sp}(u) = \mathrm{Sp}(A)$.

Définition 3. Soit λ une valeur propre de u. On définit E_λ par :

$$E_\lambda = \{x \in E \mid u(x) = \lambda x\} = \operatorname{Ker}(u - \lambda Id_E)$$

E_λ est un sous-espace vectoriel de E stable par u, appelé sous-espace propre de u associé à la valeur propre λ.

Proposition 4. *Soient $\lambda_1, \dots, \lambda_k$ des valeurs propres distinctes de u, alors les sous-espaces propres $E_{\lambda_1}, \dots, E_{\lambda_k}$ sont en somme directe.*

2) Polynôme annulateur, polynôme minimal

Définition 5. Soit $P(X) = \sum_{i=0}^{p} a_i X^i \in \mathbb{K}[X]$.
Pour tout $f \in \mathcal{L}(E)$, on note :

$$P(f) = \sum_{i=0}^{p} a_i f^i \in \mathcal{L}(E) \text{ où } f^k = \underbrace{f \circ \ldots \circ f}_{k \text{ fois}}$$

Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, on note :

$$P(A) = \sum_{i=0}^{p} a_i A^i \in \mathcal{M}_n(\mathbb{K})$$

Définition 6. L'application suivante est un morphisme de $\mathbb{K}$-algèbre :

$$\varphi_u : \left| \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathcal{L}(E) \\ X & \longmapsto & u \end{array} \right.$$

On note $\mathbb{K}[u]$ son image.

Remarque 7. *Comme $\mathbb{K}[X]$ est une algèbre commutative, $\mathbb{K}[u]$ aussi.*

Théorème 8 (Lemme des noyaux)**.** *Soient $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

$$\operatorname{Ker} P(f) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(f)$$

Proposition 9. *Si $f \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$, alors $\lambda \in \mathrm{Sp}(f) \Leftrightarrow \pi_f(\lambda) = 0$.*

3) Polynôme caractéristique

Définition 10. Soit $A \in \mathcal{M}_n(\mathbb{K})$. On appelle polynôme caractéristique de A le polynôme de $\mathbb{K}[X]$ défini par :

$$\chi_A(X) = \det(A - XI_n)$$

Remarque 11. *(i)* $\chi_A(0) = \det A$

(ii) Une matrice a même polynôme caractéristique que a transposée.

(iii) Deux matrices semblables ont même polynôme caractéristique.

Exemple 12. *Si $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$, alors $\chi_A(X) = X^2 - 5X - 2$.*

Définition 13. Soit $u \in \mathcal{L}(E)$. On appelle polynôme caractéristique de u le polynôme caractéristique de la matrice de u, on le note χ_u.

Proposition 14. *λ est valeur propre de u ssi $\chi_u(\lambda) = 0$.*

Remarque 15. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. On peut écrire :*

$$\chi_A(X) = \sum_{i=0}^{n} \beta_i X^i \text{ où } \beta_0 = (-1)^n \det A,\ \beta_{n-1} = -\operatorname{tr} A,\ \beta_n = 1$$

Proposition 16. *Soit $f \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$ tel que $P(f) = 0$.*
Si λ est valeur propre de f, alors $P(\lambda) = 0$.

Remarque 17. *χ_f et π_f ont les mêmes racines.*

Exemple 18. *(i) Si f est nilpotent d'ordre n, $\pi_f(X) = X^n = \chi_f(X)$.*

(ii) Si f est l'application nulle, $\pi_f(X) = X$ et $\chi_f(X) = X^n$.

Théorème 19 (Cayley-Hamilton)**.** *Pour $f \in \mathcal{L}(E)$, $\chi_f(f) = 0$.*

4) Diagonalisabilité et critères de diagonalisabilité

Définition 20. Un endomorphisme est dit diagonalisable s'il existe une base dans laquelle sa matrice est diagonale. Une matrice est diagonalisable si l'endomorphisme associé est diagonalisable.

Remarque 21. *Une matrice est diagonalisable si, et seulement si, elle est semblable à une matrice diagonale.*

Théorème 22. *Soit $u \in \mathcal{L}(E)$, les assertions suivantes sont équivalentes :*

(i) *u est diagonalisable*

(ii) *Il existe une base de E formés de vecteurs propres de u.*

(iii) *E est somme directe des espaces propres de u.*

Théorème 23. *Soit $u \in \mathcal{L}(E)$, les assertions suivantes sont équivalentes :*

(i) *u est diagonalisable*

(ii) *χ_u est scindé à racines simples sur $\mathbb{K}$.*

(iii) *Il existe $P \in \mathbb{K}[X] \setminus \{0\}$ scindé à racines simples tel que $P(u) = 0$.*

Corollaire 24. *Si u est diagonalisable, alors pour tout sous-espace V de E stable par u, l'endomorphisme induit $u|_V \in \mathcal{L}(V)$ est diagonalisable.*

Application 25. *Un endomorphisme est diagonalisable si, et seulement si, il admet un polynôme annulateur scindé à racines simples sur $\mathbb{K}$.*

Théorème 26. *u est diagonalisable si, et seulement si, χ_u est scindé et la multiplicité de chaque valeur propre est égale à la dimension de l'espace propre associé.*

II Résultats de diagonalisabilité

1) Codiagonalisabilité

Proposition 27. *Soient $u, v \in \mathcal{L}(E)$ tels que $u \circ v = v \circ u$, alors :*

(i) *Tout sous-espace propre de u est stable par v.*

(ii) $\operatorname{Im} u$ *est stable par v.*

Théorème 28. *Soient $u, v \in \mathcal{L}(E)$ diagonalisables tels que $u \circ v = v \circ u$, alors il existe une base commune de diagonalisation de u et v. On dit que u et v sont codiagonalisables.*

Application 29. *$\mathcal{GL}_n(\mathbb{R})$ et $GL_m(\mathbb{R})$ sont isomorphes en tant que groupes si, et seulement si, $n = m$.*

2) Endomorphisme symétrique

Définition 30. Soit E un espace euclidien, et soit $u \in \mathcal{L}(E)$ autoadjoint, alors u est un endomorphisme symétrique. On note $S(E)$ l'ensemble des endomorphismes sur E symétriques, et $\mathcal{S}_n(\mathbb{R})$ l'ensemble des matrices symétriques réelles. On a $M \in \mathcal{S}_n(\mathbb{R}) \Leftrightarrow {}^tM = M$.

Théorème 31. *$u \in S(E)$ est diagonalisable dans une base orthogonale.*

Remarque 32. *Le résultat est faux dans $\mathcal{S}_n(\mathbb{C})$.*

Exemple 33. *Pour $M = \begin{pmatrix} 1 & j & j^2 \\ j & j & 1 \\ j^2 & 1 & j^2 \end{pmatrix}$, on a $M^2 = 0$. Donc si M était diagonalisable, M serait nulle. M n'est donc pas diagonalisable.*

3) Corps finis

Théorème 34. *Soit $\mathbb{F}_q$ un corps fini de cardinal q, E un $\mathbb{F}_q$-espace vectoriel et $u \in \mathcal{L}(E)$. u est diagonalisable si, et seulement si, $X^q - X$ est un polynôme annulateur de u.*

III Applications

1) Résolution de systèmes linéaires

Théorème 35. *Soit $M \in \mathcal{M}_n(\mathbb{K})$ diagonalisable, alors $M^k = PD^kP^{-1}$.*

Exemple 36. *Si $A = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix}$, alors $A^k = \begin{pmatrix} 2\times 2^k - 3 & 2^k - 3^k \\ -2\times 2^k + 2\times 3^k & -2^k + 2\times 3^k \end{pmatrix}$.*

Application 37. *Système linéaire de suites récurrentes :*
$$Si \begin{cases} u_{n+1} = u_n - v_n \\ v_{n+1} = 2u_n + 4v_n \end{cases} \quad et \begin{cases} u_0 = 2 \\ v_0 = 1 \end{cases} \quad alors \begin{cases} u_n = 3 \times 2^{n+1} - 4 \times 3^n \\ v_n = -3 \times 2^n + 4 \times 3^n \end{cases}.$$

Application 38. *Système différentiel linéaire à coefficients constants :*
$$Si \begin{cases} \frac{dx}{dt} = x - y \\ \frac{dy}{dt} = 2x + 4y \end{cases} \quad alors \begin{cases} x = C_1 e^{2t} + C_2 e^{3t} \\ y = C_1 e^{2t} - C_2 e^{3t} \end{cases}.$$

2) Décomposition de Dunford

Proposition 39. *Soient $f \in \mathcal{L}(E)$ et $F \in \mathbb{K}[X]$ un polynôme annulateur de f. Soit $F = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ la décomposition en facteurs irréductibles dans $\mathbb{K}[X]$ du polynôme F. Pour tout i, on note $N_i = \operatorname{Ker} M_i^{\alpha_i}(f)$. Alors :*

(i) $E = \bigoplus_{i=1}^{s} N_i$

(ii) Pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j\neq i} N_j$ est un polynôme en f.

Théorème 40 (Décomposition de Dunford)**.** *Soit $f \in \mathcal{L}(E)$ dont le polynôme caractéristique χ_f est scindé sur $\mathbb{K}$. Alors il existe un unique couple (n, d) d'endomorphismes tels que :*

(i) d est diagonalisable, n est nilpotent

(ii) $f = d + n$ et n et d commutent

De plus, d et n sont des polynômes en f

Application 41. *Soit $A \in \mathcal{M}_n(\mathbb{K})$ tel que χ_A est scindé sur $\mathbb{K}$. Soit $A = D + N$ sa décomposition de Dunford, alors la décomposition de Dunford de e^A est donnée par $e^A = e^D + e^D(e^N - I_n)$ avec e^D diagonalisable et $e^D(e^N - I)$ nilpotente.*

3) Réduction des endomorphismes normaux

Soit $u \in \mathcal{L}(E)$ un endomorphisme normal.

Lemme 42. *Si F est un sous-espace vectoriel de E stable par u, alors F et $F^\perp$ sont stables par u et $u^\star$.*

Lemme 43. *Supposons que $n = 2$. Alors :*

(i) Si u a une valeur propre réelle, u est diagonalisable dans une base orthonormée.

(ii) Si u n'a pas de valeur propre réelle, la matrice de u dans une base orthonormée est de la forme $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$.

Théorème 44. *Il existe une base orthonormée $\mathcal{B}$ de E telle que :*

$$\operatorname{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & 0 & \\ & & \lambda_r & & & \\ & & & \tau_1 & & \\ & 0 & & & \ddots & \\ & & & & & \tau_s \end{pmatrix}$$

où $n = r + 2s$, $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$ et $\tau_k = \left(\begin{smallmatrix} a_k & -b_k \\ b_k & a_k \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R})$ pour $k \in [\![1, s]\!]$.

Développements

- Décomposition de Dunford (39,40) [Gou94]
- Réduction des endomorphismes normaux (42,43,44) [Gou94]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K

Cadre : $\mathbb{K}$ est le corps $\mathbb{R}$ ou $\mathbb{C}$, et $n \in \mathbb{N}^\star$. On munit $\mathcal{M}_n(\mathbb{K})$ d'une norme d'algèbre $\|.\|$.

I Définitions et premières propriétés

1) Définition

Proposition 1. *Si $A \in \mathcal{M}_n(\mathbb{K})$, la série $\sum \frac{A^k}{k!}$ converge normalement sur tout compact de $\mathcal{M}_n(\mathbb{K})$.*

Définition 2. On définit l'application exponentielle comme suit :

$$\exp : \left| \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ A & \longmapsto & \exp(A) = \sum_{k=0}^{\infty} \frac{A^k}{k!} \end{array} \right.$$

Corollaire 3. exp *est une application continue.*

Exemple 4. *(i)* $\exp(O_n) = I_n$ *et* $\exp(I_n) = eI_n$

(ii) $$\exp\left(\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}\right) = \begin{pmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix}$$

(iii) Si N est nilpotente d'indice k, $\exp(N) = \sum_{i=0}^{k-1} \frac{N^i}{i!}$.

2) Propriétés de l'exponentielle de matrices

Proposition 5. *(i)* $AB = BA \Rightarrow \exp(A+B) = \exp(A)\exp(B)$

(ii) $\forall P \in \mathcal{GL}_n(\mathbb{K}), \forall A \in \mathcal{M}_n(\mathbb{K}), \exp(PAP^{-1}) = P\exp(A)P^{-1}$

(iii) $\exp({}^{\mathrm{t}}A) = {}^{\mathrm{t}}\exp(A)$ *et* $\exp(\overline{A}) = \overline{\exp(A)}$

Contre-exemple 6. *Si* $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *et* $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, *alors on a* $\exp(A+B) = \begin{pmatrix} \cosh(1) & \sinh(1) \\ \sinh(1) & \cosh(1) \end{pmatrix}$ *différent de* $\exp(A)\exp(B) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

Proposition 7. *(i) Si $A \in \mathcal{M}_n(\mathbb{K})$, alors $\exp(A) \in \mathcal{GL}_n(\mathbb{K})$ et* $(\exp(A))^{-1} = \exp(-A)$.

(ii) $\exp(A)$ *est un polynôme en A.*

Proposition 8. $Sp(\exp(A)) = \exp(Sp(A))$

Corollaire 9. $\det(\exp(A)) = \exp(\mathrm{tr}(A))$

Corollaire 10. *Si N est nilpotente, alors* $\exp(N) - I_n$ *est nilpotente.*

Proposition 11. *Si $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable, si $(\lambda_i)_{1 \leqslant i \leqslant n}$ sont ses valeurs propres distinctes, et si $P \in \mathbb{K}[X]$ vérifie $P(\lambda_i) = e^{\lambda_i}$, alors* $\exp(A) = P(A)$.

3) Méthode de calcul

Exemple 12. *Si* $A_\theta = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}$, *alors* $\exp(A_\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

Définition 13. Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ admet une décomposition de Dunford s'il existe D diagonalisable dans $\mathcal{M}_n(\mathbb{K})$ et N nilpotente telles que $DN = ND$ et $A = D + N$.

Théorème 14. *Si le polynôme caractéristique de A est scindé, alors A admet une unique décomposition de Dunford sur $\mathbb{K}$.*

Remarque 15. *En particulier, c'est le cas pour toute matrice de $\mathcal{M}_n(\mathbb{C})$.*

Proposition 16. *Soit A de décomposition de Dunford $A = D+N$, alors :*

$$\exp(A) = \exp(D)\exp(N) = \exp(D) + \exp(D)(\exp(N) - I_n)$$

Corollaire 17. *Soit $A \in \mathcal{M}_n(\mathbb{K})$ telle que χ_A est scindé sur $\mathbb{K}$, alors A est diagonalisable si, et seulement si,* $\exp(A)$ *l'est.*

Exemple 18. *Calcul d'un bloc de Jordan de taille k :*

$$\exp\begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} = e^\lambda \begin{pmatrix} 1 & \frac{1}{1!} & \cdots & \frac{1}{(k-1)!} \\ & \ddots & \ddots & \vdots \\ & & \ddots & \frac{1}{1!} \\ 0 & & & 1 \end{pmatrix}$$

Corollaire 19. *Si χ_A est scindé sur $\mathbb{K}$, on peut calculer* $\exp(A)$ *à l'aide d'une décomposition de Jordan.*

II Étude de l'application exponentielle

1) Injectivité et surjectivité

Proposition 20. exp *n'est pas injective.*

Exemple 21. $\exp\left(\left(\begin{smallmatrix} 0 & -2\pi \\ 2\pi & 0 \end{smallmatrix}\right)\right) = \exp(0) = I_2$

Lemme 22. *Pour* $A \in \mathcal{M}_n(\mathbb{C})$, $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.

Théorème 23. $\exp(\mathcal{M}_n(\mathbb{C})) = \mathcal{GL}_n(\mathbb{C})$

Théorème 24. $\exp(\mathcal{M}_n(\mathbb{R})) = \left\{A^2 \,\middle|\, A \in \mathcal{GL}_n(\mathbb{R})\right\}$

Application 25. *(i)* $\mathcal{GL}_n(\mathbb{C})$ *est connexe par arcs.*
(ii) Si $A \in \mathcal{GL}_n(\mathbb{C})$, *alors il existe* $B \in \mathcal{GL}_n(\mathbb{C})$ *telle que* $A = B^p$.

2) Régularité

Proposition 26. *L'application* $\exp : \mathcal{M}_n(\mathbb{K}) \to \mathcal{GL}_n(\mathbb{K})$ *est* $\mathcal{C}^\infty$.

Remarque 27. *La différentielle de* exp *en 0 est l'identité.*

Définition 28. Comme $d_0 \exp = Id$, exp est un $\mathcal{C}^1$-difféomorphisme local sur un voisinage de 0. Plus précisément, on peut définir son inverse sur la boule ouverte centrée en I_n de rayon 1. Si $||H|| < 1$, on pose :

$$\exp^{-1}(I_n + H) = \log(I_n + H) = -\sum_{k \geqslant 1} \frac{(-H)^k}{k}$$

Proposition 29. *Pour* $X, H \in \mathcal{M}_n(\mathbb{K})$, *on a :*

$$d_X \exp(H) = e^X \sum_{k=0}^{\infty} \frac{(-ad\, X)^k}{(k+1)!} H \quad où \quad ad\, X(H) = XH - HX$$

Corollaire 30. *Si* $X, H \in \mathcal{M}_n(\mathbb{K})$ *commutent,* $d_X \exp(H) = e^X H$.

Proposition 31. $t \mapsto \exp(tA)$ *est dérivable de dérivée* $t \mapsto A\exp(tA)$.

III Applications

1) Équations différentielles linéaires

Définition 32. Un système différentiel linéaire du premier ordre dans $\mathbb{K}^n$ est une équation de la forme $Y' = AY + B$, où $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{K}^n$ et $A : I \to \mathcal{M}_n(\mathbb{K})$ et $B : I \to \mathbb{K}^n$ sont continues sur un intervalle I de $\mathbb{R}$.

Théorème 33. *Par tout point* $(t_0, V_0) \in I \times \mathbb{K}^n$ *il passe une solution maximale unique, définie sur* I *tout entier.*

Proposition 34. *Pour* $A \in \mathcal{M}_n(\mathbb{R})$, *la solution du problème de Cauchy* $Y'(t) = A \cdot Y(t)$ *et* $Y(t_0) = V_0$ *est donnée par :*

$$Y(t) = \exp\left((t - t_0)A\right) \cdot V_0$$

Proposition 35. *Pour* $A \in \mathcal{M}_n(\mathbb{R})$ *et* $B : I \to \mathbb{K}^n$, *la solution du problème de Cauchy* $Y'(t) = A \cdot Y(t) + B(t)$ *et* $Y(t_0) = V_0$ *est donnée par :*

$$Y(t) = \exp\left((t - t_0)A\right) \cdot V_0 + \int_{t_0}^{t} \exp((t-u)A)B(u)du$$

2) Exponentielle de matrices et topologie

Théorème 36 (Décompostion polaire)**.** $\mathcal{GL}_n(\mathbb{R}) \cong \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$

Théorème 37. $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ *est un homéomorphisme.*

Corollaire 38. $\mathcal{GL}_n(\mathbb{R}) \cong \mathcal{O}_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$

Développements

- Décomposition de Dunford (14) [Gou94]
- Surjectivité de l'exponentielle de matrice (22,23,24) [Zav13]
- Un homéomorphisme induit par l'exponentielle (37,38) [CG13]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini
[Zav13] M. Zavidovique. *Un Max de Math.* Calvage et Mounet
[Dem06] J.-P. Demailly. *Analyse numérique et équations différentielles.* EDP Sciences
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet

Cadre : $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^\star$.

I Endomorphismes trigonalisables

1) Premiers outils de réduction

Définition 1. Soit $u \in \mathcal{L}(E)$. Il existe un unique polynôme unitaire π_u qui engendre l'idéal de $\mathbb{K}[X]$ formé des polynômes annulateurs de u. On l'appelle polynôme minimal de u.

Définition 2. Soit $u \in \mathcal{L}(E)$. On appelle polynôme caractéristique de u, noté χ_u, le polynôme défini par $\chi_u(X) = \det(u - Xid_E)$.

Théorème 3 (Cayley-Hamilton)**.** *Pour $u \in \mathcal{L}(E)$, $\chi_u(u) = 0$.*

Définition 4. Les racines de χ_u dans $\mathbb{K}$ sont appelées valeurs propres de u. On note $\mathrm{Sp}(u)$ l'ensemble des valeurs propres. Pour $\lambda \in \mathrm{Sp}(u)$, on note $E_\lambda = \mathrm{Ker}(u - \lambda id_E)$ l'espace propre de u par rapport à λ.

Théorème 5 (Lemme des noyaux)**.** *Soient $u \in \mathcal{L}(E)$ et $P = P_1 \dots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

$$\mathrm{Ker}\, P(u) = \bigoplus_{i=1}^{k} \mathrm{Ker}\, P_i(u)$$

2) Définition et caractérisation

Définition 6. Soit $u \in \mathcal{L}(E)$. On dit que u est trigonalisable s'il existe une base $\mathcal{B}$ de E telle que $\mathrm{Mat}_{\mathcal{B}}(u)$ soit triangulaire supérieure.

Définition 7. Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est dite trigonalisable si A est semblable à une matrice triangulaire supérieure.

Remarque 8. *Il est équivalent de dire qu'un endomorphisme est trigonalisable et que sa matrice dans une base l'est.*

Théorème 9. *Soit $u \in \mathcal{L}(E)$. Sont équivalentes :*

(i) u est trigonalisable

(ii) Il existe un polynôme annulateur scindé sur $\mathbb{K}$.

(iii) Le polynôme minimal π_u est scindé sur $\mathbb{K}$.

(iv) Le polynôme caractéristique χ_u est scindé sur $\mathbb{K}$.

Corollaire 10. *Soit $u \in \mathcal{L}(E)$ trigonalisable. La restriction de u à un sous-espace stable par u est encore trigonalisable.*

Corollaire 11. *Dans le cas où $\mathbb{K}$ est algébriquement clos, tout endomorphisme est trigonalisable.*

Exemple 12. $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *est $\mathbb{C}$-trigonalisable mais pas $\mathbb{R}$-trigonalisable.*

Corollaire 13. *Soit $A \in \mathcal{M}_n(\mathbb{K})$ trigonalisable et $\{\lambda_1, \dots, \lambda_n\}$ son spectre. Alors* $\mathrm{tr}\, A = \sum_{i=1}^n \lambda_i$ *et* $\det A = \prod_{i=1}^n \lambda_i$.

3) Trigonalisation simultanée

Proposition 14. *Soient $u, v \in \mathcal{L}(E)$ tels que $uv = vu$. Alors :*

(i) Tout sous-espace propre de v est stable par u.

(ii) $\mathrm{Im}\, v$ *est stable par u.*

Théorème 15 (Triangulation simultanée)**.** *Soient $u_1, \dots, u_n \in \mathcal{L}(E)$ commutant entre eux deux à deux. On suppose que les u_i sont tous trigonalisables. Alors il existe une base de E dans laquelle les matrices des u_i sont toutes triangulaires supérieures. On dit alors que les u_i sont cotrigonalisables.*

Proposition 16. *Soient $u, v \in \mathcal{L}(E)$. Si u et v commutent et sont trigonalisables, alors $u + v$ et uv sont trigonalisables.*

4) Propriétés topologiques

On considère $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 17. On note :

(i) $D_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \,|\, M \text{ est diagonalisable}\}$

(ii) $T_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \,|\, M \text{ est trigonalisable}\}$

(iii) $C_n(\mathbb{K}) = \{M \in D_n(\mathbb{K}) \,|\, M \text{ a } n \text{ valeurs propres distinctes}\}$

Proposition 18. *Dans l'espace topologique $T_n(\mathbb{K})$, on a :*

(i) $\overline{C_n(\mathbb{K})} = T_n(\mathbb{K})$

(ii) $C_n(\mathbb{K}) = \overset{\circ}{D_n}(\mathbb{K})$

Proposition 19. *$T_n(\mathbb{R})$ est un fermé de $\mathcal{M}_n(\mathbb{R})$.*

Proposition 20. *$C_n(\mathbb{R})$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.*

II Endomorphismes nilpotents

1) Définition et caractérisation

Définition 21. Soit $u \in \mathcal{L}(E)$. u est dit nilpotent s'il existe $p \in \mathbb{N}$ tel que $u^p = 0$. On note $\mathcal{N}(E)$ l'ensemble des éléments nilpotents de $\mathcal{L}(E)$.

Exemple 22. *La dérivation $P \mapsto P'$ dans l'espace $\mathbb{K}_n[X]$ des polynômes de degré inférieur ou égal à n est nilpotente. Ceci est faux quand on considère la dérivation dans $\mathbb{K}[X]$.*

Définition 23. Soit $u \in \mathcal{N}(E)$. On appelle indice de nilpotence de u le plus petit entier $p \in \mathbb{N}$ tel que $u^p = 0$.

Remarque 24. *D'après le théorème de Cayley-Hamilton, l'indice de nilpotence de $u \in \mathcal{N}(E)$ est inférieur à n.*

Proposition 25. *Soit $u \in \mathcal{N}(E)$ d'indice p. Il existe $x_0 \in E$ tel que la famille $(x_0, u(x_0), \dots, u^{p-1}(x_0))$ soit libre.*

Proposition 26. *Soit $u \in \mathcal{L}(E)$. Sont équivalentes :*

(i) u *est nilpotent.*

(ii) $\chi_u(X) = X^n$

(iii) $\pi_u(X) = X^p$ *avec* $p \in [\![1, n]\!]$

(iv) u *est trigonalisable et sa seule valeur propre est 0.*

Dans ce cas, u est d'indice de nilpotence p.

Exemple 27. *Soit* $A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$. *On a alors* $\chi_A(X) = X(X^2 - 1)$. *La seule valeur propre de A sur $\mathbb{R}$ est 0, mais A n'est pas trigonalisable.*

Proposition 28. *Si $\mathbb{K}$ est de caractéristique nulle, alors u est nilpotent si, et seulement si,* $\operatorname{tr}(u^k) = 0$ *pour tout* $k \in [\![1, n]\!]$.

Exemple 29. *Si* $\operatorname{car} \mathbb{K} = p > 0$, *alors I_p vérifie la condition précédente sans être nilpotente pour autant.*

2) Structure de $\mathcal{N}(E)$

Proposition 30. *Si $u \in \mathcal{N}(E)$, alors $\lambda u \in \mathcal{N}(E)$ pour tout $\lambda \in \mathbb{K}$. On dit que $\mathcal{N}(E)$ est un cône.*

Remarque 31. *$\mathcal{N}(E)$ n'est pas stable par addition. Ce n'est pas un idéal de $\mathcal{L}(E)$, ni même un sous-espace vectoriel.*

Exemple 32. $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ *n'est pas nilpotente.*

Exemple 33. *Supposons E de dimension 2. Soit $M \in \mathcal{M}_2(\mathbb{K})$. Alors $\chi_M(X) = X^2 - \operatorname{tr}(M)X + \det(M)$. Donc M est nilpotente si, et seulement si,* $\operatorname{tr}(M) = \det(M) = 0$. *En écrivant* $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, *cela revient à $a = -d$ et $ad = bc$. Pour $\mathbb{K} = \mathbb{R}$, on peut voir $\mathcal{N}(E)$ comme le cône d'équation $a^2 + bc = 0$ dans l'espace de dimension 3 des matrices de trace nulle de $\mathcal{M}_2(\mathbb{R})$.*

Proposition 34. *Soient $u, v \in \mathcal{N}(E)$ et $f \in \mathcal{L}(E)$.*

(i) Si u et v commutent, alors $u + v \in \mathcal{N}(E)$.

(ii) Si u et f commutent, alors $uf = fu \in \mathcal{N}(E)$.

III Applications à la réduction

1) Décomposition de Dunford

Proposition 35. *Soient $f \in \mathcal{L}(E)$ et $F \in \mathbb{K}[X]$ un polynôme annulateur de f. Soit $F = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ la décomposition en facteurs irréductibles dans $\mathbb{K}[X]$ du polynôme F. Pour tout i, on note $N_i = \operatorname{Ker} M_i^{\alpha_i}(f)$. Alors :*

(i) $E = \bigoplus_{i=1}^{s} N_i$

(ii) Pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en f.

Théorème 36 (Décomposition de Dunford)**.** *Soit $f \in \mathcal{L}(E)$ dont le polynôme caractéristique χ_f est scindé sur $\mathbb{K}$. Alors il existe un unique couple (n, d) d'endomorphismes tels que :*

(i) d est diagonalisable, n est nilpotent

(ii) $f = d + n$ et n et d commutent

De plus, d et n sont des polynômes en f

2) Réduction de Jordan pour les nilpotents

Définition 37. Soit $\lambda \in \mathbb{K}$ une valeur propre de $u \in \mathcal{L}(E)$. On appelle sous-espace caractéristique de u associé à λ l'espace $N_\lambda = \mathrm{Ker}(u-\lambda Id_E)^\alpha$, où α est la multiplicité de λ dans χ_u.

Proposition 38. *Soit $u \in \mathcal{L}(E)$.*
Supposons que $\chi_u = \prod_{i=1}^{p}(X-\lambda_i)^{\alpha_i}$ et $\pi_u = \prod_{i=1}^{\rho}(X-\lambda_i)^{\beta_i}$, alors :

(i) $E = \bigoplus_{k=1}^{\rho} N_k$, $\dim_{\mathbb{K}} N_k = \alpha_k$, $N_k = Ker(u-\lambda_k Id_E)^{\beta_k}$

(ii) $(u-Id_E)|_{N_k}$ *est nilpotent d'indice* β_k.

(iii) N_k *est stable par* u *et* λ_k *est la seule valeur propre de* $u|_{N_k}$.

Lemme 39. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Pour tout $x \in E$ tel que $u^{q-1}(x) \neq 0$, la famille $\mathcal{B}_{u,x} = (u^k(x))_{1\leqslant k\leqslant q-1}$ est une famille libre de E et l'espace vectoriel $F = \mathrm{Vect}(\mathcal{B}_{u,x})$ est u-stable.*

Théorème 40. *Soit $u \in \mathscr{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Alors il existe une base $\mathcal{B} = B_1 \cup \ldots \cup B_r$ de E telle que chaque s.e.v. $E_i = \mathrm{Vect}\,\mathcal{B}_i$ soit stable par u et que la matrice de $u|_{E_i}$ soit :*

$$J_i = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_{q_i}(\mathbb{K}), \text{ avec } q_i = \dim_{\mathbb{K}} E_i$$

Théorème 41. *Soit $u \in \mathscr{L}(E)$ non nul tel que $\chi_u = \prod_{i=1}^{p}(X-\lambda_i)^{\alpha_i}$ et $\Pi_u = \prod_{i=1}^{\rho}(X-\lambda_i)^{\beta_i}$. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u soit de la forme :*

$$A = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_\rho \end{pmatrix}$$

avec pour tout $k \in [\![1,\rho]\!]$:

$$J_k = \begin{pmatrix} \lambda_k & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & \lambda_k & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{k,\alpha_k-1} & \lambda_k & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}), \text{ où } \varepsilon_{k,i} \in \{0,1\}$$

Développements

— Décomposition de Dunford (35,36) [Gou94]
— Réduction de Jordan (par la dualité) (39,40,41) [Rom20]

Références

[Gri11] J. Grifone. *Algèbre Linéaire.* Cépaduès, 4e édition
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck

Cadre : Soit $\mathbb{K}$ un corps commutatif et soit $n \in \mathbb{N}^\star$.

I Généralités

1) Définitions et premières propriétés

Définition 1. $A \in \mathcal{M}_n(\mathbb{K})$ est symétrique lorsque ${}^tA = A$. On note $\mathcal{S}_n(\mathbb{K})$ l'ensemble des matrices symétriques à coefficients dans $\mathbb{K}$.

Définition 2. $A \in \mathcal{M}_n(\mathbb{K})$ est hermitienne lorsque $A^\star = {}^t\overline{A} = A$. On note $H_n(\mathbb{K})$ l'ensemble des matrices hermitiennes à coefficients dans $\mathbb{K}$.

Exemple 3. $\left(\begin{smallmatrix}1&2\\2&8\end{smallmatrix}\right) \in \mathcal{S}_2(\mathbb{R})$, $\left(\begin{smallmatrix}1&i\\-i&1\end{smallmatrix}\right) \in \mathcal{H}_2(\mathbb{C})$, $\left(\begin{smallmatrix}1&i\\i&-1\end{smallmatrix}\right) \in \mathcal{S}_2(\mathbb{R})$

Définition 4. $A \in \mathcal{M}_n(\mathbb{K})$ est orthogonale lorsque ${}^tAA = I_n$. On note $O_n(\mathbb{K})$ l'ensemble des matrices orthogonales à coefficients dans $\mathbb{K}$.

Définition 5. $A \in \mathcal{M}_n(\mathbb{K})$ est unitaire lorsque $A^\star A = {}^t\overline{A}A = I_n$. On note $\mathcal{U}_n(\mathbb{K})$ l'ensemble des matrices unitaires à coefficients dans $\mathbb{K}$.

Définition 6. $A \in \mathcal{M}_n(\mathbb{K})$ est définie positive lorsque ${}^t\overline{X}AX > 0$ pour tout $X \in \mathbb{R}^n \setminus \{0\}$.

Définition 7. $A \in \mathcal{M}_n(\mathbb{K})$ est antisymétrique lorsque ${}^tA = -A$. On note $\mathcal{A}_n(\mathbb{K})$ l'ensemble des matrices antisymétriques à coefficients dans $\mathbb{K}$.

Proposition 8. *Si* $\mathrm{car}(\mathbb{K}) \neq 2$, *alors* $\mathcal{M}_n(\mathbb{K}) = \mathcal{S}_n(\mathbb{K}) \oplus \mathcal{A}_n(\mathbb{K})$ *et* $\mathcal{H}_n(\mathbb{C}) = \mathcal{S}_n(\mathbb{R}) \oplus i\mathcal{A}_n(\mathbb{R})$.

Remarque 9. *La famille* $((E_{i,i})_{1\leqslant i\leqslant n}, (E_{i,j}+E_{j,i})_{1\leqslant i<j\leqslant n})$ *est une base de* $\mathcal{S}_n(\mathbb{K})$. *La famille* $(E_{i,j}-E_{j,i})_{1\leqslant i<j\leqslant n}$ *est une base de* $\mathcal{A}_n(\mathbb{K})$.

Remarque 10. $H_n(\mathbb{C})$ *est un* $\mathbb{R}$*-espace vectoriel de dimension* n^2, *mais ce n'est pas un* $\mathbb{C}$*-espace vectoriel.*

Exemple 11. $\left(\begin{smallmatrix}1&2\\5&7\end{smallmatrix}\right) = \frac{1}{2}\left(\begin{smallmatrix}2&7\\7&14\end{smallmatrix}\right) + \frac{1}{2}\left(\begin{smallmatrix}0&-3\\3&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1&i\\-i&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) + i\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$

2) Lien avec les formes bilinéaires symétriques

Définition 12. Soient E un $\mathbb{K}$-espace vectoriel et $\phi : E \times E \to \mathbb{K}$. ϕ est une forme bilinéaire symétrique sur E lorsque $x \mapsto \phi(x,y)$ et $y \mapsto \phi(x,y)$ sont linéaires et, pour tous $x, y \in E$ on a $\phi(x,y) = \phi(y,x)$.

Définition 13. Soient E un $\mathbb{K}$-espace vectoriel et $\phi : E \times E \to \mathbb{K}$. ϕ est une forme sesquilinéaire hermitienne sur E lorsque $x \mapsto \phi(x,y)$ est linéaire, $y \mapsto \overline{\phi(x,y)}$ est antilinéaire et que, pour tous $x, y \in E$ on a $\phi(x,y) = \overline{\phi(y,x)}$.

Exemple 14. *La forme suivante est sesquilinéaire hermitienne :*

$$\begin{array}{ccc} (\mathcal{C}([0,1],\mathbb{C}))^2 & \longrightarrow & \mathbb{C} \\ (f,g) & \longmapsto & \int_0^1 \overline{f(t)}g(t)\,dt \end{array}$$

Proposition 15. *Supposons* E *de dimension finie. Soit* $\mathcal{B} = (e_1, \ldots, e_n)$ *une base de* E. *On note* $M = (\phi(e_i, e_j))_{1\leqslant i,j\leqslant n}$, *où* $\phi : E \times E \to \mathbb{K}$ *est bilinéaire ou sesquilinéaire.* M *est appelée matrice le* ϕ *dans la base* $\mathcal{B}$. *De plus,* ϕ *est symétrique si, et seulement si,* M *est symétrique, et* ϕ *est hermitienne si, et seulement si,* M *est hermitienne.*

3) Endomorphismes adjoints

Définition 16. Une forme bilinéaire symétrique définie positif sur E est appelée produit scalaire. Une forme sesquilinéaire hermitienne définie positif sur E est appelée produit hermitien.

Exemple 17. *La forme suivante est un produit scalaire :*

$$\begin{array}{ccc} \mathbb{R}^n \times \mathbb{R}^n & \longrightarrow & \mathbb{R} \\ \left(\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix}, \begin{pmatrix}y_1\\\vdots\\y_n\end{pmatrix}\right) & \longmapsto & \sum_{i=1}^n x_i y_i \end{array}$$

Définition 18. Un $\mathbb{R}$-espace vectoriel E est euclidien s'il est de dimension finie et s'il est muni d'un produit scalaire, noté $\langle .,. \rangle$. Un $\mathbb{C}$-espace vectoriel E est hermitien s'il est de dimension finie et s'il est muni d'un produit hermitien, noté $\langle .,. \rangle$.

Définition 19. Soit E un espace euclidien ou hermitien, et soient $f, g \in \mathcal{L}(E)$. f et g sont dits adjoints lorsque :

$$\forall\, x, y \in E,\ \langle f(x), y\rangle = \langle x, g(y)\rangle$$

Pour $f \in \mathcal{L}(E)$ donné, il existe au plus un endomorphisme adjoint à f, qu'on appelle adjoint de f, et qu'on note $f^\star$. Lorsque $f = f^\star$, on dit que f est autoadjoint.

Proposition 20. *Soit* $\mathcal{B}$ *une base orthonormée de* E, *et* $f \in \mathcal{L}(E)$. *Alors* $f^\star$ *existe et* $Mat_{\mathcal{B}}(f^\star) = Mat_{\mathcal{B}}(f)^\star$.

Proposition 21. *Soient E un espace euclidien. Alors $f \in \mathcal{L}(E)$ est autoadjoint si, et seulement si, sa matrice est symétrique.*

Proposition 22. *Soient E un espace hermitien. Alors $f \in \mathcal{L}(E)$ est autoadjoint si, et seulement si, sa matrice est hermitienne.*

Exemple 23.

$$f : \left| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & \begin{pmatrix} x+3y \\ 2x+8y \end{pmatrix} \end{array} \right. \Rightarrow \quad f^\star : \left| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & \begin{pmatrix} x+2y \\ 3x+8y \end{pmatrix} \end{array} \right.$$

II Propriétés des matrices symétriques et hermitiennes

1) Réduction des endomorphismes autoadjoints

Proposition 24. *Soient E un espace euclidien ou hermitien, et f un endomorphisme autoadjoint. Si F est un sous-espace vectoriel stable par f, alors $F^\perp$ est stable par f.*

Théorème 25. *Soient E un espace euclidien ou hermitien, et f un endomorphisme autoadjoint. Alors il existe une base orthonormée de vecteur propre pour f, les valeurs propres de f étant réelles.*

Corollaire 26. *Soit $M \in \mathcal{S}_n(\mathbb{R})$, alors il existe une matrice $C \in \mathcal{O}_n(\mathbb{R})$ telle que ${}^tCMC$ est diagonale réelle.*

Corollaire 27. *Soit $M \in H_n(\mathbb{C})$, alors il existe une matrice $U \in \mathcal{U}_n(\mathbb{R})$ telle que $U^\star MU$ est diagonale réelle.*

Exemple 28. *Si $A = \left(\begin{smallmatrix} 1 & i \\ -i & 1 \end{smallmatrix}\right)$ et $U = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right)$, alors $U^\star AU = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 2 \end{smallmatrix}\right)$.*

Contre-exemple 29. $\left(\begin{smallmatrix} 1 & i \\ i & -1 \end{smallmatrix}\right) \in \mathcal{S}_2(\mathbb{C})$ *n'est pas diagonalisable.*

Corollaire 30. *(i) Si $M \in \mathcal{M}_n(\mathbb{R})$, $M \in \mathcal{S}_n^{++}(\mathbb{R}) \Leftrightarrow \mathrm{Sp}(M) \subset \mathbb{R}^{+\star}$*
(ii) Si $M \in \mathcal{M}_n(\mathbb{C})$, $M \in \mathcal{H}_n^{++}(\mathbb{C}) \Leftrightarrow \mathrm{Sp}(M) \subset \mathbb{R}^{+\star}$

Proposition 31. *Soit $M = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{S}_n(\mathbb{R})$. Pour $k \in [\![1, n]\!]$, on note $M_k = (a_{i,j})_{1 \leqslant i,j \leqslant k} \in \mathcal{S}_k(\mathbb{R})$. M est définie positive si, et seulement si, $\forall\, k \in [\![1, n]\!]$, $\det(M_k) > 0$.*

Corollaire 32. *Soient $M, N \in \mathcal{S}_n(\mathbb{R})$ (resp. $H_n(\mathbb{C})$), telles que la matrice M soit définie positive. Alors il existe une matrice C inversible telle que $C^\star MC = I_n$ et $C^\star NC$ est diagonale réelle.*

Lemme 33. *Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ symétriques définies positives distinctes, et $\alpha, \beta > 0$ tels que $\alpha + \beta = 1$, alors :*

$$\det(\alpha A + \beta B) > \det(A)^\alpha \det(B)^\beta$$

Application 34 (Ellipsoïde de John-Loewner)**.** *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant K.*

2) Décomposition polaire

Lemme 35. *Si deux matrices sont diagonalisables et commutent, alors elles sont diagonalisables dans une même base.*

Théorème 36 (Décomposition polaire)**.** *On a les homéomorphismes :*

$$\begin{array}{ccccccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) & \quad & \mathcal{U}_n(\mathbb{R}) \times \mathcal{H}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O, S) & \longmapsto & OS & & (U, H) & \longmapsto & UH \end{array}$$

Corollaire 37. *Pour $A \in \mathcal{GL}_n(\mathbb{R})$, on a $\|A\|_2^2 = \rho({}^tAA)$.*

Lemme 38. *Pour tout $M \in \mathcal{S}_n^{++}(\mathbb{R})$, on a $\|M\|_2 = \rho(M)$.*

Théorème 39. $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ *est un homéomorphisme.*

Corollaire 40. $\mathcal{GL}_n(\mathbb{R}) \cong \mathcal{O}_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$

III Application à l'optimisation

1) Résolution de systèmes linéaires

Théorème 41. *Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. Posons :*

$$J : \left| \begin{array}{ccc} \mathbb{R}^n & \longrightarrow & \mathbb{R} \\ X & \longmapsto & \frac{1}{2}\langle AX, X\rangle - \langle b, X\rangle + c \end{array} \right.$$

Minimiser J sur $\mathbb{R}^n$ revient à résoudre le système linéaire $AX = b$.

Théorème 42 (Décomposition de Choleski)**.** *Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$. Il existe une unique matrice $P \in \mathcal{M}_n(\mathbb{R})$ triangulaire supérieure à coefficients diagonaux strictement positifs telle que $A = {}^tPP$.*

2) Algorithmes

Théorème 43 (Méthode du gradient à pas variable)**.** *On reprend la fonctionnelle quadratique J définie précédemment. Soit $(\rho^k)_{k\in\mathbb{N}}$ une suite réelle. On considère la suite $(u^k)_{k\in\mathbb{N}}$ définie par :*

$$\begin{cases} u^0 \in \mathbb{R}^n \text{ donné} \\ u^{k+1} = u^k - \rho^k \nabla J(u^k) \end{cases}$$

On note λ_1 et λ_n respectivement la plus petite et la plus grande valeur propre de A. La suite $(u^k)_{k\in\mathbb{N}}$ converge vers $u^\star \in \mathbb{R}^n$ réalisant le minimum de J si $0 < \rho^k < \frac{2}{\lambda_n}$, le meilleur choix étant $\rho^k = \frac{2}{\lambda_1+\lambda_n}$.

Théorème 44 (Méthode du gradient à pas optimal)**.** *Soit J une fonctionnelle définie sur $\mathbb{R}^n$ de classe $\mathcal{C}^1$. On considère les suites $(\rho^k)_{k\in\mathbb{N}}$ et $(u^k)_{k\in\mathbb{N}}$ définies par :*

$$\begin{cases} u^0 \in \mathbb{R}^n \text{ donné} \\ \rho^k \text{ minimise } \rho \mapsto J\left(u^k - \rho \nabla J(u^k)\right) \\ u^{k+1} = u^k - \rho^k \nabla J(u^k) \end{cases}$$

Dans le cas de la fonctionnelle quadratique, cet algorithme converge vers $u^\star \in \mathbb{R}^n$ réalisant le minimum de J si $A \in \mathcal{S}_n^{++}(\mathbb{R})$. On a alors :

$$\rho^k = \frac{\left\|\nabla J(u^k)\right\|^2}{\langle A \nabla J(u^k), \nabla J(u^k)\rangle}$$

Développements

- Décomposition polaire (36,37) [CG13]
- Ellipsoïde de John-Loewner (33,34) [FGN13c]
- Un homéomorphisme induit par l'exponentielle (38,39,40) [CG13]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson
[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3.* Cassini

Cadre : $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N}^\star$.

I Formes linéaires et espace dual

1) Généralités sur les formes linéaires

Définition 1. Une forme linéaire sur E est une application de E dans $\mathbb{K}$. On note $E^\star = \mathcal{L}(E, \mathbb{K})$ l'ensemble des formes linéaires sur E, appelé espace dual de E.

Exemple 2. *(i)* $(x_1, \dots, x_n) \mapsto x_k$ *est une forme linéaire sur* $\mathbb{K}^n$.

(ii) Pour $A \in \mathcal{M}_n(\mathbb{K})$, *l'application* $f_A : M \mapsto \mathrm{tr}(AM)$ *est une forme linéaire sur* $\mathcal{M}_n(\mathbb{K})$.

(iii) Si $\mathbb{K} = \mathbb{R}$ *et* $f : E \to \mathbb{R}$ *est différentiable en un point* a, *alors* $d_a f$ *est une forme linéaire.*

(iv) Le morphisme d'évaluation $ev_a : P \mapsto P(a)$ *en un point* $a \in \mathbb{K}$ *est un morphisme sur* $\mathbb{K}_n[X]$.

Proposition 3. *Le noyau d'une forme linéaire non nulle est un hyperplan de* E. *Réciproquement, tout hyperplan de* E *est le noyau d'une forme linéaire non nulle.*

Exemple 4. *Si* A *est non nulle,* $\{M \in \mathcal{M}_n(\mathbb{K}) \,|\, \mathrm{tr}(AM) = 0\}$ *est un hyperplan de* $\mathcal{M}_n(\mathbb{K})$.

2) Espace dual et base duale

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

Définition 5. On appelle base duale de $\mathcal{B}$ la famille $\mathcal{B}^\star = (e_1^\star, \dots, e_n^\star)$, où chaque $e_i^\star$ est défini par $e_i^\star(e_j) = \delta_{i,j}$ pour tous $i, j \in [\![1, n]\!]$.

Exemple 6. *Dans* $\mathbb{R}^2$, *si* $\mathcal{B} = ((1,0),(0,1))$, *alors* $\mathcal{B}^\star = (e_1^\star, e_2^\star)$ *avec* $e_1^\star : (x,y) \mapsto x$ *et* $e_2^\star : (x,y) \mapsto y$.

Proposition 7. *Toute base duale est une base de* $E^\star$. *En particulier,* $\dim(E) = \dim(E^\star)$, *et pour tout* $\varphi \in E^\star$ *on a* $\varphi = \sum_{i=1}^n \varphi(e_i) e_i^\star$.

Corollaire 8. *L'application suivante est un isomorphisme :*

$$\begin{array}{ccc} E & \longrightarrow & E^\star \\ x = \sum_{i=1}^n x_i e_i & \longmapsto & \varphi = \sum_{i=1}^n x_i e_i^\star \end{array}$$

Il n'est pas canonique car dépend de la base $\mathcal{B}$ *choisie.*

Théorème 9. *Soit* H *un espace de Hilbert. Alors pour toute application* $\phi \in H' = H^\star$, *il existe un unique* $f \in H$ *tel que, pour tout* $v \in H$, *on ait* $\phi(v) = \langle f, v \rangle$. *De plus,* $\phi \mapsto f$ *est une isométrie.*

Application 10. *Si* E *est l'espace euclidien (resp. hermitien)* $\mathbb{R}^n$ *(resp.* $\mathbb{C}^n$*) muni de son produit scalaire usuel, on a l'isomorphisme canonique de* E *dans* $E^\star$ *qui à* x *associe* $y \mapsto \langle x, y \rangle$.

Proposition 11. *L'application* $f : A \mapsto f_A$ *est un isomorphisme de* $\mathcal{M}_n(\mathbb{K})$ *dans son dual. De plus, toute forme linéaire* f *sur* $\mathcal{M}_n(\mathbb{K})$ *vérifiant* $f(XY) = f(YX)$ *et colinéaire à la trace.*

Application 12. *Si* $n \geqslant 2$, *tout hyperplan de* $\mathcal{M}_n(\mathbb{K})$ *coupe* $\mathcal{GL}_n(\mathbb{K})$.

3) Espace bidual et base antéduale

Définition 13. $E^{\star\star} = (E^\star)^\star$ est appelé espace bidual de E

Proposition 14. *On a un isomorphisme de* E *dans* $E^{\star\star}$ *donné par :*

$$\begin{array}{ccc} E & \longrightarrow & E^{\star\star} \\ x & \longmapsto & (f \mapsto f(x)) \end{array}$$

Proposition 15. *Soit* $\mathcal{B}^\star = (f_1, \dots, f_n)$ *une base de* $E^\star$. *Alors il existe une unique base* $\mathcal{B} = (e_1, \dots, e_n)$ *de* E *dont* $\mathcal{B}^\star$ *est la base duale.* $\mathcal{B}$ *est alors appelée base antéduale de* $\mathcal{B}^\star$.

Exemple 16. *Soient* $(x_i)_{0 \leqslant i \leqslant n}$ *une famille de points de* $\mathbb{K}$ *deux à deux distincts. Notons* $\ell_i = \prod_{i \neq j} \frac{X - x_j}{x_i - x_j} \in \mathbb{K}_n[X]$ *et* $\mathcal{B}^\star = (\ell_0, \dots, \ell_n)$ *la base de* $\mathbb{K}_n[X]^\star$ *des polynômes de Lagrange. Alors la base antéduale de* $\mathcal{B}$ *est* $(ev_{x_0}, \dots, ev_{x_n})$.

II Autour de l'orthogonalité

1) Notion d'orthogonalité

Définition 17. Pour $A \subseteq E$ et $B \subseteq E^\star$, on note :

(i) $A^\perp = \{\varphi \in E^\star \,|\, \forall x \in A, \varphi(x) = 0\}$ l'orthogonal de A dans $E^\star$.

(ii) $B^\circ = \{x \in E \,|\, \forall \varphi \in B, \varphi(x) = 0\}$ l'orthogonal de B dans E.

Proposition 18. *(i) Si* $A_1 \subset A_2 \subset E$, *on a* $A_2^\perp \subset A_1^\perp$.

(ii) Si $B_1 \subset B_2 \subset E^\star$, *on a* $B_2^\circ \subset B_1^\circ$.

Proposition 19. *(i) Si $A \subset E$, on a $A^\perp = (\mathrm{Vect}\, A)^\perp$.*

(ii) Si $B \subset E^\star$, on a $B^\circ = (\mathrm{Vect}\, B)^\circ$.

Proposition 20. *Soit F (resp. G) un sous-espace de E (resp. $E^\star$).*

(i) $\dim_{\mathbb{K}} F + \dim_{\mathbb{K}} F^\perp = \dim_{\mathbb{K}} E$ *et* $(F^\perp)^\circ = F$.

(ii) $\dim_{\mathbb{K}} G + \dim_{\mathbb{K}} G^\circ = \dim_{\mathbb{K}} E^\star$ *et* $(G^\circ)^\perp = G$.

Corollaire 21. *(i) Soient p formes linéaires $\varphi_1, \dots, \varphi_p$ de $E^\star$ de rang r. Alors $F = \bigcap_{i=1}^p \mathrm{Ker}(\varphi_i)$ est de dimension $n - r$.*

(ii) Si F est un sous-espace de dimension q, il existe $n - q$ formes linéairement indépendantes $\varphi_1, \dots, \varphi_p$ telles que $F = \bigcap_{i=1}^p \mathrm{Ker}(\varphi_i)$.

Proposition 22. *Soient A_1, A_2 (resp. B_1, B_2) deux sous-espaces vectoriels de E (resp. $E^\star$). Alors :*

(i) $(A_1 + A_2)^\perp = A_1^\perp \cap A_2^\perp$ *et* $(B_1 + B_2)^\circ = B_1^\circ \cap B_2^\circ$.

(ii) $(A_1 \cap A_2)^\perp = A_1^\perp + A_2^\perp$ *et* $(B_1 \cap B_2)^\circ = B_1^\circ + B_2^\circ$.

2) Transposée d'une application linéaire

On considère F un $\mathbb{K}$-espace vectoriel de dimension finie.

Définition 23. Soit $u \in \mathcal{L}(E, F)$. Pour tout $f \in E^\star$, on a $f \circ u \in E^\star$. On appelle transposée de u l'application :

$$ {}^{\mathrm{t}}u : \left| \begin{array}{ccc} F^\star & \longrightarrow & E^\star \\ f & \longmapsto & f \circ u \end{array} \right. $$

Remarque 24. *Pour tous $x \in E$ et $\varphi \in F^\star$, on a $\langle \varphi, u(x) \rangle = \langle {}^{\mathrm{t}}u(\varphi), x \rangle$.*

Proposition 25. *Soit $\mathcal{B}$ une base de E et $\mathcal{B}'$ une base de F. On a alors* $\mathrm{Mat}_{\mathcal{B}^\star, \mathcal{B}'^\star}({}^{\mathrm{t}}u) = {}^{\mathrm{t}}\mathrm{Mat}_{\mathcal{B}, \mathcal{B}'}(u)$ *et donc* $\mathrm{rg}({}^{\mathrm{t}}u) = \mathrm{rg}(u)$.

Corollaire 26. *En identifiant E et F à leurs biduaux, on a* ${}^{\mathrm{t}\,\mathrm{t}}u = u$.

Proposition 27. *(i)* ${}^{\mathrm{t}}(u \circ v) = {}^{\mathrm{t}}v \circ {}^{\mathrm{t}}u$

(ii) $\mathrm{Im}({}^{\mathrm{t}}u) = (\mathrm{Ker}(u))^\perp$

(iii) $\mathrm{Ker}({}^{\mathrm{t}}u) = (\mathrm{Im}(u))^\perp$

III Applications

1) Réduction de Jordan pour les nilpotents

Définition 28. Soit $\lambda \in \mathbb{K}$ une valeur propre de $u \in \mathcal{L}(E)$. On appelle sous-espace caractéristique de u associé à λ l'espace $N_\lambda = \mathrm{Ker}(u - \lambda Id_E)^\alpha$, où α est la multiplicité de λ dans χ_u.

Proposition 29. *Soit $u \in \mathcal{L}(E)$.*
Supposons que $\chi_u = \prod_{i=1}^p (X - \lambda_i)^{\alpha_i}$ et $\pi_u = \prod_{i=1}^\rho (X - \lambda_i)^{\beta_i}$, alors :

(i) $E = \bigoplus_{k=1}^{\rho} N_k$, $\dim_{\mathbb{K}} N_k = \alpha_k$, $N_k = Ker(u - \lambda_k Id_E)^{\beta_k}$

(ii) $(u - Id_E)|_{N_k}$ *est nilpotent d'indice* β_k.

(iii) N_k *est stable par u et λ_k est la seule valeur propre de* $u|_{N_k}$.

Lemme 30. *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Pour tout $x \in E$ tel que $u^{q-1}(x) \neq 0$, la famille $\mathcal{B}_{u,x} = (u^k(x))_{1 \leqslant k \leqslant q-1}$ est une famille libre de E et l'espace vectoriel $F = \mathrm{Vect}(\mathcal{B}_{u,x})$ est u-stable.*

Théorème 31. *Soit $u \in \mathscr{L}(E)$ un endomorphisme nilpotent d'indice $q \geqslant 1$. Alors il existe une base $\mathcal{B} = B_1 \cup \ldots \cup B_r$ de E telle que chaque s.e.v. $E_i = \mathrm{Vect}\, \mathcal{B}_i$ soit stable par u et que la matrice de $u|_{E_i}$ soit :*

$$ J_i = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_{q_i}(\mathbb{K}), \ \textit{avec } q_i = \dim_{\mathbb{K}} E_i $$

Théorème 32. *Soit $u \in \mathscr{L}(E)$ non nul tel que $\chi_u = \prod_{i=1}^p (X - \lambda_i)^{\alpha_i}$ et $\pi_u = \prod_{i=1}^\rho (X - \lambda_i)^{\beta_i}$. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u soit de la forme :*

$$ A = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_\rho \end{pmatrix} $$

avec pour tout $k \in [\![1, \rho]\!]$ *:*

$$J_k = \begin{pmatrix} \lambda_k & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & \lambda_k & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{k,\alpha_k-1} & \lambda_k & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}), \text{ où } \varepsilon_{k,i} \in \{0,1\}$$

2) Calcul différentiel

On se place sur $\mathbb{K} = \mathbb{R}$ et on considère $(E, \langle ., . \rangle)$ un espace euclidien.

Proposition 33. *Si* $f : E \to \mathbb{R}$ *est différentiable en* $a \in E$*, alors il existe un unique vecteur, appelé gradient de* f *en* a *et noté* $\nabla f(a)$*, tel que :*

$$\forall h \in E,\ d_a f(h) = \langle \nabla f(a), h \rangle$$

Application 34. *Géométriquement, le gradient s'interprète comme la direction de plus grande pente autour de* a*. C'est l'idée utilisée dans de nombreux algorithmes d'optimisation.*

Théorème 35 (Extrema liés)**.** *Soit* U *un ouvert de* $\mathbb{R}^n$*. Soient* $g_1, \dots, g_k$ *des fonctions de classe* $\mathcal{C}^1$ *de* U *dans* $\mathbb{R}$ *telles que les formes linéaires* $d_x g_1, \dots, d_x g_k$ *sont linéairement indépendantes pour tout* $x \in U$*. Posons :*

$$M = \{x \in U \,|\, \forall i \in [\![1, k]\!],\ g_i(x) = 0\}$$

Alors, si f *a un extremum lié en* $a \in M$*, il existe* $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ *tels que :*

$$d_a f = \sum_{i=1}^{k} \lambda_k \, d_a g_i$$

Ces réels $\lambda_1, \dots, \lambda_k$ *sont appelés multiplicateurs de Lagrange.*

Développements

- Réduction de Jordan (par la dualité) (30,31,32) [Rom20]
- Extrema liés (35) [Ave83]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Gri11] J. Grifone. *Algèbre Linéaire.* Cépaduès, 4e édition
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck
[Ave83] A. Avez. *Calcul différentiel.* Masson

Cadre : Soit $(E, \langle .,. \rangle)$ un $\mathbb{R}$-espace vectoriel euclidien de dimension finie $n \in \mathbb{N}^\star$. On note $\|.\|$ la norme issue du produit scalaire. Soit $\mathcal{B} = (e_i)_{i \in [\![1,n]\!]}$ une base orthonormée de E. Soient $u \in \mathcal{L}(E)$ et $A = \mathrm{Mat}_{\mathcal{B}}(u)$.

I Endomorphismes d'un espace euclidien

1) Adjoint d'un endomorphisme

Définition 1. Il existe un unique $v \in \mathcal{L}(E)$ tel que :

$$\forall\, x, y \in E,\ \langle u(x), y\rangle = \langle x, v(y)\rangle$$

On l'appelle adjoint de u, noté $u^\star$. On a de plus $\mathrm{Mat}_{\mathcal{B}}(u^\star) = {}^{\mathrm{t}}\mathrm{Mat}_{\mathcal{B}}(u)$.

Exemple 2.

$$f : \left|\begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & \begin{pmatrix} x+3y \\ 2x+8y \end{pmatrix} \end{array}\right. \Rightarrow f^\star : \left|\begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & \begin{pmatrix} x+2y \\ 3x+8y \end{pmatrix} \end{array}\right.$$

Proposition 3. *Soient $u, v \in \mathcal{L}(E)$, et $\lambda \in \mathbb{R}$. Alors :*

(i) $(u^\star)^\star = u$
(ii) $(u+v)^\star = u^\star + v^\star$
(iii) $(\lambda u)^\star = \lambda u^\star$
(iv) $(u \circ v)^\star = v^\star \circ u^\star$
(vi) $\mathrm{Ker}(u^\star) = \mathrm{Im}(u)^\perp$
(vii) $\mathrm{Im}(u^\star) = \mathrm{Ker}(u)^\perp$
(viii) $\mathrm{rg}(u^\star) = \mathrm{rg}(u)$
(ix) $|||u^\star||| = |||u|||$

Proposition 4. *Si $M \in \mathcal{M}_n(\mathbb{R})$ vérifie ${}^{\mathrm{t}}MM = 0$, alors $M = 0$.*

Proposition 5. *Si F est un sous-espace vectoriel de E qui est stable par u, alors $F^\perp$ est stable par $u^\star$.*

2) Exemples d'endomorphismes remarquables

Définition 6. On dit que u est orthogonal (ou une isométrie) si $u^\star = u^{-1}$, autrement dit, si u conserve le produit scalaire :

$$\forall\, x, y \in E,\ \langle u(x), u(y)\rangle = \langle x, y\rangle$$

On note $\mathcal{O}(E)$ l'ensemble des isométries de E.

Proposition 7. *$v : E \to E$ est orthogonal si, et seulement si, v est linéaire et conserve la norme.*

Exemple 8. *(i) Id_E et $-Id_E$ sont orthogonaux.*

(ii) Les rotations et les symétries orthogonales sont des isométries.

(iii) Les valeurs propres d'une isométrie ne peuvent être que ± 1.

Proposition 9. *u est orthogonal si, et seulement si, ${}^{\mathrm{t}}A = A^{-1}$.*

Définition 10. On dit que u est symétrique (ou auto-adjoint) si $u^\star = u$, autrement dit, si :

$$\forall\, x, y \in E,\ \langle u(x), y\rangle = \langle x, u(y)\rangle$$

On note $\mathcal{S}(E)$ l'ensemble des endomorphismes symétriques de E.

Définition 11. On dit que u est anti-symétrique si $u^\star = u$. On note $\mathcal{A}E$ l'ensemble des endomorphismes anti-symétriques de E.

Exemple 12. *(i) $u + u^\star$ est symétrique.*

(ii) Un projecteur orthogonal est symétrique.

Proposition 13. *(i) u est symétrique si, et seulement si, ${}^{\mathrm{t}}A = A$.*

(ii) u est anti-symétrique si, et seulement si, ${}^{\mathrm{t}}A = -A$.

Définition 14. On dit que u est symétrique (ou auto-adjoint) si u et $u^\star$ commutent.

Exemple 15. *Un endomorphisme auto-adjoint, antisymétrique ou orthogonal est normal.*

Proposition 16. *u est normal si, et seulement si, ${}^{\mathrm{t}}AA = A\,{}^{\mathrm{t}}A$.*

Proposition 17. *On a les caractérisations suivantes :*

	u	$A = \mathrm{Mat}_{\mathcal{B}}(u)$
symétrique	$u^\star = u$	${}^{\mathrm{t}}A = A$
anti-symétrique	$u^\star = -u$	${}^{\mathrm{t}}A = -A$
orthogonal	$u^\star = u^{-1}$	${}^{\mathrm{t}}A = A^{-1}$
normal	$u^\star u = uu^\star$	${}^{\mathrm{t}}AA = A\,{}^{\mathrm{t}}A$

II Endomorphismes auto-adjoints

1) Premières propriétés

Proposition 18. *$\mathcal{S}(E)$ est un sous-espace vectoriel de dimension $\frac{n(n+1)}{2}$.*

Définition 19. Soit $u \in \mathcal{S}(E)$, alors :

(i) u est dit positif si $\langle u(x), x\rangle \geqslant 0$ pour tout $x \in E$. On note $\mathcal{S}^+(E)$ l'ensemble des endomorphismes symétriques positifs.

(ii) u est dit défini positif si $\langle u(x), x\rangle > 0$ pour tout $x \in E$. On note $\mathcal{S}^{++}(E)$ l'ensemble des endomorphismes symétriques défini positifs.

Proposition 20. *Si $u \in \mathcal{S}(E)$, alors $\mathrm{Sp}(u) \subset \mathbb{R}$. Si $u \in \mathcal{S}^+(E)$, alors $\mathrm{Sp}(u) \subset \mathbb{R}^+$. Si $u \in \mathcal{S}^{++}(E)$, alors $\mathrm{Sp}(u) \subset \mathbb{R}^{+\star}$.*

Lemme 21. *Les sous-espaces propres associés à deux valeurs propres distinctes sont orthogonaux.*

Proposition 22. *Soit $A \in \mathcal{M}_{n,p}(\mathbb{R})$ de rang p avec $n \geqslant p$. Alors ${}^tAA \in \mathcal{S}_p^{++}(\mathbb{R})$.*

Application 23 (Moindre carrés)**.** *Soient $n, p \in \mathbb{N}$, $A \in \mathcal{M}_{n,p}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On cherche $x \in \mathbb{R}^p$ tel que $\|b - Ax\|_2 = \inf_{y\in\mathbb{R}^p} \|b - Ay\|_2$.*

(i) Il existe toujours une solution au problème.

(ii) $x \in \mathbb{R}^p$ est solution si, et seulement si, ${}^tAAx = {}^tAb$.

(iii) Si $n \geqslant p$ et $\mathrm{rg}(A) = p$, alors ${}^tAA$ est inversible, et il existe une unique matrice B triangulaire inférieure, à diagonale positive, telle que ${}^tAA = B\,{}^tB$. On a alors $x = (B\,{}^tB)^{-1}\,{}^tAb$ comme solution.

2) Autour du théorème spectral

Théorème 24 (Théorème spectral)**.** *Tout endomorphisme symétrique est diagonalisable dans une base orthonormée.*

Corollaire 25. *Soit $A \in \mathcal{S}_n(\mathbb{R})$. Il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que ${}^tPAP$ soit diagonale.*

Corollaire 26. *Soit $u \in \mathcal{S}(E)$. Alors $u \in \mathcal{S}^+(E)$ si, et seulement si, $\mathrm{Sp}(u) \subset \mathbb{R}^+$ et $u \in \mathcal{S}^{++}(E)$ si, et seulement si, $\mathrm{Sp}(u) \subset \mathbb{R}^{+\star}$.*

Application 27. *Pour $A \in \mathcal{S}_n(\mathbb{R})$, on a $|||A|||_2 = \rho(A)$.*

Application 28. *Pour $A \in \mathcal{S}_n^+(\mathbb{R})$, il existe une unique matrice $B \in \mathcal{S}_n^+(\mathbb{R})$ telle que $A = B^2$.*

Théorème 29. *$\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.*

III Endomorphismes normaux

Dans cette partie, u désigne un endomorphisme normal.

Proposition 30. *On a $\|u(x)\| = \|u^\star(x)\|$ pour tout $x \in E$.*

Application 31. *Les valeurs propres de u sont des complexes de module 1.*

Lemme 32. *Si F est un sous-espace vectoriel de E stable par u, alors F et $F^\perp$ sont stables par u et $u^\star$.*

Lemme 33. *Il existe un sous-espace vectoriel stable par u de dimension au plus 2.*

Lemme 34. *Si $\dim E = 2$, il existe une base orthonormée telle que :*

(i) u est diagonalisable si u a une valeur propre réelle.

(ii) sa matrice est de la forme $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ sinon.

Théorème 35. *Il existe une base orthonormée $\mathcal{B}$ de E telle que :*

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & 0 & \\ & & \lambda_r & & & \\ & & & \tau_1 & & \\ & 0 & & & \ddots & \\ & & & & & \tau_s \end{pmatrix} \text{ avec } \begin{cases} n = r + 2s \\ \lambda_1, \dots, \lambda_r \in \mathbb{R} \\ \tau_k = \left(\begin{smallmatrix} a_k & -b_k \\ b_k & a_k \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R}) \end{cases}$$

IV Endomorphismes orthogonaux

1) Propriétés et réductions

Proposition 36. *Soit $u \in \mathcal{O}(E)$. Alors :*

(i) $\mathrm{Sp}(u) \subset \mathbb{U} = \{z \in \mathbb{C} \,|\, |z| = 1\}$.

(ii) $\det(u) = \pm 1$. En particulier, u est inversible.

Proposition 37. *Soit $u \in \mathcal{L}(E)$. Alors $u \in \mathcal{O}(E)$ si, et seulement si, transforme toute base orthonormée en une base orthonormée.*

Théorème 38. *Soit $M \in \mathcal{O}_n(\mathbb{R})$, alors M est semblable à :*

$$\begin{pmatrix} I_r & & & & 0 \\ & -I_m & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_s} \end{pmatrix} \text{ avec } \begin{cases} \theta_i \in]0; 2\pi[\setminus \{\pi\} \\ R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \end{cases}$$

2) Étude en dimensions 2 et 3

Proposition 39 (Étude en dimension 2)**.** *Soient $u \in \mathcal{O}(\mathbb{R}^2)$ et A sa matrice dans la base canonique de $\mathbb{R}^2$.*

(i) Si $u \in \mathcal{O}^+(\mathbb{R}^2)$, alors il existe $\theta \in [0, 2\pi[$ tel que $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. u est alors la rotation d'angle θ centrée en l'origine.

(ii) Si $u \notin \mathcal{O}^+(\mathbb{R}^2)$, alors il existe $\theta \in [0, 2\pi[$ tel que $A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$. u est alors la symétrie par rapport à la droite d'angle polaire $\frac{\theta}{2}$.

Proposition 40 (Étude en dimension 3)**.** *Soient $u \in \mathcal{O}(\mathbb{R}^3)$. Il existe une base de $\mathbb{R}^3$ dans laquelle la matrice de u est :*

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}$$

pour un $\theta \in [0, 2\pi[$ et où $\varepsilon = \pm 1$. De plus :

(i) Si $u \in \mathcal{O}^+(\mathbb{R}^2)$, alors $\varepsilon = 1$. u est alors une rotation d'angle θ autour d'une droite.

(ii) Si $u \notin \mathcal{O}^+(\mathbb{R}^2)$, alors $\varepsilon = -1$. u est alors la composée d'une rotation d'angle θ autour d'une droite D puis d'une symétrie orthogonale par rapport à $D^\perp$.

3) Topologie du groupe orthogonal

Proposition 41. *$\mathcal{O}(E)$ est une partie compacte de $\mathcal{L}(E)$.*

Proposition 42. *Les composantes connexes de $\mathcal{O}(E)$ sont les fermés $\mathcal{O}^+(\mathbb{R}^2)$ et $\mathcal{O}^-(\mathbb{R}^2)$*

Théorème 43 (Décomposition polaire)**.** *On a les homéomorphismes :*

$$\begin{array}{ccccccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) & \quad & \mathcal{U}_n(\mathbb{R}) \times \mathcal{H}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O, S) & \longmapsto & OS & & (U, H) & \longmapsto & UH \end{array}$$

Corollaire 44. *Pour $A \in \mathcal{GL}_n(\mathbb{R})$, on a $|||A|||_2 = \sqrt{\rho({}^tAA)}$*

Corollaire 45. *Tout sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ qui contient le groupe orthogonal $\mathcal{O}_n(\mathbb{R})$ est le groupe $\mathcal{O}_n(\mathbb{R})$ lui-même.*

Développements

- Un homéomorphisme induit par l'exponentielle (29) [CG13]
- Réduction des endomorphismes normaux (32,34,35) [Gou94]
- Décomposition polaire (43) [CG13]

Références

[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie*. DeBoeck
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre*. Ellipses, 2e édition
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1*. Calvage et Mounet

Cadre : Soit $(E, \langle .,. \rangle)$ un $\mathbb{R}$-espace vectoriel euclidien de dimension finie $n \in \mathbb{N}^\star$, et soit $\mathcal{E}$ un espace affine dirigé par E. On note $\|.\|$ la norme issue du produit scalaire.

I Distances d'un espace affine euclidien

1) Définitions et premières propriétés

Définition 1. Un espace vectoriel muni d'un produit scalaire est dit espace vectoriel euclidien. Un espace affine euclidien est un espace affine dirigé par un espace vectoriel euclidien. On définit la distance de deux points A et B par $d(A,B) = \left\|\overrightarrow{AB}\right\| = AB$.

Proposition 2. *$(\mathcal{E}, d)$ définit bien un espace métrique.*

Définition 3. Pour $A \subset \mathcal{E}$ et $x \in \mathcal{E}$, on définit la distance de x à A par :

$$d(x,A) = \inf_{y \in A} d(x,y)$$

Proposition 4. *Soient $x \in E$ et F un sous-espace vectoriel de E. Alors $y \in E$ est la projection orthogonale de x sur F si, et seulement si, $y \in F$ et $d(x,F) = \|x - y\|$.*

2) Matrice et déterminant de Gram

Définition 5. On appelle matrice de Gram de $(x_i)_{1 \leqslant i \leqslant n}$ la matrice $M_G(x_1, \dots, x_n) = (\langle x_i, x_j \rangle)_{1 \leqslant i,j \leqslant n}$, et déterminant de Gram le déterminant de cette matrice, noté $G(x_1, \dots, x_n)$.

Lemme 6. *Le déterminant de Gram d'une famille de vecteurs est nul si, et seulement si, elle est liée.*

Théorème 7. *Soit F un sous-espace vectoriel de E de dimension finie $n \in \mathbb{N}^\star$ muni d'une base $(e_i)_{1 \leqslant i \leqslant n}$. Alors, pour tout $x \in E$, on a :*

$$d(x,F)^2 = \frac{G(e_1, \dots, e_n, x)}{G(e_1, \dots, e_n)}$$

Théorème 8 (Hadamard)**.** *(i) Soient $x_1, \dots, x_n$ des vecteurs de E. Alors $G(x_1, \dots, x_n) \leqslant \prod_{i=1}^n \|x_i\|^2$.*

(ii) Soient $x_1, \dots, x_n \in \mathbb{C}^n$. Alors $|\det(x_1, \dots, x_n)| \leqslant \prod_{i=1}^n \|x_i\|_2$.

Dans les deux cas, on a égalité si, et seulement si, $(x_i)_{1 \leqslant i \leqslant n}$ est orthogonale ou l'un des vecteurs est nul.

II Isométries d'un espace affine euclidien

1) Définitions et premières propriétés

Définition 9. Une isométrie vectorielle est une application linéaire qui conserve la norme. On note $\mathcal{O}(E)$ l'ensemble des isométries vectorielles de E dans E.

Remarque 10. *Une isométrie vectorielle conserve le produit scalaire, donc l'orthogonalité.*

Définition 11. Soient $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines euclidiens. Une isométrie affine est une application affine $\varphi : \mathcal{E} \to \mathcal{F}$ telle que $d(\varphi(A), \varphi(B)) = d(A,B)$ pour tous $A, B \in \mathcal{E}$. On note $\mathrm{Isom}(\mathcal{E})$ l'ensemble des isométries vectorielles de $\mathcal{E}$ dans $\mathcal{E}$.

Exemple 12. *Les translations, les rotations et les symétries orthogonales sont des isométries.*

Proposition 13. *Une application affine est une isométrie affine si, et seulement si, sa partie linéaire est une isométrie vectorielle.*

Théorème 14. *$(\mathcal{O}(E), \circ)$ et $(\mathrm{Isom}(\mathcal{E}), \circ)$ sont des groupes.*

Proposition 15. *Soit F un sous-espace vectoriel de E stable par une isométrie $f \in \mathcal{O}(E)$. Alors $F^\perp$ est stable par f.*

2) Structure des isométries

Définition 16. On appelle réflexion toute symétrie orthogonale par rapport à un hyperplan. Ce sont des isométries.

Théorème 17. *Toute isométrie de E peut s'écrire comme composée de p réflexions pour un entier $p \leqslant n$.*

Théorème 18. *Toute isométrie de $\mathrm{Isom}(\mathcal{E})$ peut s'écrire comme composée de p réflexions pour un entier $p \leqslant n+1$.*

Définition 19. On dit qu'une isométrie est un déplacement si son déterminant est positif. Une isométrie qui n'est pas un déplacement est un anti-déplacement.

Proposition 20. *(i) Les isométries sont des bijections.*

(ii) Les déplacements $\mathrm{Isom}^+(\mathcal{E})$ forment un sous-groupe de $\mathrm{Isom}(\mathcal{E})$.

(iii) Les déplacements préservent les orientations de l'espace.

III Groupe orthogonal

1) Propriétés et réductions

Proposition 21. *Soit $u \in \mathcal{L}(E)$, et soit M sa matrice dans une base de E. Alors $u \in \mathcal{O}(E)$ si, et seulement si, ${}^tMM = M\,{}^tM = I_n$.*

Proposition 22. *Soit $u \in \mathcal{O}(E)$. Alors :*

(i) $\mathrm{Sp}(u) \subset \mathbb{U} = \{z \in \mathbb{C} \,|\, |z| = 1\}$.

(ii) $\det(u) = \pm 1$. *En particulier, u est inversible.*

Proposition 23. *Soit $u \in \mathcal{L}(E)$. Alors $u \in \mathcal{O}(E)$ si, et seulement si, transforme toute base orthonormée en une base orthonormée.*

Théorème 24. *Soit $M \in \mathcal{O}_n(\mathbb{R})$, alors M est semblable à :*

$$\begin{pmatrix} I_r & & & & 0 \\ & -I_m & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_s} \end{pmatrix} \text{ avec } \begin{cases} \theta_i \in]0;2\pi[\setminus \{\pi\} \\ R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \end{cases}$$

2) Topologie du groupe orthogonal

Proposition 25. *$\mathcal{O}(E)$ est une partie compacte de $\mathcal{L}(E)$.*

Proposition 26. *Les composantes connexes de $\mathcal{O}(E)$ sont les fermés $\mathcal{O}^+(\mathbb{R}^2)$ et $\mathcal{O}^-(\mathbb{R}^2)$*

Théorème 27 (Décomposition polaire)**.** *On a les homéomorphismes :*

$$\begin{array}{ccccccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) & \quad & \mathcal{U}_n(\mathbb{R}) \times \mathcal{H}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O,S) & \longmapsto & OS & & (U,H) & \longmapsto & UH \end{array}$$

Corollaire 28. *Pour $A \in \mathcal{GL}_n(\mathbb{R})$, on a $|||A|||_2 = \sqrt{\rho({}^tAA)}$*

Corollaire 29. *Tout sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ qui contient le groupe orthogonal $\mathcal{O}_n(\mathbb{R})$ est le groupe $\mathcal{O}_n(\mathbb{R})$ lui-même.*

IV Applications en dimensions 2 et 3

1) Classification des isométries

Proposition 30 (Étude en dimension 2)**.** *Soient $u \in \mathcal{O}(\mathbb{R}^2)$ et A sa matrice dans la base canonique de $\mathbb{R}^2$.*

(i) Si $u \in \mathcal{O}^+(\mathbb{R}^2)$, alors il existe $\theta \in [0, 2\pi[$ tel que $A = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$. u est alors la rotation d'angle θ centrée en l'origine.

(ii) Si $u \notin \mathcal{O}^+(\mathbb{R}^2)$, alors il existe $\theta \in [0, 2\pi[$ tel que $A = \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{smallmatrix}\right)$. u est alors la symétrie par rapport à la droite d'angle polaire $\frac{\theta}{2}$.

Proposition 31 (Étude en dimension 3)**.** *Soient $u \in \mathcal{O}(\mathbb{R}^3)$. Il existe une base de $\mathbb{R}^3$ dans laquelle la matrice de u est :*

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}$$

pour un $\theta \in [0, 2\pi[$ et où $\varepsilon = \pm 1$. De plus :

(i) Si $u \in \mathcal{O}^+(\mathbb{R}^2)$, alors $\varepsilon = 1$. u est alors une rotation d'angle θ autour d'une droite.

(ii) Si $u \notin \mathcal{O}^+(\mathbb{R}^2)$, alors $\varepsilon = -1$. u est alors la composée d'une rotation d'angle θ autour d'une droite D puis d'une symétrie orthogonale par rapport à $D^\perp$.

2) Similitudes en dimension 2

On suppose ici E de dimension 2.

Définition 32. On dit que $f \in \mathcal{L}(E)$ est une similitude vectorielle s'il existe $k > 0$, appelé rapport de la similitude, tel que, pour tout $x \in E$, on a $\|f(x)\| = k\,\|x\|$.

Exemple 33. *Les isométries et les homothéties sont des similitudes.*

Définition 34. Une similitude est dite directe ou indirecte selon que son déterminant est positif ou négatif.

Proposition 35. *Toute similitude vectorielle directe est composée d'une homothétie de rapport positif et d'une rotation vectorielle. Toute similitude vectorielle indirecte est composée d'une homothétie de rapport positif et d'une réflexion.*

Proposition 36. *Soit f une similitude vectorielle de rapport k. Il existe une unique isométrie vectorielle u telle que $f = h_k \circ u$, où h_k est l'homothétie de rapport k.*

Définition 37. On appelle similitude affine toute application affine dont la partie linéaire est une similitude vectorielle.

Proposition 38. *Une similitude de $\mathcal{E}$ qui n'est pas une isométrie a un unique point fixe, appelé centre de la similitude.*

Proposition 39. *(i) Les similitudes directes conservent les angles.*

(ii) Les similitudes directes envoient les droites sur des droites.

(iii) Une similitude directe de rapport k envoie un cercle de rayon R sur un cercle de rayon kR dont le centre est l'image du centre.

3) Liens avec les polyèdres en dimension 3

On suppose ici E de dimension 3.

Définition 40. Un polyèdre convexe de E est dit régulier si toutes ses faces sont des polygones réguliers isométriques, et si en chaque sommet elles s'assemblent de la même manière, au sens où les figures formées par les réunions des arêtes aboutissant à un sommet sont isométriques.

Exemple 41. *Il y a 5 polyèdres réguliers : le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre.*

Théorème 42. *Soit $\mathcal{T}$ un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$.*

Application 43. *La table de caractères de $\mathfrak{S}_4$ est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

Remarque 44. *On peut lire les sous-groupes distingués de $\mathfrak{S}_4$ sur cette table de caractères.*

Développements

- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (42,43) [Ser70]
- Déterminant de Gram et inégalité de Hadamard (6,7,8) [Gou94]
- Décomposition polaire (27) [CG13]

Références

[Aud06] M. Audin. *Géométrie.* EDP Sciences
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Gri11] J. Grifone. *Algèbre Linéaire.* Cépaduès, 4e édition
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann

Cadre : Soient $\mathbb{K}$ un corps et $n, p \in \mathbb{N}^\star$. Pour tout $i \in [\![1, n]\!]$ et tout $j \in [\![1, p]\!]$, soient $a_{i,j} \in \mathbb{K}$ et $b_i \in \mathbb{K}$. On considère le système de n équations à p inconnues à coefficients dans $\mathbb{K}$ défini par :

$$\left\{ \begin{array}{ccccccc} a_{1,1}x_1 & + & \dots & + & a_{1,p}x_p & = & b_1 \\ \vdots & & & & \vdots & & \vdots \\ a_{n,1}x_1 & + & \dots & + & a_{n,p}x_p & = & b_n \end{array} \right. \quad \text{(S)}$$

I Existence et unicité des solutions

1) Définitions et premières propriétés

Définition 1. On appelle solution de (S) tout vecteur $x \in \mathbb{K}^n$ dont les coordonnées vérifient chacune des équations de (S).

Définition 2. Le système est dit compatible si (S) admet une solution.

Exemple 3. $\left\{ \begin{array}{l} x+y=1 \\ x=0 \end{array} \right.$ *est compatible, mais pas* $\left\{ \begin{array}{l} x+y=1 \\ x+y=0 \end{array} \right.$.

Définition 4. Dans (S), on pose $A = (a_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p} \in \mathcal{M}_{n,p}(\mathbb{K})$ et $b = (b_i)_{1 \leqslant i \leqslant n} \in \mathbb{K}^n$. Alors $x \in \mathbb{K}^n$ est solution de (S) si, et seulement si, $Ax = b$ dans $\mathbb{K}^n$.

Définition 5. On appelle rang du système (S) le rang de A.

Proposition 6. *Notons $A_1, \dots, A_n$ les colonnes de A. Alors (S) est compatible si, et seulement si, $b \in \mathrm{Vect}(A_1, \dots, A_n)$.*

Exemple 7. $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ *est compatible, mais pas* $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$.

Définition 8. Le système est dit compatible si $b = 0$.

Proposition 9. *Un système homogène est toujours compatible.*

2) Système de Cramer

Définition 10. On dit que (S) est de Cramer si A est inversible.

Proposition 11. *Un système de Cramer a une unique solution $x = A^{-1}b$.*

Théorème 12. *Supposons que (S) est de Cramer, et notons $A_1, \dots, A_n$ les colonnes de A. Alors :*

$$x = \frac{\det(A_1, \dots, A_{i-1}, b, A_{i+1}, \dots, A_n)}{\det A}$$

Remarque 13. *Numériquement, cette méthode utilise $(n+2)!$ opérations. C'est impossible à mettre en œuvre pour de grandes valeurs de n.*

Exemple 14. *Pour* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ *: $x = \left|\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right| = 2$ et $y = \left|\begin{smallmatrix} 1 & 2 \\ 0 & 0 \end{smallmatrix}\right| = 0$.*

3) Cas général

Soient $A \in \mathcal{M}_{n,p}(\mathbb{K})$ de rang r, et $b \in \mathbb{K}^n$. On peut supposer $(a_{i,j})_{1 \leqslant i,j \leqslant r}$ inversible de déterminant δ.

Théorème 15. *(i) Le système est compatible si, et seulement si :*

$$\forall\, s \in [\![r+1, p]\!],\ \Delta_s = \begin{vmatrix} a_{1,1} & \cdots & a_{1,r} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{r,1} & \cdots & a_{r,r} & b_r \\ a_{s,1} & \cdots & a_{s,r} & b_s \end{vmatrix} = 0$$

(ii) Si le premier point est réalisé, le système est équivalent à :

$$\left\{ \begin{array}{ccccccc} a_{1,1}x_1 & + \dots + & a_{1,r}x_r & = & b_1 & - a_{1,r+1} - \dots - & a_{1,n}x_n \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{r,1}x_1 & + \dots + & a_{r,r}x_r & = & b_r & - a_{r,r+1} - \dots - & a_{r,n}x_n \end{array} \right.$$

Il admet une infinité de solutions dépendant de $(n-r)$ paramètres (on donne à $x_{r+1}, \dots, x_n$ des valeurs arbitraires).

Exemple 16. *Soient* $A = \left(\begin{smallmatrix} 2 & 1 & -1 \\ 0 & 1 & 3 \\ 2 & k & 2 \end{smallmatrix}\right)$ *et* $b = \left(\begin{smallmatrix} \alpha \\ \beta \\ \gamma \end{smallmatrix}\right)$.

(i) Si $k \neq 2$, le système $Ax = b$ a une unique solution.

(ii) Si $k = 2$, et $\gamma \neq \alpha + \beta$, le système $Ax = b$ n'a pas de solution.

(iii) Si $k = 2$, et $\gamma = \alpha + \beta$, le système $Ax = b$ a une infinité de solutions.

Proposition 17. *Soit E un espace vectoriel de dimension finie n.*

(i) Soient $\varphi_1, \dots, \varphi_p \in E^\star$ telles que $\mathrm{rg}(\varphi_1, \dots, \varphi_p) = r$. Alors le sous-espace vectoriel $F = \{x \in E \,|\, \forall i, \varphi(x) = 0\}$ est de dimension $n - r$.

(ii) Réciproquement, si F est un sous-espace vectoriel de E de dimension q, il existe $n - q$ formes linéaires indépendantes $\varphi_1, \dots, \varphi_{n-q}$ telles que $F = \{x \in E \,|\, \forall i, \varphi(x) = 0\}$.

Remarque 18. *Les solutions de $Ax = 0$ forment un sous-espace vectoriel de dimension $n - \mathrm{rg}(A) = \dim \mathrm{Ker}(A)$. Les solutions de $Ax = b$ forment un sous-espace affine.*

Exemple 19. *Un hyperplan de E peut-être défini comme le noyau d'une forme linéaire sur E.*

II Méthode du pivot de Gauss

Définition 20. $\mathcal{GL}_n(\mathbb{K})$ agit sur $\mathcal{M}_n(\mathbb{K})$ par multiplication à gauche.

Définition 21. On appelle matrice de transvection toute matrice qui est de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$, où $\lambda \in \mathbb{K}$ et $i, j \in [\![1, n]\!]$ avec $i \neq j$.

Définition 22. On appelle matrice de dilatation toute matrice qui est de la forme $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$, où $\lambda \in \mathbb{K}$ et $i \in [\![1, n]\!]$.

Définition 23. On appelle matrice de permutation toute matrice qui est de la forme $P_{i,j} = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$, où $i, j \in [\![1, n]\!]$ avec $i \neq j$.

Remarque 24. *Ces matrices représentent également des transformations élémentaires dans l'algorithme du pivot de Gauss. Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$:*

Opération	$T_{i,j}(\lambda)A$	$D_i(\lambda)A$	$P_{i,j}A$
Résultat	$L_i \leftarrow L_i + \lambda L_j$	$L_i \leftarrow \lambda L_i$	$L_i \leftrightarrow L_j$

On a les opérations analogues sur les colonnes en multipliant à droite.

Exemple 25. $T_{3,2}(1) \times T_{3,1}(-3) \times T_{2,1}(-1) \times \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & -2 \\ 3 & 5 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & -4 \\ 0 & 0 & -2 \end{pmatrix}$

Définition 26. On appelle :

(i) pivot d'une ligne son coefficient non nul le plus à gauche.

(ii) matrice échelonnée en lignes une matrice telle que dès qu'une ligne est nulle, les suivantes le sont, et pour les lignes non nulles le pivot d'une ligne est strictement à droite du pivot de la ligne précédente. Une matrice échelonnée est dite réduite si ses pivots valent 1.

On a la définition similaire de matrice échelonnée (réduite) en colonnes.

Proposition 27. *Les orbites sont en bijections avec les sous-espaces vectoriels de $\mathbb{K}^n$: $A \sim B \Leftrightarrow \operatorname{Ker} A = \operatorname{Ker} B$.*

Proposition 28. *Toute matrice est dans l'orbite d'une unique matrice échelonnée.*

Lemme 29. *On suppose E de dimension $n \geqslant 2$. Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u ou un produit de deux transvections uv, tel que $u(x) = y$ ou $uv(x) = y$.*

Théorème 30. *Les transvections engendrent $\mathcal{SL}(E)$.*

Théorème 31. *Les transvections et les dilatations engendrent $\mathcal{GL}(E)$.*

Application 32. *L'algorithme du pivot de Gauss permet de se ramener à la matrice réduite associée à une matrice via des opérations élémentaires sur les lignes.*

III Autres algorithmes de résolution

1) Décomposition LU

Théorème 33 (Décomposition LU)**.** *Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{K})$ telle que les n sous-matrices diagonales $\Delta_k = (a_{i,j})_{1 \leqslant i,j \leqslant k} \in \mathcal{M}_k(\mathbb{K})$ soient inversibles. Alors il existe une matrice triangulaire inférieure L dont les termes diagonaux valent 1 et une matrice triangulaire supérieure U telles que $A = LU$. Cette factorisation est unique.*

Exemple 34. $\begin{pmatrix} 5 & 2 & 1 \\ 5 & -6 & 2 \\ -4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -\frac{4}{5} & -\frac{9}{20} & 1 \end{pmatrix} \begin{pmatrix} 5 & 2 & 1 \\ 0 & -8 & 1 \\ 0 & 0 & \frac{9}{4} \end{pmatrix}$

Méthode 35. *On résout alors $Ly = b$ puis $Ux = y$ par remontée.*

Théorème 36 (Décomposition de Choleski)**.** *Soit $A \in \mathcal{GL}_n(\mathbb{K})$ symétrique définie positive. Alors il existe une matrice C réelle triangulaire inférieure telle que $A = C\,{}^tC$. Cette factorisation est unique si on impose aux termes diagonaux d'être strictement positifs.*

Exemple 37. $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 5 & 5 & 5 \\ 1 & 5 & 14 & 14 \\ 1 & 5 & 14 & 15 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 2 & 3 & 0 \\ 1 & 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Méthode 38. *On résout alors ${}^tSy = b$ puis $Sx = y$ par remontée.*

2) Généralités et notions de convergence

Méthode 39. *On cherche à approximer la solution x du système $Ax = b$, où $A \in \mathcal{GL}_n(\mathbb{K})$ et $b \in \mathbb{K}^n$. On pose pour cela $A = M - N$, où $M \in \mathcal{GL}_n(\mathbb{K})$ est facile à inverser (diagonale, triangulaire, orthogonale...). On obtient la méthode itérative :*

$$x^{(k+1)} = M^{-1}Nx^{(k)} + M^{-1}b = F(x^{(k)}) \qquad \text{(M)}$$

Si la suite $(x^{(k)})_{k \in \mathbb{N}}$ converge vers x^∞, alors x^∞ est solution de $Ax = b$. De plus, x^∞ est un point fixe de F.

Définition 40. Soient $A = M - N$ et $\|.\|$ une norme sur $\mathbb{K}^n$. La méthode itérative (M) est dite convergente lorsque :

$$\forall\, b \in \mathbb{K}^n,\ \forall\, x^{(0)} \in \mathbb{K}^n,\ \lim_{k \to \infty} \left\| x^{(k)} - x \right\| = 0$$

Remarque 41. *En posant $e^{(k)} = x^{(k)} - x$ et $B = M^{-1}N$, on a $e^{(k+1)} = Be^{(k)}$, et la méthode itérative (M) converge ainsi lorsque, par exemple, $\rho(B) < 1$.*

3) Méthodes itératives

Définition 42. Soit $A \in \mathcal{GL}_n(\mathbb{K})$. On considère les sous-matrices D, E, F de A définies comme suit :

$$\begin{cases} (D)_{i,j} = a_{i,j} \text{ si } i = j, \ 0 \text{ sinon} \\ (-E)_{i,j} = a_{i,j} \text{ si } i > j, \ 0 \text{ sinon} \\ (-F)_{i,j} = a_{i,j} \text{ si } i < j, \ 0 \text{ sinon} \end{cases} \qquad A = \begin{pmatrix} D & -F \\ -E & \end{pmatrix}$$

On peut alors considérer plusieurs méthodes itératives :

(i) Jacobi : $M = D$, $N = E + F$

(ii) Gauss-Seidel : $M = D - E$, $N = F$

(iii) Relaxation : $M = \frac{1}{\omega} D - E$, $N = \frac{1-\omega}{\omega} D + F$

Remarque 43. *Avec $B = M^{-1}N$, la méthode itérative (M) devient :*

$$x^{(k+1)} = Bx^{(k)} + b \qquad \text{(M')}$$

Théorème 44. *Si la matrice A est à diagonale strictement dominante, alors la méthode de Jacobi converge.*

Exemple 45. *Si $A = \begin{pmatrix} 1 & a & a \\ a & 1 & a \\ a & a & 1 \end{pmatrix}$, la méthode de Jacobi converge si $|a| < \frac{1}{2}$.*

Théorème 46. *Si A est hermitienne définie positive, alors la méthode de relaxation converge pour $\omega \in]0, 2[$.*

Corollaire 47. *Si A est hermitienne définie positive, alors la méthode de Gauss-Seidel converge.*

4) Méthodes de gradient

Caractérisation de l'α-convexité

Définition 48. Pour $\alpha > 0$, on dit que la fonction $f : C \to \mathbb{R}$ est α-convexe si pour tous $a, b \in C$ distincts et tout $\lambda \in]0, 1[$, on a :

$$f((1-\lambda)a + \lambda b) \leqslant (1-\lambda) f(a) + \lambda f(b) - \frac{\alpha}{2} \|a - b\|^2 \lambda(1-\lambda)$$

Théorème 49. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*

(i) J est α-convexe sur C.

(ii) $\forall x, y \in C, \ \langle \nabla J(x) - \nabla J(y), x - y \rangle \geqslant \alpha \|x - y\|^2$.

(iii) $\forall x, y \in C, \ J(x) \geqslant J(y) + \langle \nabla J(y), x - y \rangle + \frac{\alpha}{2} \|x - y\|^2$.

Si J est deux fois différentiable, on a aussi : $\left\langle d^2 J(x) \cdot y, y \right\rangle \geqslant \alpha \|y\|^2$.

Méthode de gradient

Soit $J : \mathbb{R}^n \to \mathbb{R}$. On suppose J différentiable. On cherche, s'il existe, un élément $u \in \mathbb{R}^n$ tel que :

$$J(u) = \inf_{v \in \mathbb{R}^n} J(v)$$

Pour cela, on utilise les méthodes de gradient. On considère la suite :

$$u_0 \in \mathbb{R}^n \quad \text{et} \quad \forall k \in \mathbb{N}, \ u^{k+1} = u^k - \rho^k \nabla J(u^k)$$

Il existe plusieurs possibilités pour choisir les ρ^k, par exemple :

(i) Gradient à pas fixe : $\rho^k = \rho$ une constante positive fixée.

(ii) Gradient à pas optimal : ρ^k minimise $\rho \mapsto J\left(u^k - \rho \nabla J(u^k)\right)$.

Théorème 50. *Si J est α-convexe et différentiable, et que ∇J est L-lipschitzienne, alors la méthode de gradient à pas optimal converge vers l'unique minimum de J.*

Application 51. *Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. On considère la fonctionnelle quadratique $J : \mathbb{R}^n \to \mathbb{R}$ définie par :*

$$J(X) = \langle AX, X \rangle - \langle b, X \rangle + c$$

Cette fonctionnelle satisfait les conditions du théorème précédent. De plus, son minimum est atteint en $X_0 \in \mathbb{R}^n$ qui vérifie $\nabla J(X_0) = AX - b = 0$. On a donc une méthode itérative pour approcher la solution de $AX = b$.

Développements

- Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$ (30,31) [Per96]
- Algorithme de gradient à pas optimal (50) [Cia88]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gri11] J. Grifone. *Algèbre Linéaire.* Cépaduès, 4e édition
[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

Cadre : $\mathbb{K}$ est un corps avec $\operatorname{car}\mathbb{K} \neq 2$, E est un $\mathbb{K}$-espace vectoriel de dimension finie $n \geqslant 1$.

I Généralités sur les formes quadratiques

1) Forme polaire

Définition 1. (i) On dit que $f : E \times E \to \mathbb{K}$ est une forme bilinéaire si elle est linéaire en ses deux variables.

(ii) f est symétrique si $\forall x, y \in E, f(x,y) = f(y,x)$.

Définition 2. On dit que $q : E \to \mathbb{K}$ est quadratique s'il existe une forme bilinéaire symétrique $f : E \times E \to \mathbb{K}$ telle que $\forall x \in E, q(x) = f(x,x)$. f est la forme polaire de q, et est unique si $\operatorname{car}\mathbb{K} \neq 2$.

Proposition 3. *Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E identifié à $\mathbb{K}^n$. Alors toute forme quadratique sur $\mathbb{K}^n$ est un polynôme homogène de degré 2 en ses coordonnées dans $\mathcal{B}$.*

Définition 4. On pose $A = (f(e_i, e_j))_{1 \leqslant i,j \leqslant n}$ la matrice associée à f dans la base $\mathcal{B}$. On note :

$$\overline{f} : \left| \begin{array}{ccc} E & \longrightarrow & E^\star \\ y & \longmapsto & \overline{f}(y) : \left| \begin{array}{ccc} E & \longrightarrow & \mathbb{K} \\ x & \longmapsto & f(x,y) \end{array} \right. \end{array} \right.$$

On pose $\operatorname{Ker} q = \operatorname{Ker} \overline{f}$ que l'on appelle noyau de q, et $\operatorname{rg} q = \operatorname{rg} \overline{f}$ que l'on appelle rang de q.

Proposition 5. *On identifie E à $\mathbb{K}^n$, alors :*

(i) $\forall x, y \in \mathbb{K}^n$, $f(x,y) = {}^t x A y$

(ii) *A est symétrique*

(iii) $\operatorname{Ker} q = \operatorname{Ker} A$

(iv) $\operatorname{rg} q = \operatorname{rg} A$

Proposition 6. *Soit $\mathcal{B}'$ une base de E, et soit $A' = Mat_{\mathcal{B}'} f$. Soit P la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. Alors $A' = {}^t P A P$.*

Exemple 7. *Si $\mathcal{B}$ est la base canonique de $\mathbb{R}^3$, on a :*

$$q : \left| \begin{array}{ccc} \mathbb{R}^3 & \longrightarrow & \mathbb{R} \\ (x,y,z) & \longmapsto & x^2 - y^2 - xy + yz \end{array} \right. \Rightarrow Mat_{\mathcal{B}} f = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

2) Orthogonalité et isotropie

Définition 8. On dit que q est non dégénérée si $N = \{0\}$.

Définition 9. (i) Pour $x \in E$ est orthogonal à $y \in E$ si $f(x,y) = 0$.

(ii) $A \subseteq E$ est orthogonale à $B \subseteq E$ si $\forall x \in A, \forall y \in B, f(x,y) = 0$.

(iii) On note $A^\perp = \{y \in E \,|\, \forall x \in A, f(x,y) = 0\}$ l'orthogonal de A.

Théorème 10. *Soit F un sous-espace vectoriel de E. Supposons que f est non dégénérée. Alors* $\dim E^\perp = \dim E - \dim F$.

Proposition 11. *Soient V et W deux sous-espaces vectoriels de E, alors :*

(i) $(V^\perp)^\perp = V$

(ii) $(V + W)^\perp = V^\perp \cap W^\perp$

(iii) $(V \cap W)^\perp = V^\perp + W^\perp$

Définition 12. (i) Soit $x \in E \setminus \{0\}$. x est dit isotrope si $q(x) = 0$.

(ii) Un sous-espace vectoriel V de E est isotrope si $V \cap V^\perp = \{0\}$.

(iii) Un sous-espace vectoriel V de E est totalement isotrope (SETI) si $V \subseteq V^\perp$. Un tel sous-espace dit maximal (SETIM) s'il est maximal pour l'inclusion.

(iv) On appelle indice de q la quantité :

$$\nu(q) = \max\{k \in \mathbb{N} \,|\, k = \dim F,\ F \text{ totalement isotrope}\} \leqslant \frac{n}{2}$$

Exemple 13. *Si V est un sous-espace vectoriel de E non isotrope, et si f est non dégénérée, alors $E = V \oplus V^\perp$.*

Définition 14. L'ensemble $C(q) = q^{-1}(\{0\})$ est appelé cône isotrope de q . Il contient $\operatorname{Ker} q$.

Exemple 15. *Si $\operatorname{Ker} q \subsetneq C(q)$, alors q est surjective.*

Exemple 16. *Pour la forme quadratique $q(x,y) = x^2 + y^2$ on a $C(q) = \operatorname{Vect}\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right) \cup \operatorname{Vect}\left(\begin{smallmatrix} 1 \\ -i \end{smallmatrix}\right)$, et ses SETIM sont $\operatorname{Vect}\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)$ et $\operatorname{Vect}\left(\begin{smallmatrix} 1 \\ -i \end{smallmatrix}\right)$.*

Définition 17. Une base $\mathcal{B} = (e_1, \dots, e_n)$ est orthogonale si :

$$\forall i, j \in [\![1, n]\!],\ [i \neq j \Rightarrow f(e_i, e_j) = 0]$$

Théorème 18 (Réduction de Gauss)**.** *Soit $q : E \to \mathbb{K}$ une forme quadratique. Alors il existe $r \geqslant 1$, $a_1, \dots, a_r \in \mathbb{K}$ et $\varphi_1, \dots, \varphi_r \in E^\star$ libres tels que :*

$$\forall x \in E, q(x) = \sum_{i=1}^{r} a_i \varphi_i(x)^2$$

Corollaire 19. *Dans le théorème précédent, on a en fait $r = \operatorname{rg} q$ et $\ker q = \bigcap_{i=1}^{r} \varphi^{-1}(\{0\})$. Ainsi, toute forme quadratique admet une base orthogonale pour sa forme polaire.*

II Groupe orthogonal et classification des formes quadratiques

1) Introduction du groupe orthogonale

Définition 20. On appelle groupe orthogonal l'ensemble $\mathcal{O}(q)$ défini par :

$$\mathcal{O}(q) = \{u \in \mathcal{GL}(E) \,|\, \forall x \in E,\, q(u(x)) = q(x)\}$$

Les éléments de $\mathcal{O}(q)$ sont appelés les isométries de E relativement à q.

Proposition 21. *$\mathcal{O}(q)$ est un sous-groupe de $\mathcal{GL}(E)$.*

Proposition 22. *On a également :*

$$\mathcal{O}(q) = \{u \in \mathcal{GL}(E) \,|\, \forall x, y \in E, f(u(x), u(y)) = f(x, y)\}$$

Proposition 23. *On identifie E à $\mathbb{K}^n$. Si on note A la matrice de q dans une base, alors :*

$$\mathcal{O}(q) = \{P \in \mathcal{GL}_n(\mathbb{K}) \,|\, {}^tPAP = A\}$$

Définition 24. Soient $f, f' : E \times E \to \mathbb{K}$ deux formes bilinéaires symétriques. On dit que f et f' sont équivalentes, noté $f \sim f'$, si :

$$\exists\, u \in \mathcal{GL}(E),\, \forall\, x, y \in E,\, f(u(x), u(y)) = f'(u(x), u(y))$$

Si q et q' sont leurs formes quadratiques, on écrira dans ce cas : $q \sim q'$.

Proposition 25. *$\sim$ est une relation d'équivalence.*

Proposition 26. *Si $q \sim q'$, alors $\mathcal{O}(q) \cong \mathcal{O}(q')$.*

Proposition 27. *Si $q \sim q'$, alors $\operatorname{rg} q = \operatorname{rg} q'$, $\nu(q) = \nu(q')$, et si $\mathcal{B}$ est une base de E, alors il existe $\alpha \in \mathbb{K}$ tel que $\det Mat_{\mathcal{B}}(q) = \alpha^2 \det Mat_{\mathcal{B}}(q')$.*

2) Classification des formes quadratiques pour $\mathbb{K} = \mathbb{R}$

Définition 28. Soit $\mathcal{B} = (u_1, \dots, u_n)$ une base orthogonale pour q. On pose $p = \operatorname{Card}\{i \in [\![1, n]\!] \,|\, q(u_i) > 0\}$.

Théorème 29. *Le couple $(p, n-p)$ est indépendant de la base choisie. On l'appelle la signature de q.*

Théorème 30. *Il y a $n+1$ classes d'équivalence de formes quadratiques non dégénérées sur E. Dans une base convenable, on a $Mat(q) = \begin{pmatrix} I_p & 0 \\ 0 & I_{n-p} \end{pmatrix}$. De plus, $\nu(q) = \min(p, n-p)$.*

3) Classification des formes quadratiques pour $\mathbb{K}$ algébriquement clos

Théorème 31. *Toutes les formes quadratiques non dégénérées sont équivalentes. Dans une base convenable, elles ont pour matrice l'identité. De plus, $\nu = \lfloor \frac{n}{2} \rfloor$.*

Exemple 32. *Pour toute forme quadratique $q : \mathbb{K}^n \to \mathbb{K}$, avec $\mathbb{K}$ algébriquement clos, on a :*

$$\mathcal{O}(q) \cong \{P \in \mathcal{GL}_n(\mathbb{K}) \,|\, {}^tPP = I_n\} = O_n(\mathbb{K})$$

4) Classification des formes quadratiques pour $\mathbb{K} = \mathbb{F}_q$

Définition 33. On pose :

$$\mathbb{F}_q^2 = \left\{x^2 \in \mathbb{F}_q \,\middle|\, x \in \mathbb{F}_q\right\} \quad \text{et} \quad \mathbb{F}_q^{2\star} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$$

Théorème 34. *Soient $a, b \in \mathbb{F}_q^\star$. Alors l'équation en x, y : $ax^2 + by^2 = 1$ admet des solutions dans $\mathbb{F}_q$.*

Théorème 35. *Soit $\alpha \in \mathbb{F}_q^\star \setminus \mathbb{F}_q^{2\star}$. Il y a deux classes d'équivalence de formes quadratiques non dégénérées, de matrices :*

$$Q_1 = I_n \quad et \quad Q_2 = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \alpha \end{pmatrix}$$

Une forme Q est de l'un ou l'autre type suivant que $\det Mat(Q)$ est, ou non, un carré de $\mathbb{F}_q^\star$.

III Applications

1) Géométrie

Théorème 36. *Soient $v_1, \dots, v_n \in \mathbb{K}^n$, on note $Vol(v_1, \dots, v_n)$ le volume du parallélépipède engendré par $v_1, \dots, v_n$, alors :*

$$Vol(v_1, \dots, v_n) = |\det(v_1, \dots, v_n)|$$

Lemme 37. *Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ symétriques définies positives distinctes, et $\alpha, \beta > 0$ tels que $\alpha + \beta = 1$, alors :*

$$\det(\alpha A + \beta B) > \det(A)^\alpha \det(B)^\beta$$

Application 38 (Ellipsoïde de John-Loewner)**.** *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant K.*

2) Géométrie différentielle

Lemme 39. *Soit $A_0 \in \mathcal{GL}_n(\mathbb{R}) \cap \mathcal{S}_n(\mathbb{R})$. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et $\rho : V, \mathcal{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que pour tout $A \in V$, on a ${}^t\rho(A)A_0\rho(A)$.*

Théorème 40 (Lemme de Morse)**.** *Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ définie sur un ouvert U de $\mathbb{R}^n$ contenant 0. On suppose que $df(0) = 0$ et que $d^2f(0)$ est non dégénérée et de signature $(p, n-p)$. Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = \sum_{i=1}^p \varphi_i(x)^2 - \sum_{i=p+1}^n \varphi_i(x)^2$ au voisinage de 0.*

Développements

- Ellipsoïde de John-Loewner (37,38) [FGN13c]
- Lemme de Morse (39,40) [Rou15]

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini
[CG15] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 2.* Calvage et Mounet
[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3.* Cassini

Cadre : Soit E un $\mathbb{R}$-espace vectoriel de dimension finie $n \in \mathbb{N}^\star$.

I Formes quadratiques réelles

1) Formes bilinéaires symétriques

Définition 1. Une forme bilinéaire est une application $\varphi : E \times E \to \mathbb{R}$ qui est linéaire par rapport à ses deux variables.

Exemple 2. *Si α et β sont des formes linéaires, $(x,y) \mapsto \alpha(x)\beta(y)$ est une forme bilinéaire.*

Définition 3. Une forme bilinéaire φ est symétrique si, pour tous $x, y \in E$, on a $\varphi(x,y) = \varphi(y,x)$.

Exemple 4. *$(A,B) \mapsto \mathrm{tr}(AB)$ et $(f,g) \mapsto \int_{\mathbb{R}} fg\,dx$ sont symétriques.*

Définition 5. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. On définit la matrice de φ dans la base $\mathcal{B}$ par $M = \mathrm{Mat}_{\mathcal{B}}(\varphi) = (\varphi(e_i, e_j))_{1 \leqslant i,j \leqslant n}$.

Proposition 6. *Soit $\mathcal{B}$ une base de E. Alors φ est symétrique si, et seulement si,* $\mathrm{Mat}_{\mathcal{B}}(\varphi) \in \mathcal{S}_n(\mathbb{R})$.

Proposition 7. *Soit $\mathcal{B}$ une base de E, identifié à $\mathbb{R}^n$. Alors pour tous $x, y \in \mathbb{R}^n$, on a $\varphi(x,y) = {}^{\mathrm{t}}x\,\mathrm{Mat}_{\mathcal{B}}(\varphi)y$.*

Proposition 8. *Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, et soit P la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. Alors* $\mathrm{Mat}_{\mathcal{B}'}(\varphi) = P^{-1}\,\mathrm{Mat}_{\mathcal{B}}(\varphi)P$.

Définition 9. On considère l'application suivante :

$$\Phi : \left| \begin{array}{ccc} E & \longrightarrow & E^\star \\ y & \longmapsto & \varphi(.,y) \end{array} \right.$$

On pose $\mathrm{Ker}\,\varphi = \mathrm{Ker}\,\Phi$ que l'on appelle noyau de φ, et $\mathrm{rg}\,\varphi = \mathrm{rg}\,\Phi$ que l'on appelle rang de φ.

Proposition 10. *Soit $\mathcal{B}$ une base de E. Alors* $\mathrm{Ker}\,\varphi = \mathrm{Ker}(\mathrm{Mat}_{\mathcal{B}}(\varphi))$ *et* $\mathrm{rg}\,\varphi = \mathrm{rg}(\mathrm{Mat}_{\mathcal{B}}(\varphi))$. *On a donc* $\dim E = \dim \mathrm{Ker}\,\varphi + \mathrm{rg}\,\varphi$.

Définition 11. On dit que φ est non dégénérée lorsque $\mathrm{Ker}\,\varphi = \{0\}$.

2) Formes quadratiques

Définition 12. Une forme quadratique est une application de la forme :

$$q : \left| \begin{array}{ccc} E & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \varphi(x,x) \end{array} \right.$$

où φ est une forme bilinéaire symétrique.

Proposition 13. *Pour toute forme quadratique sur E, il existe une unique forme bilinéaire symétrique φ_q sur E telle que, pour tout $x \in E$, on a $q(x) = \varphi_q(x,x)$. On appelle φ_q la forme polaire de q, et on a :*

$$\forall\, x, y \in E,\ \varphi_q(x,y) = \frac{q(x+y) - q(x) - q(y)}{2}$$

Exemple 14. *Si $(E, \langle .,. \rangle)$ est un espace pré-hilbertien, alors l'application $x \mapsto \|x\|^2 = \langle x, x \rangle$ est une forme quadratique.*

Exemple 15. *Si $f : \mathbb{R}^n \to \mathbb{R}$ est une application de classe $\mathcal{C}^2$, alors, pour tout $x \in \mathbb{R}^n$, l'application $h \mapsto D_x^2 f(h,h)$ est une forme quadratique.*

Définition 16. Soit $\mathcal{B}$ une base de E. On définit la matrice de q dans la base $\mathcal{B}$, son rang et son noyau comme la matrice, le rang et le noyau de sa forme polaire.

Proposition 17. *Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E identifié à $\mathbb{K}^n$. Alors toute forme quadratique sur $\mathbb{K}^n$ est un polynôme homogène de degré 2 en ses coordonnées dans $\mathcal{B}$.*

Exemple 18. *Si $\mathcal{B}$ est la base canonique de $\mathbb{R}^3$, on a :*

$$q : \left| \begin{array}{ccc} \mathbb{R}^3 & \longrightarrow & \mathbb{R} \\ (x,y,z) & \longmapsto & x^2 - y^2 - xy + yz \end{array} \right. \Rightarrow Mat_{\mathcal{B}} f = \begin{pmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Proposition 19. *Si q est une forme quadratique positive sur E, alors, pour tous $x, y \in E$, on a $|\varphi_q(x,y)|^2 \leqslant q(x)q(y)$.*

Définition 20. Soit q est une forme quadratique sur E. On dit que deux éléments x et y de E sont orthogonaux si $\varphi_q(x,y) = 0$. Pour $A \subseteq E$, on note $A^\perp = \{y \in E \,|\, \forall\, x \in A,\ \varphi_q(x,y) = 0\}$ l'orthogonal de A.

Remarque 21. *On a* $\mathrm{Ker}\,q = E^\perp$ *et* $A \subseteq A^{\perp\perp}$.

Proposition 22. *Soit F un sous-espace vectoriel de E. Alors :*

$$\dim F + \dim F^\perp = \dim E + \dim(F \cap \mathrm{Ker}\,q)$$

Si q est non dégénérée, alors $E = F \oplus F^\perp$ et $F = F^{\perp\perp}$.

II Réduction des formes quadratiques

Soit q une forme quadratique sur E de rang r.

1) Réduction de Gauss

Théorème 23 (Gauss)**.** *Il existe $\lambda_1, \dots, \lambda_r \in \mathbb{R}^\star$ et $\ell_1, \dots, \ell_r$ des formes linéaires indépendantes tels que, pour tout $x \in E$, $q(x) = \sum_{i=1}^r \lambda_i \ell_i(x)^2$.*

Corollaire 24. *Avec les notations du théorème précédent, la forme polaire de q est $(x,y) \mapsto \sum_{i=1}^r \lambda_i \ell_i(x)\ell_i(y)$.*

Exemple 25. $q(x,y,z) = xy + xz + yz = \left(\frac{x+y+z}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2 - z^2$

Corollaire 26. *Il existe une base orthogonale pour q. La matrice de q dans cette base est alors* $\mathrm{Diag}(\lambda_1, \dots, \lambda_n)$*, où $\lambda_i = 0$ pour $i > r$.*

Corollaire 27. *On note :*

$$s = \mathrm{Card}\left(\{i \in [\![1,n]\!] \mid \lambda_i > 0\}\right) \quad et \quad t = \mathrm{Card}\left(\{i \in [\![1,n]\!] \mid \lambda_i < 0\}\right)$$

Alors la matrice de q dans une certaine base est $\mathrm{Diag}(I_s, -I_t, O_{n-s-t})$.

2) Signature d'une forme quadratique

Proposition 28 (Loi d'inertie de Sylvester)**.**

(i) s et t ne dépendent pas de la décomposition de Gauss choisie, et :

$$s = \max\{\dim F \mid F \in \mathcal{P}\} \quad et \quad t = \max\{\dim F \mid F \in \mathcal{N}\}$$

où $\mathcal{P}$ (resp. $\mathcal{N}$) désigne l'ensemble des sous-espaces de E sur lesquels la restriction de q est définie positive (resp. négative).

(ii) Soit $(e_i)_{i \in [\![1,n]\!]}$ une base orthogonale pour q. Alors s est le nombre de i tels que $q(e_i) > 0$ et t est le nombre de i tels que $q(e_i) < 0$.

Définition 29. (s,t) s'appelle la signature de q.

Exemple 30. *La signature de $M \mapsto \mathrm{tr}(M^2)$ est* $\left(\frac{n(n+1)}{2}, \frac{n(n-1)}{2}\right)$.

Corollaire 31. *Il existe $\ell_1, \dots, \ell_r$ des formes linéaires indépendantes tels que, pour tout $x \in E$, $q(x) = \sum_{i=1}^s \ell_i(x)^2 - \sum_{i=s+1}^r \ell_i(x)^2$.*

Corollaire 32. *Pour $A \in \mathcal{M}_{[}(n)]\mathbb{R}$, il existe s,t uniques et $P \in \mathcal{GL}_n(\mathbb{R})$ tels que* ${}^tPAP = \mathrm{Diag}(I_s, -I_t, O_{n-s-t})$.

Théorème 33. *Soient q et q' deux formes quadratiques, avec q définie positive. Il existe une base orthonormée pour q et orthogonale pour q'.*

3) Applications

Application 34 (Ellipsoïde de John-Loewner)**.** *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant K.*

Théorème 35 (Lemme de Morse)**.** *Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ définie sur un ouvert U de $\mathbb{R}^n$ contenant 0. On suppose que $df(0) = 0$ et que $d^2f(0)$ est non dégénérée et de signature $(p, n-p)$. Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = \sum_{i=1}^p \varphi_i(x)^2 - \sum_{i=p+1}^n \varphi_i(x)^2$ au voisinage de 0.*

III Application à l'étude des coniques

On se place dans un espace affine $\mathcal{E}$ associé à un $\mathbb{R}$-espace vectoriel E.

1) Définitions et premières propriétés

Soit q une forme quadratique sur E de forme polaire φ.

Définition 36. Une fonction polynômiale de degré 2 sur $\mathcal{E}$ est une application $f : \mathcal{E} \to \mathbb{R}$ telle qu'il existe un point $O \in \mathcal{E}$, une forme quadratique non nulle q sur E, une forme linéaire L_0 sur E et une constante $c_O \in \mathbb{R}$ tels que : $\forall\, M \in \mathcal{E},\ f(M) = q(\overrightarrow{OM}) + L_O(\overrightarrow{OM}) + c_O$.

Remarque 37. *q ne dépend pas du point d'origine O choisi.*

Définition 38. On appelle quadrique affine la classe d'équivalence d'une fonction polynômiale de degré 2 $f : \mathcal{E} \to \mathbb{R}$ sous la relation "$f \sim g$ si, et seulement si, g est un multiple scalaire de f". Une quadrique plane est appelée conique. L'ensemble des points de E vérifiant $f(M) = 0$ est l'image de la quadrique.

Remarque 39. *Les équations $x^2 + y^2 + 1 = 0$ et $x^2 + 1 = 0$ définissent le même ensemble de points du plan $\mathbb{R}^2$.*

Définition 40. La quadrique définie par $f(M) = q(\overrightarrow{OM}) + L(\overrightarrow{OM}) + c$ est dite propre si la forme quadratique $Q(x,y,z) = q(x,y) + L(x,y)z + cz^2$ définie sur $E \times \mathbb{R}$ est non dégénérée. Cette forme quadratique est dite homogénéisée de q.

Exemple 41. *Les coniques propres sont de "vraies" coniques.*

Définition 42. On dit qu'un point $\Omega \in \mathcal{E}$ est un centre pour la quadrique si $L_\Omega = 0$. Quand il y a un centre unique, on dit que la quadrique est une quadrique à centre.

Proposition 43. *$\mathcal{C}$ est à centre si, et seulement si, q est non dégénérée.*

Exemple 44. *$f(x,y) = x^2 + y^2 - 1$ définit une conique à centre, $f(x,y) = x^2 - y$ définit une conique propre mais pas à centre.*

Remarque 45. *On place dans un repère centré en O. On a en fait $df_M(x) = 2\varphi(\overrightarrow{OM}, x) + L(x)$. De plus, $df_M(x) = 0$ pour tout $x \in E$ est équivalent à $\frac{\partial f}{\partial x_1}(M) = \ldots = \frac{\partial f}{\partial x_n}(M) = 0$. Si la quadrique est à centre, il y a une solution unique. Sinon le système n'est pas de Kramer, il y a une infinité de solutions, mais il n'y a pas de centre.*

2) Classification des coniques

Proposition 46 (Classification des coniques propres)**.**

sgn(Q)	*sgn(q)*	*Classe*	*Exemple*
$(3,0)$ *ou* $(0,3)$	$(2,0)$ *ou* $(0,2)$	$\varnothing$	$x^2+y^2=-1$
$(2,1)$ *ou* $(1,2)$	$(2,0)$ *ou* $(0,2)$	*Ellipse*	$x^2+y^2=1$
$(2,1)$ *ou* $(1,2)$	$(1,1)$	*Hyperbole*	$x^2-y^2=1$
$(2,1)$ *ou* $(1,2)$	$(1,0)$ *ou* $(0,1)$	*Parabole*	$x^2+y=0$

Proposition 47 (Classification des coniques impropres)**.**

sgn(Q)	*sgn(q)*	*Classe*	*Exemple*
$(2,0)$ *ou* $(0,2)$	$(2,0)$ *ou* $(0,2)$	*Point*	$x^2+y^2=0$
$(2,0)$ *ou* $(0,2)$	$(1,0)$ *ou* $(0,1)$	$\varnothing$	$x^2=-1$
$(1,1)$	$(1,1)$	*Droites sécantes*	$x^2-y^2=0$
$(1,1)$	$(1,0)$ *ou* $(0,1)$	*Droites parallèles*	$x^2=1$
$(1,0)$ *ou* $(0,1)$	$(1,0)$ *ou* $(0,1)$	*Droite double*	$x^2=0$

3) Point de vue géométrique

On se place dans un plan affine euclidien $\mathcal{P}$.

Théorème 48. *Pour toute conique propre d'image non vide qui n'est pas un cercle, il existe un point F appelé foyer, une droite D ne contenant pas F, appelée directrice et un nombre réel positif e appelé excentricité tels que la conique soit l'ensemble des points M tels que $FM = e \times d(M,D)$. Si $e<1$, $\mathcal{C}$ est une ellipse. Si $e=1$, $\mathcal{C}$ est une parabole. Si $e>1$, $\mathcal{C}$ est une hyperbole.*

Proposition 49. *Une ellipse de foyers F et F' est l'ensemble des points M tels que $MF + MF' = 2a$, pour un certain réel positif a tel que $2a > FF'$. Une hyperbole de foyers F et F' est l'ensemble des points M tels que $|MF - MF'| = 2a$, pour un certain réel positif a tel que $2a < FF'$.*

Développements

- Ellipsoïde de John-Loewner (34) [FGN13c]
- Lemme de Morse (35) [Rou15]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck
[Aud06] M. Audin. *Géométrie.* EDP Sciences
[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3.* Cassini
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

Cadre : $(E, \overrightarrow{E})$ est un espace affine de dimension finie, où E est un $\mathbb{R}$-espace vectoriel

I Barycentre

1) Définition et premières propriétés

Définition 1. Un couple $(A, \alpha) \in E \times \mathbb{R}$ est appelé point pondéré.

Définition 2. Une suite $(A_i, \alpha_i)_{i\in[\![1,n]\!]}$ de points pondérés définie une application L de E dans $\overrightarrow{E}$, appelée fonction vectorielle de Leibniz, en posant $f(M) = \sum_{i=1}^n \alpha_i \overrightarrow{MA_i}$.

Proposition 3. *Si $\sum_{i=1}^n \alpha_i = 0$, f est constante, sinon f est bijective.*

Définition 4. Si $\sum_{i=1}^n \alpha_i \neq 0$, l'unique point $B \in E$ tel que $f(B) = \overrightarrow{0}$ est appelé barycentre de $(A_i, \alpha_i)_{i\in[\![1,n]\!]}$. On note $B = \mathrm{Bar}(A_i, \alpha_i)_{i\in[\![1,n]\!]}$.

Exemple 5. $[A, B] = \{\mathrm{Bar}((A, t), (B, 1-t)) \,|\, t \in [0, 1]\}$

Proposition 6. *Soit $\lambda \in \mathbb{R} \setminus \{0\}$, et soient $(A_i, \alpha_i)_{i\in[\![1,n]\!]}$, $(B_i, \beta_i)_{i\in[\![1,p]\!]}$ des points pondérés, on a alors :*

(i) (Homogénéité) $\mathrm{Bar}(A_i, \lambda\alpha_i)_{i\in[\![1,n]\!]} = \mathrm{Bar}(A_i, \alpha_i)_{i\in[\![1,n]\!]}$.

(ii) (Associativité) Si $G = \mathrm{Bar}(A_i, \alpha_i)$ et $G' = \mathrm{Bar}(B_i, \beta)$, alors :

$$\mathrm{Bar}\left((A_i, \alpha_i), (B_i, \beta_i)\right) = \mathrm{Bar}\left(\left(G, \sum_{i=0}^n \alpha_i\right), \left(G', \sum_{i=1}^p \beta_i\right)\right)$$

Définition 7. L'isobarycentre de $(A_i)_{i\in[\![1,n]\!]}$ est $\mathrm{Bar}(A_i, 1)_{i\in[\![1,n]\!]}$.

Exemple 8. *L'isobarycentre d'un triangle est son centre de gravité.*

2) Barycentres et sous-espaces affines

Théorème 9. *Soit $F \subset E$. Les assertions suivantes sont équivalentes :*

(i) F est un sous-espace affine de E.

(ii) F contient les barycentres de familles de points de F.

(iii) F contient les barycentres de tout couples de points de F.

Exemple 10. *Dans $\mathbb{R}^2$, les droites sont des sous-espaces affines.*

Définition 11. Soit $A \subset E$ non vide. Le sous-espace affine engendré par A, noté $\mathrm{Aff}(A)$, est l'intersection des sous-espaces affines contenant A.

Proposition 12. $\mathrm{Aff}(A)$ *est l'ensemble des barycentres de points de A.*

Définition 13. Soient $(F, \overrightarrow{F})$ un espace affine de dimension finie et $f : E \to F$. On dit que f préserve les barycentres si, pour des points pondérés $(A_i, \lambda\alpha_i)_{i\in[\![1,n]\!]}$ de E, on a :

$$f\left(\mathrm{Bar}(A_i, \lambda\alpha_i)_{i\in[\![1,n]\!]}\right) = \mathrm{Bar}(f(A_i), \lambda\alpha_i)_{i\in[\![1,n]\!]}$$

Théorème 14. *Soient $(F, \overrightarrow{F})$ un espace affine de dimension finie et $f : E \to F$. Alors f est affine si, et seulement si, elle préserve les barycentres.*

3) Coordonnées barycentriques

Soit $(A_0, A_1, \ldots, A_n)$ un repère affine de E.

Théorème 15. *Tout point de E est un barycentre des $A_0, A_1, \ldots, A_n$, et deux systèmes de poids seront proportionnels.*

Définition 16. Soit $M \in E$. Il existe un unique $(\alpha_0, \ldots, \alpha_n) \in \mathbb{R}^{n+1}$ tel que $\sum_{i=0}^n \alpha_i \overrightarrow{MA_i} = \overrightarrow{0}$ et $\sum_{i=0}^n \alpha_i = 1$. $(\alpha_0, \ldots, \alpha_n)$ sont les coordonnées barycentriques de M relativement à $(A_0, A_1, \ldots, A_n)$.

Exemple 17. *Soient A, B et C sont trois points d'un plan affine P, et soit $\mathcal{B}$ une base du plan vectoriel directeur de P. Soit $M \in P$. Les coordonnées de M relativement à A, B et C sont* $(\det_{\mathcal{B}}(\overrightarrow{MB}, \overrightarrow{MC}), \det_{\mathcal{B}}(\overrightarrow{MA}, \overrightarrow{MC}), \det_{\mathcal{B}}(\overrightarrow{MA}, \overrightarrow{MB}))$.

Application 18 (Équation barycentrique d'une droite de $\mathbb{R}^2$)**.** *Soit $M \in (AB)$. Dans un repère affine (A_0, A_1, A_2), les points A, B et M ont pour coordonnées barycentriques $(\alpha, \alpha', \alpha'')$, (β, β', β'') et (x, y, z). La droite (AB) admet pour équation :*

$$\begin{vmatrix} \alpha & \beta & x \\ \alpha' & \beta & y \\ \alpha'' & \beta'' & z \end{vmatrix} = 0$$

II Convexité

1) Définition et premières propriétés

Définition 19. Soit $C \subset E$. On dit que C est convexe si, pour tous $A, B \in C$ et tout $t \in \mathbb{R}$, $\mathrm{Bar}((A,t),(B,1-t)) \in C$.

Exemple 20. *(i)* $\overline{B(0,1}$ *est convexe.*

(ii) Les convexes de $\mathbb{R}$ *sont les intervalles.*

Proposition 21. *C est convexe si, et seulement si, C contient le barycentre de toute famille de points pondérés à poids positifs de C.*

Proposition 22. *Soient $(F, \overrightarrow{F})$ un espace affine, $f : E \to F$ une application affine, C un convexe de E et T un convexe de F. Alors $f(C)$ est convexe dans F, et $f^{-1}(T)$ est convexe de E.*

Proposition 23. *Si $F \subset E$ est un sous-espace affine, alors F est convexe.*

Proposition 24. *Si C est convexe, alors C est connexe par arcs.*

Remarque 25. *Si C est convexe, alors C est connexe.*

Exemple 26. *Soient C_1 et C_2 sont convexes, et $\lambda, \mu \in \mathbb{R}$, alors $C_1 \times C_2$ et $\lambda C_1 + \mu C_2$ sont convexes.*

Exemple 27. *Le produit de n segments est convexe.*

Proposition 28. *Si C est convexe, alors $\overline{C}$ est convexe.*

Définition 29. Soit A un convexe de E. Une fonction $f : A \to \mathbb{R}$ est dite convexe lorsque :

$$\forall\, x, y \in A,\ \forall \lambda \in [0,1],\ f(\lambda x + (1-\lambda)y) \leqslant \lambda f(x) + (1-\lambda) f(y)$$

Proposition 30. *Soit A un convexe de E, et soit $f : A \to \mathbb{R}$. Alors f est convexe si, et seulement si,* $\mathrm{Epi}(f) = \{(x,t) \in E \times \mathbb{R} \,|\, x \in A, t \geqslant f(x)\}$ *est un convexe de $E \times \mathbb{R}$.*

2) Enveloppe convexe

Proposition 31. *Une intersection de convexe est convexe.*

Définition 32. Soit $A \subset E$, l'enveloppe convexe de A est le plus petit convexe contenant A. C'est aussi l'intersection de tous les convexes contenant A. On le note $\mathrm{Conv}(A)$.

Exemple 33. *Soit ABC un triangle, alors* $ABC = \mathrm{Conv}(\{A, B, C\})$.

Théorème 34. *Soit $A \subset E$ non vide.*

(i) Si A est convexe, alors $A = \mathrm{Conv}(A)$.

(ii) Si A est ouvert, alors $\mathrm{Conv}(A)$ *est ouvert.*

Contre-exemple 35. *Si* $A = \{(0,0)\} \cup \left\{(x,y) \in (\mathbb{R}^+)^2 \,\middle|\, xy \geqslant 1\right\}$ *alors,* $\mathrm{Conv}(A) = \{(0,0)\} \cup (\mathbb{R}^{+\star})^2$. *$A$ est fermé, mais pas* $\mathrm{Conv}(A)$.

Théorème 36 (Lucas)**.** *Soit $P \in \mathbb{C}[X]$ non constant. Toute racine de P' appartient à l'enveloppe convexe des racines de P.*

Théorème 37 (Carathéodory)**.** *Soit $A \subset E$. Tout élément de* $\mathrm{Conv}(A)$ *est barycentre de au plus* $\dim E + 1$ *points pondérés de A.*

Exemple 38. *Pour le cercle, il faut 2 points. Pour le carré, il en faut 3.*

Corollaire 39. *Soit $A \subset E$.*

(i) Si A est compacte, $\mathrm{Conv}(A)$ *aussi.*

(ii) Si A est bornée, $\mathrm{Conv}(A)$ *aussi, et* $\mathrm{diam}(A) = \mathrm{diam}(\mathrm{Conv}(A))$.

3) Point extrémal

Définition 40. Soit A un convexe de E. On dit que $M \in A$ est un point extrémal de A lorsque :

$$\forall\, P, Q \in A,\ \forall\, t \in [0,1],\ M = tP + (1-t)Q \Rightarrow M = P \text{ ou } M = Q$$

On note $\mathrm{Extr}(A)$ l'ensemble de ces points.

Proposition 41. *Soit A un convexe de E, et soit $M \in A$. Les assertions suivantes sont équivalentes :*

(i) $M \in \mathrm{Extr}(A)$

(ii) $A \setminus \{0\}$ *est convexe.*

(iii) Si M est barycentre à poids positifs de points de A, alors il est égal à l'un de ces points.

Exemple 42. $\mathrm{Extr}([A,B]) = \{A, B\}$

Théorème 43 (Krein-Milgram)**.** *Soit A un convexe compact non vide de E. Alors* $A = \mathrm{Conv}(\mathrm{Extr}(A))$.

Proposition 44. *Soit A un convexe de E. Si $f : A \to \mathbb{R}$ est convexe et continue, alors* $\sup_A(f) = \sup_{\mathrm{Extr}(A)}(f)$.

III Applications

1) Théorème de séparation

Définition 45. $H \subset E$ est un hyperplan affine de E s'il existe une application affine $f : E \to \mathbb{R}$ telle que $H = f^{-1}(0)$. Les parties $f^{-1}(\mathbb{R}^{-\star})$ et $f^{-1}(\mathbb{R}^{+\star})$ sont appelées demi-espaces ouverts déterminés par H.

Proposition 46. *Soient X un espace affine, A un ouvert convexe non vide et L un sous-espace affine de X tel que $A \cap L = \varnothing$. Alors il existe un hyperplan de X qui contient L et ne rencontre pas A.*

Définition 47. Soient X un espace affine, A, B deux parties de X et H un hyperplan. On dit que H sépare strictement A et B si A est dans l'un des deux demi-espaces ouverts déterminés par H et B dans l'autre.

Théorème 48 (Hahn-Banach géométrique)**.** *Si A et B sont deux convexes avec A fermé non vide et B compact tel que $A \cap B = \varnothing$. Alors il existe un hyperplan qui sépare strictement A et B.*

2) Géométrie

Théorème 49. *Soient $v_1, \dots, v_n \in \mathbb{K}^n$, on note $Vol(v_1, \dots, v_n)$ le volume du parallélépipède engendré par $v_1, \dots, v_n$, alors :*

$$Vol(v_1, \dots, v_n) = |\det(v_1, \dots, v_n)|$$

Lemme 50. *Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ symétriques définies positives distinctes, et $\alpha, \beta > 0$ tels que $\alpha + \beta = 1$, alors :*

$$\det(\alpha A + \beta B) > \det(A)^\alpha \det(B)^\beta$$

Application 51 (Ellipsoïde de John-Loewner)**.** *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant K.*

Développements

- Théorème de Carathéodory (37,39) [Gou08]
- Ellipsoïde de John-Loewner (50,51) [FGN13c]

Références

[Tau05] P. Tauvel. *Cours de Géométrie*. Dunod
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse*. Ellipses
[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3*. Cassini

I Outils de dénombrement

1) Ensembles finis

Définition 1. On appelle cardinal d'un ensemble E, noté $\mathrm{Card}(E)$ ou $|E|$, la classe des ensembles en bijection avec E. On dit que E est fini s'il est en bijection avec un ensemble $[\![1,n]\!]$, où $n \in \mathbb{N}^\star$. On notera $|E| = n$.

Remarque 2. *On doit adjoindre à cette définition le cas de l'ensemble vide, par définition fini, et de cardinal 0.*

Proposition 3. *Soient E et F deux sous-ensembles finis d'un ensemble S. Alors $E \cap F$ est fini, et on a $|E \cup F| = |E| + |F| - |E \cap F|$.*

Proposition 4. *Soit $(E_i)_{i\in[\![1,n]\!]}$ une famille de sous-ensembles disjoints et finis d'un ensemble S. Alors $\left|\bigcup_{i=1}^n E_i\right| = \sum_{i=1}^n |E_i|$.*

Proposition 5 (Formule du crible)**.** *Soit $(E_i)_{i\in[\![1,n]\!]}$ une famille de sous-ensembles finis d'un ensemble S. Alors :*

$$\left|\bigcup_{i=1}^n E_i\right| = \sum_{i=1}^n \sum_{1\leqslant i_1<\ldots<i_n\leqslant n} (-1)^{k-1} |E_{i_1} \cap \ldots \cap E_{i_k}|$$

Théorème 6. *Le produit cartésien de p ensembles finis $A_1, \ldots, A_p$ est fini, et de cardinal $\prod_{i=1}^p |A_i|$.*

Théorème 7. *Soient E et F deux ensembles finis. L'ensemble des fonctions de E vers F est de cardinal $|F|^{|E|}$.*

Application 8. *On a $|\mathcal{P}(E)| = 2^{|E|}$.*

Proposition 9 (Lemme des bergers)**.** *Soient E et F deux ensembles finis et $\varphi : E \to F$ une surjection telle que $|\varphi^{-1}(x)| = n$ pour tout $x \in F$. Alors $|E| = n|F|$.*

Proposition 10 (Principe des tiroirs)**.** *Soit E un ensemble de partition $E_1, \ldots, E_n$. Soient $x_1, \ldots, x_k \in E$. Alors un E_i contient $\lceil \frac{k}{n} \rceil$ éléments x_j.*

2) Arrangements et permutations

Soient E un ensemble de cardinal $n \in \mathbb{N}^\star$ et $p \leqslant n$.

Définition 11. Un p-arrangement de E est une injection $[\![1,p]\!] \hookrightarrow E$.

Théorème 12. *Le nombre de p-arrangement de E est $A_n^p = \frac{p!}{(n-p)!}$.*

Définition 13. Une permutation est un n-arrangement.

Application 14. *Comme E est fini, toute permutation est une bijection. Par composition, on peut associer toute permutation à une unique bijection $E \to E$, donc $|\mathfrak{S}(E)| = A_n^n = n!$*

3) Combinaisons

Soient E un ensemble de cardinal $n \in \mathbb{N}^\star$ et $p \leqslant n$.

Définition 15. Une p-combinaison de E est une partie de E à p éléments.

Proposition 16. *Le nombre de p-combinaisons de E est $\binom{n}{p} = \frac{n!}{p!(n-p)!}$.*

Proposition 17. *Pour $n \geqslant 1$ et $1 \leqslant p \leqslant n$, on a :*

- $\binom{n}{n-p} = \binom{n}{p}$
- $\binom{n-1}{p} + \binom{n-1}{p-1} = \binom{n}{p}$ *(Formule de Pascal)*
- $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = \frac{n}{n-p}\binom{n-1}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$

Proposition 18 (Binôme de Newton)**.** *Soient $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors :*

$$(a+b)^n = \sum_{i=0}^n \binom{n}{k} a^k b^{n-k}$$

Corollaire 19. *On retrouve de cardinal de $\mathcal{P}(E)$: $\sum_{k=0}^n \binom{n}{k} = 2^n$.*

Application 20. *Si $S_{n,k} = \sum_{\ell=1}^n \ell^k$, on a $1 + \sum_{k=0}^{p-1} \binom{p}{n} S_{n,k} = (n+1)^p$. On retrouve ainsi en particulier :*

$$S_{n,1} = \sum_{k=1}^n k = \frac{n(n+1)}{2} \quad \text{et} \quad S_{n,2} = \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

Application 21. *Le nombre σ_p^n de surjections d'un ensemble à n éléments dans un ensemble à p éléments est :*

$$\sigma_p^n = \sum_{k=0}^p (-1)^{p-k} \binom{p}{k} k^n$$

Application 22. *Le nombre d_n de dérangements (permutations sans point fixe) d'un ensemble à n éléments est :*

$$d_n = n! \sum_{k=0}^p \frac{(-1)^k}{k!}$$

II Dénombrement en algèbre

1) Théorie des groupes

Soit G un groupe et H un sous-groupe de G.

Définition 23. La classe à gauche de $g \in G$ est $gH = \{gh \,|\, h \in H\}$.

Proposition 24. *Pour tout $g \in G$, on a $|gH| = |H|$.*

Définition 25. L'indice $[G : H]$ de H dans G est le cardinal de G/H.

Théorème 26. *On a $|G| = |H| \times [G : H]$.*

Théorème 27 (Lagrange)**.** *Pour tout sous-groupe H de G, on a $|H| \mid |G|$.*

Application 28. *Tout groupe d'ordre premier est cyclique.*

Définition 29. Supposons que G opère sur X. Soient $x \in X$ et $g \in G$.

(i) L'orbite de x est : $O_x = \{g \cdot x \,|\, g \in G\}$.

(ii) Le stabilisateur de x est : $\mathrm{Stab}_x = \{g \in G \,|\, g \cdot x = x\}$.

(iii) Le fixateur de g est : $\mathrm{Fix}_g = \{x \in X \,|\, g \cdot x = x\}$.

Proposition 30. *Si G est fini, alors pour tout $x \in X$, $|G| = |\mathrm{Stab}_x||O_x|$.*

Théorème 31 (Équation aux classes)**.** *On suppose X et G finis. Soit θ une partie X contenant un unique représentant de chaque orbite. Alors :*

$$|X| = \sum_{x \in \theta} |O_x| = \sum_{x \in \theta} \frac{|G|}{|\,\mathrm{Stab}_x\,|}$$

Théorème 32 (Burnside)**.** *On suppose G et X finis. Soit Ω l'ensemble des orbites distinctes. Alors :*

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_g\,|$$

Application 33. *Le nombre de colliers de 5 perles différents que l'on peut réaliser avec deux couleurs est 8.*

2) Fonctions multiplicatives

Définition 34. On appelle indicatrice d'Euler de $n \geqslant 1$ l'entier :

$$\varphi(n) = \mathrm{Card}\left(\{k \in [\![1, n]\!] \,|\, k \wedge n = 1\}\right)$$

Corollaire 35. *Si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Exemple 36. *Soient p premier, alors $\varphi(p) = p-1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

Proposition 37. *(i) Pour $d|n$, $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(d)$ éléments d'ordre d.*
(ii) (Formule de Möbius) $n = \sum_{d|n} \varphi(n)$

Proposition 38. *Si on note μ_n l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbb{C}$, on a $|\mu_n| = \varphi(n)$.*

Corollaire 39. *Le n-ième polynôme cyclotomique est de degré $\varphi(n)$.*

Définition 40. La fonction de Möbius $\mu : \mathbb{N}^\star \to \{0, 1, -1\}$ se définit par :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est sans facteur carré} \\ 0 & \text{sinon} \end{cases}$$

Proposition 41. *La fonction de Möbius est multiplicative sur $\mathbb{N}^\star$.*

Proposition 42. $\sum_{d|n} \mu(d) = 0$

Théorème 43. *Soient p premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Proposition 44 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall\, n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Corollaire 45. *Si $I(q, d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

$$I(q, n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{+\infty}{\sim} \frac{q^n}{n}$$

III Dénombrement en analyse

1) Utilisation en probabilités

Soit Ω un ensemble fini. On considère l'espace probabilisé $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$, où $\mathbb{P}$ est la loi uniforme sur Ω. Pour une partie A de Ω, on a alors $\mathbb{P}(A) = \frac{|A|}{|\Omega|}$. Ainsi, savoir dénombrer des ensembles permet de calculer des probabilités.

Exemple 46. *Dans un tirage avec remise, il y a n^p issues possibles.*

Exemple 47. *Dans un tirage sans remise, il y a A_n^p issues possibles.*

Exemple 48. *Une course de 20 chevaux a 1140 tiercés dans le désordre.*

Exemple 49. *Soit $n \leqslant 365$. En ne considérant pas les années bissextiles, la probabilité que deux personnes parmi n aient la même date d'anniversaire est $p_n = 1 - \frac{365!}{365^n \times (365-n)!}$.*

2) Séries génératrices

Définition 50. Soit $(u_n)_{n\in\mathbb{N}}$ une suite complexe. On définit sa série génératrice par $S(z) = \sum_{n\in\mathbb{N}} u_n z^n$.

Exemple 51. *La suite constante égale à 1 a pour série génératrice $S(z) = \frac{1}{1-z}$.*

Application 52 (Nombres de Catalan)**.** *On note C_n le nombre de parenthésages possibles d'un produit de $n+1$ facteurs. On a alors la relation $C_n = \sum_{k=1}^{n-1} C_k C_{n-k}$, et on obtient $C_n = \frac{1}{n+1}\binom{2n}{n}$.*

Application 53 (Nombres de Bell)**.** *Pour $n \in \mathbb{N}^\star$, on pose B_n le nombre de partitions de l'ensemble $[\![1, n]\!]$ avec la convention $B_0 = 1$, alors :*

$$\forall\, k \in \mathbb{N},\ B_k = \frac{1}{e} \sum_{n\geqslant 0} \frac{n^k}{n}$$

Développements

- Polynômes irréductibles unitaires sur $\mathbb{F}_q$ (43,44,45) [Tau08]
- Nombres de Bell (53) [FGN13a]

Références

[dB04] J. de Biasi. *Mathématiques pour le CAPES et l'agrégation interne.* Ellipses
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet

Cadre : Soit E un $\mathbb{R}$-espace vectoriel de dimension finie $n \in \mathbb{N}^\star$.

I Géométrie affine

1) Espace affine, sous-espace affine

Définition 1. Un ensemble $\mathcal{E}$ est un espace affine s'il existe une application $\mathcal{E} \times \mathcal{E} \to E$ qui à $A, B \in \mathcal{E}$ associe un vecteur $\overrightarrow{AB} \in E$ telle que :

(i) Pour tout $A \in \mathcal{E}$, l'application $B \mapsto \overrightarrow{AB}$ est linéaire.

(ii) $\forall A, B, C \in \mathcal{E},\ \overrightarrow{AB} = \overrightarrow{AC} + \overrightarrow{CB}$.

Exemple 2. *L'ensemble vide et les $\mathbb{R}^n$ sont des espaces affines.*

Proposition 3. *Pour tous $A, A', B, B' \in \mathcal{E}$, on a $\overrightarrow{AA} = 0$, $\overrightarrow{AB} = -\overrightarrow{BA}$ et $\overrightarrow{AB} = \overrightarrow{A'B'} \Leftrightarrow \overrightarrow{AA'} = \overrightarrow{BB'}$.*

Définition 4. On dit qu'un ensemble $\mathcal{F}$ de $\mathcal{E}$ est un sous-espace affine s'il est vide ou s'il contient un point A tel que $\left\{ \overrightarrow{AB} \,\middle|\, B \in \mathcal{F} \right\}$ soit un sous-espace vectoriel de E.

Proposition 5. *Soit F un sous-espace vectoriel de E et soit A un point de $\mathcal{E}$. Il existe un unique sous-espace affine dirigé par F et passant par A.*

Exemple 6. *L'ensemble des solutions d'un système linéaire est un sous-espace affine dirigé par l'ensemble des solutions du système sans second membre associé.*

Définition 7. On appelle droite (resp. plan) tout espace affine de dimension 1 (resp. 2).

Définition 8. Deux espaces affines de même direction sont dits parallèles.

Exemple 9. *Soit $f \in \mathcal{L}(E, F)$. Tous les $f^{-1}(v)$, où $v \in \mathrm{Im}(f)$, sont parallèles et dirigés par* $\mathrm{Ker}(f)$.

Proposition 10. *Pour tout point d'un espace affine, il passe une unique droite parallèle à une droite donnée.*

2) Application affine

Définition 11. Soient $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines dirigés respectivement par E et F. Une application $\varphi : \mathcal{E} \to \mathcal{F}$ est dite affine s'il existe un point $O \in \mathcal{E}$ et une application linéaire $\overrightarrow{\varphi} : E \to F$ tels que, pour tout $M \in \mathcal{E}$, on a $\overrightarrow{\varphi}(\overrightarrow{OM}) = \overrightarrow{\varphi(O)\varphi(M)}$. L'ensemble des applications affines de $\mathcal{E}$ dans $\mathcal{E}$ est noté $\mathcal{GA}(\mathcal{E})$.

Proposition 12. *$\mathcal{GA}(\mathcal{E})$ est un groupe.*

Proposition 13. *Si E et F sont deux espaces vectoriels munis de leurs structures affines naturelles, une application $\varphi : E \to F$ est affine si, et seulement si, il existe un vecteur $x_0 \in F$ et une application linéaire $\overrightarrow{\varphi} : E \to F$ telle que, pour tout $x \in E$, on a $\varphi(x) = \overrightarrow{\varphi(x)} + x_0$.*

Exemple 14. *(i) Si $\mathcal{E} = \mathcal{F} = \mathbb{R}$, les applications affines sont les applications de la forme $x \mapsto ax + b$.*

(ii) Si $\mathcal{E} = \mathcal{F}$, les applications affines dont l'application linéaire associée est Id_E sont les translations.

Proposition 15. *L'image d'un sous-espace affine par une application affine est un sous-espace affine.*

Corollaire 16. *Les applications affines conservent l'alignement, le parallélisme et les barycentres.*

3) Utilisation du groupe affine

Théorème 17 (Thalès)**.** *Soient d, d', d'' des droites parallèles distinctes, D_1, D_2 deux droites dont aucune n'est parallèle à d. Soient, pour $i \in \{1, 2\}$, $A_i = D_i \cap d$, $A'_i = D_i \cap d'$, $A''_i = D_i \cap d''$. Alors $\frac{\overline{A_1A''_1}}{\overline{A_1A'_1}} = \frac{\overline{A_2A''_2}}{\overline{A_2A'_2}}$. Réciproquement, si un point B de D_1 vérifie $\frac{\overline{A_1B}}{\overline{A_1A'_1}} = \frac{\overline{A_2A''_2}}{\overline{A_2A'_2}}$, alors $B = A''_1$.*

Corollaire 18. *Soient D_1, D_2 deux droites sécantes en A, d, d' deux droites parallèles coupant D_i en A_i, A'_i distincts de A. Alors $\frac{\overline{AA_i}}{\overline{AA'_i}} = \frac{\overline{A_1A_2}}{\overline{A'_1A'_2}}$.*

Théorème 19 (Pappus)**.** *Soient D, D' des droites distinctes, A, B, C des points de D et A', B', C' des points de D'. Si (AB') est parallèle à $(A'B)$ et (BC') est parallèle à $(B'C)$, alors (AC') est parallèle à $(A'C)$.*

Théorème 20 (Desargues)**.** *Soient ABC et $A'B'C'$ deux triangles sans sommet commun et à côtés respectivement parallèles. Alors les droites AA', BB' et CC' sont concourantes ou parallèles.*

II Géométrie euclidienne

1) Définition et groupe d'isométrie

Définition 21. Un espace vectoriel muni d'un produit scalaire est dit espace vectoriel euclidien. Un espace affine euclidien est un espace affine dirigé par un espace vectoriel euclidien. On définit la distance de deux points A et B par $d(A,B) = \left\|\overrightarrow{AB}\right\| = AB$.

Définition 22. Pour $A \subset \mathcal{E}$ et $x \in \mathcal{E}$, la distance de x à A est :

$$d(x,A) = \inf_{y\in A} d(x,y)$$

Proposition 23. *Soient $x \in E$ et F un sous-espace vectoriel de E. Alors $y \in E$ est la projection orthogonale de x sur F si, et seulement si, $y \in F$ et $d(x,F) = \|x-y\|$.*

Définition 24. Une isométrie vectorielle est une application linéaire qui conserve la norme. On note $\mathcal{O}(E)$ l'ensemble des isométries vectorielles de E dans E.

Remarque 25. *Une isométrie vectorielle conserve le produit scalaire, donc l'orthogonalité.*

Définition 26. Soient $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines euclidiens. Une isométrie affine est une application affine $\varphi : \mathcal{E} \to \mathcal{F}$ telle que $d(\varphi(A),\varphi(B)) = d(A,B)$ pour tous $A, B \in \mathcal{E}$. On note $\mathrm{Isom}(\mathcal{E})$ l'ensemble des isométries vectorielles de $\mathcal{E}$ dans $\mathcal{E}$.

Exemple 27. *Les translations, les rotations et les symétries orthogonales sont des isométries.*

Proposition 28. *Une application affine est une isométrie affine si, et seulement si, sa partie linéaire est une isométrie vectorielle.*

Théorème 29. *$(\mathcal{O}(E),\circ)$ et $(\mathrm{Isom}(\mathcal{E}),\circ)$ sont des groupes.*

Proposition 30. *Soit F un sous-espace vectoriel de E stable par une isométrie $f \in \mathcal{O}(E)$. Alors $F^\perp$ est stable par f.*

2) Matrice et déterminant de Gram

Définition 31. On appelle matrice de Gram de $(x_i)_{1\leqslant i\leqslant n}$ la matrice $M_G(x_1,\dots,x_n) = (\langle x_i, x_j\rangle)_{1\leqslant i,j\leqslant n}$, et déterminant de Gram le déterminant de cette matrice, noté $G(x_1,\dots,x_n)$.

Lemme 32. *Le déterminant de Gram d'une famille de vecteurs est nul si, et seulement si, elle est liée.*

Théorème 33. *Soit F un sous-espace vectoriel de E de dimension finie $n \in \mathbb{N}^\star$ muni d'une base $(e_i)_{1\leqslant i\leqslant n}$. Alors, pour tout $x \in E$, on a :*

$$d(x,F)^2 = \frac{G(e_1,\dots,e_n,x)}{G(e_1,\dots,e_n)}$$

Théorème 34 (Hadamard)**.** *(i) Soient $x_1,\dots,x_n$ des vecteurs de E. Alors $G(x_1,\dots,x_n) \leqslant \prod_{i=1}^n \|x_i\|^2$.*

(ii) Soient $x_1,\dots,x_n \in \mathbb{C}^n$. Alors $|\det(x_1,\dots,x_n)| \leqslant \prod_{i=1}^n \|x_i\|_2$.

Dans les deux cas, on a égalité si, et seulement si, $(x_i)_{1\leqslant i\leqslant n}$ est orthogonale ou l'un des vecteurs est nul.

3) Similitudes et nombres complexes

Définition 35. On dit que $f \in \mathcal{L}(E)$ est une similitude vectorielle s'il existe $k > 0$, appelé rapport de la similitude, tel que, pour tout $x \in E$, on a $\|f(x)\| = k\|x\|$. On appelle similitude affine toute application affine dont la partie linéaire est une similitude vectorielle.

Exemple 36. *Les isométries et les homothéties sont des similitudes.*

Définition 37. Une similitude est dite directe ou indirecte selon que son déterminant est positif ou négatif.

Proposition 38. *Soit f une similitude vectorielle de rapport k. Il existe une unique isométrie vectorielle u telle que $f = h_k \circ u$, où h_k est l'homothétie de rapport k.*

Proposition 39. *(i) Les similitudes directes conservent les angles.*

(ii) Une similitude directe de rapport k envoie un cercle de rayon R sur un cercle de rayon kR dont le centre est l'image du centre.

Application 40. *On identifie le plan affine euclidien muni d'un repère orthonormé avec le plan complexe $\mathbb{C}$. Les similitudes directes sont de la forme $z \mapsto az+b$, où $a \in \mathbb{C}^\star$ et $b \in \mathbb{C}$. Les similitudes indirectes sont de la forme $z \mapsto a\overline{z}+b$, où $a \in \mathbb{C}^\star$ et $b \in \mathbb{C}$.*

III Polygones et polyèdres convexes

Définition 41. Un polygone convexe de $\mathbb{R}^2$ est dit régulier si tous ses côtés sont de même longueur, et si les angles entre deux côtés sont égaux.

Définition 42. On appelle groupe diédral le groupe D_n formé des isométries du polygone régulier à n cotés.

Proposition 43. *D_n est engendré par une symétrie et une rotation.*

Définition 44. Un polyèdre convexe de $\mathbb{R}^3$ est dit régulier si toutes ses faces sont des polygones réguliers isométriques, et si en chaque sommet elles s'assemblent de la même manière, au sens où les figures formées par les réunions des arêtes aboutissant à un sommet sont isométriques.

Exemple 45. *Il y a 5 polyèdres réguliers : le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre.*

Théorème 46. *Soit $\mathcal{T}$ un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$.*

Application 47. *La table de caractères de $\mathfrak{S}_4$ est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

IV Coniques

Définition 48. Une fonction polynômiale de degré 2 sur $\mathcal{E}$ est une application $f : \mathcal{E} \to \mathbb{R}$ telle qu'il existe un point $O \in \mathcal{E}$, une forme quadratique non nulle q sur E, une forme linéaire L_0 sur E et une constante $c_O \in \mathbb{R}$ tels que : $\forall\, M \in \mathcal{E},\ f(M) = q(\overrightarrow{OM}) + L_O(\overrightarrow{OM}) + c_O$.

Remarque 49. *q ne dépend pas du point d'origine O choisi.*

Définition 50. On appelle quadrique affine la classe d'équivalence d'une fonction polynômiale de degré 2 $f : \mathcal{E} \to \mathbb{R}$ sous la relation "$f \sim g$ si, et seulement si, g est un multiple scalaire de f". Une quadrique plane est appelée conique. L'ensemble des points de E vérifiant $f(M) = 0$ est l'image de la quadrique.

Remarque 51. *Les équations $x^2 + y^2 + 1 = 0$ et $x^2 + 1 = 0$ définissent le même ensemble de points du plan $\mathbb{R}^2$.*

Définition 52. La quadrique définie par $f(M) = q(\overrightarrow{OM}) + L(\overrightarrow{OM}) + c$ est dite propre si la forme quadratique $Q(x, y, z) = q(x, y) + L(x, y)z + cz^2$ définie sur $E \times \mathbb{R}$ est non dégénérée. Cette forme quadratique est dite homogénéisée de q.

Proposition 53 (Classification des coniques propres)**.**

sgn(Q)	*sgn(q)*	*Classe*	*Exemple*
$(3,0)$ *ou* $(0,3)$	$(2,0)$ *ou* $(0,2)$	$\varnothing$	$x^2 + y^2 = -1$
$(2,1)$ *ou* $(1,2)$	$(2,0)$ *ou* $(0,2)$	*Ellipse*	$x^2 + y^2 = 1$
$(2,1)$ *ou* $(1,2)$	$(1,1)$	*Hyperbole*	$x^2 - y^2 = 1$
$(2,1)$ *ou* $(1,2)$	$(1,0)$ *ou* $(0,1)$	*Parabole*	$x^2 + y = 0$

Proposition 54 (Classification des coniques impropres)**.**

sgn(Q)	*sgn(q)*	*Classe*	*Exemple*
$(2,0)$ *ou* $(0,2)$	$(2,0)$ *ou* $(0,2)$	*Point*	$x^2 + y^2 = 0$
$(2,0)$ *ou* $(0,2)$	$(1,0)$ *ou* $(0,1)$	$\varnothing$	$x^2 = -1$
$(1,1)$	$(1,1)$	*Droites sécantes*	$x^2 - y^2 = 0$
$(1,1)$	$(1,0)$ *ou* $(0,1)$	*Droites parallèles*	$x^2 = 1$
$(1,0)$ *ou* $(0,1)$	$(1,0)$ *ou* $(0,1)$	*Droite double*	$x^2 = 0$

Développements

- Déterminant de Gram et inégalité de Hadamard (32,33,34) [Gou08]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (46,47) [Ser70]

Références

[Aud06] M. Audin. *Géométrie.* EDP Sciences
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann

Annexes

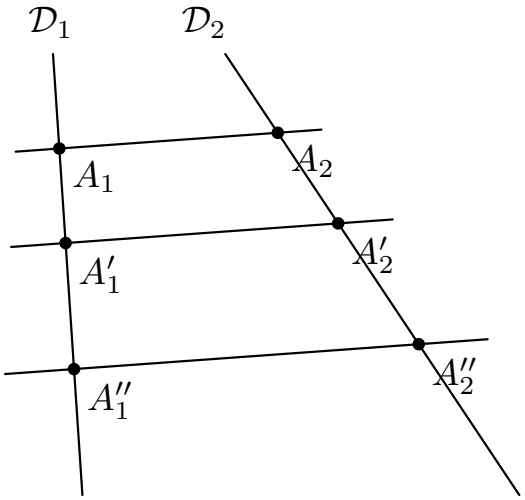


FIGURE 1 – Théorème de Thalès

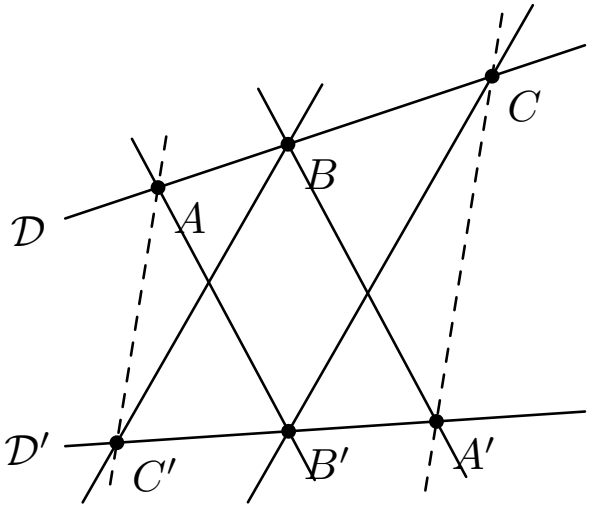


FIGURE 2 – Théorème de Pappus

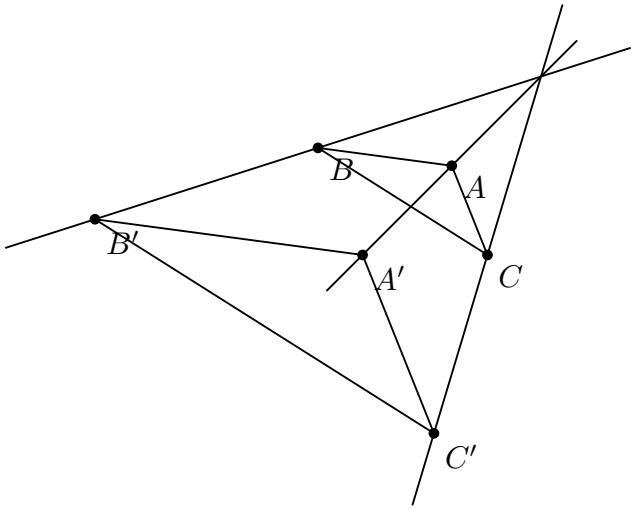


FIGURE 3 – Théorème de Desargues

Partie II

Leçons Analyse et Probabilités

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{ab}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\frac{\sqrt[n]{a}}{\sqrt[n]{b}} = \sqrt[n]{\frac{a}{b}}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$a\sqrt[n]{b} = \sqrt[n]{a^n b}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{i=n} x_i = \frac{x_1 + x_2 + \ldots + x_n}{n}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet

mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\int_0^\infty e^{-\alpha x^2}\mathrm{d}x = \frac{1}{2}\sqrt{\int_{-\infty}^\infty e^{-\alpha x^2}\mathrm{d}x \int_{-\infty}^\infty e^{-\alpha y^2}\mathrm{d}y} = \frac{1}{2}\sqrt{\frac{\pi}{\alpha}}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Liste des leçons d'analyse et de probabilités

Cadre : On considère $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soient $a, b \in \mathbb{R}$ avec $a < b$. On note $I =]a, b[$. Soient $(X, \mathcal{A}, \mu)$ un espace mesuré, $p \in [1, +\infty]$ et q son exposant conjugué tel que $\frac{1}{p} + \frac{1}{q} = 1$.

I Espaces de fonctions continues

1) Généralités

Définition 1. On définit $\mathcal{C}^0([a,b], \mathbb{K})$ comme l'ensemble des fonctions continues de $[a, b]$ dans $\mathbb{K}$.

Définition 2. Soit $f \in \mathcal{C}^0([a,b], \mathbb{K})$. On définit la norme uniforme $\|.\|_\infty$ par $\|f\|_\infty = \sup_{x \in [a,b]} |f(x)|$.

Définition 3. Soit $(f_n)_{n \in \mathbb{N}}$ une suite de $\mathcal{C}^0([a,b], \mathbb{K})$. On dit que $(f_n)_{n \in \mathbb{N}}$ converge uniformément vers une fonction $f : [a, b] \to \mathbb{K}$ lorsque :

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ \forall x \in [a,b],\ |f_n(x) - f(x)| \leqslant \varepsilon$$

Cela revient à dire que $\lim_{n \to \infty} \|f_n - f\|_\infty = 0$.

Théorème 4. *Un limite uniforme de fonctions continues est continue.*

Corollaire 5. *L'espace $(\mathcal{C}^0([a,b], \mathbb{K}), \|.\|_\infty)$ est un espace de Banach.*

Exemple 6. *La suite $(f_n)_{n \in \mathbb{N}}$ définie sur $[0, 1]$ par $f_n(x) = \left(1 - \frac{x}{n}\right)^n$ converge uniformément vers $x \mapsto e^{-x}$.*

Exemple 7. *La suite $(f_n)_{n \in \mathbb{N}}$ définie sur $[0, 1]$ par $f_n(x) = x^n$ ne converge pas uniformément.*

Théorème 8 (Heine)**.** *Toute fonction de $\mathcal{C}^0([a,b], \mathbb{K})$ est uniformément continue.*

Lemme 9 (Dini)**.** *Toute suite croissante de $\mathcal{C}^0([a,b], \mathbb{K})$ qui converge simplement dans $\mathcal{C}^0([a,b], \mathbb{K})$ converge uniformément.*

Application 10. *Soit $(P_n)_{n \in \mathbb{N}}$ la suite de $\mathcal{C}^0([a,b], \mathbb{K})$ définie par $P_0 = 0$ et $P_{n+1}(x) = P_n(x) + \frac{1}{2}(x^2 - P_n^2(x))$ pour $n \in \mathbb{N}$ et $x \in [-1, 1]$. Alors $(P_n)_{n \in \mathbb{N}}$ converge uniformément vers $x \mapsto |x|$.*

Théorème 11 (Weierstrass)**.** *Soient $f \in \mathcal{C}^0([a,b], \mathbb{R})$ et $\varepsilon > 0$. Il existe P une fonction polynomiale à coefficients réels telle que $\|f - P\|_\infty \leqslant \varepsilon$.*

Application 12. *Soit $f \in \mathcal{C}^0([a,b], \mathbb{K})$ vérifiant $\int_a^b t^n f(t)\, dt = 0$ pour tout $n \in \mathbb{N}$. Alors $f = 0$ sur $[a, b]$.*

2) Théorème d'Ascoli

Définition 13. Une partie Y de $\mathcal{C}^0([a,b], \mathbb{K})$ est dite équicontinue si :

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall f \in Y,\ |x - y| < \eta \Rightarrow |f(x) - f(y)| < \varepsilon$$

Exemple 14. *(i) Une partie finie de $\mathcal{C}^0([a,b], \mathbb{K})$ est équicontinue.*

(ii) Une suite uniformément convergente de fonctions de $\mathcal{C}^0([a,b], \mathbb{K})$ forme une famille équicontinue.

(iii) L'ensemble des fonctions lipschitziennes est équicontinu.

Théorème 15 (Ascoli)**.** *Soit $Y \subseteq \mathcal{C}^0([a,b], \mathbb{K})$. Sont équivalentes :*

(i) Y est équicontinue et bornée pour la norme uniforme.

(ii) $\overline{Y}$ est compacte.

Application 16. *Soient X et Y deux espaces métriques compacts, μ une mesure borélienne finie et $K \in \mathcal{C}^0(X \times Y, \mathbb{K})$. On considère l'application :*

$$T : \left| \begin{array}{ccc} \mathcal{C}^0(Y, \mathbb{K}) & \longrightarrow & \mathcal{C}^0(X, \mathbb{K}) \\ x & \longmapsto & \int_Y K(x,y) f(y)\, d\mu(y) \end{array} \right.$$

Alors $T\left(B_{\mathcal{C}^0(Y,\mathbb{K})}(0,1)\right)$ est relativement compact dans $\mathcal{C}^0(X, \mathbb{K})$.

II Espaces L^p

1) Définitions et premières propriétés

Définition 17. Pour tout réel $p > 0$, on définit le $\mathbb{K}$-espace vectoriel :

$$\mathscr{L}^p_{\mathbb{K}}(X, \mathcal{A}, \mu) = \left\{ f : X \to \mathbb{K} \text{ mesurable} \,\middle|\, \int_X |f|^p\, d\mu < +\infty \right\}$$

Sauf situation ambiguë, on privilégiera la notation plus concise $\mathscr{L}^p_{\mathbb{K}}(\mu)$.

Exemple 18. *Dans le cas de la mesure de comptage, cette définition donne les espaces $\ell_{\mathbb{K}}(\mathbb{N})$ des suites de puissance p sommable.*

Proposition 19. *Soient $0 < p \leqslant q$ des réels.*

(i) Si μ est finie, alors $\mathscr{L}^p_{\mathbb{K}}(\mu) \supset \mathscr{L}^q_{\mathbb{K}}(\mu)$.

(ii) Si on considère la mesure de comptage sur $\mathbb{N}$, alors $\ell^p_{\mathbb{K}}(\mathbb{N}) \supset \ell^q_{\mathbb{K}}(\mathbb{N})$.

Remarque 20. *Il n'y a pas, en général, d'inclusion entre les espaces $\mathscr{L}^p$.*

Définition 21. Pour toute fonction $f : X \to \mathbb{K}$ et tout $p > 0$, on définit :

$$\|f\|_p = \left(\int_X |f|^p \, d\mu\right)^{\frac{1}{p}} \quad \left(\text{convention : } \infty^{\frac{1}{p}} = \infty\right)$$

Théorème 22 (Hölder)**.** *Soient $f \in \mathscr{L}^p_{\mathbb{K}}(\mu)$ et $g \in \mathscr{L}^q_{\mathbb{K}}(\mu)$, où $\frac{1}{p} + \frac{1}{q} = 1$. Alors $\|fg\|_1 \leqslant \|f\|_p \|g\|_q$.*

Théorème 23 (Minkowski)**.** *Soient $p \in [1, +\infty[$ et $f, g \in \mathscr{L}^p_{\mathbb{K}}(\mu)$. Alors $\|f + g\|_p \leqslant \|f\|_p + \|g\|_p$.*

Définition 24. Pour $1 \leqslant p < +\infty$, on définit $L^p_{\mathbb{K}}(\mu)$ comme l'espace vectoriel normé quotient de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ par les fonctions presque nulles. On associera par abus de langage un élément de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ à sa classe dans $L^p_{\mathbb{K}}(\mu)$.

Définition 25. On définit le supremum essentiel de $f : X \to \overline{\mathbb{R}^+}$ par :

$$\|f\|_\infty = \text{supess}(f) = \inf\{M > 0 \,|\, \mu(\{f > M\}) = 0\} \geqslant 0$$

On note $\mathscr{L}^\infty_{\mathbb{K}}(\mu)$ l'ensemble des fonctions essentiellement bornées.

Définition 26. On définit $L^\infty_{\mathbb{K}}(\mu)$ comme l'espace vectoriel normé quotient de $\mathscr{L}^\infty_{\mathbb{K}}(\mu)$ par les fonctions presque nulles.

Remarque 27. *En considérant 1 et ∞ comme exposants conjugués, on retrouve les inégalités de Hölder et de Minkowski.*

Théorème 28 (Riesz-Fischer)**.** *Pour tout $1 \leqslant p \leqslant +\infty$, $L^p_{\mathbb{K}}(\mu)$ est un espace de Banach.*

2) Convolution, densité et régularisation

Définition 29. On appelle convolution de f et g la fonction $f * g$ définie par $f * g(x) = \int_{\mathbb{R}^d} f(y)g(x-y)\,dy$ lorsque celle-ci est bien définie.

Proposition 30. *(i) $f \in L^1$, $g \in L^p \Rightarrow \|f * g\|_p \leqslant \|f\|_1 \|g\|_p$.*
(ii) $f \in L^p$, $g \in L^q \Rightarrow \|f * g\|_\infty \leqslant \|f\|_p \|g\|_q$.

Proposition 31. *$(L^1, +, *)$ est une algèbre de Banach.*

Définition 32. Une suite $(\rho_n)_{n\in\mathbb{N}}$ de fonctions positives de L^1 d'intégrale 1 sur $\mathbb{R}^d$ est une approximation de l'unité si elles sont d'intégrale 1 sur $\mathbb{R}^d$, et si, pour tout $\varepsilon > 0$, $\lim_{n\to\infty} \int_{\{|x|>\varepsilon\}} \rho_n = 0$. Si les ρ_n sont $\mathcal{C}^\infty$ à support compact, on parle de suite régularisante.

Théorème 33. *Soient $f \in L^p(\mathbb{R}^d)$ et $(\rho_n)_n$ une approximation de l'identité ($p \in [1, +\infty[$), alors $\lim\limits_{n\to+\infty} (\rho_n * f) = f$ dans $L^p(\mathbb{R}^d)$.*

Théorème 34. *Pour tout $p \in [1, +\infty[$, $\mathcal{C}^\infty_c(\mathbb{R}^d)$ est dense dans $L^p(\mathbb{R}^d)$.*

3) Cas particulier de L^2

Définition 35. L'application $(f, g) \mapsto \langle f, g\rangle_{L^2_{\mathbb{K}}} = \int_X fg\,d\mu$ définit un produit scalaire. On note $\|.\|_{L^2_{\mathbb{K}}} = \|.\|_2$ la norme associée.

Corollaire 36. *$\left(L^2_{\mathbb{K}}(\mu), \langle ., .\rangle_{L^2_{\mathbb{K}}}\right)$ est un espace de Hilbert.*

Théorème 37. *Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. S'il existe $a > 0$ tel que $\int_I e^{a|x|}\rho(x)dx < \infty$, alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I, \rho)$.*

III Espaces de Sobolev

Définition 38. Soit $f \in L^1(I)$. On dit que f admet une dérivée faible s'il existe $g \in L^1(I)$ tel que, pour tout $\varphi \in \mathcal{C}^\infty_c(I)$, on a $\int_I f\varphi' = -\int_I g\varphi$. On note alors $g = f'$, qui est unique.

Définition 39. On définit $H^1(I) = \left\{f \in L^2(I) \,\middle|\, f' \in L^2(I)\right\}$, que l'on munit du produit scalaire défini par $\langle f, g\rangle_{H^1} = \langle f, g\rangle_{L^2} + \langle f', g'\rangle_{L^2}$.

Théorème 40. *$\left(H^1(I), \langle ., .\rangle_{H^1}\right)$ est un espace de Hilbert.*

Définition 41. On définit $H^1_0(I)$ comme l'adhérence de $\mathcal{C}^\infty_c(I)$ dans $H^1(I)$. $H^1_0(I)$ est un espace de Hilbert lorsqu'il est munit du produit scalaire $\langle ., .\rangle_{H^1}$.

Théorème 42 (Riesz)**.** *Soient H un espace de Hilbert et $\varphi : H \to \mathbb{R}$ une forme linéaire continue. Alors il existe un unique $u \in H$ tel que $\langle u, v\rangle = \varphi(v)$ pour tout $v \in H$.*

Théorème 43 (Lax-Milgram)**.** *Soient H un espace de Hilbert, a une forme bilinéaire continue et coercive sur H, et ℓ une forme linéaire et continue sur H. Alors :*

$$\exists!\, u \in H,\ \forall\, v \in H,\ a(u, v) = \ell(v)$$

Si de plus a est symétrique, u est caractérisé par :

$$\frac{1}{2}a(u, u) - \ell(u) = \min_{v\in H}\left\{\frac{1}{2}a(v, v) - \ell(v)\right\}$$

Application 44 (Dirichlet)**.** *Pour $f \in L^2$, on considère le problème :*

$$\begin{cases} -u'' + u = f & sur\ ]0,1[\\ u(0) = u(1) = 0 \end{cases}$$

Il existe une unique solution faible $u \in H_0^1$ à ce problème.

Développements

— Théorème de Riesz-Fischer (28) [Bre87]
— Densité des polynômes orthogonaux (37) [BMP05]
— Théorème de Weierstrass (11) [Gou08]

Références

[BP12] M. Briane et G. Pagès. *Théorie de l'intégration.* Vuilbert
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[Bre87] H. Brezis. *Analyse fonctionelle.* Masson
[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod

Cadre : On fixe (E, d) un espace métrique, qui est donc séparable.

I Généralités sur la compacité

1) Propriété de Borel-Lebesgue

Définition 1. Un espace métrique (E, d) est compact s'il vérifie la propriété de Borel-Lebesgue : de tout recouvrement de E par des ouverts, on peut extraire un sous-recouvrement fini. On dit qu'une partie $A \subset E$ est compacte si elle est compact pour la topologie induite.

Remarque 2. *Cette définition a un analogue en topologie générale, mais on y adjoint une condition de séparation, toujours réalisée dans le cas d'un espace métrique.*

Exemple 3. *(i)* $\mathbb{R}$ *n'est pas compact*

(ii) Tout espace métrique fini est compact.

(iii) $[0, 1] \subset \mathbb{R}$ *est compact.*

Exemple 4. *Tout espace métrique compact est borné.*

Proposition 5. (E, d) *est un compact si, et seulement si, de toute intersection vide de fermés de* E *on peut extraire une sous-famille finie d'intersection vide.*

Proposition 6. *Toute suite décroissante de fermés non vides d'un espace compact* E *admet une intersection non vide.*

Contre-exemple 7. *Dans* $\mathbb{R}^n$, $F_n = [n, +\infty[$ *contredit cette conclusion.*

Proposition 8. *Une réunion finie de compacts est compacte. Une intersection de compacts est compacte.*

2) Théorème de Bolzano-Weierstrass

Théorème 9 (Bolzano-Weierstrass)**.** *Un espace métrique* (E, d) *est compact si, et seulement si, de toute suite de points de* E *on peut extraire une sous-suite convergente dans* E.

Corollaire 10. *Un espace métrique* (E, d) *est compact si, et seulement si, toute partie infinie de* E *admet un point d'accumulation dans* E.

Corollaire 11. *Un fermé d'un compact est compact.*

Corollaire 12. *Tout espace métrique compact est complet.*

Définition 13. E est dit précompact si, pour tout $\varepsilon > 0$, il existe un recouvrement de E par une famille finie de boules ouvertes de rayon ε.

Théorème 14. *Un espace métrique* (E, d) *est compact si, et seulement si, il est précompact et complet.*

Corollaire 15. *Les segments de* $\mathbb{R}$ *sont compacts.*

Proposition 16. *Soit* (E, d) *un espace métrique compact et* $(u_n)_{n\in\mathbb{N}}$ *une suite de* E *telle que* $\lim_{n\to+\infty} d(u_n, u_{n+1}) = 0$. *Alors l'ensemble des valeurs d'adhérence de* $(u_n)_{n\in\mathbb{N}}$ *est connexe.*

Application 17. *Soient* $f : [0, 1] \to [0, 1]$ *une fonction continue et* $(x_n)_{n\in\mathbb{N}}$ *la suite définie par* $x_0 \in [0, 1]$ *et* $u_{n+1} = f(u_n)$ *pour tout* $n \in \mathbb{N}$. *Alors* $(x_n)_{n\in\mathbb{N}}$ *converge si, et seulement si,* $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.

II Fonctions continues sur un compact

1) Continuité et extrema

Soit $f : E \to F$ continue avec E compact et F un espace métrique.

Proposition 18. $f(E)$ *est compact.*

Proposition 19. *Si* f *est bijective, c'est un homéomorphisme.*

Corollaire 20. *Si* $F = \mathbb{R}$, *alors* f *est bornée et atteint ses bornes.*

Application 21 (Rolle)**.** *Soit* $f : [a, b] \to \mathbb{R}$ *continue et dérivable sur* $]a, b[$ *telle que* $f(a) = f(b)$. *Alors il existe* $c \in]a, b[$ *tel que* $f'(c) = 0$.

Application 22 (Ellipsoïde de John-Loewner)**.** *Soit* K *un compact d'intérieur non vide de* $\mathbb{R}^n$, *alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant* K.

Proposition 23. *Soit* E *un espace vectoriel normé de dimension finie et* $f : E \to \mathbb{R}$ *continue et coercive. Alors* f *admet un minimum sur* E.

Application 24 (D'Alembert-Gauss)**.** *Tout polynôme de* $\mathbb{C}[X]$ *admet une racine dans* $\mathbb{C}$.

Application 25. *Soient* $F \subset E$ *compact et* $a \in E$. *Il existe* $x \in F$ *tel que* $d(a, F) = d(a, x)$.

Application 26. *Soit* $f : [0, 1] \to \mathbb{R}$ *continue et* $n \in \mathbb{N}^\star$. *Il existe* $P \in \mathbb{R}_n[X]$ *qui réalise la distance de* f *à* $\mathbb{R}_n[X]$. *C'est le polynôme de meilleure approximation de* f *de degré* n.

2) Théorème de Heine

Théorème 27 (Heine)**.** *Toute application continue $f : E \to F$ où E est compact est uniformément continue.*

Exemple 28. *$x \mapsto \sin(x^2)$ n'est pas continue sur $\mathbb{R}$, contrairement à* sin.

Proposition 29. *Toute fonction continue de $\mathbb{R}$ dans $\mathbb{C}$ et périodique est uniformément continue.*

Proposition 30. *Toute fonction continue de $\mathbb{R}$ dans $\mathbb{R}$ admettant des limites finies en $\pm\infty$ est uniformément continue.*

Application 31. *Soit $f : [0,1] \to \mathbb{R}$ continue. Alors $\int_0^1 f(t)dt = \lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} f\left(\frac{k}{n}\right)$.*

Théorème 32 (Dini)**.** *Soit $f_n : [a,b] \to \mathbb{R}$ continues et convergeant simplement vers $f : [a,b] \to \mathbb{R}$ continue. Si les f_n sont croissantes, alors la convergence est uniforme.*

3) Théorèmes de points fixes

Théorème 33. *Soient E compact et $f : E \to E$ continue telle que, pour tous $x, y \in E$ distincts, on a $d(f(x), f(y)) < d(x,y)$. Alors f admet un unique point fixe.*

Contre-exemple 34. *Ceci est faux si E est seulement complet. La fonction définie sur $\mathbb{R}$ par $f : x \mapsto \mathbb{1}_{\mathbb{R}^{-\star}}(x) + \mathbb{1}_{\mathbb{R}^{+\star}}\left(x + \frac{1}{x}\right)$ ne possède pas de point fixe sur $\mathbb{R}$.*

Proposition 35. *Soient E compact et $f : E \to E$ continue telle que, pour tous $x, y \in E$ distincts, on a $d(f(x), f(y)) \geqslant d(x,y)$. Alors f est une isométrie bijective.*

Théorème 36 (Brouwer)**.** *Toute application continue de la boule unité fermée de $\mathbb{R}^n$ dans elle-même admet (au moins) un point fixe.*

4) Résultats de densité

On fixe (E,d) compact. Soit $\mathcal{C}^0(E,K)$ l'ensemble des fonctions continues de E dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Proposition 37. *$(\mathcal{C}^0(E,\mathbb{K}), \|.\|_\infty)$ est un espace de Banach séparable.*

Définition 38. Soit V un sous-espace vectoriel de $\mathcal{C}^0(E,\mathbb{K})$. On dit que V est séparant si, pour tous $x, y \in E$, distincts, il existe $h \in V$ tel que $h(x) \neq h(y)$. On dit que V est réticulé s'il est stable par passage au sup et à l'inf de deux éléments.

Théorème 39. *Tout sous-espace vectoriel réticulé séparant de $\mathcal{C}^0(E,\mathbb{R})$ contenant les fonctions constantes est dense dans $\mathcal{C}^0(E,\mathbb{R})$.*

Exemple 40. *Les fonctions lipschitziennes sont denses dans $\mathcal{C}^0(E,\mathbb{R})$.*

Proposition 41. *Toute sous-algèbre de $\mathcal{C}^0(E,\mathbb{K})$ est réticulée.*

Théorème 42 (Stone-Weierstrass)**.** *Toute sous-algèbre de $\mathcal{C}^0(E,\mathbb{R})$ séparante et contenant les fonctions constantes est dense dans $\mathcal{C}^0(E,\mathbb{R})$*

Exemple 43. *Si $E \subset \mathbb{R}^d$ est compact, les fonctions polynômiales sont denses dans $\mathcal{C}^0(E,\mathbb{R})$. En particulier pour $d = 1$, on retrouve le théorème de Weierstrass.*

Théorème 44 (Weierstrass)**.** *L'ensemble des polynômes sur $[a,b]$ est dense dans $(\mathcal{C}^0([a,b],\mathbb{R}), \|.\|_\infty)$.*

III Compacité en dimension finie

1) Espaces vectoriels normés

On fixe (E,d) un espace vectoriel normé.

Proposition 45. *Si E est de dimension finie, toutes les normes sont équivalentes.*

Théorème 46. *Les parties compactes d'un espace vectoriel de dimension finie sont ses parties fermées bornées.*

Corollaire 47. *Toute application linéaire $E \to F$, où E est de dimension finie, est continue.*

Contre-exemple 48. *Munissons $\mathbb{R}[X]$ de la norme $\|.\|_\infty$ définie par $\left\|\sum_{i=0}^n a_i X^i\right\|_\infty = \sup_{i\in[\![0,n]\!]} |a_i|$. La dérivation sur $(\mathbb{R}[X], \|.\|_\infty)$ n'est pas continue.*

Théorème 49 (Riesz)**.** *La boule unité fermée de E est compacte si, et seulement si, E est de dimension finie.*

Exemple 50. *La boule unité de $\mathcal{C}^0([0,1])$ n'est pas compacte. En effet, les fonctions $f_n : x \mapsto x^n$ convergent vers une fonction non continue.*

2) Théorème d'Ascoli

On considère un intervalle $[a,b]$ de $\mathbb{R}$ et $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 51. Une famille de fonctions $Y \subseteq \mathcal{C}^0([a,b],\mathbb{K})$ est dite équicontinue lorsque :

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall f \in Y,\ |x-y| < \eta \Rightarrow |f(x) - f(y)| < \varepsilon$$

Exemple 52. *(i) Une partie finie de $\mathcal{C}^0([a,b],\mathbb{K})$ est équicontinue.*

(ii) Une suite uniformément convergente de fonctions de $\mathcal{C}^0([a,b],\mathbb{K})$ forme une famille équicontinue.

(iii) L'ensemble des fonctions lipschitziennes est équicontinu.

Théorème 53 (Ascoli)**.** *Soit $Y \subseteq \mathcal{C}^0([a,b],\mathbb{K})$. Sont équivalentes :*

(i) Y est équicontinue et bornée pour la norme uniforme.

(ii) $\overline{Y}$ est compacte.

Application 54. *Soient X et Y deux espaces métriques compacts, μ une mesure borélienne finie et $K \in \mathcal{C}^0(X \times Y, \mathbb{K})$. On considère l'application :*

$$T : \left| \begin{array}{ccc} \mathcal{C}^0(Y,\mathbb{K}) & \longrightarrow & \mathcal{C}^0(X,\mathbb{K}) \\ x & \longmapsto & \int_Y K(x,y) f(y)\, d\mu(y) \end{array} \right.$$

Alors $T\left(B_{\mathcal{C}^0(Y,\mathbb{K})}(0,1)\right)$ est relativement compact dans $\mathcal{C}^0(X,\mathbb{K})$.

Développements

- Ellipsoïde de John-Loewner (22) [FGN13c]
- Connexité des valeurs d'adhérence d'une suite (16,17) [Gou08] [FGN13d]
- Théorème de Weierstrass (44) [Gou08]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Pom97] A. Pommelet. *Cours d'Analyse.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3.* Cassini

Cadre : On fixe (E, d) un espace métrique et A une partie de E.

I Espaces connexes

1) Définitions

Proposition 1. *Les assertions suivantes sont équivalentes :*

(i) Il n'existe pas de partition de E en deux ouverts non vides disjoints.

(ii) Il n'existe pas de partition de E en deux fermés non vides disjoints.

(iii) Les seuls ouverts et fermés de E sont $\varnothing$ et E.

Définition 2. Un espace métrique vérifiant l'une des assertions de la proposition précédente est dit connexe.

Remarque 3. *La connexité est une notion topologique.*

Exemple 4. *$\mathbb{R}$ est connexe, $\{0,1\}$ n'est pas connexe.*

Proposition 5. *Dire que A est connexe pour la topologie induite équivaut aux propositions suivantes :*

(i) Si $A \subset O_1 \cup O_2$, où O_1 et O_2 sont deux ouverts disjoints, alors :

$$(A \cap O_1 = \varnothing \quad et \quad A \subset O_2) \quad ou \quad (A \cap O_2 = \varnothing \quad et \quad A \subset O_1)$$

(ii) Si $A \subset F_1 \cup F_2$, où F_1 et F_2 sont deux fermés disjoints, alors :

$$(A \cap F_1 = \varnothing \quad et \quad A \subset F_2) \quad ou \quad (A \cap F_2 = \varnothing \quad et \quad A \subset F_1)$$

Exemple 6. *$\mathbb{Q} \subset \mathbb{R}$ n'est pas connexe.*

2) Propriétés

Théorème 7. *Soit $f : (E, d) \to (E', d')$ une application continue entre espaces métriques. Si E est connexe, alors $f(E)$ est connexe.*

Proposition 8. *(E, d) est connexe si, et seulement si, toute application continue de (E, d) dans $\{0, 1\}$ muni de la distance discrète est constante.*

Remarque 9. *On peut remplacer $\{0, 1\}$ par tout espace discret ayant plus de deux points, comme $\mathbb{Z}$ par exemple.*

Proposition 10. *Soient A connexe et $B \subseteq E$ vérifiant $A \subseteq B \subseteq \overline{A}$. Alors B est connexe. En particulier, $\overline{A}$ est connexe.*

Proposition 11. *Soit $(C_i)_{i\in I}$ une famille de connexes de E. S'il existe $i_0 \in I$ tel que $C_i \cap C_{i_0} \neq \varnothing$ pour tout $i \in I$, alors $\bigcup_{i\in I} C_i$ est connexe.*

Remarque 12. *En particulier, si $\bigcap_{i\in I} C_i \neq \varnothing$ alors $\bigcup_{i\in I} C_i$ est connexe.*

Proposition 13. *Soit $(C_i)_{i\in I}$ une famille de connexes de E, avec $I = \mathbb{N}$ ou $[\![0, n]\!]$. Si $C_{i-1} \cap C_i \neq \varnothing$ pour tout $i \in I \setminus \{0\}$, alors $\bigcup_{i\in I} C_i$ est connexe.*

Théorème 14. *Soient $(E_1, d_1), \dots, (E_n, d_n)$ des espaces métriques. L'espace produit $E = \prod_{i=1}^{n} E_i$ est connexe si et seulement si E_i est connexe pour tout $i \in [\![1, n]\!]$.*

Remarque 15. *Une intersection de connexes n'est pas toujours connexe.*

Proposition 16. *Soit (E, d) un espace métrique compact et $(u_n)_{n\in\mathbb{N}}$ une suite de E telle que $\lim_{n\to+\infty} d(u_n, u_{n+1}) = 0$. Alors l'ensemble des valeurs d'adhérence de $(u_n)_{n\in\mathbb{N}}$ est connexe.*

Application 17. *Soient $f : [0, 1] \to [0, 1]$ une fonction continue et $(x_n)_{n\in\mathbb{N}}$ la suite définie par $x_0 \in [0, 1]$ et $u_{n+1} = f(u_n)$ pour tout $n \in \mathbb{N}$. Alors $(x_n)_{n\in\mathbb{N}}$ converge si, et seulement si, $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.*

3) Composantes connexes

Définition 18. On définit la relation d'équivalence $\sim$ sur E pour $x, y \in E$ par $x \sim y$ si, et seulement si, il existe un connexe C de E tel que $x \in C$ et $y \in C$. Les classes sont appelées composantes connexes de E.

Proposition 19. *La composante connexe de $x \in E$, notée $C(x)$, est l'union des connexes de E contenant x. Les composantes connexes de E sont des ouverts deux à deux disjointe.*

Proposition 20. *Soit $f : E \to F$ un homéomorphisme. Alors f induit une bijection entre les composantes connexes de E et F.*

Théorème 21 (Jordan, admis)**.** *Toute courbe continue fermé simple à valeurs dans $\mathbb{C}$ d'image J est telle que $\mathbb{C} \setminus J$ a deux composantes connexes, une bornée C_0 et une non bornée C_∞, toutes deux de frontière J.*

4) Connexité par arcs

Définition 22. On appelle chemin de E toute application continue $\gamma : [0,1] \to E$. Son image $\gamma([0,1])$ est appelée un arc, $\gamma(0)$ son origine et $\gamma(1)$ son but. On dit que γ lie $\gamma(0)$ et $\gamma(1)$.

Définition 23. L'espace E est dit connexe par arcs si, pour tous $a, b \in E$, il existe un chemin liant a et b.

Théorème 24. *La connexité par arcs entraîne la connexité.*

Exemple 25. *La réciproque est fausse : l'adhérence du graphe de la fonction $x \mapsto \sin(\frac{1}{x})$ définie sur $\mathbb{R}^{+\star}$ est connexe non connexe par arcs.*

Proposition 26. *Pour un ouvert d'un espace vectoriel normé, la connexité est équivalente à la connexité par arcs.*

II Connexité et applications

1) Analyse réelle

Proposition 27. *Les connexes de $\mathbb{R}$ sont exactement les intervalles de $\mathbb{R}$. Ce sont aussi les convexes de $\mathbb{R}$.*

Application 28. *L'image d'un intervalle par une application continue est un intervalle.*

Théorème 29 (Darboux)**.** *Soit $f : \mathbb{R} \to \mathbb{R}$ dérivable et I un intervalle ouvert non vide de $\mathbb{R}$. Alors $f'(I)$ est un intervalle de $\mathbb{R}$.*

Théorème 30. *Soient E et F deux $\mathbb{K}$-espaces vectoriels, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soient $U \subseteq E$ un ouvert et $f : U \to F$ différentiable sur U. Soient $a, b \in U$ et $k > 0$. Alors :*

$$\forall\, x \in [a,b],\ \|d_x f\|_{L(E,F)} \leqslant k \quad \Rightarrow \quad \|f(b) - f(a)\|_F \leqslant k\,\|b - a\|_E$$

Corollaire 31. *Avec les notations du théorème précédent, si U est connexe, et si $d_x f = 0$ pour tout $x \in U$, alors f est constante sur U.*

Théorème 32 (Brouwer)**.** *Toute application continue de la boule unité fermée de $\mathbb{R}^n$ dans elle-même admet (au moins) un point fixe.*

2) Analyse complexe

Définition 33. Un domaine de $\mathbb{C}$ est un ouvert connexe de $\mathbb{C}$ non vide. On fixe un tel Ω par la suite. On appelle lacet dans $\mathbb{C}$ un chemin $\mathcal{C}^1$ par morceaux tel que $\gamma(0) = \gamma(1)$.

Définition 34. Soit γ un lacet de $\mathbb{C}$ et $a \in \mathbb{C} \setminus \mathrm{Im}(\gamma)$. On définit l'indice $\mathrm{Ind}_\gamma(a)$ de a par rapport à γ par :

$$\mathrm{Ind}_\gamma(a) = \frac{1}{2i\pi} \int_\gamma \frac{1}{z-a} dz$$

Proposition 35. *La fonction Ind_γ est à valeurs entières sur Ω, constante sur les composantes connexes de Ω, et nulle sur la composante non bornée.*

Théorème 36 (Cauchy)**.** *Soient Ω un ouvert convexe et $z_0 \in \Omega$ et $f \in \mathcal{H}(\Omega \setminus \{z_0\})$, alors pour tout lacet γ de Ω, on a $\int_\gamma f = 0$.*

Théorème 37 (Formule de Cauchy)**.** *Soient Ω est un ouvert convexe, $z \in \Omega$, γ un lacet de $\Omega \setminus \{z\}$ et $f \in \mathcal{H}(\Omega)$, alors on a :*

$$\mathrm{Ind}_\gamma(z) f(z) = \frac{1}{2i\pi} \int_\gamma \frac{f(\xi)}{\xi - z} d\xi$$

Théorème 38 (Liouville)**.** *Toute fonction holomorphe sur $\mathbb{C}$ et bornée est constante.*

Corollaire 39 (Théorème de d'Alembert)**.** *Tout polynôme non constant à coefficients dans $\mathbb{C}$ admet au moins une racine.*

Théorème 40. *Soient $\Omega \subset \mathbb{C}$ connexe, $f \in \mathcal{H}(\mathbb{C})$ et $z_0 \in \Omega$. Les assertions suivantes sont équivalentes :*

(i) $\forall k \in \mathbb{N}, f^{(k)}(z_0) = 0$
(ii) f *est nulle sur un voisinage de* z_0
(iii) f *est nulle sur* Ω

Corollaire 41. *Soient f et g holomorphes sur Ω un connexe de $\mathbb{C}$. Si f et g coïncident sur un voisinage d'un point de Ω, alors $f = g$.*

Théorème 42 (Zéros isolés)**.** *Soient Ω un connexe de $\mathbb{C}$ et f holomorphe sur Ω et non identiquement nulle, alors les zéros de f sont isolés.*

Corollaire 43. *Si deux fonctions holomorphes coïncident sur un ensemble admettant un point d'accumulation, alors elles sont égales.*

Exemple 44. *Il n'existe pas de fonction holomorphe sur $D(0,1)$ tel que pour tout $n \geqslant 1$, $f(\frac{1}{n}) = f(-\frac{1}{n}) = -\frac{1}{n^3}$.*

Théorème 45 (Principe du maximum). *Soit $f \in \mathcal{H}(\Omega)$. Si $|f|$ atteint son maximum en un point de Ω, alors f est constante.*

Théorème 46 (Théorème des résidus). *Soient $S \subset \Omega$ fini, $f \in \mathcal{H}(\mathbb{C} \setminus S)$ et γ un lacet dans Ω ne rencontrant pas S, alors :*

$$\int_\gamma f(z)dz = 2i\pi \sum_{c \in S} \mathrm{Ind}_\gamma(c)\,\mathrm{Res}(f,c)$$

Exemple 47. $\int_0^{+\infty} \frac{\sin x}{x} dx = \frac{\pi}{2}$

Exemple 48. *Soit $\alpha \in]-1,1[$. Alors* $\int_0^{+\infty} \frac{x^\alpha \ln x}{x^2-1}\, dx = \frac{\pi^2}{4\cos^2(\frac{\alpha\pi}{2})}$.

III Connexité des espaces de matrices

Proposition 49. *$\mathcal{GL}_n(\mathbb{C})$, $\mathcal{SL}_n(\mathbb{R})$, $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{S}_n^{++}(\mathbb{R})$ sont connexes.*

Proposition 50. *$\mathcal{GL}_n(\mathbb{R})$, $\mathcal{O}_n(\mathbb{R})$ ne sont pas connexes.*

Lemme 51. *Pour $A \in \mathcal{M}_n(\mathbb{C})$, $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.*

Théorème 52. $\exp(\mathcal{M}_n(\mathbb{C})) = \mathcal{GL}_n(\mathbb{C})$

Théorème 53. $\exp(\mathcal{M}_n(\mathbb{R})) = \left\{A^2 \,\middle|\, A \in \mathcal{GL}_n(\mathbb{R})\right\}$

Développements

- Connexité des valeurs d'adhérence d'une suite (16,17) [Gou08] [FGN13d]
- Surjectivité de l'exponentielle de matrice (51,52,53) [Zav13]
- Calcul d'une intégrale par le théorème des résidus (48) [Tau06]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod
[Rud09] W. Rudin. *Analyse réelle et complexe.* Dunod
[Tau06] P. Tauvel. *Analyse complexe pour la licence 3.* Dunod
[FGN13d] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 1.* Cassini
[Zav13] M. Zavidovique. *Un Max de Math.* Calvage et Mounet

Cadre : On considère (X, d) un espace métrique et $(E, \|.\|)$ un $\mathbb{K}$-espace vectoriel normé, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I Généralités sur les espaces complets

1) Suites de Cauchy et complétude

Définition 1. On dit que (u_n) est de Cauchy lorsque :

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ \forall p \in \mathbb{N},\ |u_{n+p} - u_n| < \varepsilon$$

Proposition 2. *(i) Toute suite convergente est de Cauchy.*

(ii) Toute suite de Cauchy est bornée.

(iii) Toute suite de Cauchy ayant une valeur d'adhérence converge.

Définition 3. On dit que (X, d) est complet si toute suite de Cauchy de X est convergente.

Exemple 4. $(\mathbb{R}, |.|)$ *et* $(\mathbb{R}^n, \|.\|)$ *sont complets,* $(\mathbb{Q}, |.|)$ *ne l'est pas.*

Exemple 5. $(\mathbb{R}, d)$*, où* $d(x, y) = |\arctan x - \arctan y|$ *n'est pas complet.*

Remarque 6. *Les notions de suites de Cauchy et d'espaces complets ne sont pas topologique mais métriques.*

2) Propriétés générales des espaces complets

Théorème 7. *Il existe un espace métrique complet* $(\widehat{X}, \widehat{d})$*, appelé complété de* X*, et une isométrie* $i : (X, d) \to (\widehat{X}, \widehat{d})$ *d'image dense.*

Exemple 8. $\widehat{\mathbb{Q}} = \mathbb{R}$ *pour la distance usuelle.*

Proposition 9. *Si* (X, d) *est complet et* $A \subset X$*, alors* (A, d) *est complet si, et seulement si,* A *est fermé dans* X*.*

Théorème 10 (Fermés emboîtés)**.** *Si* (X, d) *est complet, alors, pour toute suite* $(F_n)_{n\in\mathbb{N}}$ *décroissante de fermés non vides de* X *dont le diamètre tend vers 0,* $\bigcap_{n\in\mathbb{N}} F_n$ *est un singleton.*

Proposition 11. *Un espace métrique est compact se, et seulement si, il est précompact et complet.*

II Exemples d'espaces complets

1) Espaces de Banach

Définition 12. On dit que $(E, \|.\|)$ est espace de Banach s'il est complet.

Théorème 13. $(E, \|.\|)$ *est un espace de Banach si, et seulement si, toute série absolument convergente de* E *est convergente.*

Proposition 14. *Si* F *est un Banach, alors* $\mathcal{L}(E, F)$ *est un Banach.*

Corollaire 15. E' *est un espace de Banach.*

Proposition 16. *L'espace* $\mathcal{C}^k([0, 1], \mathbb{R})$*, si on le munit de la norme* $\|f\| = \sum_{i=0}^{k} \left\|f^{(i)}\right\|_\infty$*, est un espace de Banach, contrairement à si on le munit de la norme* $\|.\|_\infty$*.*

2) Espaces L^p

Définition 17. Pour tout réel $p > 0$, on définit le $\mathbb{K}$-espace vectoriel :

$$\mathscr{L}^p_{\mathbb{K}}(X, \mathcal{A}, \mu) = \left\{ f : X \to \mathbb{K} \text{ mesurable} \,\middle|\, \|f\|_p < +\infty \right\}$$

Théorème 18 (Hölder)**.** *Soient* $f \in \mathscr{L}^p_{\mathbb{K}}(\mu)$ *et* $g \in \mathscr{L}^q_{\mathbb{K}}(\mu)$*, où* $\frac{1}{p} + \frac{1}{q} = 1$*. Alors* $\|fg\|_1 \leqslant \|f\|_p \|g\|_q$*.*

Théorème 19 (Minkowski)**.** *Soient* $p \in [1, +\infty[$ *et* $f, g \in \mathscr{L}^p_{\mathbb{K}}(\mu)$*. Alors* $\|f + g\|_p \leqslant \|f\|_p + \|g\|_p$*.*

Définition 20. Pour $1 \leqslant p < +\infty$, on définit $L^p_{\mathbb{K}}(\mu)$ comme l'espace vectoriel normé quotient de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ par les fonctions presque nulles. On associera par abus de langage un élément de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ à sa classe dans $L^p_{\mathbb{K}}(\mu)$.

Définition 21. On définit $L^\infty_{\mathbb{K}}(\mu)$ comme l'espace vectoriel normé quotient de $\mathscr{L}^\infty_{\mathbb{K}}(\mu)$ par les fonctions presque nulles.

Remarque 22. *En considérant 1 et* ∞ *comme exposants conjugués, on retrouve les inégalités de Hölder et de Minkowski.*

Théorème 23 (Riesz-Fischer)**.** *Pour tout* $1 \leqslant p \leqslant +\infty$*,* $L^p_{\mathbb{K}}(\mu)$ *est un espace de Banach.*

3) Espaces de Hilbert

Définition 24. Un espace vectoriel est dit préhilbertien s'il est muni d'un produit scalaire. S'il est complet pour la norme issue du produit scalaire, on dit que c'est un espace de Hilbert (ou hilbertien).

Exemple 25. *$(L^2, \|.\|_2)$ est un espace de Hilbert.*

Proposition 26. *Un espace vectoriel normé E est un espace préhilbertien si, et seulement si, $\|.\|$ vérifie l'identité du parallélogramme, c'est-à-dire :*

$$\forall\, x, y \in E,\ \|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right)$$

Proposition 27 (Cauchy-Schwarz)**.** *Si H est préhilbertien, alors :*

$$\forall\, x, y \in H,\ |\langle x, y\rangle| \leqslant \|x\|\,\|y\|$$

Définition 28. Pour une partie A de H, son orthogonal est défini par $A^\perp = \{x \in H \,|\, \forall a \in A, \langle x, a\rangle = 0\}$.

Proposition 29. *Si $A \subseteq H$, $A^\perp$ est un sous-espace vectoriel fermé.*

Théorème 30. *Soit $K \subset E$ un convexe fermé non vide. Pour tout $f \in H$, il existe un unique élément de K, noté $P_K(f)$, et appelé projection de f sur K, tel que :*

$$\|P_K(f) - f\| = \inf_{v \in K} \|v - f\|$$

De plus, $P_K(f)$ est caractérisée par :

$$\forall v \in K,\ \langle f - P_K(f), v - P_K(f)\rangle \leqslant 0$$

Corollaire 31. *Soient M un sous-espace vectoriel fermé de H et $f \in H$. Alors $P_M(f)$ est caractérisé par :*

$$P_M(f) \in M \qquad et \qquad \forall\, v \in M,\ \langle f - P_M(f), v\rangle = 0$$

De plus, P_M est un opérateur linéaire.

Théorème 32 (Riesz-Fréchet)**.** *Soit $\varphi \in H'$. Alors il existe un unique $f \in H$ tel que :*

$$\forall\, v \in H,\ \langle \varphi, v\rangle = \langle f, v\rangle$$

Application 33. *Soit F un sous-espace vectoriel fermé d'un Hilbert H, alors $F \oplus F^\perp = H$*

Application 34. *Soit $u \in \mathcal{L}(H)$, il existe un unique $u^\star \in \mathcal{L}(H)$ tel que :*

$$\forall\, x, y \in H,\ \langle u(x), y\rangle = \langle x, u^\star(y)\rangle \quad avec \quad \|u\| = \|u^\star\|$$

Proposition 35. *Un sous-espace vectoriel F de H est dense si, et seulement si, $F^\perp = \{0\}$.*

III Utilisations de la complétude

1) Prolongement de fonctions

Théorème 36. *Soient H un espace de Hilbert, F un sous-espace vectoriel de H, et $f \in F'$. Il existe $g \in H'$ qui prolonge f et telle que $\|g\| = \|f\|$.*

Remarque 37. *L'énoncé général dans un espace vectoriel normé s'appuie sur le lemme de Zorn. Dans un espace de Hilbert, on peut en fait construire explicitement un prolongement.*

Théorème 38. *Soient E et F des espaces métriques, et $A \subset E$ dense.*

(i) Si $f : A \to F$ est continue, et si, pour tout $x \in E \setminus A$, $\lim_{y \to x, y \in A} f(y)$ existe, alors il existe une unique fonction $g : E \to F$ continue telle que $g|_A = f$.

(ii) On suppose F complet. Si $f : A \to F$ est uniformément continue, il existe une unique fonction $g : E \to F$ uniformément continue telle que $g|_A = f$.

Théorème 39. *Soient E et F deux espaces métriques, D une partie dense de E. Si F est complet alors toute application uniformément continue de D dans F admet un unique prolongement continu sur E. Ce prolongement est de plus uniformément continu.*

Corollaire 40. *Soient E un espace vectoriel normé, D un sous-espace vectoriel dense de E et F un espace de Banach. Toute application linéaire continue de D dans F a un unique prolongement linéaire continu sur E.*

2) Théorème de point fixe

Théorème 41 (Banach-Picard)**.** *Soient (E, d) un espace métrique complet (non vide), et $F : E \to E$ une application k-contractante. Alors F admet un unique point fixe et toute suite définie par $u_0 \in E$ puis $u_{n+1} = F(u_n)$ converge vers ce point à une vitesse géométrique.*

Remarque 42. *Si F^p est contractante, on a le même résultat.*

Contre-exemple 43. *Si $E =]0, 1[$ et $F : x \mapsto \frac{x}{2}$, F est contractante mais sans point fixe (E n'est pas complet).*

Contre-exemple 44. *Si $E = [0, 1]$ et $F : x \mapsto \sqrt{1+x^2}$, E est complet, F est contractante, mais sans point fixe ($F([0, 1]) = [1, \sqrt{2}]$).*

Contre-exemple 45. *Si $E = \mathbb{R}$ et $F : x \mapsto \sqrt{1+x^2}$, E est complet, F applique E dans lui-même, mais sans point fixe (F n'est pas contractante).*

3) Théorème de Baire et applications

Théorème 46 (Baire)**.** *Soit E un espace métrique complet. Toute réunion dénombrable de fermés d'intérieurs vides de E est d'intérieur vide dans E.*

Corollaire 47. *Soit E un espace métrique complet. Toute intersection dénombrable d'ouverts denses est dense.*

Application 48. *Un espace de Banach est de dimension finie ou non dénombrable. Par exemple $\mathbb{R}[X]$ n'est complet pour aucune norme.*

Théorème 49 (Banach-Steinhaus)**.** *Soit E un espace de Banach et F un espace vectoriel normé. Soit $(u_i)_{i\in I}$ une famille d'opérateurs continus de E dans F. On suppose que, pour tout $x \in E$, $\sup_{i\in I} \|u_i(x)\| < +\infty$. Alors $\sup_{i\in I} \|u_i\| < +\infty$.*

Application 50. *Il existe des fonctions continues et 2π-périodique qui diffèrent de leur série de Fourier.*

Théorème 51 (Application ouverte)**.** *Une application linéaire continue surjective entre espaces de Banach est ouverte.*

Corollaire 52. *Une application linéaire continue bijective entre espaces de Banach est d'inverse continue*

Théorème 53 (Graphe fermé)**.** *Une application linéaire $T : E \to F$ entre deux espaces de Banach est continue si, et seulement si, son graphe $\{(x, T(x)) \,|\, x \in E\}$ est fermé pour la norme produit.*

Développements

- Théorème de Riesz-Fischer (23) [Bre87]
- Projection sur un convexe fermé et théorème de Riesz (30,31,32) [Bre87]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Bre87] H. Brezis. *Analyse fonctionelle.* Masson

I Prolongement par continuité

1) Prolongement ponctuel

A est une partie de $\mathbb{R}$ et $(F, \|.\|)$ un espace vectoriel normé.

Définition 1. Soit $f : A \to F$ et $a \in A$. f est dite continue lorsque $\lim_{x\to a} f(x)$ existe et vaut $f(a)$.

Proposition 2. *Si $a \in \overline{A}\setminus A$, et si f admet ℓ comme limite en a, on peut définir une application continue $\tilde{f}$ par :*

$$\tilde{f} : \left| \begin{array}{ccc} A\cup\{a\} & \longrightarrow & F \\ x & \longmapsto & \left\{ \begin{array}{ccc} f(x) & si & x \neq a \\ \ell & si & x = a \end{array} \right. \end{array} \right.$$

Définition 3. $\tilde{f}$ est le prolongement par continuité de f en a.

Exemple 4. *(i)* $f : \left| \begin{array}{ccc} \mathbb{R}^\star & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{\sin x}{x} \end{array} \right.$ *se prolonge en 0 par 1.*

(ii) $f : \left| \begin{array}{ccc} \mathbb{R}^2\setminus\{(0,0)\} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & \frac{x^2y^2}{x^2+y^2} \end{array} \right.$ *se prolonge en $(0,0)$ par 0.*

2) Prolongement par densité

Théorème 5 (Principe de prolongement des identités)**.** *Soient f et g deux fonctions continues de l'espace topologique E dans l'espace vectoriel normé F. Si f et g coïncident sur une partie dense de E, elles coïncident sur E tout entier.*

Définition 6. Soient I un intervalle de $\mathbb{R}$, et $f : I \to \mathbb{R}$. On dit que f est uniformément continue sur I si :

$$\forall\,\varepsilon > 0,\ \exists\,\delta > 0,\ \forall\, x, y \in I,\ |x-y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon$$

Théorème 7. *Soient E et F deux espaces métriques, avec F complet. Soient A une partie dense de E et $f : A \to F$ uniformément continue. Il existe une unique application uniformément continue $g : E \to F$ qui prolonge f.*

Application 8 (Construction de l'intégrale de Riemann sur des fonctions réglées)**.** *Une fonction est réglée si elle est limite uniforme de fonctions en escalier. Pour une fonction en escalier $f(x) = \sum_{i=0}^{n-1}(x_{i+1} - x_i)\lambda_i$, avec $(x_0, \dots, x_n)$ une subdivision de $[a, b]$ et λ_i des constantes, on a $\int_a^b f(t)dt \leqslant \|f\|_\infty \sum_{i=0}^{n-1}(x_{i+1} - x_i) = (b-a)\|f\|_\infty$. L'intégration est alors une fonction lipschitzienne, donc uniformément continue, de l'espace des fonctions en escaliers dans $\mathbb{R}$. Par le théorème, elle se prolonge de façon unique en une forme linéaire sur l'espace des fonctions réglées.*

Théorème 9. *Soit $f \in L^2(\mathbb{R})$, alors :*

(i) Il existe $(f_n)_n$ une suite de $L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$ qui converge vers f dans $L^2(\mathbb{R}^d)$.

(ii) Pour une telle suite $(f_n)_n$, la suite $(\widehat{f_n})_n$ converge dans $L^2(\mathbb{R}^d)$ vers une limite $\tilde{f}$ indépendante de la suite choisie.

Définition 10. $\tilde{f}$ est la transformée de Fourier de f dans $L^2(\mathbb{R}^d)$.

Théorème 11 (Plancherel)**.** *Soit $f \in L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$, alors $\tilde{f} \in L^2(\mathbb{R}^d)$ et $\left\|\tilde{f}\right\|_2^2 = (2\pi)^d \|f\|_2$. De plus, $f \mapsto \tilde{f}$ est un isomorphisme de $L^2(\mathbb{R}^d)$ sur $L^2(\mathbb{R}^d)$*

3) Prolongement des applications linéaires continues

Théorème 12 (Hahn-Banach)**.** *Soit $(E, \|.\|)$ un $\mathbb{K}$-espace vectoriel normé, et soit F un sous-espace vectoriel de E. Soit $f : F \to \mathbb{K}$ linéaire continue. Il existe un prolongement continu g de f sur E tel que $\|g\| = \|f\|$.*

Application 13. *Si F est un sous-espace vectoriel de $(E, \|.\|)$, F est dense dans E si, et seulement si, toute forme linéaire qui s'annule sur F est nulle sur E.*

II Prolongement et différentiabilité

1) Prolongement ponctuel et régularité

Théorème 14. *Soient E un espace vectoriel normé et I un intervalle de $\mathbb{R}$. Soit $f : I \to E$ continue et $a \in I$. Si f est dérivable sur $I\setminus\{a\}$ et si f' possède une limite ℓ au point a, alors f est dérivable en a et $f'(a) = \ell$.*

Contre-exemple 15. *Ce théorème est faux si f n'est pas continue, comme avec $a = 0$ et :*

$$f : x \mapsto \left\{ \begin{array}{ccc} x & si & x \leqslant 0 \\ x+1 & si & x > 0 \end{array} \right.$$

Exemple 16. *On pose :*

$$f : x \mapsto \begin{cases} e^{-\frac{1}{x^2}} & si \quad x \neq 0 \\ 0 & si \quad x = 0 \end{cases}$$

Alors f est $\mathcal{C}^\infty$, non nulle sur $\mathbb{R}^\star$, et dont les dérivées sont nulles en 0.

2) Prolongement des solutions d'équations différentielles

On s'intéresse aux équations différentielles du premier ordre de la forme :

$$\frac{dx}{dt}(t) = f(t, x(t)) \qquad (\star)$$

où $f : I \times \Omega \to \mathbb{R}^n$ est continue, avec I un intervalle de $\mathbb{R}$ et Ω un ouvert de $\mathbb{R}^n$, et x une fonction $\mathcal{C}^1$ de t à valeur dans Ω.

Définition 17. (i) Une solution de $(\star)$ est un couple (x, J), où $J \subseteq I$ est un intervalle, et x est une fonction $\mathcal{C}^1$ de J dans Ω qui vérifie $(\star)$ en tout point de J.

(ii) Si $J = I$, on dit que la solution est globale.

(iii) (x_1, J_1) et (x_2, J_2) sont deux solutions de $(\star)$, on dit que (x_2, J_2) prolonge (x_1, J_1) si $J_1 \subset J_2$ et $x_1 = x_2$ sur J_1.

(iv) Une solution est dite maximale si elle n'admet aucun prolongement.

Théorème 18. *On suppose que $I =]a, b[$ et que $\Omega = \mathbb{R}^n$. Soit (x, J) une solution maximale de $(\star)$, où $J =]T_\star, T^\star[$, alors :*

(i) Si $T^\star < b$, alors $\lim\limits_{t \to T^\star} |x(t)| = +\infty$

(ii) Si $T_\star > a$, alors $\lim\limits_{t \to T_\star} |x(t)| = +\infty$

Corollaire 19 (Critère de prolongement)**.** *Soit (x, J) une solution de $(\star)$, où $J =]\alpha, \beta[$ et $a < \alpha < \beta < b$. Supposons qu'il existe $\delta > 0$ et $A > 0$ tels que $|x(t)| \leqslant A$ pour tout $t \in [\beta - \delta, \beta[$ (resp. $]\alpha, \alpha + \delta]$). Alors x peut être prolongée au-delà de β (resp. α) en une solution de $(\star)$.*

Corollaire 20. *Soit $f :]a, b[\times \mathbb{R}^n \to \mathbb{R}^n$ continue et bornée, alors toute solution du problème $(\star)$ est globale.*

Exemple 21. *Sur $\mathbb{R} \times \mathbb{R}$, le problème*

$$x'(t) = \frac{x(t)^2}{1 + x(t)^2} \qquad et \qquad x(0) = x_0$$

admet pour tout $x_0 \in \mathbb{R}$ une solution unique définie sur $\mathbb{R}$.

III Prolongement des fonctions analytiques

1) Comportement des séries entières sur le bord du disque de convergence

Théorème 22 (Abel angulaire)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 telle que $\sum a_n$ converge. On note f sa somme et :*

$$\Delta_\theta = \left\{ z \in \mathbb{C} \,\middle|\, 1 - z = \rho e^{i\varphi},\ \rho > 0,\ |\varphi| < \theta \right\} \quad pour \quad 0 \leqslant \theta < \frac{\pi}{2}$$

Alors :

$$\lim_{\substack{z \to 1 \\ z \in \Delta_\theta}} f(z) = \sum_{n \geqslant 0} a_n$$

Application 23. $\sum\limits_{n \geqslant 0} \frac{(-1)^n}{2n+1} = \arctan(1) = \frac{\pi}{4}$ *et* $\sum\limits_{n \geqslant 1} \frac{(-1)^{n-1}}{n} = \ln(2)$

Théorème 24 (Taubérien faible)**.** *Soit f la somme d'une série entière $\sum a_n z^n$ de rayon de convergence 1. On suppose que $\lim\limits_{x \to 1^-} f(z) = \ell$ existe, et $a_n = o\left(\frac{1}{n}\right)$. Alors $\sum a_n$ converge et $\ell = \sum\limits_{n \geqslant 0} a_n$.*

2) Principe du prolongement analytique

Théorème 25 (Zéros isolés)**.** *Soit f une fonction analytique sur un ouvert connexe $\mathcal{U}$ non identiquement nulle. Alors les zéros de f sont isolés.*

Corollaire 26 (Prolongement analytique)**.** *Soit $\mathcal{U}$ un ouvert connexe. Si deux fonctions analytiques coïncident sur un sous-ensemble $D \subset \mathcal{U}$ ayant un point d'accumulation dans $\mathcal{U}$, alors elles sont égales sur $\mathcal{U}$.*

Exemple 27. *(i)* $\cos^2 z + \sin^2 z = 1$

(ii) Il existe une unique fonction f holomorphe sur $\mathbb{C}$ telle que, pour tout $n \in \mathbb{N}^\star$, $f\left(\frac{1}{n}\right) = \frac{1}{n}$, qui est l'identité.

Proposition 28. *Soit $P = \{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > 0\}$. On définit sur P la fonction holomorphe :*

$$\Gamma(z) = \int_0^{+\infty} e^{-t} t^{z-1} dt$$

Proposition 29. *Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$.*

Développements

— Théorèmes d'Abel angulaire et taubérien faible (22,24) [Gou08]
— Fonction Gamma (28,29) [Les14]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod
[BSF05] B. Beck, I. Selon, et C. Feuillet. *HPrépa Maths 2e année MP-MP*.* Hachette
[Les14] A. Lesfari. *Variables complexes.* Ellipses

Cadre : Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit E un $\mathbb{K}$-espace vectoriel.

I Généralités

1) Espaces vectoriels normés

Définition 1. On appelle norme sur E toute application $\|.\| : E \to \mathbb{R}^+$ telle que, pour tous $x, y \in E$ et $\lambda \in \mathbb{K}$:

(i) $\|x\| = 0 \Leftrightarrow x = 0$

(ii) $\|\lambda x\| = |\lambda| \, \|x\|$

(iii) $\|x + y\| \leqslant \|x\| + \|y\|$

On note $(E, \|.\|)$ l'espace E muni d'une norme $\|.\|$, on parle d'espace vectoriel normé.

On fixe par la suite une norme $\|.\|$ sur E.

Exemple 2. *Pour $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, on a les normes classiques :*

$$\|x\|_1 = \sum_{i=1}^{n} |x_i| \quad et \quad \|x\|_2 = \sqrt{\sum_{i=1}^{n} x_i^2} \quad et \quad \|x\|_\infty = \max_{1 \leqslant i \leqslant n} |x_i|$$

Remarque 3. *L'application $d : (x, y) \mapsto \|x - y\|$ est une distance sur E.*

Définition 4. Deux normes $\|.\|_A$ et $\|.\|_B$ sont équivalentes lorsque :

$$\exists \, a, b > 0, \quad \forall \, x \in E, \quad a \|x\|_A \leqslant \|x\|_B \leqslant b \|x\|_A$$

Exemple 5. *Sur $\mathbb{R}$, les normes $\|.\|_1$, $\|.\|_2$ et $\|.\|_\infty$ sont équivalentes.*

Exemple 6. *Sur $E = \mathcal{C}([0,1], \mathbb{R})$, ces normes ne sont pas équivalentes :*

$$\|.\|_1 : f \mapsto \int_0^1 |f(t)| \, dt \quad et \quad \|.\|_\infty : f \mapsto \sup_{t \in [0,1]} |f(t)|$$

Proposition 7. *Si V est un sous-espace vectoriel de $(E, \|.\|)$, alors $\overline{V}$ est aussi un sous-espace vectoriel de E. En particulier, un hyperplan de E est fermé ou dense.*

2) Applications linéaires continues

On fixe $(E, \|.\|_E)$ et $(F, \|.\|_F)$ deux espaces vectoriels normés.

Théorème 8. *Soit $f : E \to F$ linéaire. Sont équivalents :*

(i) f continue sur E.

(ii) f continue en 0.

(iii) f bornée sur $\overline{B(0,1)}$.

(iv) f bornée sur $Sph(0,1)$.

(v) $\exists M > 0, \forall x \in E, \|f(x)\|_F \leqslant M \|x\|_E$

(vi) f lipschitzienne.

(vii) f uniformément continue sur E.

Définition 9. L'ensemble des applications linéaires continues $E \to F$, noté $\mathcal{L}(E, F)$, est naturellement muni d'une norme par :

$$|||f||| = \sup_{\|x\|_E = 1} \|f(x)\|_F = \sup_{\|x\|_E \leqslant 1} \|f(x)\|_F$$

Remarque 10. *La norme $|||f|||$ de f est son rapport de Lipschitz.*

Définition 11. Si $F = \mathbb{K}$, alors $\mathcal{L}(E, \mathbb{K})$ est noté E'. Il s'agit d'un sous-espace de $E^\star$, qu'on appelle dual topologique de E.

Proposition 12. *Pour $f \in E^\star$, on a $f \in E'$ si, et seulement si,* $\operatorname{Ker} f$ *est un hyperplan fermé de E.*

Exemple 13. *Dans l'espace $(\mathcal{C}([0,1]), \|.\|_1)$, l'application $f \mapsto f(0)$ est une forme linéaire discontinue.*

Théorème 14 (Hahn-Banach analytique)**.** *Soit $p : E \to \mathbb{R}$ telle que :*

$$\forall x \in E, \forall \lambda > 0, \, p(\lambda x) = \lambda p(x) \quad et \quad \forall x, y \in E, \, p(x + y) \leqslant p(x) + p(y)$$

Soit G un sous-espace vectoriel de E et $g \in G^\star$ tels que $g \leqslant p$ sur G. Alors il existe $f \in E^\star$ prolongeant g et telle que $f \leqslant p$ sur E.

Corollaire 15. *Soient G est un sou-espace vectoriel de E et $g \in G'$, alors il existe $f \in E'$ prolongeant g et telle que $|||f||| = |||g|||$.*

Corollaire 16. *Pour tout $x \in E$, on a $\|x\| = \sup_{f \in \overline{B_{E'}(0,1)}} |f(x)|$.*

Proposition 17. *Soient E, F et G des espaces vectoriels normés, et soient $f \in \mathcal{L}_c(E, F)$ et $f \in \mathcal{L}_c(F, G)$. Alors $g \circ f \in \mathcal{L}_c(E, G)$ et on a $|||g \circ f||| \leqslant |||g||| \, |||f|||$.*

3) Cas de la dimension finie

Ici, on suppose E de dimension finie $n \in \mathbb{N}$.

Théorème 18. *Toutes les normes sur E sont équivalentes*

Corollaire 19. *Si F est un espace vectoriel, toute application linéaire $E \to F$ est continue.*

Corollaire 20. *Tout sous-espace vectoriel de dimension finie d'un espace vectoriel est fermé.*

Corollaire 21 (Heine-Borel)**.** *Les parties compactes de E sont exactement les parties fermées bornées.*

Contre-exemple 22. *Dans $E = (\mathcal{C}^0([0,1],\mathbb{R}), \|.\|_1)$, la boule unité fermé est fermée et bornée, mais n'est pas compacte.*

Remarque 23. *Tous ces corollaires sont faux en dimension infinie.*

Théorème 24 (Riesz)**.** *Un $\mathbb{K}$-espace vectoriel normé est de dimension finie si, et seulement si, sa boule unité fermé est compacte si, et seulement si, il est localement compact.*

II Cas des espaces de Banach

1) Généralités

Définition 25. On dit que $(E, \|.\|)$ est espace de Banach s'il est complet.

Théorème 26. *$(E, \|.\|)$ est un espace de Banach si, et seulement si, toute série absolument convergente de E est convergente.*

Proposition 27. *Si F est un Banach, alors $\mathcal{L}(E,F)$ est un Banach.*

Théorème 28. *Tout espace vectoriel normé de dimension finie est un espace de Banach.*

Exemple 29. *Pour tout $1 \leqslant p \leqslant +\infty$, $L^p_{\mathbb{K}}(\mu)$ est un espace de Banach.*

Proposition 30. *L'espace $\mathcal{C}^k([0,1],\mathbb{R})$, si on le munit de la norme $\|f\| = \sum_{i=0}^{k} \left\|f^{(i)}\right\|_\infty$, est un espace de Banach, contrairement à si on le munit de la norme $\|.\|_\infty$.*

2) Théorème de Baire et applications

Théorème 31 (Baire)**.** *Soit E un espace métrique complet. Toute réunion dénombrable de fermés d'intérieurs vides de E est d'intérieur vide.*

Corollaire 32. *Soit E un espace métrique complet. Toute intersection dénombrable d'ouverts denses est dense.*

Application 33. *Un espace de Banach est de dimension finie ou non dénombrable. Par exemple $\mathbb{R}[X]$ n'est complet pour aucune norme.*

Théorème 34 (Banach-Steinhaus)**.** *Soit E un espace de Banach et F un espace vectoriel normé. Soit $(u_i)_{i\in I}$ une famille d'opérateurs continus de E dans F. On suppose que, pour tout $x \in E$, $\sup_{i\in I} \|u_i(x)\| < +\infty$. Alors $\sup_{i\in I} \|u_i\| < +\infty$.*

Application 35. *Il existe des fonctions continues et 2π-périodique qui diffèrent de leur série de Fourier.*

Théorème 36 (Application ouverte)**.** *Une application linéaire continue surjective entre espaces de Banach est ouverte.*

Corollaire 37. *Une application linéaire continue bijective entre espaces de Banach est d'inverse continue*

Théorème 38 (Graphe fermé)**.** *Une application linéaire $T : E \to F$ entre deux espaces de Banach est continue si, et seulement si, son graphe $\{(x, T(x)) \,|\, x \in E\}$ est fermé pour la norme produit.*

III Cas des espaces de Hilbert

Définition 39. Un espace vectoriel est dit préhilbertien s'il est muni d'un produit scalaire. S'il est complet pour la norme issue du produit scalaire, on dit que c'est un espace de Hilbert (ou hilbertien).

Exemple 40. *$(L^2, \|.\|_2)$ est un espace de Hilbert.*

Proposition 41. *Un espace vectoriel normé E est un espace préhilbertien si, et seulement si, $\|.\|$ vérifie l'identité du parallélogramme, c'est-à-dire :*

$$\forall\, x, y \in E,\ \|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right)$$

Proposition 42 (Cauchy-Schwarz)**.** *Si H est préhilbertien, alors :*

$$\forall\, x, y \in H,\ |\langle x, y\rangle| \leqslant \|x\|\,\|y\|$$

Définition 43. Pour une partie A de H, son orthogonal est défini par $A^\perp = \{x \in H \,|\, \forall a \in A, \langle x, a\rangle = 0\}$.

Proposition 44. *Si $A \subseteq H$, $A^\perp$ est un sous-espace vectoriel fermé.*

Théorème 45. *Soit $K \subset E$ un convexe fermé non vide. Pour tout $f \in H$, il existe un unique élément de K, noté $P_K(f)$, et appelé projection de f sur K, tel que :*

$$\|P_K(f) - f\| = \inf_{v \in K} \|v - f\|$$

De plus, $P_K(f)$ est caractérisée par :

$$\forall v \in K,\ \langle f - P_K(f), v - P_K(f)\rangle \leqslant 0$$

Corollaire 46. *Soient M un sous-espace vectoriel fermé de H et $f \in H$. Alors $P_M(f)$ est caractérisé par :*

$$P_M(f) \in M \qquad et \qquad \forall\, v \in M,\ \langle f - P_M(f), v\rangle = 0$$

De plus, P_M est un opérateur linéaire.

Théorème 47 (Riesz-Fréchet)**.** *Soit $\varphi \in H'$. Alors il existe un unique $f \in H$ tel que :*

$$\forall\, v \in H,\ \langle \varphi, v\rangle = \langle f, v\rangle$$

Application 48. *Soit F un sous-espace vectoriel fermé d'un Hilbert H, alors $F \oplus F^\perp = H$*

Application 49. *Soit $u \in \mathcal{L}(H)$, il existe un unique $u^\star \in \mathcal{L}(H)$ tel que :*

$$\forall\, x, y \in H,\ \langle u(x), y\rangle = \langle x, u^\star(y)\rangle \quad avec \quad \|u\| = \|u^\star\|$$

Proposition 50. *Un sous-espace vectoriel F de H est dense si, et seulement si, $F^\perp = \{0\}$.*

Développements

- Théorème de Riesz-Fischer (29) [Bre87]
- Projection sur un convexe fermé et théorème de Riesz (45,46,47) [Bre87]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Bre87] H. Brezis. *Analyse fonctionelle.* Masson

I Approximation des fonctions régulières

1) Approximation locale de fonctions régulières

Théorème 1 (Taylor-Young). *Soient $n \in \mathbb{N}$ et f dérivable n fois en a. Alors :*

$$\forall\, x \in I,\ f(x) = \sum_{k=0}^{n} \frac{(x-a)^k}{k!} f^{(k)}(a) + \mathrm{o}\left((x-a)^n\right)$$

Théorème 2 (Taylor-Lagrange). *Soient $n \in \mathbb{N}$ et f de classe $\mathcal{C}^n$ de $[a,b]$ dans $\mathbb{R}$, et dérivable $n+1$ fois sur $]a,b[$. Alors :*

$$\exists\, c \in \mathring{I},\ f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \frac{(b-a)^{n+1}}{(n+1)!} f^{(n+1)}(c)$$

Théorème 3 (Taylor avec reste intégral). *Soient $n \in \mathbb{N}$ et f de classe $\mathcal{C}^{n+1}$ de $[a,b]$ dans $\mathbb{R}$. Alors :*

$$f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\, dt$$

Théorème 4 (Bernstein). *Soit $a > 0$ et $f :]-a,a[\to \mathbb{R}$ une fonction de classe $\mathcal{C}^\infty$ telle que, pour tout entier k, $f^{(2k)} \geqslant 0$ sur $]-a,a[$. Alors f admet un développement en série entière sur $]-a,a[$.*

2) Densité dans l'espace des fonctions continues

Théorème 5 (Weierstrass). *L'ensemble des polynômes sur $[a,b]$ est dense dans $(\mathcal{C}^0([a,b],\mathbb{R}), \|.\|_\infty)$.*

Remarque 6. *On a aussi le théorème de Stone-Weierstrass : L'ensemble des polynômes trigonométriques sur $[a,b]$ est dense dans $(\mathcal{C}^0([a,b],\mathbb{R}), \|.\|_\infty)$.*

Application 7. *Soit $f \in \mathcal{C}^0([a,b],\mathbb{K})$ vérifiant $\int_a^b t^n f(t)\, dt = 0$ pour tout $n \in \mathbb{N}$. Alors $f = 0$ sur $[a,b]$.*

Remarque 8. *Ce résultat n'est plus vrai si l'intervalle n'est pas borné. Si $f : \mathbb{R} \to \mathbb{R}$ est limite uniforme de polynômes alors f est un polynôme.*

II Approximation des fonctions intégrables

1) Convolution, densité et régularisation

Définition 9. On appelle convolution de f et g la fonction $f * g$ définie par $f * g(x) = \int_{\mathbb{R}^d} f(y) g(x-y)\, dy$ lorsque celle-ci est bien définie.

Proposition 10. *(i)* $f \in L^1,\ g \in L^p \Rightarrow \|f * g\|_p \leqslant \|f\|_1 \|g\|_p$.
(ii) $f \in L^p,\ g \in L^q \Rightarrow \|f * g\|_\infty \leqslant \|f\|_p \|g\|_q$.

Proposition 11. *$(L^1, +, *)$ est une algèbre de Banach.*

Définition 12. Une suite $(\rho_n)_{n\in\mathbb{N}}$ de fonctions positives de L^1 d'intégrale 1 sur $\mathbb{R}^d$ est une approximation de l'unité si elles sont d'intégrale 1 sur $\mathbb{R}^d$, et si, pour tout $\varepsilon > 0$, $\lim_{n\to\infty} \int_{\{|x|>\varepsilon\}} \rho_n = 0$. Si les ρ_n sont $\mathcal{C}^\infty$ à support compact, on parle de suite régularisante.

Théorème 13. *Soient $f \in L^p(\mathbb{R}^d)$ et $(\rho_n)_n$ une approximation de l'identité ($p \in [1,+\infty[$), alors $\lim\limits_{n\to+\infty} (\rho_n * f) = f$ dans $L^p(\mathbb{R}^d)$.*

Théorème 14. *Pour tout $p \in [1,+\infty[$, $\mathcal{C}_c^\infty(\mathbb{R}^d)$ est dense dans $L^p(\mathbb{R}^d)$.*

2) Cas particulier de L^2

Soit I un intervalle de $\mathbb{R}$.

Définition 15. Soit $\rho : I \to \mathbb{R}$ une fonction mesurable et strictement positive, vérifiant $\forall\, n \in \mathbb{N},\ \int_I |x|^n \rho(x)\, dx < +\infty$. On dit alors que ρ est une fonction poids.

Définition 16. On définit $L^2(I,\rho)$ comme l'ensemble des fonctions $f : I \to \mathbb{C}$ mesurables vérifiant $\int_I |f(x)|^2 \rho(x)\, dx < +\infty$.

Proposition 17. *$L^2(I,\rho)$ est un espace de Hilbert pour le produit scalaire $\langle f, g\rangle_\rho = \int_X f(x)\overline{g}(x)\rho(x)\, dx$.*

Théorème 18. *Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. S'il existe $a > 0$ tel que $\int_I e^{a|x|}\rho(x)dx < \infty$, alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I,\rho)$.*

III Interpolation polynômiale

1) Interpolation de Lagrange

Soit $f : [a,b] \to \mathbb{R}$ une fonction continue. On se donne $(x_i)_{0\leqslant i\leqslant n}$ des points deux à deux distincts de $[a,b]$.

Théorème 19. *Il existe un unique polynôme $P_n \in \mathbb{R}_n[X]$ tel que $P_n(x_i) = f(x_i)$ pour tout $i \in [\![0,n]\!]$. P_n est appelé polynôme interpolateur de Lagrange associé à f et à $(x_i)_{0\leqslant i\leqslant n}$. On a :*

$$P_n(X) = \sum_{i=0}^{n} f(x_i)\ell_i(X) \quad où \quad \ell_i(X) = \prod_{i\neq j} \frac{X - x_j}{x_i - x_j}$$

Théorème 20. *Supposons que f est $(n+1)$ fois dérivable. Alors, pour tout $x \in [a,b]$, il existe $\zeta_x \in [a,b]$ tel que :*

$$f(x) - P_n(x) = \frac{1}{(n+1)!}\Pi_{n+1}(x)f^{(n+1)}(\zeta_x) \quad où \quad \Pi_{n+1}(x) = \prod_{j=0}^{n} X - x_j$$

On a ainsi : $\|f - P_n\|_\infty \leqslant \frac{\|\Pi_{n+1}\|_\infty}{(n+1)!} \left\|f^{(n+1)}\right\|_\infty$.

Exemple 21. *La précision des polynômes interpolateurs provient alors du contrôle de $\|\Pi_{n+1}\|_\infty$, c'est-à-dire de la répartition des points. Dans le cas de points équidistants, on a :*

$$|f - P_n| \leqslant \frac{h^{n+1}}{n+1} \max_{0\leqslant i\leqslant n} \left|f^{(n+1)}(x_i)\right| \quad et \quad \|\Pi_{n+1}\|_\infty = \mathcal{O}\left(\left(\frac{b-a}{e}\right)^{n+1}\right)$$

Application 22 (Phénomène de Runge)**.** *Soit $f : x \mapsto \frac{1}{1+x^2}$ sur $[-1,1]$. C'est une fonction de classe $\mathcal{C}^\infty$ mais dont les dérivées augmentent rapidement en norme infinie vers 0. Pour des points équidistants, on a :*

$$\frac{\|\Pi_{n+1}\|_\infty}{(n+1)!} \left\|f^{(n+1)}\right\|_\infty \xrightarrow[n\to\infty]{\not\longrightarrow} 0$$

On observe alors que les polynômes d'interpolation ne converge pas uniformément vers f.

Définition 23. On définit par récurrence la suite $(T_n)_{n\in\mathbb{N}}$ de polynômes par $T_0 = 1$, $T_1 = X$ et $T_{n+1} = 2XT_n - T_{n-1}$. On vérifie alors que $T_n(\cos(\theta)) = \cos(n\theta)$ pour tout $\theta \in \mathbb{R}$.

Proposition 24. *Les racines de T_{n+1} sont les $\left(\cos\left(\frac{2k+1}{2n}\pi\right)\right)_{0\leqslant k\leqslant n}$ et sont appelés points d'interpolation de Tchebychev.*

Exemple 25. *Avec les points d'interpolation de Tchebychev, on a :*

$$\|\Pi_{n+1}\|_\infty = \mathcal{O}\left(\left(\frac{b-a}{4}\right)^{n+1}\right)$$

On obtient alors que les polynômes d'interpolation de Tchebychev sont plus précis que ceux associés à des points équidistants.

Application 26. *Le phénomène de Runge n'est plus observé avec les polynômes d'interpolation de Tchebychev.*

2) Application aux méthodes de quadrature

Soit $f : [a,b] \to \mathbb{R}$ une fonction continue. On cherche des formules pour approcher $I(f) = \int_a^b f(x)dx$. Fixons $a = x_0 < x_1 < \cdots < x_n = b$ une subdivision de $[a,b]$. On pose $h_i = x_{i+1} - x_i$.

Définition 27. Une méthode de quadrature consiste, pour $0 \leqslant i < n$ à approcher $I_i = \int_{x_i}^{x_{i+1}} f(x)dx$ par $A_i(f)$ défini par :

$$A_i(f) = h_i \sum_{j=0}^{n_i} \omega_{i,j} f(\zeta_{i,j}) \quad \text{où} \quad \zeta_{i,j} \in [\alpha_i, \alpha_{i+1}] \quad \text{et} \quad \sum_{i=0}^{n_i} \omega_{i,j} = 1$$

On note alors $E(f) = I(f) - \sum_{i=0}^{n-1} A_i(f)$ l'erreur de la méthode.

Définition 28. Une méthode de quadrature est d'ordre N si $E(f) = 0$ pour tout $f \in \mathbb{R}_N[X]$ et s'il existe $f \in \mathbb{R}_{N+1}[X]$ telle qu'elle soit inexacte.

Application 29. *En fixant $(\zeta_j)_{0\leqslant j\leqslant n}$ associé à une subdivision de $[x_i, x_{i+1}]$, on peut prendre pour fonction de poids $\omega_j = \frac{1}{h_i}\int_{[x_i,x_{i+1}]} \ell_j$, où $\ell_j = \prod_{k\neq j} \frac{X-\zeta_k}{\zeta_j-\zeta_k}$. Ce sont les méthodes par interpolation de Lagrange.*

(i) Méthode des rectangles : $I(f) \sim \sum_{i=0}^{n-1} h_i f(z_i)$ où $z_i = x_i$ ou x_{i+1}. Méthode d'ordre 0.

(ii) Méthode des points milieux : $I(f) \sim \sum_{i=0}^{n-1} h_i f(z_i)$ où $z_i = \frac{x_i+x_{i+1}}{2}$. Méthode d'ordre 1 et $E(f) \leqslant \frac{1}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iii) Méthode des trapèzes : $I(f) \sim \sum_{i=0}^{n-1} h_i \frac{f(x_i)+f(x_{i+1})}{2}$. Méthode d'ordre 1 et $E(f) \leqslant \frac{2}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iv) Méthode de Simpson : $I(f) \sim \sum_{i=0}^{n-1} h_i \frac{f(x_{i+1})+4f(\frac{x_i)+x_{i+1}}{2})+f(x_i)}{6}$. Méthode d'ordre 3 et $E(f) = \mathcal{O}\left(\left\|f^{(4)}\right\|_\infty\right)$ si f est $\mathcal{C}^4$.

IV Approximation de fonctions périodiques

On pose $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$, et on considère des fonction 2π-périodiques que l'on identifie à des fonctions $f : \mathbb{T} \to \mathbb{C}$.

1) Définition des séries de Fourier

Définition 30. On pose $CM(\mathbb{T})$ l'espace vectoriel des fonctions $f : \mathbb{T} \to \mathbb{R}$ continues par morceaux, et $C(\mathbb{T})$ le sous-espace vectoriel formé des fonctions continues. On considère $L^p(\mathbb{T})$ comme identifié avec $L^p([0, 2\pi])$.

Définition 31. Les coefficients exponentiels de Fourier de $f \in L^1(\mathbb{T})$ sont :

$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}\,dt \quad (n \in \mathbb{Z})$$

Les coefficients trigonométriques de Fourier de $f \in L^1(\mathbb{T})$ sont :

$$a_n(f) = \frac{1}{\pi}\int_0^{\pi} f(t)\cos(nt)\,dt\ ,\ b_n(f) = \frac{1}{\pi}\int_0^{\pi} f(t)\sin(nt)\,dt \quad (n \in \mathbb{N})$$

Définition 32. Soit $f \in L^1(\mathbb{T})$. On appelle série de Fourier de f la série :

$$S(f) = \sum_{n=-\infty}^{\infty} c_n(f)e^{int} = \frac{a_0(f)}{2} + \sum_{n=1}^{\infty}(a_n(f)\cos(nt) + b_n(f)\sin(nt))$$

Pour $N \in \mathbb{N}$, on appelle somme de Fourier d'ordre N :

$$S_N(f) = \sum_{n=-N}^{N} c_n(f)e^{int} = \frac{a_0(f)}{2} + \sum_{n=1}^{N}(a_n(f)\cos(nt) + b_n(f)\sin(nt))$$

Proposition 33. *Soient $f \in L^1(\mathbb{T})$, $a \in \mathbb{R}$ et $k, n \in \mathbb{Z}$. Alors :*

(i) $c_n(\check{f}) = c_{-n}(f)$ *(où $\check{f}(x) = f(-x)$)*
(ii) $c_n(\overline{f}) = \overline{c_{-n}(f)}$
(iii) $c_n(\tau_a f) = e^{-ina}c_n(f)$ *(où $(\tau_a f)(x) = f(x-a)$)*
(iv) $c_n(e_k f) = c_{n-k}(f)e_n$ *(où $e_k(t) = t^{ikt}$)*

Proposition 34. *Soit $f \in C(\mathbb{T})$ de classe $\mathcal{C}^1$ par morceaux. Alors $f' \in CM(\mathbb{T})$ et, pour tout $n \in \mathbb{Z}$, on a $c_n(f') = in\,c_n(f)$.*

Théorème 35 (Riemann-Lebesgue)**.** *Soit $f \in L^1(\mathbb{T})$. Alors $c_n(f)$ tend vers 0 lorsque n tend vers $\pm\infty$.*

2) Convergence de Fejér

Théorème 36 (Fejér)**.** *Pour $f \in C(\mathbb{T})$, la moyenne de Cesàro des sommes partielles de la série de Fourier de f converge uniformément vers f sur $\mathbb{T}$.*

Corollaire 37. *Tout élément de $C(\mathbb{T})$ est limite uniforme d'une suite de polynômes trigonométriques.*

Corollaire 38. *Soit $f \in C(\mathbb{T})$. Si $(c_n(f))_{n\in\mathbb{Z}} = 0$, alors $f = 0$.*

3) Convergence dans L^2

Proposition 39. *Pour $f \in L^2(\mathbb{T})$, la somme $S_N(f)$ est la projection orthogonale de f sur l'ensemble des polynômes trigonométriques de degré inférieur ou égal à N.*

Théorème 40 (Bessel)**.** *Pour $f \in L^2(\mathbb{T})$ et $N \in \mathbb{N}$, on a :*

$$\|c_n(f)\|_2^2 = \sum_{n=-N}^{N} |c_n(f)|^2 \leqslant \frac{1}{2\pi}\int_0^{2\pi} |f(t)|^2\,dt = \|f\|_2^2$$

Théorème 41 (Parseval)**.** *Pour $f \in L^2(\mathbb{T})$, $\sum_{n=-\infty}^{\infty} |c_n(f)|^2 = \|f\|_2$.*

Corollaire 42. *Pour $f \in L^2(\mathbb{T})$, $S_N(f)$ converge vers f dans $L^2(\mathbb{T})$.*

Développements

- Théorème de Weierstrass (5) [Gou08]
- Densité des polynômes orthogonaux (18) [BMP05]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[Dem06] J.-P. Demailly. *Analyse numérique et équations différentielles.* EDP Sciences

Cadre : Soit H un $\mathbb{K}$-espace vectoriel, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I Espaces de Hilbert

1) Produit scalaire, espace pré-hilbertien

Définition 1. $\langle .,. \rangle : H \times H \to \mathbb{K}$ est un produit scalaire si :

(i) Pour tout $y \in H$, $x \mapsto \langle x, y \rangle$ est linéaire.

(ii) Pour tous $x, y \in H$, $\langle x, y \rangle = \overline{\langle y, x \rangle}$.

(iii) Pour tout $x \in H$, $\langle x, x \rangle \in \mathbb{R}^+$.

(iv) Pour tout $x \in H$, $\langle x, x \rangle = 0 \Leftrightarrow x = 0$.

L'espace H muni d'un produit scalaire est appelé espace pré-hilbertien. On fixe pour la suite un produit scalaire $\langle .,. \rangle$ sur H.

Remarque 2. *Pour $x, y \in H$, $\langle x+y, x+y \rangle = \langle x, x \rangle + \langle y, y \rangle + 2 \operatorname{Re} \langle x, y \rangle$.*

Exemple 3. *Soit $H = \mathbb{C}^d$. Le produit scalaire canonique est défini pour $x = (x_1, \dots, x_d), y = (y_1, \dots, y_d) \in H$ par $\langle x, y \rangle = \sum_{i=1}^{d} x_i \overline{y_i}$.*

Proposition 4 (Cauchy-Schwarz)**.** *Si H est pré-hilbertien, alors :*

$$\forall\, x, y \in H,\ |\langle x, y \rangle|^2 \leqslant \langle x, x \rangle \langle y, y \rangle$$

Avec égalité si, et seulement si, x et y sont colinéaires.

Corollaire 5. *La relation $\|x\| = \sqrt{\langle x, x \rangle}$ définit une norme sur H*

Exemple 6. *Dans $\mathbb{C}^d$, on retrouve la norme usuelle.*

Proposition 7. *Un espace vectoriel normé H est un espace pré-hilbertien si, et seulement si, $\|.\|$ vérifie l'identité du parallélogramme, c'est-à-dire :*

$$\forall\, x, y \in H,\ \|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right)$$

Définition 8. On dit que deux éléments x et y de H sont orthogonaux si $\langle x, y \rangle = 0$. Pour $A \subset H$, on définit son orthogonal par $A^\perp = \{x \in H \,|\, \forall\, a \in A,\ \langle x, a \rangle = 0\}$. C'est un sous-espace vectoriel fermé de H.

Théorème 9 (Pythagore)**.** *Si $x, y \in H$ sont orthogonaux, alors $\|x+y\|^2 = \|x\|^2 + \|y\|^2$.*

Définition 10. On dit que H est un espace de Hilbert s'il est complet pour la norme induite par son produit scalaire.

Exemple 11. *Tout espace pré-hilbertien de dimension finie est de Hilbert.*

2) Théorème de projection sur un convexe fermé

On fixe H un espace de Hilbert et K un convexe fermé non vide de H.

Théorème 12. *Pour tout $f \in H$, il existe un unique élément de K, noté $P_K(f)$, et appelé projection de f sur K, tel que :*

$$\|P_K(f) - f\| = \inf_{v \in K} \|v - f\|$$

De plus, $P_K(f)$ est caractérisée par :

$$\forall v \in K,\ \operatorname{Re}\left(\langle f - P_K(f), v - P_K(f) \rangle\right) \leqslant 0$$

Remarque 13. *L'application $x \mapsto P_K(x)$ est 1-lipschitzienne.*

Corollaire 14. *Soient M un sous-espace vectoriel fermé de H et $f \in H$. Alors $P_M(f)$ est caractérisé par :*

$$P_M(f) \in M \qquad et \qquad \forall\, v \in M,\ \operatorname{Re}\left(\langle f - P_M(f), v \rangle\right) = 0$$

De plus, P_M est un opérateur linéaire.

Corollaire 15. *Soit F un sous-espace vectoriel de H.*

(i) Si F est fermé, alors $F \oplus F^\perp = H$.

(ii) F est dense si, et seulement si, $F^\perp = \{0\}$.

3) Dualité

Théorème 16 (Riesz-Fréchet)**.** *Soit $\varphi \in H'$. Alors :*

$$\exists!\, f \in H,\ \forall\, v \in H,\ \langle \varphi, v \rangle = \langle f, v \rangle$$

Application 17. *Soit $T \in \mathcal{L}(H)$, il existe un unique $T^\star \in \mathcal{L}(H)$ tel que :*

$$\forall\, x, y \in H,\ \langle Tx, y \rangle = \langle x, T^\star y \rangle \quad avec \quad \|T\| = \|T^\star\|$$

On appelle $T^\star$ l'opérateur adjoint de T.

Proposition 18. *Pour $T, S \in \mathcal{L}(H)$, on a $T^{\star\star} = T$, $(TS)^\star = S^\star T^\star$.*

Exemple 19. *En dimension finie, les notions d'opérateurs adjoints sont traduites par les notions de matrices transposées ou transconjuguées.*

Théorème 20 (Lax-Milgram)**.** *Soient H un espace de Hilbert, a une forme bilinéaire continue et coercive sur H, et $\ell \in H'$. Alors il existe un unique $u \in H$ tel que, pour tout $v \in H$, $a(u, v) = \ell(v)$. Si de plus a est symétrique, u réalise le minimum sur H de $v \mapsto \frac{1}{2} a(v, v) - \ell(v)$.*

Théorème 21 (Hahn-Banach)**.** *Soit F un sous-espace vectoriel strict de H. Tout $f \in F'$ admet un prolongement continu sur H de même norme.*

II Bases hilbertiennes

1) Définitions et premières propriétés

Définition 22. Une famille d'un espace pré-hilbertien sera dite orthogonale si ses éléments sont deux à deux orthogonaux, et orthonormales si ses éléments sont de plus de norme 1.

Proposition 23. *Toute famille orthonormale est libre*

Définition 24. Une famille orthonormale est appelée base hilbertienne si l'espace vectoriel qu'elle engendre est dense.

Proposition 25 (Gram-Schmidt)**.** *Soit $N \in \mathbb{N}^\star \cup \{\infty\}$ et $(f_n)_{1\leqslant n<N}$ une famille libre de H. Il existe une famille orthonormale $(e_n)_{1\leqslant n<N}$ de H telle que, pour tout $n < N$,* $\mathrm{Vect}(e_1, \dots, e_n) = \mathrm{Vect}(f_1, \dots, f_n)$.

Exemple 26. *Les suites $\mathbb{1}_n$ sont une base hilbertienne de $\ell^2(\mathbb{N})$, mais pas une base algébrique. Les applications $e_n : t \mapsto e^{int}$ pour $n \in \mathbb{Z}$ forment une base hilbertienne de $L^2(\mathbb{T})$.*

Théorème 27. *Tout espace de Hilbert admet une base hilbertienne.*

Proposition 28. *Soit $(e_j)_{j\in J}$ une famille orthonormale finie de H, et soit F l'espace vectoriel engendré par cette famille. La projection orthogonale P_F sur F est définie pour $x \in H$ par $P_F(x) = \sum_{j\in J} \langle x, e_j\rangle\, e_j$. En conséquence $\|x\|^2 = \|x - P_F(x)\| + \sum_{j\in J} \left|\langle x, e_j\rangle\right|^2$.*

Proposition 29 (Bessel)**.** *Soit $(e_j)_{j\in J}$ une famille orthonormale de H. Alors, pour tout $x \in H$, on a $\sum_{j\in J} \left|\langle x, e_j\rangle\right|^2 \leqslant \|x\|^2$.*

Théorème 30. *Soit $(e_j)_{j\in J}$ orthonormale dans H. Sont équivalents :*

(i) $(e_j)_{j\in J}$ *est une base hilbertienne.*

(ii) $\forall x \in H,\ \|x\|^2 = \sum_{j\in J} \left|\langle x, e_j\rangle\right|^2$ *(Bessel)*

(iii) $\forall x, y \in H,\ \langle x, y\rangle = \sum_{j\in J} \langle x, e_j\rangle \langle y, e_j\rangle$ *(Parseval)*

2) Polynômes orthogonaux

Soit I un intervalle de $\mathbb{R}$.

Définition 31. Soit $\rho : I \to \mathbb{R}$ une fonction mesurable et strictement positive, vérifiant $\forall n \in \mathbb{N},\ \int_I |x|^n \rho(x)\, dx < +\infty$. On dit alors que ρ est une fonction poids.

Définition 32. On définit $L^2(I, \rho)$ comme l'ensemble des fonctions $f : I \to \mathbb{C}$ mesurables vérifiant $\int_I |f(x)|^2 \rho(x)\, dx < +\infty$.

Proposition 33. *$L^2(I, \rho)$ est un espace de Hilbert pour le produit scalaire $\langle f, g\rangle_\rho = \int_X f(x)\overline{g}(x)\rho(x)\, dx$.*

Théorème 34. *Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. S'il existe $a > 0$ tel que $\int_I e^{a|x|}\rho(x)dx < \infty$, alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I, \rho)$.*

3) Séries de Fourier

Définition 35. Soit $f : \mathbb{R} \to \mathbb{C}$ continue par morceaux et 2π-périodique. Les coefficients exponentiels de Fourier de f sont :

$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}\, dt \quad (n \in \mathbb{Z})$$

En posant $e_n : t \mapsto e^{int}$, la série de Fourier associée à f est la série trigonométrique $\sum_{n\in\mathbb{Z}} c_n(f)e_{-n}$.

Proposition 36 (Riemann-Lebesgue)**.** *Si f est continue par morceaux et 2π-périodique, alors* $\lim_{|n|\to+\infty} c_n(f) = 0$.

Théorème 37. *La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de l'espace des fonctions 2π-périodiques de carré intégrable sur $[0, 2\pi]$. On a en particulier :*

$$\frac{1}{2\pi}\|f\|_2^2 = \sum_{n\in\mathbb{Z}} c_n(f)^2$$

Proposition 38. *Si f est $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge simplement vers la régularisation $\tilde{f}$ de f donnée pour $x \in \mathbb{R}$ par $\tilde{f}(x) = \frac{f(x^+)+f(x^-)}{2}$.*

Remarque 39. *L'hypothèse $\mathcal{C}^1$ par morceaux est nécessaire.*

Théorème 40. *Si f est continue, $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge normalement vers f.*

III Applications

1) Convergence faible

Définition 41. On dit qu'une suite $(x_n)_{n\in\mathbb{N}}$ de H converge faiblement vers $x \in H$, noté $x_n \xrightarrow{H} x$, lorsque :

$$\forall\, y \in H,\ \lim_{n\to+\infty} \langle x_n, y\rangle = \langle x, y\rangle$$

Remarque 42. *Ceci est en réalité une caractérisation d'une définition plus générale. La convergence forte entraîne la convergence faible, mais la réciproque est fausse.*

Proposition 43. *Soit $(x_n)_{n\in\mathbb{N}}$ qui converge faiblement vers x dans H. Alors $\liminf_{n\to+\infty} \|x_n\| \geqslant \|x\|$. De plus, sont équivalents :*

(i) $(x_n)_{n\in\mathbb{N}}$ *converge vers* x.

(ii) $\limsup_{n\to+\infty} \|x_n\| \leqslant \|x\|$.

(iii) $\lim_{n\to+\infty} \|x_n\| = \|x\|$.

Théorème 44. *De toute suite bornée de H on peut extraire une sous-suite qui converge faiblement.*

Proposition 45. *Le rayon spectral d'un opérateur autoadjoint sur H est égal à sa norme.*

Application 46. *Soient H un espace de Hilbert réel, et $J : E \to \mathbb{R}$ convexe continue et coercive. Alors J admet un minimum sur H.*

2) Espaces de Sobolev

On considère $I =]a, b[$ un intervalle de $\mathbb{R}$.

Définition 47. Soit $f \in L^1(I)$. On dit que f admet une dérivée faible s'il existe $g \in L^1(I)$ tel que, pour tout $\varphi \in \mathcal{C}_c^\infty(I)$, on a $\int_I f\varphi' = -\int_I g\varphi$. On note alors $g = f'$, qui est unique.

Définition 48. On définit $H^1(I) = \left\{f \in L^2(I) \,\middle|\, f' \in L^2(I)\right\}$, que l'on munit du produit scalaire défini par $\langle f, g\rangle_{H^1} = \langle f, g\rangle_{L^2} + \langle f', g'\rangle_{L^2}$.

Théorème 49. $\left(H^1(I), \langle .,.\rangle_{H^1}\right)$ *est un espace de Hilbert.*

Définition 50. On définit $H_0^1(I)$ comme l'adhérence de $\mathcal{C}_c^\infty(I)$ dans $H^1(I)$. $H_0^1(I)$ est un espace de Hilbert lorsqu'il est munit du produit scalaire $\langle .,.\rangle_{H^1}$.

Application 51. *Grâce à une formulation faible d'un problème différentiel et au théorème de Lax-Milgram, on peut démontrer l'existence d'une solution faible à ce problème.*

Application 52 (Dirichlet)**.** *Pour $f \in L^2$, on considère le problème :*

$$\begin{cases} -u'' + u = f & \text{sur }]0,1[\\ u(0) = u(1) = 0 \end{cases}$$

Il existe une unique solution faible $u \in H_0^1([0,1])$ à ce problème.

Développements

- Projection sur un convexe fermé et théorème de Riesz (12,14,16) [Bre87]
- Densité des polynômes orthogonaux (34) [Rou15]

Références

[HL99] F. Hirsch et G. Lacombe. *Éléments d'analyse fonctionnelle.* Dunod
[Bre87] H. Brezis. *Analyse fonctionelle.* Masson
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

I Théorème d'inversion locale

1) Énoncé et premières variantes

Définition 1. Soient U un ouvert de $\mathbb{R}^p$ et V un ouvert de $\mathbb{R}^q$, pour $p, q \in \mathbb{N}^\star$. Une application $f : U \to V$ est un difféomorphisme de classe $\mathcal{C}^k$ si elle est bijective de réciproque $\mathcal{C}^k$.

Exemple 2. *Tout intervalle ouvert de $\mathbb{R}$ est difféomorphe à $\mathbb{R}$.*

Théorème 3 (Théorème d'inversion locale)**.** *Soient U un ouvert de $\mathbb{R}^n$, $a \in U$ et $f : U \to \mathbb{R}^n$ de classe $\mathcal{C}^k$. On suppose que la matrice jacobienne $Df(a)$ est inversible. Il existe alors un ouvert $V \subset U$ contenant a tels que $f|_V$ soit un difféomorphisme de classe $\mathcal{C}^k$ de V sur $f(V)$.*

Exemple 4. *L'application $f : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $f(x, y) = (x^2 - y^2, 2xy)$ est un difféomorphisme de classe $\mathcal{C}^k$ au voisinage de tout point de $\mathbb{R}^2 \setminus \{0\}$.*

Remarque 5. *L'équation $f(x) = y$ admet une unique solution dans V donnée par $x = f^{-1}(y)$, mais pas en dehors de V.*

Définition 6. Un difféomorphisme local est une application de classe $\mathcal{C}^k$ d'un ouvert U de $\mathbb{R}^n$ dans $\mathbb{R}^n$ dont la différentielle en tout point est inversible.

Remarque 7. *Dans le théorème d'inversion locale, on dit alors que f est un $\mathcal{C}^k$-difféomorphisme local en a.*

Exemple 8. *L'application $(r, \theta) \mapsto (r\cos\theta, r\sin\theta)$ est un difféomorphisme local de $]0, +\infty[\times\mathbb{R}$ sur $\mathbb{R}^2 \setminus \{0\}$.*

Théorème 9 (Théorème d'inversion globale)**.** *Soient U un ouvert de $\mathbb{R}^n$ et $f : U \to \mathbb{R}^n$ de classe $\mathcal{C}^1$. On suppose que f est injective sur U et que, pour tout $x \in U$, la matrice jacobienne $Df(x)$ est inversible. Alors $f(U)$ est un ouvert de $\mathbb{R}^n$, et f est un $\mathcal{C}^1$-difféomorphisme de U sur $f(U)$.*

Contre-exemple 10. *L'application $f : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $f(x, y) = (x^2 - y^2, 2xy)$ est un difféomorphisme local au voisinage de tout point de $\mathbb{R}^2 \setminus \{(0, 0)\}$, mais n'est pas un difféomorphisme global.*

2) Applications

Changement de coordonnées

Définition 11. On appelle changement de coordonnées sur $V \subset \mathbb{R}^n$ la donnée de n fonctions $f_1, \dots, f_n : V \to \mathbb{R}$ telles que $f = (f_1, \dots, f_n)$ soit un difféomorphisme $\mathcal{C}^1$ de V sur $f(V)$.

Théorème 12. *Soient $f_1, \dots, f_n$ des fonctions de classe $\mathcal{C}^1$ au voisinage de $a \in \mathbb{R}^n$. Les relations $u_i = f_i(x_1, \dots, x_n)$ pour tout $i \in [\![1, n]\!]$ définissent un changement de coordonnées sur un voisinage de a si, et seulement si, le déterminant jacobien est non nul.*

Racine k-ième d'une matrice

Application 13. *Soient $k \in \mathbb{N}^\star$ et $A \in \mathcal{M}_n(\mathbb{R})$. Si A est suffisamment proche de I_n, alors il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que $B^k = A$.*

Lemme de Morse

Lemme 14. *Soit $A_0 \in \mathcal{GL}_n(\mathbb{R}) \cap \mathcal{S}_n(\mathbb{R})$. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et $\rho : V, \mathcal{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que pour tout $A \in V$, on a ${}^t\rho(A)A_0\rho(A)$.*

Théorème 15 (Lemme de Morse)**.** *Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ définie sur un ouvert U de $\mathbb{R}^n$ contenant 0. On suppose que $df(0) = 0$ et que $d^2f(0)$ est non dégénérée et de signature $(p, n-p)$. Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = \sum_{i=1}^{p} \varphi_i(x)^2 - \sum_{i=p+1}^{n} \varphi_i(x)^2$ au voisinage de 0.*

II Théorème des fonctions implicites

1) Énoncé du théorème

Théorème 16 (Théorème des fonctions implicites)**.** *Soient U un ouvert de $\mathbb{R}^n \times \mathbb{R}^p$, (a, b) un point de U, et $f : U \to \mathbb{R}^p$ une application de classe $\mathcal{C}^1$. On suppose que $f(a, b) = 0$ et que la matrice jacobienne $D_y f(a, b)$, formée des dérivées partielles par rapport à y, est inversible. Alors l'équation $f(x, y) = 0$ peut être résolue localement par rapport aux variables y : il existe un voisinage ouvert V de a dans $\mathbb{R}^n$, un voisinage ouvert W de b*

dans $\mathbb{R}^p$, avec $V \times W \subset U$, et une application $\varphi : V \to W$, de classe $\mathcal{C}^1$, unique, telle que :

$$(x \in V,\, y \in W \text{ et } f(x,y) = 0) \Leftrightarrow (x \in V \text{ et } y = \varphi(x))$$

Exemple 17. *L'équation $x^2+y^2-1=0$ définit deux fonctions implicites :*

$$\varphi_1 : \left| \begin{array}{ccc}]-1,1[& \longrightarrow &]0,+\infty[\\ x & \longmapsto & \sqrt{1-x^2} \end{array} \right. \text{ et } \varphi_2 : \left| \begin{array}{ccc}]-1,1[& \longrightarrow &]-\infty,0[\\ x & \longmapsto & -\sqrt{1-x^2} \end{array} \right.$$

2) Différentielle de la fonction implicite

Développement limité

Exemple 18. *Soit* $f : \left| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & \sin y + xy^4 + x^2 \end{array} \right.$ *. Par le théorème des fonctions implicites, il existe V et W des voisinages ouverts de 0 dans $\mathbb{R}$ et $\varphi : V \to W$ de classe $\mathcal{C}^\infty$ telle que $\varphi(x) = y$. Cette application φ admet un développement limité à l'ordre 6 au voisinage de 0 : $\varphi(x) = -x^2 - \frac{x^6}{6} + \mathcal{O}(x^7)$.*

Expression générale

Remarque 19. *Le théorème des fonctions implicites assure l'existence de $D\varphi(x)$ sur V.*

Proposition 20. *On a $D\varphi(x) = -(D_y f(x,\varphi(x)))^{-1} \circ D_x f(x,\varphi(x))$.*

Exemple 21. *En reprenant l'équation $x^2 + y^2 - 1 = 0$, on obtient $2x + 2yy' = 0$ en dérivant par rapport à x. y étant pris sur un ouvert de sorte que $y \neq 0$, on peut finalement écrire que $\varphi'(x) = y' = -\frac{x}{y}$.*

3) Application

Proposition 22. *Soient $P_0 \in \mathbb{R}_n[X]$ et x_0 une racine simple de P_0. Alors il existe une application φ de classe $\mathcal{C}^\infty$ définie sur un voisinage U de P_0 dans $\mathbb{R}_n[X]$ à valeurs dans un voisinage V de x_0 dans $\mathbb{R}$ telle que :*

$$\forall\, P \in U,\ \forall\, x \in V,\ x = \varphi(P) \Leftrightarrow P(x) = 0$$

Définition 23. On dit que la racine x_0 dépend localement du polynôme P_0 de manière $\mathcal{C}^\infty$.

III Applications aux sous-variétés

1) Sous-variétés

Définition 24. Une partie M de $\mathbb{R}^n$ est une sous-variété de $\mathbb{R}^n$ de classe $\mathcal{C}^k$ et de dimension d si, pour tout $a \in M$, il existe un voisinage U de a dans $\mathbb{R}^n$ et $\phi : U \to \mathbb{R}^n$ un difféomorphisme sur son image tel que :

$$\phi(U \cap M) = \phi(U) \cap (\mathbb{R}^d \times \{0\})$$

On dit que (U, ϕ) est une carte locale en a.

Théorème 25. *Soit M une partie de $\mathbb{R}^n$. Les deux assertions suivantes sont équivalentes :*

(i) M est une sous-variété de classe $\mathcal{C}^k$ et de dimension d.

(ii) Pour tout $a \in M$, il existe un voisinage U de a dans $\mathbb{R}^n$ et des applications $g_1, \dots, g_{n-d} : U \to \mathbb{R}$ de classe $\mathcal{C}^k$ telles que :

(a) Les formes linéaires $d_x g_1, \dots, d_x g_{n-d}$ sont linéairement indépendantes pour tout $x \in U$.

(b) $U \cap M = \{x \in U \,|\, \forall\, i \in [\![1, n-d]\!],\ g_i(x) = 0\}$

2) Espaces tangents

Définition 26. Soit M une sous-variété de $\mathbb{R}^n$. Un vecteur $v \in \mathbb{R}^n$ est dit tangent à M en $a \in M$ s'il existe une application différentiable $\gamma :]-\varepsilon, \varepsilon[\to \mathbb{R}^n$, où $\varepsilon > 0$, telle que :

(i) $\forall\, t \in]-\varepsilon, \varepsilon[,\ \gamma(t) \in M$

(ii) $\gamma(0) = a,\ \gamma'(0) = v$

On note $T_a M$ l'ensemble des vecteurs tangents à M en a, appelé espace tangent à M en a.

Théorème 27. *L'ensemble $T_a M$ est un sous-espace vectoriel de $\mathbb{R}^n$ de dimension d.*

Lemme 28. *Soit $\ell_1, \dots, \ell_d$ des formes linéaires sur $\mathbb{R}^n$ qui sont linéairement indépendantes. Alors* $\dim \bigcap_{i=1}^{n-d} \operatorname{Ker} \ell_i = n - d$.

Proposition 29. *Soit M une sous-variété de dimension d de $\mathbb{R}^n$. Soient $a \in M$ et U un voisinage de a dans $\mathbb{R}^n$. Soient $g_1, \dots, g_{n-d} : U \to \mathbb{R}$ des fonctions de classe $\mathcal{C}^k$ telles que :*

(i) Les formes linéaires $d_x g_1, \dots, d_x g_{n-d}$ sont linéairement indépendantes pour tout $x \in U$.

(ii) $U \cap M = \{x \in U \,|\, \forall\, i \in [\![1, n-d]\!],\ g_i(x) = 0\}$

Alors $T_a M = \bigcap_{i=1}^{n-d} \operatorname{Ker} d_a g_i$.

3) Extrema liés

Définition 30. Soit M une sous-variété de $\mathbb{R}^n$. On dit qu'une fonction $f : \mathbb{R}^n \to \mathbb{R}$ a un extremum lié (ou relatif) en $a \in M$ s'il existe un voisinage U de a dans $\mathbb{R}^n$ tel que $f(a)$ est un extremum de f sur $M \cap U$.

Théorème 31 (Extrema liés)**.** *Soit U un ouvert de $\mathbb{R}^n$. Soient $g_1, \dots, g_k$ des fonctions de classe $\mathcal{C}^1$ de U dans $\mathbb{R}$ telles que les formes linéaires $d_x g_1, \dots, d_x g_k$ sont linéairement indépendantes pour tout $x \in U$. Posons :*

$$M = \{x \in U \,|\, \forall\, i \in [\![1, k]\!],\ g_i(x) = 0\}$$

Alors, si f a un extremum lié en $a \in M$, il existe $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ tels que :

$$d_a f = \sum_{i=1}^{k} \lambda_k \, d_a g_i$$

Ces réels $\lambda_1, \dots, \lambda_k$ sont appelés multiplicateurs de Lagrange.

Développements

- Lemme de Morse (14,15) [Rou15]
- Extrema liés (28,29,31) [Ave83]

Références

[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini
[Ave83] A. Avez. *Calcul différentiel.* Masson

Annexes

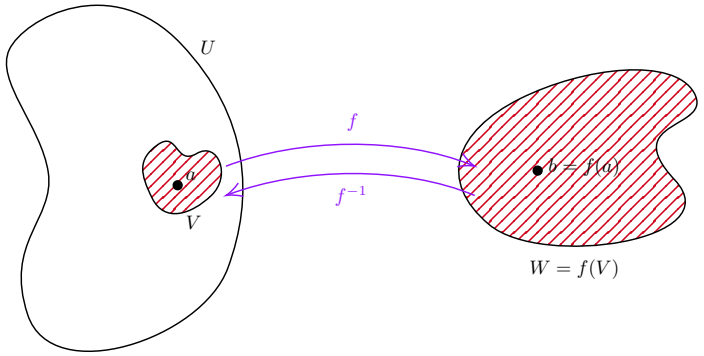


FIGURE 1 – Théorème d'inversion locale

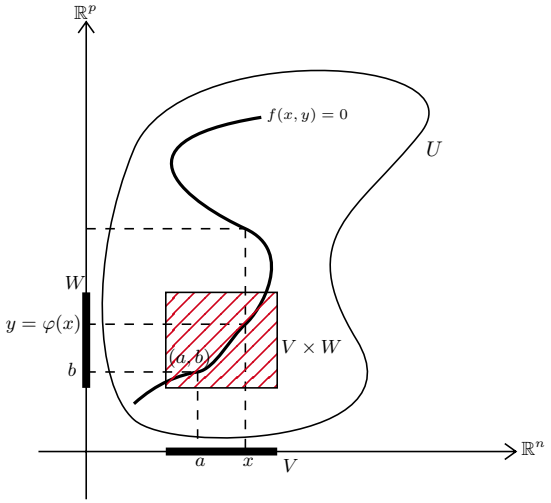


FIGURE 2 – Théorème des fonctions implicites

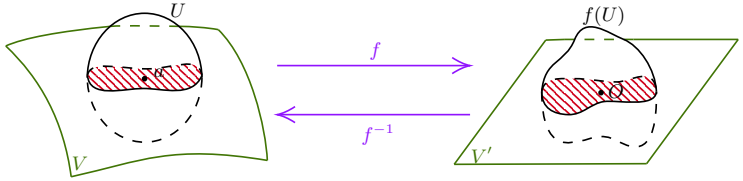


FIGURE 3 – Sous-variété

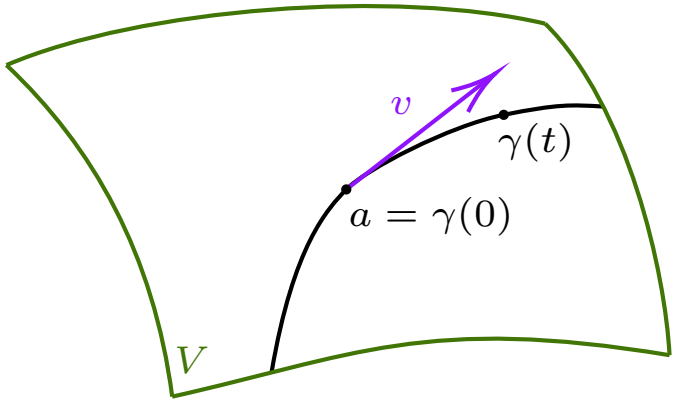


FIGURE 4 – Vecteur tangent à V en a

Cadre : E et F sont deux $\mathbb{R}$-espaces vectoriels normés de dimensions finies. U est un ouvert de E.

I Définitions et premières propriétés

1) Différentielle

Définition 1. Une application $f : U \to F$ est dite différentiable au point $a \in U$ s'il existe une application linéaire $L \in \mathcal{L}(E, F)$ telle que :

$$f(a+h) - f(a) = L(h) + o(\|h\|)$$

Proposition 2. *Si f est différentiable au point $a \in U$, L est unique.*

Remarque 3. *On notera $L = Df(a)$ la différentielle de f au point a.*

Exemple 4. *Si $E = F = \mathbb{R}$, alors $Df(a)$ est la multiplication par $f'(a)$.*

Proposition 5. *Si f est différentiable en $a \in U$, f est continue en a.*

Définition 6. Une application $f : U \to F$ est de classe $\mathcal{C}^1$ sur U si elle est différentiable en tout point de U et si l'application $Df : x \mapsto Df(x)$ est continue de U dans $\mathcal{L}(E, F)$.

Exemple 7. *(i) Si f est linéaire, alors $Df(a) = f$.*

(ii) Si f est constante, alors Df est nulle sur E.

(iii) Si f est quadratique, on écrit $f(x) = B(x, x)$ où B est une forme bilinéaire symétrique sur $\mathbb{R}^n$, et on a $Df(a) \cdot h = 2B(a, h)$.

Application 8. *Soient $y_1, \dots, y_n$ les solutions du système différentiel $y'(t) = A(t)y(t)$, où $A(t) \in \mathcal{M}_n(\mathbb{R})$ est une fonction continue et soit $w(t) = \det(y_1(t), \dots, y_n(t))$ leur wronskien. Alors $w'(t) = \operatorname{tr}(A(t))w(t)$, et si A est constante $\det(e^{tA}) = e^{t \operatorname{tr}(A)}$.*

Proposition 9. *Si f et g sont différentiables en a, et si $\lambda \in \mathbb{R}$, alors $f + g$ est différentiable avec $D(f + g)(a) = Df(a) + Dg(a)$ et λf est différentiable avec $D(\lambda f)(a) = \lambda Df(a)$.*

Proposition 10. *Si f est différentiable en a, et si g est différentiable en $f(a)$, alors $g \circ f$ est différentiable en a avec $D(g \circ f)(a) = Dg(f(a)) \circ Df(a)$.*

Définition 11. Soit V un ouvert de F. Une fonction $f : U \to V$ est un difféomorphisme de classe $\mathcal{C}^1$ si f est bijective de classe $\mathcal{C}^1$ sur U et si l'application réciproque f^{-1} est de classe $\mathcal{C}^1$ sur V.

Application 12. *Soit V un ouvert de F et $f : U \to V$ un difféomorphisme. Alors $D(f^{-1})(f(x)) \circ Df(x) = Id_{\mathbb{R}^n}$.*

Remarque 13. *Si $f, g : U \to \mathbb{R}$ sont différentiables en $a \in U$, alors fg est différentiable avec $D(fg)(a) = Df(a)g(a) + f(a)Dg(a)$.*

2) Accroissements finis

Théorème 14 (Accroissements finis)**.** *Soient $f : U \to F$ et $a, b \in U$ tels que le segment $[a, b] \subset U$. Si f est continue sur $[a, b]$ et différentiable sur $]a, b[$, et s'il existe $M > 0$ tel que, pour tout $x \in]a, b[$, $\|Df(x)\| \leqslant M$, alors $\|f(b) - f(a)\| \leqslant M \|b - a\|$.*

Corollaire 15. *Soit $f : U \to F$ différentiable sur U convexe. S'il existe $M > 0$ tel que, pour tout $x \in U$, $\|Df(x)\| \leqslant M$, alors, pour tous $a, b \in U$, $\|f(b) - f(a)\| \leqslant M \|b - a\|$.*

Corollaire 16. *Si U est un ouvert connexe, et si $Df(x) = 0$ sur U, alors f est constante sur U.*

Application 17. *Soit $(f_k)_k$ un suite d'applications définies de U dans F et différentiables sur U. On suppose de plus :*

(i) $(f_k)_k$ converge simplement sur U vers $f : U \to F$.

(ii) $(D(f_k))_k$ converge uniformément sur U.

Alors f est différentiable sur U et $Df = \lim_{k \to +\infty} D(f_k)$.

Exemple 18. *Si $E = F = \mathcal{M}_n(\mathbb{K})$, $\exp : M \mapsto \sum_{k=0}^{\infty} \frac{M^k}{k!}$ est $\mathcal{C}^1$.*

3) Dérivées partielles

Définition 19. Soient $f : U \to F$ une application, $a \in U$ et $v \in E$. Si la fonction à variable réelle $t \mapsto f(a + tv)$ est dérivable en 0, f est dite dérivable en a selon le vecteur v. On note alors :

$$D_v f(a) = \lim_{\substack{t \to 0 \\ t \neq 0}} \frac{f(a + tv) - f(a)}{t}$$

Proposition 20. *Si $f : U \to F$ est différentiable en $a \in U$ alors f admet une dérivée selon tout vecteur v et on a $D_v f(a) = Df(a) \cdot v$.*

Exemple 21. *La fonction $f : \mathbb{R}^2 \to \mathbb{R}$ définie par $f(x, y) = \frac{y^2}{x}$ si $x \neq 0$ et $f(0, y) = y$ admet des dérivées directionnelles selon tous les vecteurs en $(0, 0)$, mais n'est pas continue.*

Définition 22. Soient U un ouvert de $\mathbb{R}^n$ et $f : U \to F$. Soient $a \in U$ et $(e_1, \dots, e_n)$ la base de $\mathbb{R}^n$. Si, pour $i \in [\![1, n]\!]$, f est dérivable en a selon e_i, on dit que f admet une dérivée partielle en a d'indice i, et on note :

$$\frac{\partial f}{\partial x_i}(a) = D_{e_i} f(a)$$

Théorème 23. *Soient U un ouvert de $\mathbb{R}^n$ et $f : U \to F$, alors f est de classe $\mathcal{C}^1$ sur U si, et seulement si, f admet des dérivées partielles continues sur U.*

Exemple 24. $Inv : \left| \begin{array}{ccc} \mathcal{GL}_n(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ M & \longmapsto & M^{-1} \end{array} \right.$ *est de classe $\mathcal{C}^\infty$, et $D(Inv)(M) \cdot H = -M^{-1}HM^{-1}$ pour tout $M \in \mathcal{GL}_n(\mathbb{R})$ et $H \in \mathcal{M}_n(\mathbb{R})$.*

Définition 25. Si $F = \mathbb{R}$ et si $\mathbb{R}^n$ est muni d'un produit scalaire, il existe un unique vecteur $\nabla f(a) \in \mathbb{R}^n$, appelé gradient de f en a, tel que $Df(a) \cdot h = \nabla f(a) \cdot h$.

Remarque 26. $\nabla f(a) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) e_i$

Définition 27. Pour $E = \mathbb{R}^n$, $F = \mathbb{R}^p$ et $f = (f_1, \dots, f_p)$, la différentielle $Df(a)$ est l'application linéaire définie, dans les bases canoniques de $\mathbb{R}^n$ et $\mathbb{R}^p$, par la matrice jacobienne $\left(\frac{\partial f_i}{\partial x_j}\right)_{1 \leqslant i,j \leqslant n}$. Si $n = p$, le jacobien, noté $J(f)$, est le déterminant de la matrice jacobienne.

Théorème 28. *Soient $\varphi : U \to \mathbb{R}^n$ un $\mathcal{C}^1$-difféomorphisme, $V = \varphi(U)$ et $f : V \to \mathbb{R}$ une fonction continue. Alors :*

$$\int_V f(u)\, du = \int_V f(\varphi(u))\, |J(\varphi)(u)|\, du$$

Application 29 (Intégrale de Gauss)**.** $\displaystyle\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$

II Inversion locale et fonctions implicites

1) Théorème d'inversion locale

Théorème 30 (Théorème d'inversion locale)**.** *Soient U un ouvert de $\mathbb{R}^n$, $a \in U$ et $f : U \to \mathbb{R}^n$ de classe $\mathcal{C}^k$. On suppose que la matrice jacobienne $Df(a)$ est inversible. Il existe alors un ouvert $V \subset U$ contenant a tels que $f|_V$ soit un difféomorphisme de classe $\mathcal{C}^k$ de V sur $f(V)$.*

Application 31. *Soient $k \in \mathbb{N}^\star$ et $A \in \mathcal{M}_n(\mathbb{K})$. Si A est suffisamment proche de I_n, alors il existe $B \in \mathcal{M}_n(\mathbb{K})$ tel que $A = B^k$.*

Théorème 32 (Théorème d'inversion globale)**.** *Soient U un ouvert de $\mathbb{R}^n$ et $f : U \to \mathbb{R}^n$ de classe $\mathcal{C}^1$. On suppose que f est injective sur U et que, pour tout $x \in U$, la matrice jacobienne $Df(x)$ est inversible. Alors $f(U)$ est un ouvert de $\mathbb{R}^n$, et f est un $\mathcal{C}^1$-difféomorphisme de U sur $f(U)$.*

Contre-exemple 33. *La fonction* $f : \left| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (x,y) & \longmapsto & (x^2 - y^2, 2xy) \end{array} \right.$ *est un difféomorphisme local au voisinage de tout point de $\mathbb{R}^2 \setminus \{(0,0)\}$, mais n'est pas un difféomorphisme global.*

2) Théorème des fonctions implicites

Théorème 34 (Théorème des fonctions implicites)**.** *Soient U un ouvert de $\mathbb{R}^n \times \mathbb{R}^p$, (a,b) un point de U, et $f : U \to \mathbb{R}^p$ une application de classe $\mathcal{C}^1$. On suppose que $f(a,b) = 0$ et que la matrice jacobienne $D_y f(a,b)$, formée des dérivées partielles par rapport à y, est inversible. Alors l'équation $f(x,y) = 0$ peut être résolue localement par rapport aux variables y : il existe un voisinage ouvert V de a dans $\mathbb{R}^n$, un voisinage ouvert W de b dans $\mathbb{R}^p$, avec $V \times W \subset U$, et une application $\varphi : V \to W$, de classe $\mathcal{C}^1$, unique, telle que :*

$$(x \in V,\, y \in W \text{ et } f(x,y) = 0) \Leftrightarrow (x \in V \text{ et } y = \varphi(x))$$

Exemple 35. *L'équation $x^2 + y^2 - 1 = 0$ définit deux fonctions implicites :*

$$\varphi_1 : \left| \begin{array}{ccc}]-1,1[& \longrightarrow &]0,+\infty[\\ x & \longmapsto & \sqrt{1-x^2} \end{array} \right. \quad et \quad \varphi_2 : \left| \begin{array}{ccc}]-1,1[& \longrightarrow &]-\infty,0[\\ x & \longmapsto & -\sqrt{1-x^2} \end{array} \right.$$

III Différentielles d'ordres supérieurs

1) Différentielle seconde

Définition 36. Soit $f : U \to \mathbb{R}$ différentiable en tout point de U un ouvert de $\mathbb{R}^n$. Alors si $x = (x_1, \dots, x_n) \mapsto Df(x) = \left(\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right)$ est différentiable en un point $a \in U$, on dit que f est deux fois différentiable

en a, et on note $D^2f(a)$ la matrice hessienne de f en a définie par :

$$D^2f(a) = D(Df)(a) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_1^2} & \cdots & \frac{\partial^2 f}{\partial x_n \partial x_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 f}{\partial x_1 \partial x_n} & \cdots & \frac{\partial^2 f}{\partial x_n^2} \end{pmatrix}$$

Théorème 37 (Schwarz)**.** *Soit $f : U \to \mathbb{R}^n$ une application supposée de classe $\mathcal{C}^2$ sur U, alors :*

$$\forall\, i,j \in [\![1,n]\!],\ \frac{\partial^2 f}{\partial x_i \partial x_j}(a) = \frac{\partial^2 f}{\partial x_j \partial x_i}(a)$$

Exemple 38. *La fonction $f : \mathbb{R}^2 \to \mathbb{R}$ définie par $f(x,y) = \frac{xy(x^2-y^2)}{x^2+y^1}$ si $(x,y) \neq (0,0)$ et $f(0,0) = 0$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}^2$ et admet des dérivées $\frac{\partial^2 f}{\partial x_1 \partial x_2}(a)$ et $\frac{\partial^2 f}{\partial x_2 \partial x_1}(a)$ en tout point mais distinctes à l'origine.*

2) Formule de Taylor

Définition 39. On définit la différentielle d'ordre k par récurrence : si f est k fois différentiable en $a \in U$, sa différentielle k-ième sera une application k-linéaire symétrique. On note $D^k f(a)$ la k-ième différentielle, f est dite de classe $\mathcal{C}^k$ sur U si ses dérivées partielles sont de classe $\mathcal{C}^{k-1}$ sur U.

Théorème 40 (Reste intégral)**.** *Soit $f : U \to F$ une fonction de classe $\mathcal{C}^{k+1}$. Si, pour $a \in U$, le segment $[a, a+h]$ est contenu dans U, alors :*

$$f(a+h) = f(a) + \sum_{i=1}^{k} \frac{1}{i!} D^i f(a) \cdot (h)^i + \int_0^1 \frac{(1-t)^k}{k!} D^{k+1} f(a+th)(h)^{k+1} dt$$

Lemme 41. *Soit $A_0 \in \mathcal{GL}_n(\mathbb{R}) \cap \mathcal{S}_n(\mathbb{R})$. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et $\rho : V, \mathcal{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que pour tout $A \in V$, on a ${}^t\rho(A) A_0 \rho(A)$.*

Théorème 42 (Lemme de Morse)**.** *Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ définie sur un ouvert U de $\mathbb{R}^n$ contenant 0. On suppose que $df(0) = 0$ et que $d^2f(0)$ est non dégénérée et de signature $(p, n-p)$. Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = \sum_{i=1}^{p} \varphi_i(x)^2 - \sum_{i=p+1}^{n} \varphi_i(x)^2$ au voisinage de 0.*

3) Problèmes d'extrema

Théorème 43. *Soient $f : U \to \mathbb{R}$ et $a \in U$.*

(i) Si a est un extremum local de f et si $Df(a)$ existe, alors $Df(a) = 0$.

(ii) Si a est un minimum local de f et si $D^2f(a)$ existe, alors $Df(a) = 0$ et $D^2f(a)$ est une forme quadratique positive.

(iii) Si $Df(a) = 0$ et $D^2f(a)$ est définie positive, alors f admet en a un minimum local strict.

IV Extrema liés

Définition 44. Soit M une sous-variété de $\mathbb{R}^n$. On dit qu'une fonction $f : \mathbb{R}^n \to \mathbb{R}$ a un extremum lié (ou relatif) en $a \in M$ s'il existe un voisinage U de a dans $\mathbb{R}^n$ tel que $f(a)$ est un extremum de f sur $M \cap U$.

Théorème 45 (Extrema liés)**.** *Soit U un ouvert de $\mathbb{R}^n$. Soient $g_1, \dots, g_k$ des fonctions de classe $\mathcal{C}^1$ de U dans $\mathbb{R}$ telles que les formes linéaires $d_x g_1, \dots, d_x g_k$ sont linéairement indépendantes pour tout $x \in U$. Posons :*

$$M = \{x \in U \,|\, \forall\, i \in [\![1,k]\!],\ g_i(x) = 0\}$$

Alors, si f a un extremum lié en $a \in M$, il existe $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ tels que :

$$d_a f = \sum_{i=1}^{k} \lambda_k\, d_a g_i$$

Ces réels $\lambda_1, \dots, \lambda_k$ sont appelés multiplicateurs de Lagrange.

Développements

- Lemme de Morse (41,42) [Rou15]
- Extrema liés (45) [Ave83]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini
[Ave83] A. Avez. *Calcul différentiel.* Masson

Annexes

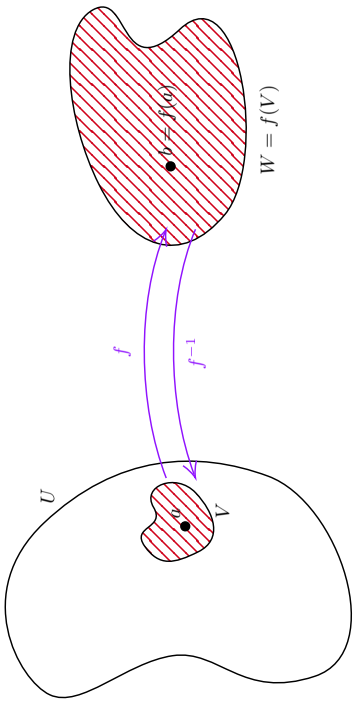


FIGURE 1 – Théorème d'inversion locale

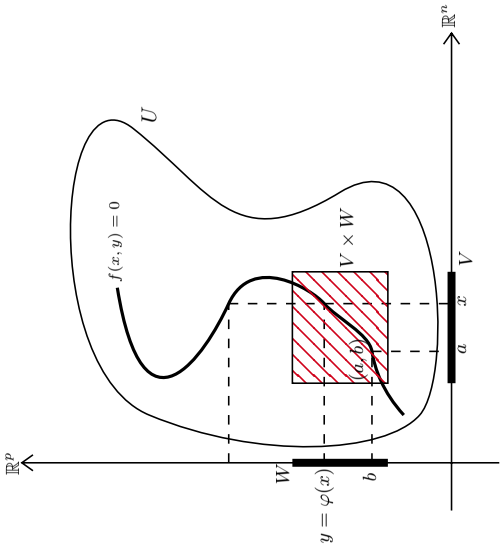


FIGURE 2 – Théorème des fonctions implicites

Cadre : Soient $(E, \|.\|)$ un $\mathbb{R}$-espace vectoriel normé et $J : E \to \mathbb{R}$.

I Existence et unicité d'extrema

Définition 1. On dit que J admet un minimum (resp. maximum) local en $x_0 \in E$ s'il existe un voisinage V de x_0 tel que $\forall x \in V, J(x) \geqslant J(x_0)$ (resp. $\forall x \in V, J(x) \leqslant J(x_0)$). On dit que J admet un minimum (resp. maximum) global en $x_0 \in E$ si $\forall x \in E, J(x) \geqslant J(x_0)$ (resp. $\forall x \in E, J(x) \geqslant J(x_0)$). Un extremum de J est un maximum ou un minimum de J.

1) Compacité et fermeture

Proposition 2. *Si K est un compact de E, et si J est continue, alors J est bornée sur K et atteint ses bornes.*

Application 3. *Si K et K' sont deux compacts de E, il existe $(x, x') \in K \times K'$ tel que $(x, x') = d(K, K')$.*

Définition 4. On dit que J est coercive si $\lim_{\|x\| \to \infty} J(x) = +\infty$.

Théorème 5. *Si $E = \mathbb{R}^n$, et si J est coercive et continue, alors J admet un minimum global.*

Contre-exemple 6. *Sur l'espace de Hilbert $\ell^2(\mathbb{N})$, la fonctionnelle $J(x) = (\|x\|^2 - 1) + \sum_{i=1}^{\infty} \frac{x_i^2}{i}$ est coercive mais n'admet pas de minimum.*

2) Convexité

Définition 7. Soit C un convexe non vide de E. On dit que $J : C \to \mathbb{R}$ est convexe si, pour tous $a, b \in C$ et tout $\lambda \in [0, 1]$, on a :

$$J((1-\lambda)a + \lambda b) \leqslant (1-\lambda)J(a) + \lambda J(b)$$

On dit que J concave si $-J$ est convexe. Lorsque l'inégalité est stricte pour $a \neq b$ et $0 < \lambda < 1$, J est strictement convexe. Pour $\alpha > 0$, on dit que J est α-convexe si pour tous $a, b \in C$ distincts et tout $\lambda \in]0, 1[$, on a :

$$J((1-\lambda)a + \lambda b) \leqslant (1-\lambda)J(a) + \lambda J(b) - \frac{\alpha}{2} \|a - b\|^2 \lambda(1-\lambda)$$

Théorème 8. *On considère $J : C \to \mathbb{R}$.*

(i) Si J est convexe, tout minimum local est global.

(ii) Si J est strictement convexe, J admet au plus un minimum global.

(iii) Si J est α-convexe, J admet un unique minimum global.

3) Cas des espaces de Hilbert

Soit $(H, \langle ., . \rangle)$ un espace de Hilbert. Soit $K \subset E$ convexe fermé non vide.

Théorème 9. *Pour tout $f \in H$, il existe un unique élément de K, noté $P_K(f)$, et appelé projection de f sur K, tel que :*

$$\|P_K(f) - f\| = \inf_{v \in K} \|v - f\|$$

De plus, $P_K(f)$ est caractérisée par :

$$\forall v \in K,\ \mathrm{Re}\left(\langle f - P_K(f), v - P_K(f) \rangle\right) \leqslant 0$$

Corollaire 10. *Soient M un sous-espace vectoriel fermé de H et $f \in H$. Alors $P_M(f)$ est caractérisé par :*

$$P_M(f) \in M \qquad et \qquad \forall\, v \in M,\ \mathrm{Re}\left(\langle f - P_M(f), v \rangle\right) = 0$$

De plus, P_M est un opérateur linéaire.

Théorème 11 (Riesz-Fréchet)**.** *Soit $\varphi \in H'$. Alors :*

$$\exists!\, f \in H,\ \forall\, v \in H,\ \langle \varphi, v \rangle = \langle f, v \rangle$$

Théorème 12 (Lax-Milgram)**.** *Soient H un espace de Hilbert, a une forme bilinéaire continue et coercive sur H, et $\ell \in H'$. Alors il existe un unique $u \in H$ tel que, pour tout $v \in H$, $a(u, v) = \ell(v)$. Si de plus a est symétrique, u réalise le minimum sur H de $v \mapsto \frac{1}{2} a(v, v) - \ell(v)$.*

Application 13 (Dirichlet)**.** *Pour $f \in L^2$, on considère le problème :*

$$\begin{cases} -u'' + u = f & sur\ ]0, 1[\\ u(0) = u(1) = 0 \end{cases}$$

Il existe une unique solution faible $u \in H_0^1([0, 1])$ à ce problème.

4) Holomorphie

On considère $E = \mathbb{C}$, $\Omega \subset \mathbb{C}$ un ouvert connexe non vide et $J \in \mathcal{H}(\Omega)$.

Théorème 14. *Soient $z_0 \in \Omega$ et $r > 0$ tels que $B(z_0, r) \subset \Omega$. Alors $J(z_0) = \frac{1}{2\pi} \int_0^{2\pi} J(z_0 + re^{i\theta})\, d\theta$.*

Théorème 15 (Principe du maximum)**.** *Si $|J|$ atteint son maximum en un point de Ω, alors J est constante.*

Application 16 (D'Alembert-Gauss)**.** *Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine dans $\mathbb{C}$.*

II Caractérisation des extrema

1) Différentiabilité et points critiques

Soit U un ouvert de $\mathbb{R}^n$. On considère $J : U \to \mathbb{R}$.

Ordre 1

Définition 17. Soit $x_0 \in U$. On dit que x_0 est un point critique pour J si J est différentiable en x_0 et $dJ(x_0) = 0$.

Proposition 18. *Si x_0 est un extremum local de J, et si J est différentiable en x_0, alors x_0 est un point critique.*

Remarque 19. *Cette condition est nécessaire, mais pas suffisante : $x \mapsto x^3$ n'admet pas d'extremum en 0.*

Théorème 20 (Rolle)**.** *Soit $J : [a, b] \to \mathbb{R}$ continue et dérivable sur $]a, b[$. Si $J(a) = J(b)$, alors il existe $c \in]a, b[$ tel que $J'(c) = 0$.*

Corollaire 21 (Accroissements finis)**.** *Soit $J : [a, b] \to \mathbb{R}$ continue et dérivable sur $]a, b[$. Alors il existe $c \in]a, b[$ tel que $J'(c)(b-a) = J(b)-J(a)$.*

Ordre 2

Proposition 22. *Soit $x_0 \in U$ un point critique de J. On suppose J de classe $\mathcal{C}^2$ en x_0. Alors :*

(i) Si x_0 est un minimum (resp. maximum) local, alors $d^2J(x_0)$ est positive (resp. négative).

(ii) Si $d^2J(x_0)$ est définie positive (resp. définie négative), alors x_0 est un minimum (resp. maximum) local.

Remarque 23. *Encore une fois, ces conditions laissent un cas douteux : $x \mapsto x^3$ n'admet pas d'extremum en 0.*

Exemple 24. *Dans le cas où $n = 2$, on pose $A = \left(\begin{smallmatrix} r & s \\ s & t \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R})$ la hessienne de J en x_0. Par le théorème précédent, on a :*

(i) Si $rt - s^2 > 0$ et $r > 0$, J admet un minimum relatif en x_0.

(ii) Si $rt - s^2 > 0$ et $r < 0$, J admet un maximum relatif en x_0.

(iii) Si $rt - s^2 < 0$, J n'a pas d'extremum en x_0.

(iv) Si $rt - s^2 = 0$: cas douteux.

Exemple 25. *Si $J(x, y) = x^4 + y^4 - 2(x - y)^2$, alors J a trois points critiques : $(0, 0)$ et $\pm(\sqrt{2}, -\sqrt{2})$. Il y a un minimum local en $\pm(\sqrt{2}, -\sqrt{2})$, mais on ne peut pas conclure en $(0, 0)$.*

2) Fonctions convexes

Théorème 26. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*

(i) J est convexe sur C.

(ii) $\forall\, x, y \in C,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geqslant 0$.

(iii) $\forall\, x, y \in C,\ J(x) \geqslant J(y) + \langle \nabla J(y), x - y\rangle$.

Si J est deux fois différentiable, on a aussi : $\left\langle d^2J(x) \cdot y, y\right\rangle \geqslant 0$.

Théorème 27. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*

(i) J est α-convexe sur C.

(ii) $\forall\, x, y \in C,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geqslant \alpha \|x - y\|^2$.

(iii) $\forall\, x, y \in C,\ J(x) \geqslant J(y) + \langle \nabla J(y), x - y\rangle + \frac{\alpha}{2} \|x - y\|^2$.

Si J est deux fois différentiable, on a aussi : $\left\langle d^2J(x) \cdot y, y\right\rangle \geqslant \alpha \|y\|^2$.

Exemple 28. *Si A est une matrice symétrique définie positive, alors la fonctionnelle quadratique $J : X \mapsto \langle AX, X\rangle - \langle B, X\rangle$ est λ_1-convexe, où λ_1 est la plus petite valeur propre de A.*

Théorème 29. *Si $J : C \to \mathbb{R}$ est différentiable en $u \in C$ et admet un minimum local en u, alors $\langle \nabla J(u), v - u\rangle \geqslant 0$ pour tout $v \in C$.*

Corollaire 30. *Soit $J : C \to \mathbb{R}$ est convexe et différentiable en $u \in C$. Alors u est un extremum local si, et seulement si, $\nabla J(u) = 0$.*

3) Optimisation sous contraintes

Définition 31. Soit M une sous-variété de $\mathbb{R}^n$. On dit qu'une fonction $f : \mathbb{R}^n \to \mathbb{R}$ a un extremum lié (ou relatif) en $a \in M$ s'il existe un voisinage U de a dans $\mathbb{R}^n$ tel que $f(a)$ est un extremum de f sur $M \cap U$.

Théorème 32 (Extrema liés)**.** *Soit U un ouvert de $\mathbb{R}^n$. Soient $g_1, \dots, g_k$ des fonctions de classe $\mathcal{C}^1$ de U dans $\mathbb{R}$ telles que les formes linéaires $d_xg_1, \dots, d_xg_k$ sont linéairement indépendantes pour tout $x \in U$. Posons :*

$$M = \{x \in U \,|\, \forall\, i \in [\![1, k]\!],\ g_i(x) = 0\}$$

Alors, si f a un extremum lié en $a \in M$, il existe $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ tels que :

$$d_af = \sum_{i=1}^{k} \lambda_k\, d_ag_i$$

Ces réels $\lambda_1, \dots, \lambda_k$ sont appelés multiplicateurs de Lagrange.

Application 33. *Tout endomorphisme symétrique de E admet une valeur propre réelle.*

III Optimisation numérique

1) Méthode de Newton

La méthode de Newton consiste à approcher une solution d'une équation $f(x) = 0$ en partant d'une approximation plus grossière. L'idée est de remplacer la courbe de f par sa tangente.

Théorème 34 (Méthode de Newton)**.** *Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f : [a,b] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ telle que $f(a) < 0 < f(b)$ et $f' > 0$ sur $[a,b]$. On considère la suite $(x_n)_{n\in\mathbb{N}}$ définie par :*

$$x_0 \in [a,b] \quad et \quad \forall\, n \in \mathbb{N},\ x_{n+1} = \phi(x_n) = x_n - \frac{f(x_n)}{f'(x_n)}$$

La fonction f admet un unique zéro $\alpha \in]a,b[$, et on a :

(i) Il existe $\varepsilon > 0$ tel que, pour $x_0 \in I =]\alpha - \varepsilon, \alpha + \varepsilon[$, la suite $(x_n)_{n\in\mathbb{N}}$ converge quadratiquement vers α, et il existe $C > 0$ tel que :

$$\forall\, n \in \mathbb{N},\ |x_{n+1} - \alpha| \leqslant C|x_n - \alpha|^2$$

(ii) Si de plus $f'' > 0$ sur $[\alpha, b]$, alors, pour $x \in]\alpha, b]$, la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante, et pour tout $n \in \mathbb{N}$ on a :

$$0 \leqslant x_{n+1} - \alpha \leqslant C(x_n - \alpha)^2 \quad et \quad x_{n+1} - \alpha \sim \frac{f''(\alpha)}{2f'(\alpha)}(x_n - \alpha)^2$$

2) Méthodes de gradient

Soit $J : \mathbb{R}^n \to \mathbb{R}$. On suppose J différentiable. On cherche, s'il existe, un élément $u \in \mathbb{R}^n$ tel que :

$$J(u) = \inf_{v\in\mathbb{R}^n} J(v)$$

Pour cela, on utilise les méthodes de gradient. On considère la suite :

$$u_0 \in \mathbb{R}^n \quad \text{et} \quad \forall\, k \in \mathbb{N},\ u^{k+1} = u^k - \rho^k \nabla J(u^k)$$

Il existe plusieurs possibilités pour choisir les ρ^k, par exemple :

(i) Gradient à pas fixe : $\rho^k = \rho$ une constante positive fixée.

(ii) Gradient à pas optimal : ρ^k minimise $\rho \mapsto J\left(u^k - \rho \nabla J(u^k)\right)$.

Théorème 35. *Si J est α-convexe et différentiable, et que ∇J est L-lipschitzienne, alors la méthode de gradient à pas optimal converge vers l'unique minimum de J.*

Application 36. *Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. On considère la fonctionnelle quadratique $J : \mathbb{R}^n \to \mathbb{R}$ définie par :*

$$J(X) = \langle AX, X\rangle - \langle b, X\rangle + c$$

Cette fonctionnelle satisfait les conditions du théorème précédent. De plus, son minimum est atteint en $X_0 \in \mathbb{R}^n$ qui vérifie $\nabla J(X_0) = AX - b = 0$. On a donc une méthode itérative pour approcher la solution de $AX = b$.

Développements

- Projection sur un convexe fermé et théorème de Riesz (9,10,11) [Bre87]
- Extrema liés (32) [Ave83]
- Méthode de Newton (34) [Rou15]
- Algorithme de gradient à pas optimal (35) [Cia88]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[Bre87] H. Brezis. *Analyse fonctionelle.* Masson
[Ave83] A. Avez. *Calcul différentiel.* Masson
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini
[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

Annexes

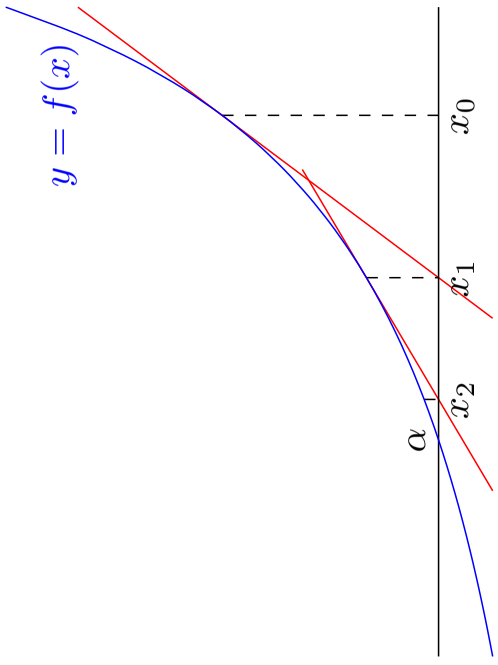


FIGURE 1 – Méthode de Newton

Cadre : E est un espace vectoriel normé de dimension finie et de norme $\|.\|$, Ω est un ouvert de $\mathbb{R}\times E^k$ pour $k\in\mathbb{N}^\star$, et $f:\Omega\to E$ une application.

I Étude générale des équations différentielles

1) Définitions. Solutions maximales et globales.

On considère l'équation différentielle d'ordre k :

$$\forall\, t\in\mathbb{R},\ \forall\, y\in E,\ y^{(k)}=f(t,y,y',\dots,y^{(k-1)}) \tag{E}$$

Définition 1. Une solution de (E) est un couple (I,y), où I est un intervalle de $\mathbb{R}$ et $y:I\to E$ une fonction k fois dérivable telle que :

$$\forall\, t\in I,\ y^{(k)}(t)=f(t,y(t),y'(t),\dots,y^{(k-1)}(t))$$

Remarque 2. *On peut toujours se ramener à une équation d'ordre 1 en posant $Y=(y,\dots,y^{(k-1)})$. On a alors $Y'(t)=F(t,Y(t))$ où $F(t,y)=(y',\dots,y^{(k-1)},f(t,y,y',\dots,y^{(k-1)}))$. Dans la suite, on ne considérera que des équations d'ordre 1.*

Exemple 3. *Si $f(t,y)=y$, alors $(\mathbb{R},\exp)$ est solution de (E).*

Définition 4. (E) est dite autonome si f ne dépend pas de t.

Définition 5. Étant donné un point $(t_0,y_0)\in\Omega$, le problème de Cauchy consiste à trouver une solution $y:I\to E$ de (E) sur un intervalle I contenant t_0 dans son intérieur et telle que $y(t_0)=y_0$.

Définition 6. (i) Soient (I_1,y_1) et (I_2,y_2) deux solutions de (E). On dit que (I_1,y_1) prolonge (I_2,y_2) si $I_2\subset I_1$ et $y_1|_{I_2}=y_2$.

(ii) Une solution est maximale si elle n'a aucun prolongement.

Exemple 7. *On considère le problème de Cauchy $y'=y^2$ de données $(0,y_0)$ avec $y_0>0$. Alors $\left]-\infty,\frac{1}{y_0}\right[,t\mapsto\frac{y_0}{1-y_0t}\Big)$ est solution maximale.*

Définition 8. Si $\Omega=I\times O$, avec I un intervalle de $\mathbb{R}$ et O un ouvert de E, on appelle solution globale une solution de la forme (I,y).

Remarque 9. *(i) Toute solution globale est maximale.*

(ii) Si (E) est autonome, alors une solution globale est définie sur $\mathbb{R}$.

2) Résultats d'existence et d'unicité

Lemme 10 (Grönwall). *Soient $f,g:I\to\mathbb{R}$ continues, avec g positive. Soient $t_0,a\in\mathbb{R}$ tels que $f(t)\leqslant a+\int_{t_0}^t f(s)g(s)ds$, alors :*

$$\forall\, t\geqslant t_0,\ f(t)\leqslant a\exp\left(\int_{t_0}^t g(s)ds\right)$$

Théorème 11 (Cauchy-Lipschitz global). *Soient I un intervalle de $\mathbb{R}$ et $f:I\times E\to E$ une application continue et globalement lipschitzienne en sa seconde variable, donc telle que pour tout intervalle $K\subset I$ on a :*

$$\exists\, k>0,\ \forall\, t\in K,\ \forall\, y,z\in E,\ \|f(t,y)-f(t,z)\|\leqslant k\,\|y-z\|$$

Alors tout problème de Cauchy admet une unique solution globale.

Théorème 12 (Cauchy-Lipschitz local). *Si f est continue et localement lipschitzienne en sa seconde variable, tout problème de Cauchy admet une unique solution maximale.*

Proposition 13. *Toute fonction $\mathcal{C}^1$ est localement lipschitzienne.*

Théorème 14 (Peano-Arzela). *Si f est continue, pour tout point $(t_0,y_0)\in\Omega$ il existe une solution maximale (I,y) telle que $y(t_0)=y_0$.*

Contre-exemple 15. *Si $f(t,y)=3|y|^{\frac{2}{3}}$, f n'est pas localement lipschitzienne en 0. Le problème de Cauchy de données $(0,0)$ admet au moins deux solutions maximales : 0 et $(t\mapsto t^3)$.*

Proposition 16. *Si (E) est autonome, et si (I,y) est solution, alors, pour tout $\tau\in\mathbb{R}$, la translatée $(I+\tau,x\mapsto y(x-\tau))$ est encore solution.*

3) Propriétés des solutions

Proposition 17. *Si f est de classe $\mathcal{C}^p$, les solutions d'une équation différentielle d'ordre k sont de classe $\mathcal{C}^{k+p}$.*

Théorème 18 (Théorème de sortie de tout compact). *Sous les hypothèses du théorème de Cauchy-Lipschitz, soit (I,y) une solution maximale de (E). Alors, pour tout compact K de Ω, il existe $T^\star$ (resp. $T_\star$) tel que, pour tout $t\in I$ avec $t>T^\star$ (reps. $t<T_\star$), on a $(t,y(t))\notin K$.*

Exemple 19. *On considère le problème de Cauchy $y'=y^2$ de données $(0,y_0)$ avec $y_0>0$, et on note $\left]-\infty,\frac{1}{y_0}\right[,y_1:t\mapsto\frac{y_0}{1-y_0t}\Big)$ une solution maximale. On a $\lim_{t\to y_0^-}y_1(t)=-\infty$ et $\lim_{t\to-\infty}t=-\infty$.*

Théorème 20 (Théorème des bouts)**.** *Sous les hypothèses du théorème de Cauchy-Lipschitz, soit (I, y) une solution maximale de (E). On suppose que $\Omega = J \times E$, avec J un intervalle de $\mathbb{R}$. Si $\sup I < \sup J$, alors $\lim_{t\to\sup I} \|y(t)\| = +\infty$.*

II Étude des équations autonomes

On se place sous les hypothèses du théorème de Cauchy-Lipschitz, et on suppose (E) autonome. f est une fonction d'un ouvert Ω de $\mathbb{R}^n$ dans $\mathbb{R}^n$.

1) Définitions

Définition 21. Un point y_0 de E est un point d'équilibre si $f(y_0) = 0$.

Remarque 22. *Si y_0 est un point d'équilibre, le problème de Cauchy $y' = f(y)$ de données (t_0, y_0) admet pour solution maximale la fonction constante égale à y_0.*

Définition 23. Soit y_0 un point d'équilibre.

(i) y_0 est dit stable si, pour tout $\varepsilon > 0$, il existe $\delta > 0$ tel que, si (I, y) est une solution de (E) qui vérifie $|y(t_0) - y_0| < \delta$, alors $[t_0, +\infty[\subset I$ et $|y(t) - y_0| < \varepsilon$ pour tout $t \geqslant t_0$.

(ii) y_0 est dit instable s'il n'est pas stable.

(iii) y_0 est dit asymptotiquement stable s'il existe $\delta > 0$ tel que, si (I, y) est une solution de (E) qui vérifie $|y(t_0) - y_0| < \delta$, alors $[t_0, +\infty[\subset I$ et $\lim_{t\to+\infty} y(t) = y_0$.

Ces définitions sont illustrées par la Figure 1.

Définition 24. Soit $x \in \Omega$. On appelle orbite de x l'image commune des solutions maximales passant par x.

Proposition 25. *Soit $x \in \Omega$. Toutes les solutions qui passent par x sont translatées les unes des autres.*

Proposition 26. *L'ensemble des orbites forme une partition de Ω.*

Définition 27. On appelle portrait de phase cette partition.

Proposition 28. *Soit (I, y) une solution maximale telle qu'il existe $t_1 < t_2$ tels que $y(t_1) = y(t_2)$. Alors $I = \mathbb{R}$ et y est périodique.*

2) Cas linéaire

On considère l'équation différentielle $Y' = AY$, où $A \in \mathcal{M}_n(\mathbb{R})$.

Théorème 29. *Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres de A. Alors les solutions du système linéaire $Y' = AY$ sont :*

(i) asymptotiquement stables si, et seulement si, $\mathrm{Re}(\lambda_j) < 0$ pour tout $j \in [\![1, n]\!]$.

(ii) stables si, et seulement si, pour tout $j \in [\![1, n]\!]$, ou bien $\mathrm{Re}(\lambda_j) < 0$, ou bien $\mathrm{Re}(\lambda_j) = 0$ et le bloc correspondant est diagonalisable.

Théorème 30. *Dans le cas $n = 2$, on peut classifier les différents types de portraits de phase possibles en fonction de $\det A$ et de $\mathrm{tr}\, A$. Cette classification est illustrée par la Figure 3.*

III Exemples d'études

1) Utilisation des séries entières

Si l'équation est à coefficients polynômiaux, on peut chercher les solutions développables en séries entières autour de 0. Si cette solution est maximale, elle est unique par le théorème de Cauchy-Lipschitz.

Exemple 31. *Le problème de Cauchy $y' = y$ de données $(0, 1)$ admet pour solution $t \mapsto \sum_{n\in\mathbb{N}} \frac{t^n}{n!} = e^t$.*

Exemple 32 (Bessel)**.** *On considère l'équation différentielle de Bessel $xy'' + y' + xy = 0$. Sa solution f_0 valant 1 en 0 se développe en série entière sur $\mathbb{R}$. De plus, si f est une autre solution sur un intervalle $]0, a[$, alors (f, f_0) est libre si, et seulement si, f n'est pas bornée au voisinage de 0.*

2) Système de Lotka-Volterra

Exemple 33. *Soient $a, b, c, d, x_0, y_0 \in \mathbb{R}^{+\star}$. On considère le système :*

$$\begin{cases} x' = x(a - by) \\ y' = y(-c + dx) \\ x(0) = x_0, y(0) = y_0 \end{cases}$$

Il s'agit d'un système classique modélisant une interaction proie-prédateur. Il admet une unique solution maximale globale, qui est périodique, et admet deux points d'équilibre : un point-selle en $(0, 0)$ et un centre en $\left(\frac{c}{d}, \frac{a}{b}\right)$. Son portrait de phase est illustré par la Figure 2.

3) Équation de Hill-Mathieu

Théorème 34 (Hill-Mathieu)**.** *On considère l'équation $y'' + qy = 0$, où $q : \mathbb{R} \to \mathbb{R}$ est continue, paire et π-périodique. On note W l'espace des solutions, et $A : W \to W$ défini par $Ay(x) = y(x + \pi)$.*

(i) Si $|\operatorname{tr}(A)| < 2$, alors toutes les solutions sont bornées.

(ii) Si $|\operatorname{tr}(A)| = 2$, alors il existe une solution non nulle bornée.

(iii) On a $|\operatorname{tr}(A)| < 2$ si, et seulement si, $y_1'(\pi)y_2(\pi) = 0$.

(iv) Si $|\operatorname{tr}(A)| > 2$, alors aucune solution non triviale n'est bornée.

Application 35. *Les solutions de $y'' + y = 0$ sont toutes bornées, alors que les solutions non triviales de $y'' - y = 0$ sont toutes non bornées.*

Développements

— Équation de Bessel (32) [FGN13e]
— Équation de Hill-Mathieu (34) [ZQ13]

Références

[Dem06] J.-P. Demailly. *Analyse numérique et équations différentielles.* EDP Sciences
[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod
[FGN13e] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 4.* Cassini

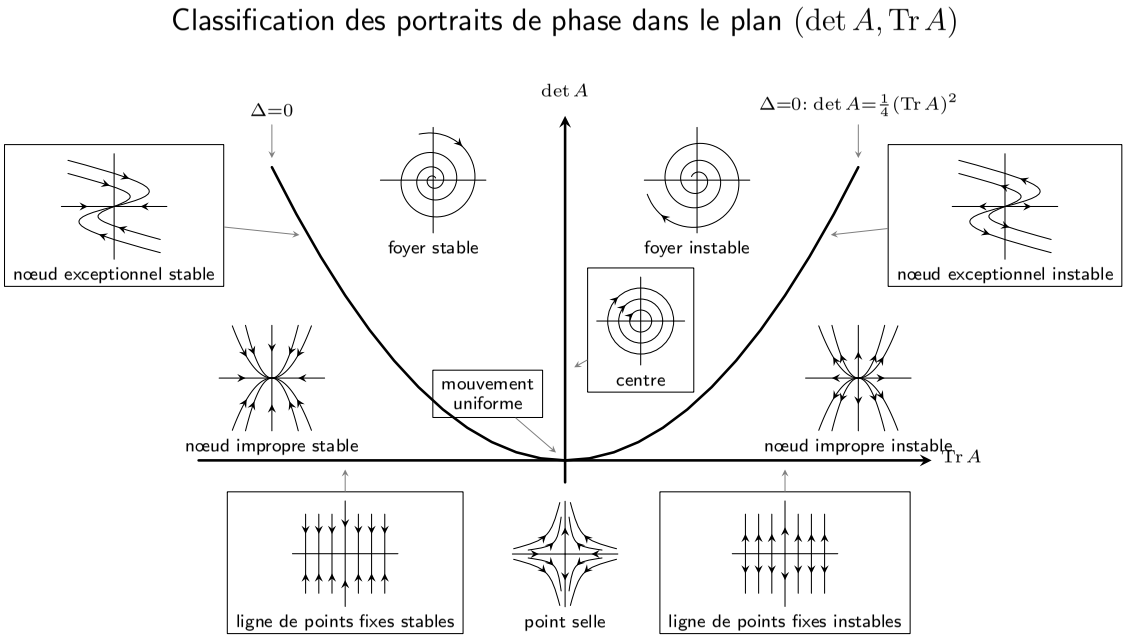


FIGURE 3 – Portraits de phase

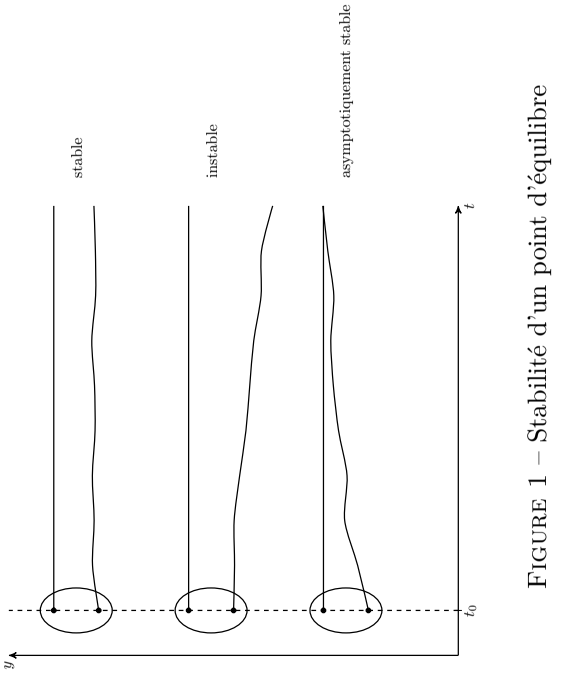


FIGURE 1 – Stabilité d'un point d'équilibre

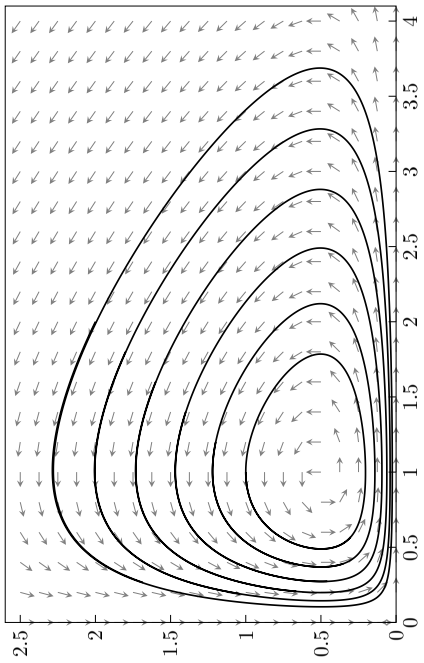


FIGURE 2 – Lotka Volterra

Annexes

Cadre : On fixe $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $I \subseteq \mathbb{R}$ un intervalle.

I Définitions, existence, structure

1) Définitions

Définition 1. Soient $p, n \in \mathbb{N}^\star$. Une équation différentielle linéaire d'ordre p sur $\mathbb{K}^n$ est une équation de la forme :

$$y^{(p)}(t) = \sum_{k=0}^{p-1} A_k(t) y^{(i)}(t) + B(t) \quad \text{où} \quad \left\{ \begin{array}{l} \forall\, i,\ A_i \in \mathcal{C}^0\left(I, \mathcal{M}_n(\mathbb{K})\right) \\ B \in \mathcal{C}^0\left(I, \mathbb{K}^n\right) \end{array} \right. \tag{E}$$

On appelle équation différentielle linéaire homogène associée :

$$y^{(p)}(t) = \sum_{k=0}^{p-1} A_k(t) y^{(i)}(t) \tag{EH}$$

Si $n = 1$, l'équation est dite scalaire. Sinon, on parle de système d'équations différentielles linéaires.

Exemple 2. $\begin{pmatrix} x \\ y \end{pmatrix}' = \begin{pmatrix} -t & -1 \\ 1 & -t \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ *est un système homogène linéaire.*

Remarque 3. *Ce sont bien les coefficients en Y qui doivent être linéaires. L'équation $y' = t^2 y$ est bien linéaire.*

Remarque 4. *On peut ramener toute équation différentielle d'ordre p sur $\mathbb{K}^n$ à un système différentiel d'ordre 1 sur $\mathbb{K}^{np}$ par :*

$$\begin{pmatrix} y \\ y' \\ \vdots \\ y^{p-1} \end{pmatrix}' = \begin{pmatrix} 0 & I_n & & 0 \\ \vdots & \ddots & \ddots & \\ 0 & \cdots & 0 & I_n \\ A_0(t) & \cdots & \cdots & A_{p-1}(t) \end{pmatrix} \begin{pmatrix} y \\ y' \\ \vdots \\ y^{p-1} \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ B(t) \end{pmatrix}$$

On limitera donc l'étude aux équations différentielles d'ordre 1 :

$$y'(t) = A(t)y(t) + B(t) \quad \text{où} \quad \left\{ \begin{array}{l} A \in \mathcal{C}^0\left(I, \mathcal{M}_n(\mathbb{K})\right) \\ B \in \mathcal{C}^0\left(I, \mathbb{K}^n\right) \end{array} \right.$$

2) Existence et unicité des solutions

Définition 5. Une solution de (E) est un couple (J, φ), où $J \subseteq I$ et y vérifie l'équation (E) sur J. Une solution (J, φ) est maximale s'il n'existe pas de prolongement Φ de φ défini sur $J' \supsetneq J$ tel que (J', Φ) soit solution.

Définition 6. Étant donné un point $(t_0, y_0) \in I \times \mathbb{K}^n$, le problème de Cauchy consiste à trouver une solution (J, y) de (E) sur un intervalle J contenant t_0 dans son intérieur et telle que $y(t_0) = y_0$.

Exemple 7 (Chute libre)**.** $z''(t) = -g$, $z(0) = h$, $z'(0) = v_z$

Théorème 8 (Cauchy-Lipschitz linéaire)**.** *Tout problème de Cauchy admet une unique solution maximale définie sur I tout entier.*

Remarque 9. *La version pour les équations d'ordre p nécessite de connaître $y_0, \ldots, y_{p-1}$ tels que $Y(t_0) = y_0, \ldots, Y^{(p-1)}(t_0) = y_{p-1}$.*

Remarque 10. *Dans le cas non linéaire, on n'a pas unicité. Le problème de Cauchy $y' = 3|y|^{\frac{3}{2}}$ de données $(0,0)$ admet au moins deux solutions maximales : 0 et $(t \mapsto t^3)$.*

3) Structure de l'espace des solutions

Théorème 11. *(i) L'ensemble $\mathscr{S}_H$ des solutions de (EH) est un sous-espace vectoriel de dimension n de $\mathcal{C}^1(I, \mathbb{K}^n)$.*

(ii) L'ensemble $\mathscr{S}$ des solutions de (E) est un sous-espace affine de dimension n de $\mathcal{C}^1(I, \mathbb{K}^n)$ de direction $\mathscr{S}_H$.

Corollaire 12. *L'application suivante est un isomorphisme :*

$$\Phi_{t_0} : \left| \begin{array}{ccc} \mathscr{S}_H & \longrightarrow & \mathbb{K}^n \\ Y & \longmapsto & Y(t_0) \end{array} \right.$$

Contre-exemple 13. *L'ensemble des solutions sur $\mathbb{R}$ de $xy' = 2y$ est un espace vectoriel de dimension 2.*

Proposition 14 (Principe de superposition)**.** *Si Y_1 est solution de $Y' = AY + B_1$ et si Y_2 est solution de $Y' = AY + B_2$ avec A, B_1 et B_2 continues, alors $\lambda Y_1 + \mu Y_2$ est solution de $Y' = AY + \lambda B_1 + \mu B_2$.*

II Résolution explicite

1) Solutions générales de l'équation homogène

Proposition 15. *On suppose que A est de la forme $\mathrm{Diag}(\lambda_1, \dots, \lambda_n)$ dans une base $Y_1, \dots, Y_n$. Une solution générale de (EH) s'écrit :*

$$Y(t) = \sum_{k=1}^{n} \alpha_k e^{\lambda_k t} V_k \quad \text{où} \quad \alpha_k \in \mathbb{K}$$

Exemple 16. *Si $a \neq 1$, les solutions de $Y' = \left(\begin{smallmatrix} 1 & 1 \\ 0 & a \end{smallmatrix}\right) Y$ ont pour base $\left(e^t \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), e^{at} \left(\begin{smallmatrix} 1 \\ a-1 \end{smallmatrix}\right)\right)$.*

Proposition 17. *Pour $A \in \mathcal{M}_n(\mathbb{R})$, la solution du problème de Cauchy $Y'(t) = AY(t)$ et $Y(t_0) = V_0$ est donnée par :*

$$Y(t) = e^{(t-t_0)A} V_0$$

2) Solutions générales

Remarque 18. *Les solutions générales de (E) sont données par la somme d'une solution particulière et des solutions homogènes. Comme on a déjà vu le cas des équations homogènes (EH), il suffit de trouver une solution particulière.*

Proposition 19 (Variation de la constante)**.** *Pour $A \in \mathcal{M}_n(\mathbb{R})$ et $B : I \to \mathbb{K}^n$, une solution particulière de (E) est :*

$$Y(t) = \int_{t_0}^{t} e^{(t-u)A} B(u) du$$

Corollaire 20. *Pour $A \in \mathcal{M}_n(\mathbb{R})$ et $B : I \to \mathbb{K}^n$, la solution du problème de Cauchy $Y'(t) = AY(t) + B(t)$ et $Y(t_0) = V_0$ est donnée par :*

$$Y(t) = e^{(t-t_0)A} V_0 + \int_{t_0}^{t} e^{(t-u)A} B(u) du$$

Remarque 21. *Dans le cas où le second membre a une forme particulière (polynômiale, exponentielle, ...), on peut chercher une solution particulière sous cette forme.*

III Stabilité des solutions

On considère une équation différentielle homogène quelconque $Y' = f(t, Y)$, avec $f \in \mathcal{C}^1(I \times \mathbb{K}^n, \mathbb{K}^n)$.

Définition 22. Un point y_0 de E est un point d'équilibre si $f(y_0) = 0$.

Remarque 23. *Si y_0 est un point d'équilibre, le problème de Cauchy $y' = f(y)$ de données (t_0, y_0) admet pour solution maximale la fonction constante égale à y_0.*

Définition 24. Soit y_0 un point d'équilibre.

(i) y_0 est dit stable si, pour tout $\varepsilon > 0$, il existe $\delta > 0$ tel que, si (I, y) est une solution qui vérifie $|y(t_0) - y_0| < \delta$, alors $[t_0, +\infty[\subset I$ et $|y(t) - y_0| < \varepsilon$ pour tout $t \geqslant t_0$.

(ii) y_0 est dit instable s'il n'est pas stable.

(iii) y_0 est dit asymptotiquement stable s'il existe $\delta > 0$ tel que, si (I, y) est une solution qui vérifie $|y(t_0) - y_0| < \delta$, alors $[t_0, +\infty[\subset I$ et $\lim_{t \to +\infty} y(t) = y_0$.

Ces définitions sont illustrées par la Figure 1.

Définition 25. Soit $x \in \Omega$. On appelle orbite de x l'image commune des solutions maximales passant par x.

Proposition 26. *L'ensemble des orbites forme une partition de Ω.*

Définition 27. On appelle portrait de phase cette partition.

Proposition 28. *Soit (I, y) une solution maximale telle qu'il existe $t_1 < t_2$ tels que $y(t_1) = y(t_2)$. Alors $I = \mathbb{R}$ et y est périodique.*

IV Exemples d'études

1) Étude qualitative des systèmes linéaires dans $\mathbb{R}^2$

On considère l'équation différentielle $Y' = AY$, où $A \in \mathcal{M}_n(\mathbb{R})$.

Théorème 29. *Soient $\lambda_1, \dots, \lambda_n$ les valeurs propres de A. Alors les solutions du système linéaire $Y' = AY$ sont :*

(i) asymptotiquement stables si, et seulement si, $\mathrm{Re}(\lambda_j) < 0$ pour tout $j \in [\![1, n]\!]$.

(ii) stables si, et seulement si, pour tout $j \in [\![1, n]\!]$, ou bien $\mathrm{Re}(\lambda_j) < 0$, ou bien $\mathrm{Re}(\lambda_j) = 0$ et le bloc correspondant est diagonalisable.

Théorème 30. *Dans le cas $n = 2$, on peut classifier les différents types de portraits de phase possibles en fonction de $\det A$ et de $\mathrm{tr}\, A$. Cette classification est illustrée par la Figure 2.*

2) Utilisation des séries entières

Si l'équation est à coefficients polynômiaux, on peut chercher les solutions développables en séries entières autour de 0. Si cette solution est maximale, elle est unique par le théorème de Cauchy-Lipschitz.

Exemple 31. *Le problème de Cauchy $y' = y$ de données $(0, 1)$ admet pour solution $t \mapsto \sum_{n\in\mathbb{N}} \frac{t^n}{n!} = e^t$.*

Exemple 32 (Bessel)**.** *On considère l'équation différentielle de Bessel $xy'' + y' + xy = 0$. Sa solution f_0 valant 1 en 0 se développe en série entière sur $\mathbb{R}$. De plus, si f est une autre solution sur un intervalle $]0, a[$, alors (f, f_0) est libre si, et seulement si, f n'est pas bornée au voisinage de 0.*

3) Équation de Hill-Mathieu

Théorème 33 (Hill-Mathieu)**.** *On considère l'équation $y'' + qy = 0$, où $q : \mathbb{R} \to \mathbb{R}$ est continue, paire et π-périodique. On note W l'espace des solutions, et $A : W \to W$ défini par $Ay(x) = y(x + \pi)$.*

(i) Si $|\mathrm{tr}(A)| < 2$, alors toutes les solutions sont bornées.

(ii) Si $|\mathrm{tr}(A)| = 2$, alors il existe une solution non nulle bornée.

(iii) On a $|\mathrm{tr}(A)| < 2$ si, et seulement si, $y_1'(\pi)y_2(\pi) = 0$.

(iv) Si $|\mathrm{tr}(A)| > 2$, alors aucune solution non triviale n'est bornée.

Application 34. *Les solutions de $y'' + y = 0$ sont toutes bornées, alors que les solutions non triviales de $y'' - y = 0$ sont toutes non bornées.*

Développements

- Équation de Bessel (32) [FGN13e]
- Équation de Hill-Mathieu (33) [ZQ13]

Références

[Dem06] J.-P. Demailly. *Analyse numérique et équations différentielles.* EDP Sciences
[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod
[FGN13e] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 4.* Cassini

Classification des portraits de phase dans le plan $(\det A, \operatorname{Tr} A)$

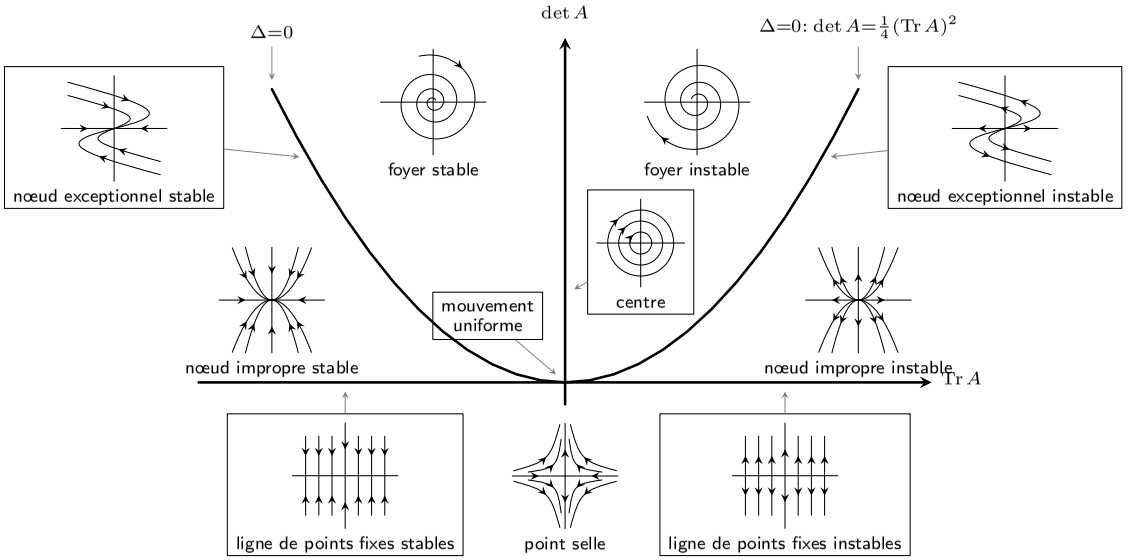


FIGURE 2 – Portraits de phase

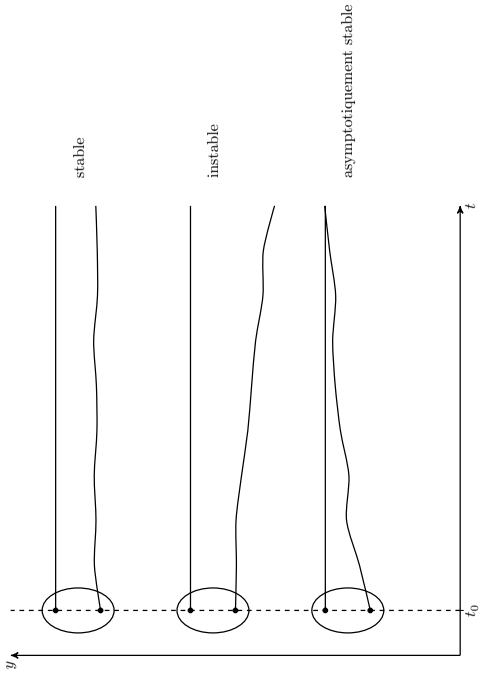


FIGURE 1 – Stabilité d'un point d'équilibre

Annexes

Cadre : On n'étudiera que des équations d'ordre 1 ou 2 en espace. Soit $u : \mathbb{R}^n \to \mathbb{R}$ suffisamment régulière pour que les expressions aient un sens.

I Généralités

1) Définitions

Définition 1. On appelle équation aux dérivées partielles linéaires (EDPL) une équation de la forme :

$$\sum_{1\leqslant i<j\leqslant n} a_{i,j}\frac{\partial^2 u}{\partial x_i \partial x_j} + \sum_{1\leqslant i\leqslant n} b_i \frac{\partial u}{\partial x_i} + cu + d = 0$$

où les $a_{i,j}$, les b_i, c et d sont des fonctions de $\mathbb{R}^n$ dans $\mathbb{R}$. L'équation est dite d'ordre 2 si les $a_{i,j}$ ne sont pas tous nuls, et d'ordre 1 sinon. L'équation est dite homogène si $d = 0$.

Exemple 2 (Transport). $\frac{\partial u}{\partial t} + \nu \frac{\partial u}{\partial x} = 0$ *sur* $\mathbb{R}^+ \times \mathbb{R}$ *avec* $u = u(x,t)$.

Définition 3. On appelle problème aux frontières une EDPL munie de conditions sur le bord complet du domaine sur lequel est est posée.

Exemple 4 (Chaleur). $\frac{\partial u}{\partial t} - a\frac{\partial^2 u}{\partial x^2} = 0$ *sur* $]x_0, +\infty[$ *avec* $u(x_0, t) = u_0(t)$ *donné, où* $u(x,t)$ *désigne la température d'une tige en contact avec un thermostat.*

Définition 5. On appelle problème de Cauchy une EDPL où les conditions ne portent que sur une partie du bord du domaine sur lequel on connait la valeur de la fonction et de ses dérivées de degré inférieur à l'ordre de l'équation.

Exemple 6. $y\frac{\partial u}{\partial x} - x\frac{\partial u}{\partial y} = 0$ *sur* $\mathbb{R}^+ \times \mathbb{R}$ *avec* $u(x,0) = u_0(x)$.

Exemple 7 (Ondes). $\frac{\partial^2 u}{\partial t^2} = c^2 \frac{\partial^2 u}{\partial x^2}$ *dans* $\Omega \times \mathbb{R}^{+\star}$ *avec* $u = 0$ *sur* $\partial\Omega \times \mathbb{R}^{+\star}$, *et* $u(.,0) = u_0$ *et* $\frac{\partial u}{\partial t}(.,0) = u_1$ *dans* Ω. *C'est un problème aux frontières en espace et de Cauchy en temps.*

Définition 8. Soit une EDPL sur un domaine Ω avec éventuellement des conditions aux limites ou initiales. On dit que le problème est bien posé au sens de Hadamard, s'il existe une unique solution qui dépend des données de façon continue.

2) EDPL d'ordre 1

Dans ce paragraphe, on étudie les équations de la forme :

$$\frac{\partial u}{\partial t}(t,x) + \sum_{i=1}^{n} a_i(t,x)\frac{\partial u}{\partial x_i}(t,x) = f(t,x)$$

où les a_i sont des fonctions réelles continues bornées ainsi que leurs dérivées d'ordre 1 sur $\overline{\Omega_T} = [0,T] \times \mathbb{R}^n$. On associe le champs de vecteurs défini sur $\overline{\Omega_T}$ par :

$$(t,x) \mapsto (t, A(t,x)) = (t, a_1(t,x), \ldots, a_n(t,x))$$

Proposition 9. *Pour tout* $(t_0, x_0) \in \overline{\Omega_T}$, *il existe une unique courbe* $t \mapsto (t, X(t))$ *de classe* $\mathcal{C}^1$ *sur* $[0,T]$ *telle que* $X(t)$ *soit solution de* $X'(t) = A(t, X(t))$ *sur* $[0,T]$ *avec* $X(t_0) = x_0$.

Définition 10. La courbe $t \mapsto (t, X(t))$ est appelée courbe caractéristique issue de (t_0, x_0).

Théorème 11. *Soit* $h : \mathbb{R}^n \to \mathbb{R}$ *de classe* $\mathcal{C}^1$ *et bornée. On considère le problème de Cauchy* $\frac{\partial u}{\partial t} + \sum_{i=1}^n a_i \frac{\partial u}{\partial x_i} = 0$ *sur* $\overline{\Omega_T}$ *avec* $u(0,.) = h$ *sur* $\mathbb{R}^n$. *Ce problème a une unique solution donnée par* $u(t,x) = h(X(t))$.

3) Classification des EDPL d'ordre 2

Soit $u : \mathbb{R}^2 \to \mathbb{R}$ et l'EDPL d'ordre 2 et d'inconnue u :

$$a\frac{\partial^2 u}{\partial x^2} + b\frac{\partial^2 u}{\partial x \partial y} + c\frac{\partial^2 u}{\partial y^2} + d\frac{\partial u}{\partial x} + e\frac{\partial u}{\partial y} + fu + g = 0$$

avec $a, b, c, d, e, f, g : \mathbb{R}^2 \to \mathbb{R}$.

Définition 12. On dit que l'équation est :

(i) elliptique : si $b(x,y)^2 - a(x,y)c(x,y) < 0$.

(ii) parabolique : si $b(x,y)^2 - a(x,y)c(x,y) = 0$.

(iii) hyperbolique : si $b(x,y)^2 - a(x,y)c(x,y) > 0$.

Remarque 13. *Le caractère hyperbolique, parabolique ou elliptique d'une équation aux dérivées partielles du second ordre n'est pas modifié par un changement de variable.*

II Exemples d'EDPL hyperboliques

1) Équation de transport

On souhaite modéliser le déplacement d'un contaminant de concentration $u(t,x)$ dans un fluide en mouvement de vitesse $c(x)$.

Définition 14. On appelle équation de transport l'équation :

$$\begin{cases} \frac{\partial u}{\partial t}(t,x) + c(x)\frac{\partial u}{\partial x}(t,x) = 0 & x \in \mathbb{R}, t > 0 \\ u(0,x) = u_0(x) & x \in \mathbb{R} \end{cases} \tag{1}$$

avec $c, u_0 \in \mathcal{C}^1(\mathbb{R},\mathbb{R})$.

Proposition 15. *On suppose c constante. Alors la courbe caractéristique vérifie $X'(t) = c$ et $X(0) = x_0$. Si u est solution de (1), alors $u(t,X(t)) = u(0,X(0)) = u_0(x_0)$, donc $u(x,t) = u_0(x-ct)$ est l'unique solution $\mathcal{C}^1$ de (1).*

Proposition 16. *On suppose que $c(x) = x$ constante. Alors les courbe caractéristique ont pour équation $\ln(x) - t = d \in \mathbb{R}$, donc $xe^{-t} = \lambda \in \mathbb{R}$. Ainsi, la solution est $u(t,x) = u_0(xe^{-t})$.*

2) Équation des ondes

On souhaite modéliser la propagation d'une onde $u(t,x)$ se déplaçant à une vitesse c.

Définition 17. On appelle équation des ondes l'équation :

$$\begin{cases} \frac{\partial^2 u}{\partial t^2} - c^2\Delta u = 0 & x \in \mathbb{R}^n, t > 0 \\ u(0,x) = u_0(x) & x \in \mathbb{R}^n \\ \frac{\partial u}{\partial t}(0,x) = v_0(x) & x \in \mathbb{R}^n \end{cases} \tag{2}$$

avec $c > 0$, $u_0 \in \mathcal{C}^2(\mathbb{R},\mathbb{R})$ et $v_0 \in \mathcal{C}^1(\mathbb{R},\mathbb{R})$.

Théorème 18. *La solution de l'équation des ondes unidimensionnelle est donnée par la formule de d'Alembert :*

$$u(t,x) = \frac{1}{2}\left[u_0(x-ct) + u_0(x+ct)\right] + \frac{1}{2c}\int_{x-ct}^{x+ct} v_0(y)\,dy$$

Remarque 19. *La formule de d'Alembert met en évidence deux classes de solutions : l'une se propageant à la vitesse c et l'autre à la vitesse $-c$.*

III Exemples d'EDPL elliptiques

1) Forumlation faible

Définition 20. Soit $f \in L^1(\Omega)$. On dit que f admet une dérivée faible s'il existe $g \in L^1(\Omega)$ tel que, pour tout $\varphi \in \mathcal{C}_c^\infty(\Omega)$, on a $\int_\Omega f\varphi' = -\int_\Omega g\varphi$. On note alors $g = f'$, qui est unique.

Définition 21. On définit $H^1(\Omega) = \left\{f \in L^2(\Omega) \,\middle|\, f' \in L^2(\Omega)\right\}$, que l'on munit du produit scalaire défini par $\langle f,g\rangle_{H^1} = \langle f,g\rangle_{L^2} + \langle f',g'\rangle_{L^2}$.

Théorème 22. *$\left(H^1(\Omega), \langle .,.\rangle_{H^1}\right)$ est un espace de Hilbert.*

Définition 23. On définit $H_0^1(\Omega)$ comme l'adhérence de $\mathcal{C}_c^\infty(\Omega)$ dans $H^1(\Omega)$. C'est un espace de Hilbert s'il est muni du produit scalaire $\langle .,.\rangle_{H^1}$.

Théorème 24 (Lax-Milgram)**.** *Soient H un espace de Hilbert, a une forme bilinéaire continue et coercive sur H, et $\ell \in H'$. Alors il existe un unique $u \in H$ tel que, pour tout $v \in H$, $a(u,v) = \ell(v)$.*

Application 25. *Soient D un opérateur différentiel et f une fonction définie sur Ω, on s'intéresse à $Du = f$ sur Ω. Sa formulation variationnelle est alors $\int_\Omega Du\,v = \int_\Omega fv$ pour tout v défini sur Ω. Grâce à une formulation faible d'un problème différentiel et au théorème de Lax-Milgram, on peut démontrer l'existence d'une solution faible à ce problème.*

2) Équation de Laplace et de Poisson

Définition 26. On appelle équation de Poisson l'équation $-\Delta u = f$ sur Ω avec $u = 0$ sur $\partial\Omega$ et f définie sur Ω. Si $f = 0$, on parle d'équation de Laplace.

Définition 27. Une fonction $u : \Omega \to \mathbb{C}$ est dite harmonique sur Ω un ouvert de $\mathbb{R}^2$ si u est de classe $\mathcal{C}^2$ et vérifie $\Delta u = 0$.

Exemple 28. *$(x,y) \to \ln(\sqrt{x^2+y^2})$ est harmonique sur $\mathbb{R}^2 \setminus \{(0,0)\}$.*

Corollaire 29. *La partie réelle d'une fonction holomorphe est harmonique. Ainsi, ces fonctions sont solutions de l'équation de Laplace.*

Théorème 30. *Pour $f \in L^2(\Omega)$, l'équation de Poisson admet une unique solution faible.*

IV Un exemple d'EDPL parabolique

1) Séries de Fourier

Définition 31. Soit $f : \mathbb{R} \to \mathbb{C}$ continue par morceaux et 2π-périodique. Les coefficients exponentiels de Fourier de f sont :

$$c_n(f) = \frac{1}{2\pi} \int_0^{2\pi} f(t) e^{-int}\, dt \quad (n \in \mathbb{Z})$$

En posant $e_n : t \mapsto e^{int}$, la série de Fourier associée à f est la série trigonométrique $\sum_{n\in\mathbb{Z}} c_n(f) e_{-n}$.

Proposition 32 (Riemann-Lebesgue)**.** *Si f est continue par morceaux et 2π-périodique, alors* $\lim_{|n|\to+\infty} c_n(f) = 0$.

Théorème 33. *La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de l'espace des fonctions 2π-périodiques de carré intégrable sur $[0, 2\pi]$. On a en particulier :*

$$\frac{1}{2\pi} \|f\|_2^2 = \sum_{n\in\mathbb{Z}} c_n(f)^2$$

Proposition 34. *Si f est $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge simplement vers la régularisation $\tilde{f}$ de f donnée pour $x \in \mathbb{R}$ par $\tilde{f}(x) = \frac{f(x^+)+f(x^-)}{2}$.*

Remarque 35. *L'hypothèse $\mathcal{C}^1$ par morceaux est nécessaire.*

Théorème 36. *Si f est continue, $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge normalement vers f.*

2) Équation de la chaleur

On souhaite modéliser la température $u(t, x)$ dans une barre. On va résoudre l'équation de la chaleur sur un anneau.

Définition 37. On appelle équation de la chaleur l'équation :

$$\begin{cases} \frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 & \text{sur } \mathbb{R}^{+\star} \times \mathbb{T} \\ u(0, x) = u_0(x) & \text{dans } L^2(\mathbb{T}) \end{cases} \tag{3}$$

avec $c > 0$ et $u_0 \in L^2(\mathbb{T})$.

Théorème 38. *Il existe une unique solution u de (3) de classe $\mathcal{C}^2$ sur $\mathbb{R}^{+\star} \times \mathbb{T}$, avec $u(t, .)$ tendant vers u_0 dans $L^2(\mathbb{T})$ quand t tend vers 0.*

Développements

- Équation de la chaleur sur le cercle (38) [Can09]
- Théorème de Lax-Milgram et application (24,30)

Références

[DG12] C. David et P. Gosselet. *Équations aux dérivées partielles.* Dunod

[Bre87] H. Brezis. *Analyse fonctionelle.* Masson

[FGN13e] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 4.* Cassini

[El 08] M. El Amrani. *Analyse de Fourier dans les espaces fonctionnels.* Ellipses

[Can09] B. Candelpergher. *Calcul intégral.* Cassini

Cadre : On appelle suite numérique toute suite à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $(u_n)_{n\in\mathbb{N}}$ une telle suite.

I Suites numériques et convergence

1) Limite d'une suite

Définition 1. On dit que (u_n) converge vers une limite $\ell \in \mathbb{K}$ lorsque :

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ |u_n - \ell| < \varepsilon$$

Si (u_n) ne converge pas, on dit qu'elle diverge.

Proposition 2. *Si (u_n) converge sa limite est unique. On note alors $\lim_{n\to+\infty} u_n = \ell$, ou encore $u_n \to \ell$.*

Application 3. *Une fonction $f : \mathbb{K} \to \mathbb{K}$ est continue si, et seulement si, pour toute suite (u_n) convergeant vers ℓ, $(f(u_n))$ converge vers $f(\ell)$.*

Exemple 4. *La fonction $x \mapsto \sin\left(\frac{1}{x}\right)$ se prolonge par continuité en 0.*

Proposition 5. *Toute suite convergente de $\mathbb{K}$ est bornée.*

Contre-exemple 6. *La suite $u_n = (-1)^n$ est bornée et ne converge pas.*

Proposition 7. *Les suites convergente forment un $\mathbb{K}$-espace vectoriel.*

Proposition 8. *Le produit d'une suite bornée et d'une suite convergeant vers 0 converge vers 0.*

Exemple 9. *La suite $\frac{\sin n}{n}$ converge vers 0.*

On s'intéresse maintenant au cas des suites réelles.

Définition 10. Une suite réelle (u_n) est dite majorée (resp. minorée) s'il existe $M \in \mathbb{R}$ tel que $u_n \leqslant M$ (resp. $u_n \geqslant M$) quel que soit $n \in \mathbb{N}$.

Proposition 11. *Soient (u_n), (v_n) et (w_n) trois suites réelles vérifiant :*

$$\forall n \in \mathbb{N},\ u_n \leqslant v_n \leqslant w_n$$

Si (u_n) et (v_n) convergent vers ℓ, alors (v_n) converge vers ℓ.

Définition 12. Deux suites réelles (u_n) et (v_n) sont dites adjacentes si l'une est croissante, l'autre décroissantes, et si $\lim_{n\to+\infty} u_n - v_n = 0$.

Proposition 13. *Deux suites adjacentes convergent vers la même limite.*

Application 14 (Critère des séries alternées)**.** *Soit (a_n) une suite à termes positifs décroissante vers 0. Alors la série $\sum(-1)^n a_n$ converge, le reste R_n vérifiant $R_n \leqslant a_{n+1}$.*

2) Valeurs d'adhérence

Définition 15. On dit que $a \in \mathbb{K}$ est valeur d'adhérence de (u_n) lorsque :

$$\forall \varepsilon > 0,\ \forall N \in \mathbb{N},\ \exists n \geqslant N,\ |u_n - \ell| < \varepsilon$$

Remarque 16. *Si (u_n) converge, sa limite est une valeur d'adhérence.*

Exemple 17. *-1 et 1 sont valeurs d'adhérence de la suite $(-1)^n$.*

Définition 18. On appelle suite extraite (ou sous-suite) de (u_n) une suite de la forme $u_{\varphi(n)}$) où $\varphi : \mathbb{N} \to \mathbb{N}$ est strictement croissante.

Proposition 19. *Toute suite extraite d'une suite convergente converge vers la même limite.*

Proposition 20. *Soit $a \in \mathbb{K}$. Les assertions suivantes sont équivalentes :*

(i) a est valeur d'adhérence de (u_n).

(ii) Il existe une sous-suite de (u_n) qui converge vers a.

(iii) Pour tout $N \in \mathbb{N}$, $a \in \overline{\{u_n \,|\, n \geqslant N\}}$.

(iv) a est point d'accumulation de $\{u_n | n \geqslant N\}$ ou $\{n | u_n = a\}$ est infini.

L'ensemble des valeurs d'adhérence d'une suite est fermé.

Remarque 21. *Si $u_n \to \ell$, ℓ est l'unique valeur d'adhérence de (u_n).*

Exemple 22. *La suite $u_n = \cos n$ admet $[-1, 1]$ comme ensemble de valeurs d'adhérence.*

Théorème 23 (Bolzano-Weierstrass)**.** *Toute suite numérique bornée admet une valeur d'adhérence.*

Corollaire 24. *Une suite réelle est convergente si, et seulement si, elle est bornée et admet une unique valeur d'adhérence.*

Proposition 25. *Soit (E, d) un espace métrique compact et $(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de I telle que $\lim_{n\to+\infty} d(u_n, u_{n+1}) = 0$. Alors l'ensemble des valeurs d'adhérence de $(u_n)_{n\in\mathbb{N}}$ est connexe.*

Application 26. *Soient $f : [0, 1] \to [0, 1]$ une fonction continue et $(x_n)_{n\in\mathbb{N}}$ la suite définie par $x_0 \in [0, 1]$ et $u_{n+1} = f(u_n)$ pour tout $n \in \mathbb{N}$. Alors $(x_n)_{n\in\mathbb{N}}$ converge si, et seulement si, $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.*

3) Suites de Cauchy

Définition 27. On dit que (u_n) est de Cauchy lorsque :

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ \forall p \in \mathbb{N},\ |u_{n+p} - u_n| < \varepsilon$$

Proposition 28. *(i) Toute suite convergente est de Cauchy.*
(ii) Toute suite de Cauchy est bornée.
(iii) Toute sous-suite d'une suite de Cauchy est de Cauchy.
(iv) Toute suite de Cauchy ayant une valeur d'adhérence converge.

Théorème 29. *Toute suite numérique de Cauchy est convergente.*

Exemple 30. *Toute série numérique absolument convergente converge.*

Exemple 31. *La série harmonique diverge car elle n'est pas de Cauchy.*

II Exemples de suites particulières

1) Suites arithmétiques et géométriques

Définition 32. On dit que (u_n) est arithmétique (resp. géométrique) de raison $a \in \mathbb{K}$ si $u_{n+1} = u_n + a$ (resp. $u_{n+1} = au_n$).

Proposition 33. *Si (u_n) est arithmétique (resp. géométrique) de raison $a \in \mathbb{K}$, alors $u_n = u_0 + na$ (resp. $u_n = a^n u_0$).*

Proposition 34. *Une suite géométrique converge si, et seulement si, $|a| < 1$ et est bornée si, et seulement si, $|a| \leqslant 1$.*

2) Suites homographiques

Définition 35. On dit que (u_n) est homographique lorsqu'elle vérifie :

$$\forall n \in \mathbb{N},\ u_{n+1} = h(u_n) \quad \text{avec} \quad h(x) = \frac{ax+b}{cx+d},\ ad - bc \neq 0$$

Proposition 36. *Soit (u_n) une suite homographique. Soient α et β les solutions de $h(x) = x \Leftrightarrow cx^2 - (a-d)x - b = 0$.*

(i) Si $\alpha \neq \beta$, la suite $\left(\frac{u_n - \alpha}{u_n - \beta}\right)$ est géométrique de raison $\frac{a - \alpha c}{a - \beta c}$.

(ii) Si $\alpha = \beta$, la suite $\left(\frac{1}{u_n - \beta}\right)$ est arithmétique de raison $\frac{c}{a - \beta c}$.

Exemple 37. *Si $u_{n+1} = \frac{u_n}{1+u_n}$ avec $u_0 = 1$, $u_n \to 0$.*

3) Suites récurrentes d'ordre 1

Définition 38. Soit $I \subseteq \mathbb{R}$ un intervalle, et soit $f : I \to I$ continue. On dit que (u_n) est définie par récurrence si $u_0 \in I$ et $u_{n+1} = f(u_n)$.

Remarque 39. *Il s'agit d'une généralisation des cas précédents.*

Corollaire 40. *Si une suite (u_n) est définie par récurrence converge vers $\ell \in I$, alors ℓ est un point fixe de f.*

Exemple 41. *La suite (u_n) définie par $u_0 = 1$ et $u_{n+1} = u_n^2 - u_n - 3$ ne peut converger que vers -1 ou 3.*

Théorème 42. *Si (u_n) est définie par récurrence, alors :*

(i) Si f est croissante, la suite (u_n) est monotone et son sens de monotonie est donné par le signe de $u_1 - u_0$.

(ii) Si f est décroissante, alors $f \circ f$ est croissante, ainsi les suites (u_{2n}) et (u_{2n+1}) sont monotones, et leur sens de monotonie est opposé.

Exemple 43. *Pour $u_0 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ et $u_{n+1} = sin(u_n)$, $u_n \to 0$.*

Exemple 44. *Pour $u_0 \in [0,1]$ et $u_{n+1} = \frac{1}{2 - \sqrt{u_n}}$, $u_n \to 1$.*

Théorème 45 (Méthode de Newton)**.** *Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f : [a,b] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ telle que $f(a) < 0 < f(b)$ et $f' > 0$ sur $[a,b]$. On considère la suite $(x_n)_{n\in\mathbb{N}}$ définie par :*

$$x_0 \in [a,b] \quad et \quad \forall n \in \mathbb{N},\ x_{n+1} = \phi(x_n) = x_n - \frac{f(x_n)}{f'(x_n)}$$

La fonction f admet un unique zéro $\alpha \in]a,b[$, et on a :

(i) Il existe $\varepsilon > 0$ tel que, pour $x_0 \in I =]\alpha - \varepsilon, \alpha + \varepsilon[$, la suite $(x_n)_{n\in\mathbb{N}}$ converge quadratiquement vers α, et il existe $C > 0$ tel que :

$$\forall n \in \mathbb{N},\ |x_{n+1} - \alpha| \leqslant C|x_n - \alpha|^2$$

(ii) Si de plus $f'' > 0$ sur $[\alpha, b]$, alors, pour $x \in]\alpha, b]$, la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante, et pour tout $n \in \mathbb{N}$ on a :

$$0 \leqslant x_{n+1} - \alpha \leqslant C(x_n - \alpha)^2 \quad et \quad x_{n+1} - \alpha \sim \frac{f''(\alpha)}{2f'(\alpha)}(x_n - \alpha)^2$$

III Comportement asymptotique

1) Comparaison asymptotique

On s'intéresse ici au cas des suites réelles.

Définition 46. Soient $u = (u_n)$ et $v = (v_n)$ deux suites réelles. On dit qu'au voisinage de $+\infty$:

(i) v domine u, noté $u_n = \mathcal{O}(v_n)$, lorsque :

$$\exists C > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ |u_n| \leqslant C|v_n|$$

(ii) u est négligeable devant v, noté $u_n = \mathrm{o}(v_n)$, lorsque :

$$\forall \varepsilon > 0,\ \exists n_0 \in \mathbb{N},\ \forall n \geqslant n_0,\ |u_n| \leqslant \varepsilon|v_n|$$

(iii) u et v sont équivalentes, noté $u_n \sim v_n$, si $u_n - v_n = \mathrm{o}(v_n)$.

Exemple 47. *$n^2 + \sin n = \mathcal{O}(n^2)$ et $n^2 + \sin n \sim n^2$.*

Proposition 48. *On a les propriétés suivantes :*

(i) *o et $\mathcal{O}$ sont stables par somme.*

(ii) *o, $\mathcal{O}$ et $\sim$ sont stables par produit et passage à une puissance.*

Remarque 49. *$\sim$ n'est pas compatible avec l'addition : $n+2 \sim n+1$ et $-n \sim -n$, mais $2 \not\sim 1$.*

2) Moyenne de Cesàro

Définition 50. On appelle suite des moyennes de Cesàro la suite $(v_n)_{n\in\mathbb{N}}$ définie par $v_n = \frac{1}{n}\sum_{k=0}^{n-1} u_k$.

Proposition 51. *La moyenne de Cesàro d'une suite convergente converge vers la même limite.*

Définition 52. Si la moyenne de Cesàro d'une suite converge, on dit qu'elle converge en moyenne de Cesàro.

Contre-exemple 53. *La suite $(-1)^n$ converge en moyenne de Cesàro, mais ne converge pas.*

Application 54. *Si (u_n) converge vers $\ell \neq 0$, et si $u_n \neq 0$ pour $n \in \mathbb{N}$, alors la suite (v_n) définie par $\frac{n}{v_n} = \sum_{k=0}^{n-1} \frac{1}{u_k}$ converge vers ℓ.*

Développements

- Connexité des valeurs d'adhérence d'une suite (25,26) [FGN13d]
- Méthode de Newton (45) [Rou15]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions.* Ellipses
[FGN13d] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 1.* Cassini
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

Annexes

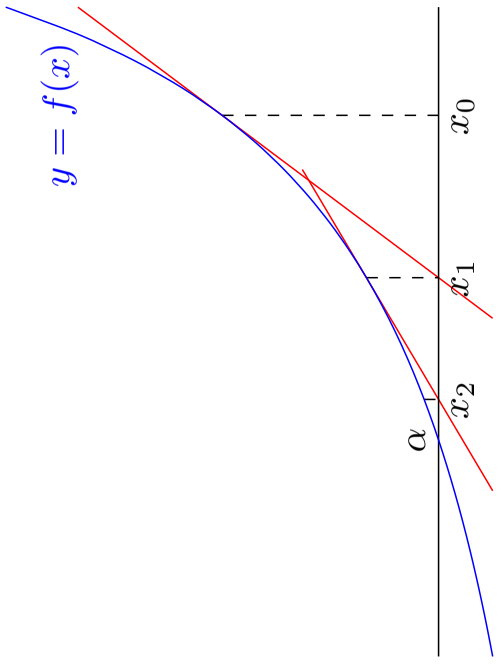


FIGURE 1 – Méthode de Newton

Cadre : Soient $(E, \|.\|)$ un $\mathbb{R}$-espace vectoriel normé et $(u_n)_{n\in\mathbb{N}}$ une suite.

I Généralités sur les suites récurrentes

1) Définition et premières propriétés

Définition 1. On dit que (u_n) et une suite récurrente d'ordre k s'il existe une fonction $f : E^k \to E$ telle que :

$$\forall\, n \in \mathbb{N},\ u_{n+k} = f(u_n, \dots, u_{n+k-1})$$

Proposition 2. *Soit (u_n) une suite récurrente d'ordre k. Si la suite (u_n) converge vers une limite ℓ et si f est continue en $(\ell, \dots, \ell)$, alors on a $\ell = f(\ell, \dots, \ell)$. Si $k = 1$, ℓ est un point fixe de f.*

Exemple 3. *Considérons la suite $u_{n+1} = \frac{u_n}{2} + \mathbb{1}_{\{0\}}(u_n)$ pour $u_0 > 0$. On a alors $u_n \to 0$, mais $\frac{0}{2} + \mathbb{1}_{\{0\}}(0) = 1 \neq 0$.*

Remarque 4. *Soit (u_n) une suite récurrente d'ordre k. On se ramène à une suite récurrente d'ordre 1 en posant :*

$$U_n = \begin{pmatrix} u_n \\ \vdots \\ u_{n+k-1} \end{pmatrix} \quad et \quad U_{n+1} = \begin{pmatrix} u_{n+1} \\ \vdots \\ f(u_n, \dots, u_{n+k-1}) \end{pmatrix} = F(U_n)$$

Mais cette suite est dans l'espace E^k, ce qui peut rendre l'étude de F plus délicate que celle de f.

Proposition 5. *Soient $I \subset \mathbb{R}$ un intervalle tel que $f(I) \subset I$, et $u_0 \in I$.*

(i) Si f est croissante, la suite (u_n) est monotone et son sens de monotonie est donné par le signe de $u_1 - u_0$.

(ii) Si f est décroissante, alors $f \circ f$ est croissante, ainsi les suites (u_{2n}) et (u_{2n+1}) sont monotones, et leur sens de monotonie est opposé.

Exemple 6. *Pour $u_0 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ et $u_{n+1} = sin(u_n)$, $u_n \to 0$.*

Exemple 7. *Pour $u_0 \in [0, 1]$ et $u_{n+1} = \frac{1}{2-\sqrt{u_n}}$, $u_n \to 1$.*

Proposition 8. *Soient $f : [0, 1] \to [0, 1]$ une fonction continue et $(x_n)_{n\in\mathbb{N}}$ la suite définie par $x_0 \in [0, 1]$ et $u_{n+1} = f(u_n)$ pour tout $n \in \mathbb{N}$. Alors $(x_n)_{n\in\mathbb{N}}$ converge si, et seulement si, $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.*

2) Suites récurrentes linéaires

Définition 9. On dit que la relation de récurrence est linéaire si f est une application linéaire. Si $E = \mathbb{R}$, alors f est une forme linéaire, donnée par un vecteur $(a_1, \dots, a_k)$. Le polynôme $X^k + \sum_{i=1}^{k-1} a_i X^{k-i}$ est appelé polynôme caractéristique de la relation de récurrence.

Proposition 10. *Soit (u_n) une suite récurrente d'ordre k, de polynôme caractéristique P. On note $r_1, \dots, r_q$ ses racines et $\alpha_1, \dots, \alpha_q$ leur multiplicité. Alors (u_n) est de la forme :*

$$u_n = \sum_{i=1}^{q} P_i(n) r_i^n \quad avec \quad P_i \in \mathbb{R}_{\alpha_i - 1}[X]$$

Exemple 11 (Fibonacci)**.** *On considère la suite définie par $u_0 = 0$, $u_1 = 1$ et pour tout $n \geqslant 2$ par $u_n = u_{n-1} + u_{n-2}$. Alors :*

$$u_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

3) Quelques exemples classiques

Définition 12. On dit que (u_n) est arithmétique (resp. géométrique) de raison $a \in E$ (resp. $a \in \mathbb{R}$) si $u_{n+1} = u_n + a$ (resp. $u_{n+1} = au_n$).

Proposition 13. *Si (u_n) est arithmétique (resp. géométrique) de raison $a \in \mathbb{R}$, alors $u_n = u_0 + na$ (resp. $u_n = a^n u_0$).*

Proposition 14. *(i) Une suite arithmétique converge si, et seulement si, elle est constante.*

(ii) Une suite géométrique converge si, et seulement si, $|a| < 1$.

(iii) Une suite géométrique est bornée si, et seulement si, $|a| \leqslant 1$.

Définition 15. On dit que (u_n) est arithmético-géométrique si, pour tout $n \in \mathbb{N}$, $u_{n+1} = au_n + b$. Si $a \neq 1$, la suite définie par $v_n = u_n - \frac{b}{1-a}$ est géométrique de raison a. On a dans ce cas $u_n = a^n \left(u_0 - \frac{b}{1-a} \right) + \frac{b}{1-a}$, qui converge si , et seulement si $|a| < 1$.

Définition 16. On dit que (u_n) est homographique lorsqu'elle vérifie :

$$\forall\, n \in \mathbb{N},\ u_{n+1} = h(u_n) \quad \text{avec} \quad h(x) = \frac{ax+b}{cx+d},\ ad - bc \neq 0$$

Proposition 17. *Soit (u_n) une suite homographique. Soient α et β les solutions de $h(x) = x \Leftrightarrow cx^2 - (a-d)x - b = 0$.*

(i) Si $\alpha \neq \beta$, la suite $\left(\frac{u_n - \alpha}{u_n - \beta}\right)$ est géométrique de raison $\frac{a - \alpha c}{a - \beta c}$.

(ii) Si $\alpha = \beta$, la suite $\left(\frac{1}{u_n - \beta}\right)$ est arithmétique de raison $\frac{c}{a - \beta c}$.

Exemple 18. *Si $u_{n+1} = \frac{u_n}{1+u_n}$ avec $u_0 = 1$, $u_n \to 0$.*

II Suites récurrentes et points fixes

1) Théorème de point fixe de Banach-Picard

Définition 19. Soient X un ensemble, $f : X \to X$ une application et $a \in X$. On dit que a est un point fixe de f si $f(x) = x$.

Théorème 20 (Banach-Picard)**.** *Soient (X, d) un espace métrique complet (non vide), et $F : X \to X$ une application k-contractante. Alors F admet un unique point fixe et toute suite définie par $u_0 \in X$ puis $u_{n+1} = F(u_n)$ converge vers ce point à une vitesse géométrique.*

Remarque 21. *Si F^p est contractante, on a le même résultat.*

Contre-exemple 22. *Si $X =]0,1[$ et $F : x \mapsto \frac{x}{2}$, F est contractante mais sans point fixe (X n'est pas complet).*

Contre-exemple 23. *Si $X = [0,1]$ et $F : x \mapsto \sqrt{1+x^2}$, X est complet, F est contractante, mais sans point fixe ($F([0,1]) = [1, \sqrt{2}]$).*

Contre-exemple 24. *Si $X = \mathbb{R}$ et $F : x \mapsto \sqrt{1+x^2}$, X est complet, F applique X dans lui-même, mais sans point fixe (F n'est pas contractante).*

Application 25. *On souhaite résoudre une équation de la forme $f(x) = 0$ avec $f : [a,b] \to \mathbb{R}$ dérivable. Posons $\varphi(x) = x - Cf(x)$ avec $C \neq 0$ une constante. Le problème revient alors à trouver les points fixes de φ. Supposons $f(a) < 0$, $f(b) > 0$, et qu'il existe $m, M \in \mathbb{R}^{+\star}$ tels que $m \leqslant f' \leqslant M$. Prendre $C = \frac{1}{M}$ permet alors à φ d'être contractante et d'envoyer $[a,b]$ dans $[a,b]$ qui est complet. Il existe donc un unique point fixe de φ, donc une unique solution de $f(x) = 0$, qui peut être approché par une suite récurrente définie par $x_0 \in [a,b]$ et $x_{n+1} = \varphi(x_n)$ pour $n \in \mathbb{N}$.*

Application 26 (Cauchy-Lipschitz)**.** *Soient $I \subset \mathbb{R}$ un intervalle et $f : I \times \mathbb{R}^n \to \mathbb{R}^n$ continue et lipschitzienne en sa deuxième variable. Alors tout problème de Cauchy $y' = f(t,y)$ et $y(t_0) = x_0$ admet une unique solution maximale.*

2) Étude des points fixes dans le cas réel d'ordre 1

On considère $f : \mathbb{R} \to \mathbb{R}$ de classe $\mathcal{C}^1$ admettant un point fixe $\alpha \in \mathbb{R}$.

Définition 27. (i) On dit que α est attractif, si $|f'(\alpha)| < 1$.

(ii) On dit que α est répulsif, si $|f'(\alpha)| > 1$.

Proposition 28. *(i) Si α est attractif, il existe un intervalle I autour de α tel que toute suite définie par $x_0 \in I$ et $x_{n+1} = f(x_n)$ pour $n \in \mathbb{N}$ converge géométriquement vers ce point fixe.*

(ii) Si α est répulsif, il n'existe pas de suite non stationnaire définie par $x_0 \in I$ et $x_{n+1} = f(x_n)$ pour $n \in \mathbb{N}$ qui converge vers ce point fixe.

Remarque 29. *Si $|f'(\alpha)| = 1$, on ne peut rien dire sur la nature du point fixe, comme le montrent les prochains exemples.*

Exemple 30. *Soit $f(x) = \sin x$ sur $\left[0, \frac{\pi}{2}\right]$. On a $\sin x < x$ pour $x > 0$. Toute suite définie par $x_0 \in \left]0, \frac{\pi}{2}\right]$ et $x_{n+1} = f(x_n)$ pour $n \in \mathbb{N}$ est strictement décroissante et minorée, donc convergente vers un point fixe de f, donc vers 0, qui est attractif.*

Exemple 31. *Soit $f(x) = \sinh x$ sur $\mathbb{R}^+$. On a $\sinh x > x$ pour $x > 0$. Toute suite définie par $x_0 \in \mathbb{R}^{+\star}$ et $x_{n+1} = f(x_n)$ pour $n \in \mathbb{N}$ diverge vers $+\infty$, et le point fixe est répulsif.*

III Méthodes itératives à un pas

1) Méthode de Newton

La méthode de Newton consiste à approcher une solution d'une équation $f(x) = 0$ en partant d'une approximation plus grossière. L'idée est de remplacer la courbe de f par sa tangente.

Théorème 32 (Méthode de Newton)**.** *Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f : [a,b] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ telle que $f(a) < 0 < f(b)$ et $f' > 0$ sur $[a,b]$. On considère la suite $(x_n)_{n \in \mathbb{N}}$ définie par :*

$$x_0 \in [a,b] \quad et \quad \forall\, n \in \mathbb{N},\ x_{n+1} = \phi(x_n) = x_n - \frac{f(x_n)}{f'(x_n)}$$

La fonction f admet un unique zéro $\alpha \in]a,b[$, et on a :

(i) Il existe $\varepsilon > 0$ tel que, pour $x_0 \in I =]\alpha - \varepsilon, \alpha + \varepsilon[$, la suite $(x_n)_{n\in\mathbb{N}}$ converge quadratiquement vers α, et il existe $C > 0$ tel que :

$$\forall\, n \in \mathbb{N},\ |x_{n+1} - \alpha| \leqslant C|x_n - \alpha|^2$$

(ii) Si de plus $f'' > 0$ sur $[\alpha, b]$, alors, pour $x \in]\alpha, b]$, la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante, et pour tout $n \in \mathbb{N}$ on a :

$$0 \leqslant x_{n+1} - \alpha \leqslant C(x_n - \alpha)^2 \quad \text{et} \quad x_{n+1} - \alpha \sim \frac{f''(\alpha)}{2f'(\alpha)}(x_n - \alpha)^2$$

2) Méthodes de gradient

Soit $J : \mathbb{R}^n \to \mathbb{R}$. On suppose J différentiable. On cherche, s'il existe, un élément $u \in \mathbb{R}^n$ tel que :

$$J(u) = \inf_{v\in\mathbb{R}^n} J(v)$$

Pour cela, on utilise les méthodes de gradient. On considère la suite :

$$u_0 \in \mathbb{R}^n \quad \text{et} \quad \forall\, k \in \mathbb{N},\ u^{k+1} = u^k - \rho^k \nabla J(u^k)$$

Il existe plusieurs possibilités pour choisir les ρ^k, par exemple :

(i) Gradient à pas fixe : $\rho^k = \rho$ une constante positive fixée.

(ii) Gradient à pas optimal : ρ^k minimise $\rho \mapsto J\left(u^k - \rho \nabla J(u^k)\right)$.

Théorème 33. *Si J est α-convexe et différentiable, et que ∇J est L-lipschitzienne, alors la méthode de gradient à pas optimal converge vers l'unique minimum de J.*

Application 34. *Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. On considère la fonctionnelle quadratique $J : \mathbb{R}^n \to \mathbb{R}$ définie par :*

$$J(X) = \langle AX, X\rangle - \langle b, X\rangle + c$$

Cette fonctionnelle satisfait les conditions du théorème précédent. De plus, son minimum est atteint en $X_0 \in \mathbb{R}^n$ qui vérifie $\nabla J(X_0) = AX - b = 0$. On a donc une méthode itérative pour approcher la solution de $AX = b$.

Développements

- Méthode de Newton (32) [Rou15]
- Algorithme de gradient à pas optimal (33) [Cia88]
- Connexité des valeurs d'adhérence d'une suite (8) [Gou08] [FGN13d]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini
[Dem06] J.-P. Demailly. *Analyse numérique et équations différentielles.* EDP Sciences
[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

Annexes

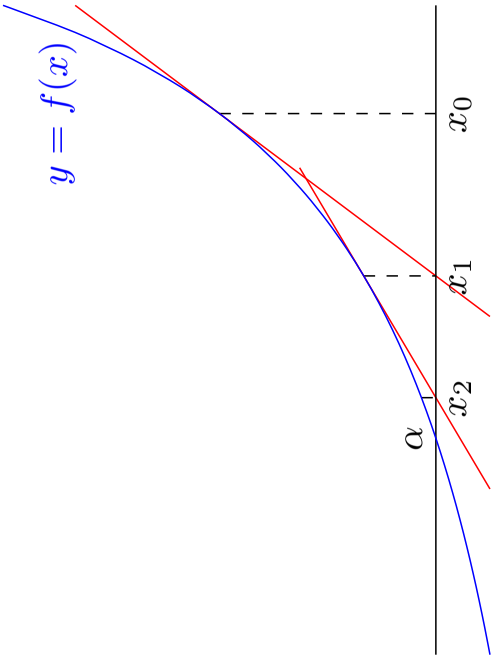


FIGURE 3 – Méthode de Newton

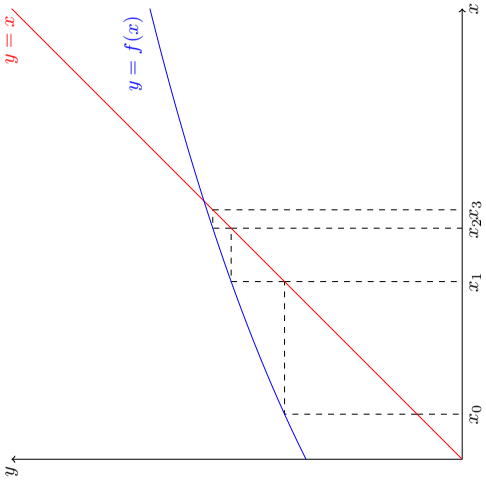


FIGURE 1 – Point fixe attractif

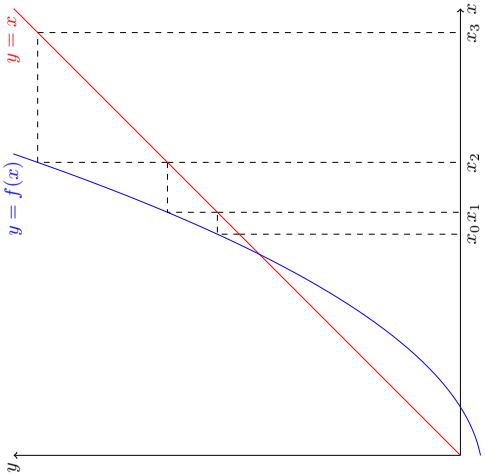


FIGURE 2 – Point fixe répulsif

Cadre : $I =]a, b[$ est un intervalle ouvert de $\mathbb{R}$, avec $a, b \in \overline{\mathbb{R}}$.

I Continuité et dérivabilité

1) Continuité

Définition 1. Une fonction $f : I \to \mathbb{R}$ est continue en $x_0 \in I$ lorsque :

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall y \in I,\ |x_0 - y| \Rightarrow |f(x_0) - f(y)| < \varepsilon$$

Autrement dit, lorsque $\lim_{x \to x_0} f(x) = f(x_0)$. On dit que f est continue sur I si elle est continue en tout point de I. On note $\mathcal{C}^0(I, \mathbb{R})$ l'ensemble des fonctions continues de I dans $\mathbb{R}$.

Lemme 2. *Soit $f : I \to \mathbb{R}$ continue en $x \in I$, et soit $g : \mathbb{R} \to \mathbb{R}$ définie et continue en $f(x)$. Alors $g \circ f : I \to \mathbb{R}$ est continue en x.*

Proposition 3. *Si f est est continue et bijective d'un compact I dans J, alors f^{-1} est continue sur J.*

Exemple 4. *(i) $\mathbb{1}_{\mathbb{Q}}$ n'est continue au aucun point.*
(ii) Les fonctions polynômiales sont continues.

Proposition 5. *$f : I \to \mathbb{R}$ est continue en $x \in I$ si, et seulement si, toute suite $(x_n)_{n \in \mathbb{N}}$ qui converge vers x est telle que $\lim_{n \to +\infty} f(x_n) = f(x)$.*

Exemple 6. *$x \mapsto \cos\left(\frac{1}{x}\right)$ n'est pas continue en 0.*

Théorème 7. *Soit $x_0 \in I$, et soit $f : I \setminus \{x_0\} \to \mathbb{R}$. Si $\lim_{x \to x_0} f(x)$ existe et vaut ℓ, alors la fonction :*

$$g : \left| \begin{array}{ccc} I & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \left\{ \begin{array}{rcl} f(x) & si & x \in I \setminus \{x_0\} \\ \ell & si & x = x_0 \end{array} \right. \end{array} \right.$$

est continue en x_0. g est un prolongement de f par continuité.

Théorème 8. *$\mathcal{C}^0(I, \mathbb{R})$ est une $\mathbb{R}$-algèbre.*

Définition 9. Une fonction $f : I \to \mathbb{R}$ est uniformément continue si :

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x, y \in I,\ |x - y| \Rightarrow |f(x) - f(y)| < \varepsilon$$

Remarque 10. *L'uniforme continuité implique la continuité, mais la réciproque est fausse en général.*

Exemple 11. *$x \mapsto x^2$ est continue sur $\mathbb{R}$, mais pas uniformément.*

Théorème 12 (Heine)**.** *Toute fonction continue sur un compact y est uniformément continue.*

2) Dérivabilité

Définition 13. Une fonction $f : I \to \mathbb{R}$ est dérivable à droite (resp. à gauche) en $x_0 \in I$ lorsque la limite suivante existe :

$$\lim_{x \to x_0^+} \frac{f(x) - f(x_0)}{x - x_0} \qquad \left(\text{resp. } \lim_{x \to x_0^-} \frac{f(x) - f(x_0)}{x - x_0} \right)$$

On dit que f est dérivable en x_0 si elle est dérivable à droite et à gauche et que les limites coïncident. Dans ce cas, cette limite est notée $f'(x_0)$. La fonction $f' : x \mapsto f'(x)$ est appelée fonction dérivée de f. On dit que f est dérivable sur I si elle est continue en tout point de I. On dit que f est dérivable sur I si elle est dérivable en tout point de I. On note $\mathcal{D}^1(I, \mathbb{R})$ l'ensemble des fonctions dérivables de I dans $\mathbb{R}$.

Remarque 14. *La dérivée n'est pas forcément continue.*

Proposition 15. *Toute fonction dérivable est continue.*

Théorème 16. *Soient $f : I \to \mathbb{R}$ dérivable en a et $g : f(I) \to \mathbb{R}$ dérivable en $f(a)$. Alors $g \circ f$ est dérivable en a, et on a :*

$$(g \circ f)'(a) = g'(f(a)) f'(a)$$

Corollaire 17. *Si $f : I \to J$ est bijective et dérivable en a, alors f^{-1} est dérivable en $f(a)$ si, et seulement si, $f'(a) \neq 0$. Dans ce cas, on a :*

$$(f^{-1})'(b) = \frac{1}{f'(a)} \quad \text{où} \quad b = f(a)$$

Théorème 18. *Soient $f, g : I \to \mathbb{R}$ dérivables en a. Alors fg est dérivable en a, et on a :*

$$(fg)'(a) = f'(a)g(a) + f(a)g'(a)$$

Corollaire 19. *$\mathcal{D}^1(I, \mathbb{R})$ est une $\mathbb{R}$-algèbre.*

Définition 20. Pour $n \geqslant 1$, on pose $\mathcal{D}^n(I, \mathbb{R})$ l'ensemble des fonctions n fois dérivables de I dans $\mathbb{R}$, et $\mathcal{C}^n(I, \mathbb{R})$ l'ensemble des fonctions n fois dérivables de I dans $\mathbb{R}$ avec $f^{(n)}$ continue.

Remarque 21. $\mathcal{C}^0(I, \mathbb{R}) \subset \mathcal{D}^1(I, \mathbb{R}) \subset \mathcal{C}^1(I, \mathbb{R}) \subset \ldots \subset \mathcal{D}^n(I, \mathbb{R}) \subset \mathcal{C}^n(I, \mathbb{R}) \subset \mathcal{D}^{n+1}(I, \mathbb{R}) \subset \ldots$

Théorème 22 (Leibniz)**.** *Soient $f, g : I \to \mathbb{R}$ dérivables n fois en a. Alors fg est dérivable n fois en a, et on a :*

$$(fg)^{(n)}(a) = \sum_{k=0}^{n} \binom{n}{i} f^{(i)}(a) g^{(n-1)}(a)$$

II Résultats fondammentaux

1) Théorèmes des valeurs intermédiaires et de Rolle

Théorème 23. *Si $f : I \to \mathbb{R}$ est continue, alors $f(I)$ est un intervalle.*

Corollaire 24. *Si $f : [a,b] \to \mathbb{R}$ est continue, avec $f(a)$ et $f(b)$ de signes différents, alors l'équation $f(x) = 0$ admet des solutions sur $[a,b]$.*

Théorème 25 (Darboux)**.** *Si $f \in \mathcal{D}^1(I,\mathbb{R})$, alors $f'(I)$ est un intervalle.*

Proposition 26. *Soit $f : I \to \mathbb{R}$ continue et dérivable en $c \in \mathring{I}$. Si f admet un extremum local en c, alors $f'(c) = 0$.*

Théorème 27 (Rolle)**.** *Soit $f : I \to \mathbb{R}$ continue sur I et dérivable sur $\mathring{I}$. Si $f(a) = f(b)$, alors il existe $c \in \mathring{I}$ tel que $f'(c) = 0$.*

Théorème 28 (Accroissements finis)**.** *Soit $f : I \to \mathbb{R}$ continue sur I et dérivable sur $\mathring{I}$. Alors il existe $c \in \mathring{I}$ tel que $f'(c)(b-a) = f(b) - f(a)$.*

Corollaire 29. *Soit $f : I \to \mathbb{R}$ dérivable sur $\mathring{I}$.*

(i) f est croissante sur I si, et seulement si, f' est positive sur $\mathring{I}$.

(ii) f est constante si, et seulement si, f' est constante égale à 0.

Remarque 30. *Ces résultats sont faux si I n'est pas un intervalle : $x \mapsto -\frac{1}{x}$ n'est pas croissante sur $\mathbb{R}$, même si sa dérivée est positive.*

2) Formule de Taylor

Théorème 31 (Taylor-Young)**.** *Soient $n \in \mathbb{N}$ et f dérivable n fois en a.*

$$\forall\, x \in I,\ f(x) = \sum_{k=0}^{n} \frac{(x-a)^k}{k!} f^{(k)}(a) + \mathrm{o}\left((x-a)^n\right)$$

Théorème 32 (Taylor-Lagrange)**.** *Soient $n \in \mathbb{N}$ et f de classe $\mathcal{C}^n$ de $[a,b]$ dans $\mathbb{R}$, et dérivable $n+1$ fois sur $]a,b[$.*

$$\exists\, c \in \mathring{I},\ f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \frac{(b-a)^{n+1}}{(n+1)!} f^{(n+1)}(c)$$

Théorème 33 (Taylor avec reste intégral)**.** *Soient $n \in \mathbb{N}$ et f de classe $\mathcal{C}^{n+1}$ de $[a,b]$ dans $\mathbb{R}$.*

$$f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\, dt$$

III Étude de certaines classes de fonctions

1) Fonctions lipschitziennes

Définition 34. On dit que $f : I \to \mathbb{R}$ est lipschitzienne de rapport k si :

$$\exists\, k \in \mathbb{R},\ \forall\, x, y \in I,\ |f(x) - f(y)| \leqslant k|x-y|$$

Proposition 35. *Une fonction de dérivée bornée est lipschitzienne.*

Proposition 36. *Une fonction lipschitzienne est uniformément continue.*

2) Suites de fonctions

Théorème 37. *Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions de I dans $\mathbb{R}$ qui converge uniformément vers une fonction $f : I \to \mathbb{R}$. Si toutes les fonctions f_n sont continues en $x_0 \in I$, alors c'est aussi le cas de f.*

Théorème 38. *Soit $(f_n)_n$ une suite de fonctions $\mathcal{C}^1$. On suppose que :*

(i) Il existe $x_0 \in [a,b]$ tel que la suite $(f_n(x_0))_n$ converge.

(ii) $(f_n')_n$ converge uniformément sur $[a,b]$ vers une fonction g.

Alors $(f_n)_n$ converge uniformément vers $f \in \mathcal{C}^1([a,b])$ telle que $f' = g$.

Théorème 39 (Dini)**.** *Soit $(f_n)_n$ une suite de fonctions de $[a,b]$ dans $\mathbb{R}$ qui converge simplement vers f. Alors la convergence est uniforme si $(f_n)_n$ est monotone ou si les f_n sont croissantes.*

Théorème 40 (Weierstrass)**.** *L'ensemble des polynômes sur $[a,b]$ est dense dans $(\mathcal{C}^0([a,b],\mathbb{R}), \|.\|_\infty)$.*

3) Intégrales à paramètre

Théorème 41. *Soit $f : \Lambda \times I \to \mathbb{K}$, avec $\Lambda \subset \mathbb{R}$ un intervalle, telle que :*

(i) Pour tout $t \in I$, $\lambda \mapsto f(\lambda, t)$ est continue sur Λ.

(ii) Pour tout $\lambda \in \Lambda$, $t \mapsto f(\lambda, t)$ est intégrable sur I.

(iii) $\exists\, g \in L^1(I, \mathbb{R}^+), \forall \lambda \in \Lambda, |f(\lambda, t)| \leqslant g(t)$ p.p.

Alors $\lambda \mapsto \int_I f(\lambda, t)dt$ est continue sur Λ.

Théorème 42. *Soit $f : \Lambda \times I \to \mathbb{K}$, avec $\Lambda \subset \mathbb{R}$ un intervalle, telle que :*

(i) Pour tout $t \in I$, $\lambda \mapsto f(\lambda, t)$ est dérivable sur Λ.

(ii) Pour tout $\lambda \in \Lambda$, $t \mapsto f(\lambda, t)$ est intégrable sur I.

(iii) $\exists\, g \in L^1(I, \mathbb{R}^+), \forall \lambda \in \Lambda, |f'(\lambda, t)| \leqslant g(t)$ p.p.

Alors $\lambda \mapsto \int_I f(\lambda, t)dt$ est dérivable sur Λ de dérivée $\lambda \mapsto \int_I f'(\lambda, t)dt$.

IV Cas des distributions, dérivée faible

1) Définitions et dérivation faible

Définition 43. Soit $\varphi : \mathbb{R} \to \mathbb{R}$. On appelle support de φ l'adhérence de $\{x \in \mathbb{R} \,|\, \varphi(x) \neq 0\}$. On pose, pour $\Omega \subseteq \mathbb{R}$ ouvert, $\mathcal{D}(\Omega)$ l'ensemble des fonctions de classe $\mathcal{C}^\infty$ sur Ω à support compact.

Définition 44. On dit que $T : \mathcal{D}(\Omega) \to \mathbb{R}$ est une distribution s'il s'agit d'une forme linéaire telle que, pour tout $K \subset \Omega$ compact, on a :

$$\exists p_K \in \mathbb{N},\ \exists C_K > 0,\ \forall \varphi \in \mathcal{D}(\Omega),\ |\langle T, \varphi\rangle| \leqslant C_K \sup_{n \leqslant p_K} \left\|\varphi^{(n)}\right\|_{\infty, K}$$

On note $\mathcal{D}'(\Omega)$ l'ensemble des distributions sur $\mathcal{D}(\Omega)$.

Définition 45. On dit qu'une suite $(T_n)_{n\in\mathbb{N}}$ de distributions sur Ω converge (dans $\mathcal{D}'(\Omega)$) vers $T \in \mathcal{D}'(\Omega)$ si :

$$\forall \varphi \in \mathcal{D}(\Omega),\ \lim_{n\to\infty} \langle T_n, \varphi\rangle = \langle T, \varphi\rangle$$

Proposition 46. *La convergence L^1 sur tout compact est plus forte que la convergence des distributions.*

Définition 47. Pour $T \in \mathcal{D}'(\Omega)$, on note T' la distribution définie par $\langle T', \varphi\rangle = -\langle T, \varphi'\rangle$. On l'appelle la dérivée de T.

Proposition 48. *L'application de dérivation sur $\mathcal{D}'(\Omega)$ est bien définie et est continue : si (T_n) converge vers T, alors $(T_n^{(k)})$ converge vers $T^{(k)}$.*

2) Exemples et lien avec la dérivée usuelle

Proposition 49. *Si f est $\mathcal{C}^1$, f induit $D_f \in \mathcal{D}'$ avec $D_{f'} = (D_f)'$.*

Exemple 50. *Soit $H = \mathbb{1}_{\mathbb{R}^+}$. Alors $H \in L^1_{loc}(\mathbb{R})$ et $D_{H'} = \delta_0$.*

Théorème 51 (Formule des sauts)**.** *Soit f une fonction de classe $\mathcal{C}^1$ par morceaux sur $]a, b[$. Soit a_i les points où f n'est pas $\mathcal{C}^1$. Alors :*

$$D_{f'} = (D_f)' + \sum_{i=1}^{N} \left(\lim_{x\to a_i^+} f(x) - \lim_{x\to a_i^-} f(x)\right) \delta_{a_i}$$

Exemple 52. *La fonction $x \mapsto \ln|x|$ admet comme dérivée au sens des distributions $vp\left(\frac{1}{x}\right)$, définie, pour tout $\varphi \in \mathcal{D}(\mathbb{R})$, par :*

$$\left\langle vp\left(\frac{1}{x}\right), \varphi \right\rangle = \lim_{\varepsilon\to 0^+} \int_{|x|\geqslant\varepsilon} \frac{\varphi(x)}{x}\, dx$$

V Méthode de Newton

La méthode de Newton consiste à approcher une solution d'une équation $f(x) = 0$ en partant d'une approximation plus grossière. L'idée est de remplacer la courbe de f par sa tangente.

Théorème 53 (Méthode de Newton)**.** *Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f : [a, b] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ telle que $f(a) < 0 < f(b)$ et $f' > 0$ sur $[a, b]$. On considère la suite $(x_n)_{n\in\mathbb{N}}$ définie par :*

$$x_0 \in [a, b] \quad et \quad \forall n \in \mathbb{N},\ x_{n+1} = \phi(x_n) = x_n - \frac{f(x_n)}{f'(x_n)}$$

La fonction f admet un unique zéro $\alpha \in]a, b[$, et on a :

(i) Il existe $\varepsilon > 0$ tel que, pour $x_0 \in I =]\alpha - \varepsilon, \alpha + \varepsilon[$, la suite $(x_n)_{n\in\mathbb{N}}$ converge quadratiquement vers α, et il existe $C > 0$ tel que :

$$\forall n \in \mathbb{N},\ |x_{n+1} - \alpha| \leqslant C|x_n - \alpha|^2$$

(ii) Si de plus $f'' > 0$ sur $[\alpha, b]$, alors, pour $x \in]\alpha, b]$, la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante, et pour tout $n \in \mathbb{N}$ on a :

$$0 \leqslant x_{n+1} - \alpha \leqslant C(x_n - \alpha)^2 \quad et \quad x_{n+1} - \alpha \sim \frac{f''(\alpha)}{2f'(\alpha)}(x_n - \alpha)^2$$

Développements

- Théorème de Weierstrass (40) [Gou08]
- Méthode de Newton (53) [Rou15]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Pom97] A. Pommelet. *Cours d'Analyse.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

Cadre : I est un intervalle de $\mathbb{R}$ non réduit à un singleton, et C un convexe d'un espace vectoriel E.

I Fonctions monotones

1) Définition et premières propriétés

Définition 1. Une application $f : D \to \mathbb{R}$, où $D \subseteq \mathbb{R}$, est dite croissante (resp. strictement croissante) lorsque :

$$\forall\, x, y \in D, x < y \Rightarrow f(x) \leqslant f(y) \quad (\text{resp. } x < y \Rightarrow f(x) < f(y))$$

f est dite (strictement) décroissante si $-f$ est (strictement) croissante.
f est dite (strictement) monotone si f est (strictmnt) croissante ou (strictement) décroissante.

Exemple 2. *$x \mapsto \frac{1}{x}$ est décroissante sur $\mathbb{R}^{-\star}$ et $\mathbb{R}^{+\star}$, mais pas sur $\mathbb{R}^{\star}$.*

Proposition 3. *Une application monotone est injective si, et seulement si, elle est strictement monotone.*

Proposition 4. *(i) Le produit d'une application monotone par un scalaire positif est monotone de même variation.*

(ii) La somme de deux applications croissantes est croissante.

(iii) Le produit de deux fonctions croissantes positives est croissant.

(iv) La composée d'applications croissantes ou décroissantes est croissante. La composée d'une application croissante et d'une application décroissante est décroissante.

Remarque 5. *L'ensemble des fonctions monotones n'est pas un espace vectoriel. L'espace engendré par les fonctions monotones est l'espace des fonctions à variations bornées.*

2) Monotonie, limites et continuité

Théorème 6. *Soient $f : D \to \mathbb{R}$ monotone, où $D \subset \mathbb{R}$, et $a \in \overline{\mathbb{R}}$ un point adhérent à $D \cap]a, +\infty[$ (resp. $D \cap]-\infty, a[$). Alors f admet une limite à droite (resp. à gauche) au point a.*

Corollaire 7. *Soient $f : D \to \mathbb{R}$ croissante et $a \in \overline{\mathbb{R}}$ un point adhérent à $D \cap]a, +\infty[$. Alors f admet une limite finie à droite, au point a si, et seulement si, f est minorée sur $D \cap]a, +\infty[$.*

Théorème 8. *Soit $f : I \to \mathbb{R}$ monotone. L'ensemble des points de discontinuité de f est au plus dénombrable.*

Exemple 9. *Posons $u_n(x) = \frac{1}{2^n}\mathbb{1}_{\{\varphi(n)<x\}}$, où φ est une bijection de $\mathbb{N}$ sur $\mathbb{Q} \cap]0, 1[$. Soit $f(x) = \sum_n u_n(x)$. Alors f est strictement croissante sur $[0, 1]$ et discontinue en tout point de $\mathbb{Q} \cap]0, 1[$.*

Théorème 10. *Soit $f : I \to \mathbb{R}$ monotone. f est continue sur I si, et seulement si, $f(I)$ est un intervalle.*

Corollaire 11. *Soit $f : I \to \mathbb{R}$ continue et strictement monotone. Alors $J = f(I)$ est un intervalle et f induit un homéomorphisme de I sur J. Réciproquement, un homéomorphisme entre deux intervalles est une fonction strictement monotone.*

Exemple 12. *La fonction sinus induit un homéomorphisme de $\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$ sur $[-1; 1]$ croissant, dont la réciproque est l'arcsinus.*

3) Monotonie et dérivabilité

Théorème 13. *Soit $f : I \to \mathbb{R}$ continue, et dérivable à droite sur $\mathring{I}$.*

(i) f est constante si, et seulement si : $\forall\, t \in \mathring{I}, f'_d(t) = 0$

(ii) f est croissante si, et seulement si : $\forall\, t \in \mathring{I}, f'_d(t) \geqslant 0$

(iii) f est décroissante si, et seulement si : $\forall\, t \in \mathring{I}, f'_d(t) \leqslant 0$

Théorème 14. *Soit $f : I \to \mathbb{R}$ continue sur I et dérivable à droite sur $\mathring{I}$. f est strictement croissante sur I si, et seulement si, $f'_d \geqslant 0$ et l'ensemble $\left\{t \in \mathring{I} \,\middle|\, f'_d(t) = 0\right\}$ est d'intérieur vide.*

Exemple 15. *$t \mapsto t^3$ est strictement croissante sur $\mathbb{R}$, mais sa dérivée $t \mapsto 3t^2$ s'annule sur $\mathbb{R}$.*

Théorème 16. *Une fonction monotone est dérivable presque partout.*

Remarque 17. *L'escalier de Cantor est une fonction monotone dérivable presque partout, de dérivée nulle presque partout, sans être constante.*

II Fonctions convexes

1) Définition et premières propriétés

Définition 18. On dit que la fonction $f : C \to \mathbb{R}$ est convexe lorsque, pour tous $a, b \in C$ et tout $\lambda \in [0,1]$, on a :

$$f((1-\lambda)a + \lambda b) \leqslant (1-\lambda)f(a) + \lambda f(b)$$

On dit que f concave si $-f$ est convexe. Lorsque l'inégalité est stricte pour $a \neq b$ et $0 < \lambda < 1$, f est strictement convexe. Pour $\alpha > 0$, on dit que f est α-convexe si pour tous $a, b \in C$ distincts et tout $\lambda \in]0,1[$, on a :

$$f((1-\lambda)a + \lambda b) \leqslant (1-\lambda)f(a) + \lambda f(b) - \frac{\alpha}{2}\|a-b\|^2 \lambda(1-\lambda)$$

Remarque 19. *L'α-convexité implique la stricte convexité, qui implique la convexité.*

Remarque 20. *Une fonction $f : C \to \mathbb{R}$ est convexe si l'ensemble $\{(x,y) \in C \times \mathbb{R} \,|\, y \geqslant f(x)\}$ est convexe.*

Exemple 21. *L'application $x \mapsto \|x\|$ est convexe*

Théorème 22. *Une fonction $f : C \to \mathbb{R}$ est convexe si, et seulement si, pour tous $x, y \in C$, $t \mapsto f((1-t)x + ty)$ est convexe sur $[0,1]$.*

Proposition 23. *(i) Une combinaison linéaire à coefficients réels positifs de fonctions convexes est convexe.*

(ii) La composée d'une fonction convexe croissante avec une fonction convexe est convexe.

(iii) Une limite simple de fonctions convexes est convexe.

(iv) Le maximum de deux fonctions convexes est convexe.

Remarque 24. *Le produit de deux fonctions convexes n'est pas nécessairement convexe ($-x \cdot x^2 = x^3$), et leur composition non plus ($(x \mapsto -x) \circ (x \mapsto x^2) = (x \mapsto -x^2)$).*

Proposition 25. *Une fonction convexe $f : I \to \mathbb{R}$ possède en tout point de $\mathring{I}$ une dérivée à droite et une dérivée à gauche. De plus, les applications f'_d et f'_g sont croissantes sur $\mathring{I}$, et $f'_g \leqslant f'_q$.*

Corollaire 26. *Une fonction convexe sur I est continue sur $\mathring{I}$.*

2) Caractérisation des fonctions convexes

En dimension 1

Théorème 27. *Pour $f : I \to \mathbb{R}$, il y a équivalence entre :*

(i) f est convexe sur I.

(ii) Pour $a < b < c$ dans I, on a : $\frac{f(b)-f(a)}{b-a} \leqslant \frac{f(c)-f(a)}{c-a} \leqslant \frac{f(c)-f(b)}{c-b}$

(iii) Pour $a \in I$, la fonction $x \mapsto \frac{f(x)-f(a)}{x-a}$ est croissante sur $I \setminus \{a\}$.

Corollaire 28. *Une fonction de $\mathbb{R}$ dans $\mathbb{R}$ est affine si, et seulement si, elle est convexe et concave.*

Théorème 29. *Soit $f : I \to \mathbb{R}$ dérivable. Il y a équivalence entre :*

(i) f est (strictement) convexe sur I.

(ii) La fonction dérivée f' est (strictement) croissante.

(iii) La courbe représentative de f est située (strictement) au-dessus de sa tangente en tout point de I.

Proposition 30. *Si f est deux fois dérivable sur I, elle est alors convexe si, et seulement si, $f'' \geqslant 0$.*

En dimension $n \geqslant 1$

Théorème 31. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*

(i) J est convexe sur C.

(ii) $\forall\, x, y \in C,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geqslant 0$.

(iii) $\forall\, x, y \in C,\ J(x) \geqslant J(y) + \langle \nabla J(y), x - y\rangle$.

Si J est deux fois différentiable, on a aussi : $\left\langle d^2J(x)\cdot y, y\right\rangle \geqslant 0$.

Théorème 32. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*

(i) J est α-convexe sur C.

(ii) $\forall\, x, y \in C,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geqslant \alpha\|x-y\|^2$.

(iii) $\forall\, x, y \in C,\ J(x) \geqslant J(y) + \langle \nabla J(y), x - y\rangle + \frac{\alpha}{2}\|x-y\|^2$.

Si J est deux fois différentiable, on a aussi : $\left\langle d^2J(x)\cdot y, y\right\rangle \geqslant \alpha\|y\|^2$.

Exemple 33. *Si A est une matrice symétrique définie positive, alors la fonctionnelle quadratique $J : X \mapsto \langle AX, X\rangle - \langle B, X\rangle$ est λ_1-convexe, où λ_1 est la plus petite valeur propre de A.*

III Applications

1) Inégalité de convexité

Proposition 34. *Soient $n \in \mathbb{N}^\star$ et $a_1, \dots, a_n \in \mathbb{R}^+$, alors :*

$$\sqrt[n]{\prod_{i=1}^{n} a_i} \leqslant \frac{1}{n} \sum_{i=1}^{n} a_i$$

Il y a égalité si, et seulement si, tous les a_i sont égaux.

Proposition 35 (Young)**.** *Soient $p, q > 0$ tels que $\frac{1}{p} + \frac{1}{q} = 1$ et $a, b \in \mathbb{R}^+$:*

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

Il y a égalité si, et seulement si, $a^p = b^q$.

Corollaire 36 (Hölder et Minkowski)**.** *Soient $p, q > 0$ tels que $\frac{1}{p} + \frac{1}{q} = 1$ et $a, b \in \mathbb{R}^+$ et $f, g : E \to \mathbb{K}$ mesurables, alors :*

$$\|fg\|_1 \leqslant \|f\|_p \|g\|_q \quad \text{et} \quad \|f+g\|_p \leqslant \|f\|_p + \|g\|_p$$

Lemme 37. *Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ symétriques définies positives distinctes, et $\alpha, \beta > 0$ tels que $\alpha + \beta = 1$, alors :*

$$\det(\alpha A + \beta B) > \det(A)^\alpha \det(B)^\beta$$

Application 38 (Ellipsoïde de John-Loewner)**.** *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant K.*

2) Optimisation

Théorème 39. *Si $J : C \to \mathbb{R}$ est différentiable en $u \in C$ et admet un minimum local en u, alors :*

$$\forall\, v \in C,\ \langle \nabla J(u), v - u \rangle \geqslant 0$$

Théorème 40. *On considère $J : C \to \mathbb{R}$.*

(i) Si J est convexe, tout minimum local est global.

(ii) Si J est strictement convexe, J admet au plus un minimum global.

(iii) Si J est α-convexe, J admet un unique minimum global.

(iv) Si J est définie sur un ouvert contenant C et différentiable en $u \in C$, alors le théorème précédent donne en fait une équivalence.

(v) Si C est ouvert, le théorème précédent équivaut à $\nabla J(u) = 0$.

3) Méthodes de gradient

Soit $J : \mathbb{R}^n \to \mathbb{R}$. On suppose J différentiable. On cherche, s'il existe, un élément $u \in \mathbb{R}^n$ tel que :

$$J(u) = \inf_{v \in \mathbb{R}^n} J(v)$$

Pour cela, on utilise les méthodes de gradient. On considère la suite :

$$u_0 \in \mathbb{R}^n \quad \text{et} \quad \forall\, k \in \mathbb{N},\ u^{k+1} = u^k - \rho^k \nabla J(u^k)$$

Il existe plusieurs possibilités pour choisir les ρ^k, par exemple :

(i) Gradient à pas fixe : $\rho^k = \rho$ une constante positive fixée.

(ii) Gradient à pas optimal : ρ^k minimise $\rho \mapsto J\left(u^k - \rho \nabla J(u^k)\right)$.

Théorème 41. *Si J est α-convexe et différentiable, et que ∇J est L-lipschitzienne, alors la méthode de gradient à pas optimal converge vers l'unique minimum de J.*

Développements

- Ellipsoïde de John-Loewner (37,38) [FGN13c]
- Algorithme de gradient à pas optimal (41) [Cia88]

Références

[RDO91] E. Ramis, C. Deschamps, et J. Odoux. *Cours de Mathématiques, Topologie et éléments d'analyse.* Masson

[Rom19] J.-E. Rombaldi. *Éléments d'analyse réelle.* EDP Sciences

[Hau07] B. Hauchecorne. *Les Contre-exemples en Mathématiques.* Ellipses

[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3.* Cassini

[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

Annexes

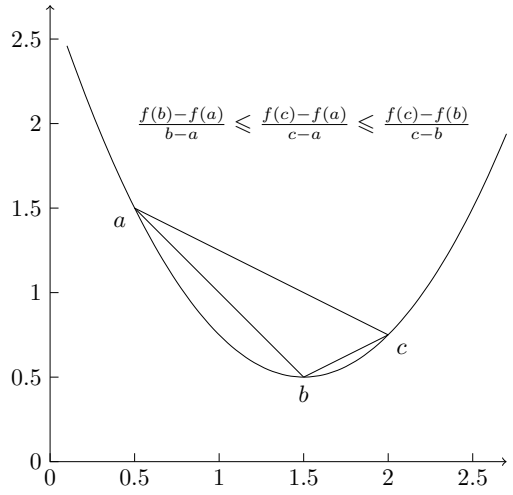


FIGURE 1 – Inégalité des trois pentes

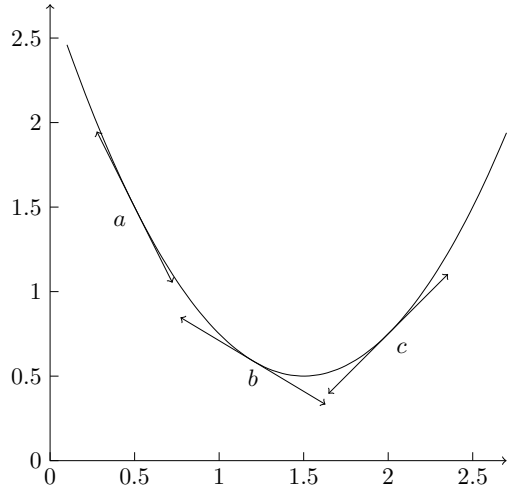


FIGURE 2 – Tangentes d'une fonction convexe

Cadre : Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soient $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ deux suites de $\mathbb{K}$.

I Convergence des séries numériques

Définition 1. On appelle série de terme général u_n la suite $(S_n)_{n\in\mathbb{N}}$ des sommes partielles définie par $S_n = \sum_{k=0}^{n} u_k$. On note $\sum u_n$ cette suite. On note $R_n = \sum_{k=0}^{\infty} u_k - S_n = \sum_{k=n+1}^{\infty} u_k$ le reste de la série à l'ordre n.

Définition 2. On dit que la série $\sum u_n$ converge lorsque la suite $(S_n)_{n\in\mathbb{N}}$ converge. Dans ce cas, sa limite est appelée somme et notée $\sum_{n=0}^{\infty} u_n$, $\sum_{n\in\mathbb{N}} u_n$ ou $\sum_{n\geqslant 0} u_n$. Une série non convergente est divergente.

Exemple 3. *Si $u_n = q^n$ est une suite géométrique ($q \neq 1$), on a $S_n = \frac{1-q^{n+1}}{1-q}$. Donc la série $\sum u_n$ converge si, et seulement si, $|q| < 1$, et alors sa somme est $\frac{1}{1-q}$.*

Proposition 4. *Si la série $\sum u_n$ converge, alors $\lim_{n\to\infty} R_n = 0$.*

Théorème 5. *L'ensemble des séries numériques est un $\mathbb{K}$-espace vectoriel, dont l'ensemble des séries convergente est un sous-espace vectoriel.*

Remarque 6. *La somme d'une série convergente et d'une série divergente est divergente. On ne peut en revanche rien dire de la convergence d'une somme de séries divergentes.*

Exemple 7. $\sum(-1)^n + \sum(-1)^{n+1} = 0$.

Proposition 8. *Le terme général d'une série convergente converge vers 0, mais la réciproque est fausse.*

Exemple 9. *$\sum \frac{1}{n}$ diverge, mais $\lim_{n\to\infty} \frac{1}{n} = 0$.*

Remarque 10. *Si u_n ne converge pas vers 0, on parlera de série grossièrement divergente.*

Définition 11. On dit que la série $\sum u_n$ est télescopique s'il existe une suite $(a_n)_{n\in\mathbb{N}}$ telle que $u_n = a_n - a_{n-1}$. On a alors $\sum_{k=0}^{n} = a_n - a_0$.

Exemple 12. *La série de terme général $\frac{1}{\sqrt{n+1}+\sqrt{n}}$ diverge, la série de terme général $\frac{1}{n(n-1)}$ converge.*

II Séries à termes positifs

On suppose que $\sum u_n$ et $\sum v_n$ sont des séries à terme général positif.

1) Comparaison

Proposition 13. *Une série à termes positifs converge si, et seulement si, la suite des sommes partielles est majorée. Si la série diverge, c'est vers $+\infty$.*

Théorème 14. *Soit $\alpha \in \mathbb{R}$. $\sum \frac{1}{n^\alpha}$ converge si, et seulement si, $\alpha > 1$.*

Théorème 15. *Si $u_n \leqslant v_n$ pour tout $n \in \mathbb{N}$, alors :*

(i) Si $\sum v_n$ converge, alors $\sum u_n$ converge et $\sum_{n=0}^{\infty} u_n \leqslant \sum_{n=0}^{\infty} v_n$.

(ii) Si $\sum u_n$ diverge, alors $\sum v_n$ diverge également.

Exemple 16. *Comme $\frac{1}{n(n-1)}$ est le terme général d'une série convergente, la suite $\frac{1}{n^2}$ est le terme général d'une série convergente.*

Exemple 17. *$\frac{1}{\sqrt{n}} \geqslant \frac{1}{n}$ donne que $\sum \frac{1}{\sqrt{n}}$ est divergente.*

Théorème 18. *Soit $f : \mathbb{R}^+ \to \mathbb{R}^+$ une fonction décroissante continue par morceaux. Alors la série de terme général $\int_{n-1}^{n} f(t)\,dt - f(n)$ converge. En particulier, $\sum f(n)$ et $\left(\int_0^n f(t)\,dt\right)_{n\in\mathbb{N}}$ ont même nature, et on a :*

(i) Si $\sum f(n)$ converge, alors $\int_{n+1}^{\infty} f(t)\,dt \leqslant \sum_{k\geqslant n} f(k) \leqslant \int_n^{\infty} f(t)\,dt$.

(ii) Si $\sum f(n)$ diverge, alors $\sum_{k\geqslant n} f(k) \sim \int_0^n f(t)\,dt$.

Application 19. *Soient $\alpha, \beta \in \mathbb{R}$. Alors $\sum \frac{1}{n^\alpha \ln(n)^\beta}$ converge si, et seulement si, $\alpha > 1$ ou $(\alpha = 1, \beta > 1)$.*

Théorème 20. *Notons $S_n(u)$, $R_n(u)$ (resp. $S_n(v)$, $R_n(v)$) les sommes partielles et restes associés à u (resp. v). Alors :*

	$\sum_{n\in\mathbb{N}} v_n < \infty$	$\sum_{n\in\mathbb{N}} v_n = \infty$
$u_n = o(v_n)$	$R_n(u) = o(R_n(v))$	$S_n(u) = o(S_n(v))$
$u_n = \mathcal{O}(v_n)$	$R_n(u) = \mathcal{O}(R_n(v))$	$S_n(u) = \mathcal{O}(S_n(v))$
$u_n \sim v_n$	$R_n(u) \sim R_n(v)$	$S_n(u) \sim S_n(v)$

2) Critères de convergence

Théorème 21 (Règle de Cauchy)**.** *On pose* $L = \limsup_{n\to\infty} \sqrt[n]{u_n}$.
(i) Si $L < 1$*, alors* $\sum u_n$ *converge absolument.*
(ii) Si $L > 1$*, alors* $\sum u_n$ *diverge.*

Exemple 22. *La série* $\sum \left(1 - \frac{1}{n}\right)^{n^2}$ *converge.*

Théorème 23 (Règle de d'Alembert)**.** *Supposons* u_n *non nul à partir d'un certain rang. On pose* $\ell = \liminf_{n\to\infty} \frac{u_{n+1}}{u_n}$ *et* $L = \limsup_{n\to\infty} \frac{u_{n+1}}{u_n}$.
(i) Si $L < 1$*, alors* $\sum u_n$ *converge absolument.*
(ii) Si $\ell > 1$*, alors* $\sum u_n$ *diverge.*

Exemple 24. *Pour* $a > 0$*, on a* $\lim_{n\to+\infty} \frac{a^{n+1}}{n+1} \times \frac{n}{a^n} = \lim_{n\to+\infty} \frac{na}{n+1} = a$*, donc la série de terme général* $\frac{a^n}{n}$ *converge si* $a < 1$ *et diverge si* $a > 1$.

Théorème 25 (Règle de Raab-Duhamel)**.** *Supposons* u_n *non nul à partir d'un certain rang. Si* $\frac{u_{n+1}}{u_n} = \frac{1}{1+\frac{a}{n}+\mathcal{O}\left(\frac{1}{n^2}\right)}$*, il existe* $\lambda > 0$ *tel que* $u_n \sim \frac{\lambda}{n^a}$.

III Séries à termes quelconques

1) Absolue convergence

Définition 26. On dit que $\sum u_n$ est absolument convergente si $\sum |u_n|$ est convergente. Une série convergente et non absolument convergente est dite semi-convergente.

Théorème 27 (Riemann)**.** *Soit* $\sum u_n$ *une série réelle semi-convergente et* $\alpha \in \mathbb{R}$*. Il existe une permutation* σ *de* $\mathbb{N}$ *telle que la série* $\sum u_{\sigma(n)}$ *soit convergente de somme* α.

Proposition 28. *Soit* $\sum u_n$ *une série absolument convergente. Pour toute permutation* σ *de* $\mathbb{N}$*, on a* $\sum_{n\in\mathbb{N}} u_{\sigma(n)} = \sum_{n\in\mathbb{N}} u_n$.

Proposition 29. $\left|\sum_{n\in\mathbb{N}} u_n\right| \leqslant \sum_{n\in\mathbb{N}} |u_n|$

Proposition 30 (Produit de Cauchy)**.** *Si* $\sum u_n$ *et* $\sum v_n$ *sont absolument convergentes, alors la série de terme général* $w_n = \sum_{k=0}^{n} u_k\, v_{n-k}$ *est absolument convergente, et on a :*

$$\left(\sum_{n\in\mathbb{N}} u_n\right)\left(\sum_{n\in\mathbb{N}} v_n\right) = \sum_{n\in\mathbb{N}} w_n$$

Application 31. $\exp : \mathbb{C} \to \mathbb{C}^\star$ *est un morphisme de groupes.*

2) Séries alternées

On suppose que pour tout $n \in \mathbb{N}$, $u_n \geqslant 0$.

Définition 32. Les séries alternées sont des séries de la forme $\sum (-1)^n u_n$.

Proposition 33. *Si la suite* $(u_n)_{n\in\mathbb{N}}$ *est décroissante et converge vers 0, alors la série alternée converge, et on a* $|R_n| < a_{n+1}$ *pour tout* $n \in \mathbb{N}$.

Exemple 34. *En prenant* $u_n = \frac{1}{n}$*, la série alternée* $\sum \frac{(-1)^n}{n}$ *converge.*

Application 35. $\sum_{n=1}^{\infty} (-1)^n \frac{\ln n}{n} = \gamma \ln 2 - \frac{\ln(2)^2}{2}$

Proposition 36 (Abel)**.** *Supposons que* $u_n = a_n v_n$*, où* $(a_n)_{n\in\mathbb{N}}$ *est une suite décroissante de réels positifs tendant vers 0 et* v_n *est le terme général d'une série bornée (c'est-à-dire telle que la suite* $(\sum_{k=0}^{n} v_n)_{n\in\mathbb{N}}$ *est bornée). Alors* $\sum u_n$ *est convergente.*

Exemple 37. *La série de terme général* $\frac{e^{in\theta}}{n^\alpha}$*, où* $\theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$*, est convergente pour* $\alpha > 0$.

IV Séries entières

Définition 38. On appelle série entière toute série de fonctions de la forme $\sum_{n\geqslant 0} a_n z^n$ où z est une variable complexe, et $a_n \in \mathbb{C}$.

Définition 39. Soit $\sum a_n z^n$ une série entière. On appelle rayon de convergence de $\sum a_n z^n$ le réel R défini par :

$$R = \sup\left\{r \in \mathbb{R}^+ \,\middle|\, \exists M \in \mathbb{R}, \forall n \in \mathbb{N}, |a_n| r^n \leqslant M\right\}$$

Théorème 40 (Abel angulaire)**.** *Soit* $\sum a_n z^n$ *une série entière de rayon de convergence 1 telle que* $\sum a_n$ *converge. On note* f *sa somme et :*

$$\Delta_\theta = \left\{z \in \mathbb{C} \,\middle|\, 1 - z = \rho e^{i\varphi},\ \rho > 0,\ |\varphi| < \theta\right\} \quad \textit{pour} \quad 0 \leqslant \theta < \frac{\pi}{2}$$

Alors :

$$\lim_{\substack{z\to 1 \\ z\in\Delta_\theta}} f(z) = \sum_{n\geqslant 0} a_n$$

Application 41. $\sum_{n\geqslant 0} \frac{(-1)^n}{2n+1} = \arctan(1) = \frac{\pi}{4}$ *et* $\sum_{n\geqslant 1} \frac{(-1)^n}{n} = \ln(2)$

Théorème 42 (Taubérien faible)**.** *Soit f la somme d'une série entière $\sum a_n z^n$ de rayon de convergence 1. On suppose que $\lim_{x\to 1^-} f(z) = \ell$ existe, et $a_n = o\left(\frac{1}{n}\right)$. Alors $\sum a_n$ converge et $\ell = \sum_{n\geqslant 0} a_n$.*

Application 43 (Nombres de Catalan)**.** *On note C_n le nombre de parenthésages possibles d'un produit de $n+1$ facteurs. On a alors la relation $C_n = \sum_{k=1}^{n-1} C_k C_{n-k}$, et on obtient $C_n = \frac{1}{n+1}\binom{2n}{n}$.*

Application 44 (Nombres de Bell)**.** *Pour $n \in \mathbb{N}^\star$, on pose B_n le nombre de partitions de l'ensemble $[\![1, n]\!]$ avec la convention $B_0 = 1$, alors :*

$$\forall\, k \in \mathbb{N},\ B_k = \frac{1}{e} \sum_{n\geqslant 0} \frac{n^k}{n}$$

Développements

— Théorèmes d'Abel angulaire et taubérien faible (40,42) [Gou08]
— Nombres de Bell (44) [FGN13a]

Références

[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions.* Ellipses
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[FGN13d] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 1.* Cassini
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Cadre : Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $n \in \mathbb{N}^\star$.

I Éléments d'analyse matricielle

1) Norme matricielle

Définition 1. On appelle norme matricielle toute norme sur l'espace $\mathcal{M}_n(\mathbb{K})$. On dit qu'une norme matricielle est sous-multiplicative lorsque, pour tous $A, B \in \mathcal{M}_n(\mathbb{K})$, on a $\|AB\| \leqslant \|A\| \, \|B\|$.

Définition 2. Soit $\|.\|$ une norme vectorielle sur $\mathbb{K}^n$. L'application $|||.||| : \mathcal{M}_n(\mathbb{K}) \to \mathbb{R}$ définie pour $A \in \mathcal{M}_n(\mathbb{K})$ par :

$$|||A||| = \sup_{\substack{v \in \mathbb{K}^n \\ v \neq 0}} \frac{\|Av\|}{v} = \sup_{\substack{v \in \mathbb{K}^n \\ \|v\| \leqslant 1}} \frac{\|Av\|}{v} = \sup_{\substack{v \in \mathbb{K}^n \\ \|v\| 11}} \|Av\|$$

est une norme matricielle multiplicative,dite subordonnée à la norme $\|.\|$.

Proposition 3. *Soit $|||.|||$ une norme matricielle subordonnée à la norme $\|.\|$. Pour tout $v \in \mathbb{K}^n$ et tout $A \in \mathcal{M}_n(\mathbb{K})$, on a $\|Av\| \leqslant |||A||| \, \|v\|$.*

Définition 4. Pour $p \in [1, +\infty]$, on définit la norme $\|.\|_p$ par :

$$\|v\|_p = \left(\sum_{i=1}^{n} |v_i|^p \right)^{\frac{1}{p}} \text{ si } p < +\infty \quad \text{et} \quad \|v\|_\infty = \max_{1 \leqslant i \leqslant n} |v_i|$$

On notera $|||.|||_p$ la norme matricielle subordonnée associée.

Proposition 5. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors :*

(i) Pour toute norme subordonnée $|||.|||$, on a $|||I_n||| = 1$.

(ii) $|||A|||_1 = \max_{1 \leqslant j \leqslant n} \sum_{i=1}^{n} |a_{i,j}|$

(iii) $|||A|||_\infty = \max_{1 \leqslant i \leqslant n} \sum_{j=1}^{n} |a_{i,j}|$

Contre-exemple 6. *La norme $A \mapsto \sqrt{A^\star A}$ n'est pas subordonnée.*

Proposition 7. *Soit $|||.|||$ une norme subordonnée et $B \in \mathcal{M}_n(\mathbb{K})$ telle que $|||B||| \leqslant 1$. Alors $I_n + B$ est inversible et $\left|\left|\left|(I+B)^{-1}\right|\right|\right| = \frac{1}{1-|||B|||}$.*

2) Rayon spectral

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

Définition 8. On note $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ les valeurs propres de A. On définit le rayon spectral de A par $\rho(A) = \max_{1 \leqslant i \leqslant n} |\lambda_i|$.

Exemple 9. *Si* $A = \begin{pmatrix} 2 & 0 & 4 \\ 3 & -4 & 12 \\ 1 & -2 & 5 \end{pmatrix}$, *on a* $\rho(A) = 2$.

Proposition 10. *On a* $|||A|||_2 = \sqrt{\rho(A^\star A)} = \sqrt{\rho(AA^\star)}$. *De plus, si U est unitaire, alors* $|||A|||_2 = |||UA|||_2 = |||AU|||_2 = |||U^\star AU|||_2$. *Enfin, si A est normale, alors* $|||A|||_2 = \rho(A)$.

Exemple 11. *Si $U \in \mathcal{M}_n(\mathbb{K})$ est unitaire, on a* $|||U|||_2 = 1$.

Théorème 12. *Pour toute norme matricielle $|||.|||$, on a $\rho(A) \leqslant |||A|||$.*

Théorème 13. *Les assertions suivantes sont équivalentes :*

(i) $\lim_{k \to +\infty} A^k = 0$ *(iii)* $\rho(A) < 1$

(ii) $\forall \, v \in \mathbb{K}^n$, $\lim_{k \to +\infty} A^k v = 0$ *(iv)* $\sum_{k=0}^{\infty} A^k$ *converge.*

(v) Il existe une norme subordonnée telle que $|||A||| < 1$.

Dans ce cas, on a $(I_n - A)^{-1} = \sum_{k=0}^{\infty} A^k$.

3) Conditionnement

Soit $A \in \mathcal{GL}_n(\mathbb{K})$. Soit $|||.|||$ une norme matricielle subordonnée à $\|.\|$.

Proposition 14. *Soient $b \in \mathbb{K}^n \setminus \{0\}$ et $x \in \mathbb{K}^n$ la solution de $Ax = b$. Pour une perturbation δb de b, $x + \delta x$ désigne la solution de $A(x + \delta x) = b + \delta b$. Alors :*

$$\frac{\|\delta x\|}{\|x\|} \leqslant \left|\left|\left|A^{-1}\right|\right|\right| \, |||A||| \, \frac{\|\delta b\|}{\|b\|}$$

Définition 15. On appelle conditionnement de A relativement $|||.|||$ le nombre $\text{cond}(A) = \left|\left|\left|A^{-1}\right|\right|\right| \, |||A|||$. Lorsque $|||.||| = |||.|||_p$, on note $\text{cond}_p(A)$.

Exemple 16. *Si A est unitaire,* $\text{cond}_2(A) = 1$.

Proposition 17. *Soit $\alpha \in \mathbb{K}^\star$. Alors :*

(i) $\text{cond}(A) = \text{cond}(A^{-1})$ *(iii)* $\text{cond}(A) \geqslant 1$

(ii) $\text{cond}(I_n) = 1$ *(iv)* $\text{cond}(\alpha A) = \text{cond}(A)$

Proposition 18. *Si A est hermitienne,* $\text{cond}_2(A) = \frac{\max_{\lambda \in \text{Sp}(A)} |\lambda|}{\min_{\lambda \in \text{Sp}(A)} |\lambda|}$.

II Systèmes linéaires : méthodes directes

1) Méthode de Gauss

Méthode 19 (Gauss). *On souhaite résoudre le système $Ax = b$, où $A \in \mathcal{GL}_n(\mathbb{K})$ et $b \in \mathbb{K}^n$.*

(i) Processus d'élimination, qui équivaut à déterminer $M \in \mathcal{GL}_n(\mathbb{K})$ telle que MA soit triangulaire supérieure.

(ii) On calcule simultanément le vecteur Mb.

(iii) On résout le système $MAx = MB$.

Remarque 20. *En pratique, on ne calcule pas M, mais MA et Mb.*

Exemple 21. *Pour* $A = \begin{pmatrix} 5 & 2 & 1 \\ 5 & -6 & 2 \\ -4 & 2 & 1 \end{pmatrix}$ *et* $b = {}^{t}(12\ -1\ 3)$, *on trouve* $MA = \begin{pmatrix} 5 & 2 & 1 \\ 0 & -8 & 1 \\ 0 & 0 & \frac{9}{4} \end{pmatrix}$ *et* $Mb = {}^{t}(12\ -13\ \frac{27}{4})$.

Théorème 22. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. Il existe au moins une matrice $M \in \mathcal{GL}_n(\mathbb{K})$ telle que MA soit triangulaire supérieure.*

Corollaire 23. *Pour $A \in \mathcal{GL}_n(\mathbb{K})$ et $b \in \mathbb{K}^n$, il existe une matrice M telle que l'on puisse résoudre le système $MAx = Mb$ par une méthode de remontée.*

2) Factorisation LU

Théorème 24. *Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{K})$ telle que les n sous-matrices diagonales $\Delta_k = (a_{i,j})_{1 \leqslant i,j \leqslant k} \in \mathcal{M}_k(\mathbb{K})$ soient inversibles. Alors il existe une matrice triangulaire inférieure L dont les termes diagonaux valent 1 et une matrice triangulaire supérieure U telles que $A = LU$. Cette factorisation est unique.*

Exemple 25. $\begin{pmatrix} 5 & 2 & 1 \\ 5 & -6 & 2 \\ -4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -\frac{4}{5} & -\frac{9}{20} & 1 \end{pmatrix} \begin{pmatrix} 5 & 2 & 1 \\ 0 & -8 & 1 \\ 0 & 0 & \frac{9}{4} \end{pmatrix}$

Méthode 26. *On souhaite résoudre le système $Ax = b$, où $A \in \mathcal{GL}_n(\mathbb{K})$ et $b \in \mathbb{K}^n$, grâce à la factorisation LU.*

(i) Écrire $A = LU$.

(ii) Trouver $y \in \mathbb{K}^n$ tel que $Ly = b$.

(iii) Trouver $x \in \mathbb{K}^n$ tel que $Ux = y$.

Exemple 27. *Pour* $A = \begin{pmatrix} 5 & 2 & 1 \\ 5 & -6 & 2 \\ -4 & 2 & 1 \end{pmatrix}$ *et* $b = {}^{t}(12\ -1\ 3)$, *on trouve* $y = {}^{t}(12\ 11\ \frac{351}{20})$ *et* $x = {}^{t}(1\ 2\ 3)$.

III Systèmes linéaires : méthodes itératives

1) Généralités et notions de convergence

Méthode 28. *On cherche à approximer la solution x du système $Ax = b$, où $A \in \mathcal{GL}_n(\mathbb{K})$ et $b \in \mathbb{K}^n$. On pose pour cela $A = M - N$, où $M \in \mathcal{GL}_n(\mathbb{K})$ est facile à inverser (diagonale, triangulaire, orthogonale...). On obtient la méthode itérative :*

$$x^{(k+1)} = M^{-1}Nx^{(k)} + M^{-1}b = F(x^{(k)}) \qquad \text{(M)}$$

Si la suite $(x^{(k)})_{k \in \mathbb{N}}$ converge vers x^{∞}, alors x^{∞} est solution de $Ax = b$. De plus, x^{∞} est un point fixe de F.

Définition 29. Soient $A = M - N$ et $\|.\|$ une norme sur $\mathbb{K}^n$. La méthode itérative (M) est dite convergente lorsque :

$$\forall\, b \in \mathbb{K}^n,\ \forall\, x^{(0)} \in \mathbb{K}^n,\ \lim_{k \to \infty} \left\| x^{(k)} - x \right\| = 0$$

Remarque 30. *En posant $e^{(k)} = x^{(k)} - x$ et $B = M^{-1}N$, on a $e^{(k+1)} = Be^{(k)}$, et la méthode itérative (M) converge ainsi lorsque, par exemple, $\rho(B) < 1$.*

2) Méthode de Jacobi

Définition 31. On considère la décomposition $A = M - N$, avec $M = D$ et $N = E + F$, où les matrices D, E, F sont définies comme suit :

$$\begin{cases} (D)_{i,j} = a_{i,j} \text{ si } i = j,\ 0 \text{ sinon} \\ (-E)_{i,j} = a_{i,j} \text{ si } i > j,\ 0 \text{ sinon} \\ (-F)_{i,j} = a_{i,j} \text{ si } i < j,\ 0 \text{ sinon} \end{cases} \qquad A = \begin{pmatrix} & & -F \\ & D & \\ -E & & \end{pmatrix}$$

On appelle matrice de Jacobi la matrice $J = M^{-1}N$ obtenue à partir de la décomposition précédente : $J = D^{-1}(E + F) = I_n - D^{-1}A$.

Remarque 32. *La méthode itérative (M) devient alors :*

$$Dx^{(k+1)} = (E + F)x^{(k)} + b \qquad \text{(J)}$$

Théorème 33. *Si la matrice A est à diagonale strictement dominante, alors la méthode de Jacobi converge.*

Exemple 34. *Si* $A = \begin{pmatrix} 1 & a & a \\ a & 1 & a \\ a & a & 1 \end{pmatrix}$, *la méthode de Jacobi converge si* $|a| < \frac{1}{2}$.

3) Méthode de gradient

Caractérisation de l'α-convexité

Définition 35. Pour $\alpha > 0$, on dit que la fonction $f : C \to \mathbb{R}$ est α-convexe si pour tous $a, b \in C$ distincts et tout $\lambda \in]0,1[$, on a :

$$f((1-\lambda)a + \lambda b) \leqslant (1-\lambda)f(a) + \lambda f(b) - \frac{\alpha}{2}\|a-b\|^2 \lambda(1-\lambda)$$

Théorème 36. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*

(i) J *est α-convexe sur C.*

(ii) $\forall x, y \in C,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geqslant \alpha \|x-y\|^2$.

(iii) $\forall x, y \in C,\ J(x) \geqslant J(y) + \langle \nabla J(y), x-y\rangle + \frac{\alpha}{2}\|x-y\|^2$.

Si J est deux fois différentiable, on a aussi : $\left\langle d^2J(x)\cdot y, y\right\rangle \geqslant \alpha\|y\|^2$.

Méthode de gradient

Soit $J : \mathbb{R}^n \to \mathbb{R}$. On suppose J différentiable. On cherche, s'il existe, un élément $u \in \mathbb{R}^n$ tel que :

$$J(u) = \inf_{v \in \mathbb{R}^n} J(v)$$

Pour cela, on utilise les méthodes de gradient. On considère la suite :

$$u_0 \in \mathbb{R}^n \quad \text{et} \quad \forall k \in \mathbb{N},\ u^{k+1} = u^k - \rho^k \nabla J(u^k)$$

Il existe plusieurs possibilités pour choisir les ρ^k, par exemple :

(i) Gradient à pas fixe : $\rho^k = \rho$ une constante positive fixée.

(ii) Gradient à pas optimal : ρ^k minimise $\rho \mapsto J\left(u^k - \rho \nabla J(u^k)\right)$.

Théorème 37. *Si J est α-convexe et différentiable, et que ∇J est L-lipschitzienne, alors la méthode de gradient à pas optimal converge vers l'unique minimum de J.*

Application 38. *Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. On considère la fonctionnelle quadratique $J : \mathbb{R}^n \to \mathbb{R}$ définie par :*

$$J(X) = \langle AX, X\rangle - \langle b, X\rangle + c$$

Cette fonctionnelle satisfait les conditions du théorème précédent. De plus, son minimum est atteint en $X_0 \in \mathbb{R}^n$ qui vérifie $\nabla J(X_0) = AX - b = 0$. On a donc une méthode itérative pour approcher la solution de $AX = b$.

IV Recherche d'éléments propres

1) Localisation des valeurs propres

Définition 39. Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{C})$. Le i-ième disque de Gerschgorin est le disque fermé de centre $a_{i,j}$ et de rayon $r_i = \sum_{j=1}^n \sum_{i \neq j} |a_{i,j}|$.

Théorème 40. *Les valeurs propres d'une matrice complexe sont situées dans la réunion des disques de Gerschgorin.*

2) Méthode QR

Théorème 41. *Soit $A \in \mathcal{GL}_n(\mathbb{K})$. Il existe une matrice unitaire Q et une matrice triangulaire supérieure R telles que $A = QR$. De plus, on peut s'arranger pour que les éléments diagonaux de R soient des réels strictement positifs. La factorisation QR correspondante est alors unique. Cette factorisation forme un homéomorphisme $\mathcal{U}_n(C) \times T_n^+(\mathbb{C}) \to \mathcal{GL}_n(\mathbb{C})$.*

Théorème 42 (Méthode QR)**.** *Soit $A \in \mathcal{GL}_n(\mathbb{K})$ diagonalisable. On suppose que ses valeurs propres sont de modules distincts et on les classe par modules décroissants : $|\lambda_1| > |\lambda_2| > \ldots > |\lambda_n|$. On construit la suite :*

$$\begin{cases} A_0 = A \\ A_{k+1} = R_k Q_k \text{ où } A_k = Q_k R_k \text{ est la décomposition } QR \text{ de } A_k \end{cases}$$

On suppose qu'il existe $P \in \mathcal{GL}_n(\mathbb{K})$ tel que $A = P\,\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)P^{-1}$ et P^{-1} admet une décomposition LU. Alors la diagonale de A_k converge vers $\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$, et les coefficients sous la diagonale tendent vers 0.

Développements

— Algorithme de gradient à pas optimal (37) [Cia88]

— Méthode QR (42) [Cia88]

Références

[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

[All12] G. Allaire. *Analyse numérique et optimisation.* Éditions de l'École Polytechnique

Cadre : Soient $(X, \mathcal{A}, \mu)$ un espace mesuré, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $p \in [1, +\infty]$ et q son exposant conjugué tel que $\frac{1}{p} + \frac{1}{q} = 1$.

I Construction de l'intégrale de Lebesgue

1) Intégrale de fonctions étagées

Définition 1. Une fonction $f : X \to \mathbb{K}$ est dite étagée si elle est mesurable et ne prend qu'un nombre fini de valeurs.

Remarque 2. *Les fonctions étagée sont les fonctions de la forme :*

$$f = \sum_{i \in I} \alpha_i \mathbb{1}_{A_i} \text{ avec } I \text{ fini, } \alpha_i \in \mathbb{K}, (A_i)_{i \in I} \text{ partition } \mathcal{A}\text{-mesurable de } X$$

Définition 3. Soit $f : X \to \mathbb{K}$ une fonction étagée. L'intégrale de f par rapport à la mesure μ est définie par :

$$\int_X f \, d\mu = \sum_{\alpha \in f(X)} \alpha \, \mu(\{f = \alpha\}) \in \overline{\mathbb{R}^+}$$

Proposition 4. *Soit $f : X \to \mathbb{K}$ une fonction étagée. Pour toute décomposition de la forme $f = \sum_{i \in I} \alpha_i \mathbb{1}_{A_i}$, on a :*

$$\int_X f \, d\mu = \sum_{i \in I} \alpha_i \, \mu(A_i)$$

Remarque 5. *On a :* $\int_X f \, d\mu < \infty \Leftrightarrow \mu(\{f \neq 0\}) < \infty$.

Proposition 6. *L'intégrale des fonctions étagées positives est additive, croissante et homogène positive.*

Proposition 7. *Soient $A, B \in \mathcal{A}$, f étagée positive. On pose :*

$$\int_A f \, d\mu = \int_X \mathbb{1}_A f \, d\mu$$

Si A et B sont disjoints, on a alors :

$$\int_{A \cup B} f \, d\mu = \int_A f \, d\mu + \int_B f \, d\mu$$

Proposition 8. *Soit $(E_n)_{n \geqslant 1}$ une suite croissante d'éléments de $\mathcal{A}$ telle que $X = \bigcup_{n \geqslant 1} E_n$. Alors, pour toute fonction f étagée positive, on a :*

$$\lim_{n \to \infty} \int_{E_n} f \, d\mu = \int_X f \, d\mu$$

2) Intégrales de fonctions mesurables positives

Définition 9. Pour $f : X \to \overline{\mathbb{R}^+}$ mesurable, on pose :

$$\int_X f \, d\mu = \sup \left\{ \int_X \varphi \, d\mu \,\middle|\, \varphi \leqslant f, \, \varphi \text{ étagée positive} \right\}$$

On dit que f est intégrable si $\int_X f d\mu < \infty$.

Remarque 10. *Lorsque f est étagée positive, cette définition coïncide bien avec la première. De plus, cette intégrale est croissante.*

Théorème 11 (Beppo Levi)**.** *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré et $(f_n)_n$ une suite croissante de fonctions mesurables positives, alors :*

$$\lim_{n \to \infty} f_n \text{ est mesurable et } \int_X \lim_{n \to \infty} f_n d\mu = \lim_{n \to \infty} \int_X f_n d\mu$$

Proposition 12. *L'intégrale des fonctions mesurables positives est additive, croissante et homogène positive.*

Proposition 13. *Soit $f : X \to \overline{\mathbb{R}^+}$ mesurable, alors :*

$$\int_X f \, d\mu = 0 \Longleftrightarrow \mu(\{f \neq 0\}) = 0$$

Définition 14. Deux fonctions mesurables f et g coïncident presque partout, noté $f = g$ p.p., si elles différent sur un ensemble négligeable.

Proposition 15. *Soient $f, g : X \to \overline{\mathbb{R}^+}$ mesurables. Si $f = g$ p.p., alors $\int_X f \, d\mu = \int_X g \, d\mu$.*

Proposition 16 (Markov)**.** *Soit $f : X \to \overline{\mathbb{R}^+}$ mesurable, alors :*

$$\forall \, a > 0, \ \mu(\{f \geqslant \alpha\}) \leqslant \frac{1}{a} \int_X f \, d\mu$$

3) Fonctions intégrables

Définition 17. Une fonction mesurable $f : X \to \mathbb{K}$ est dite intégrable si $|f|$ est intégrable. On note $\mathscr{L}^1_{\mathbb{K}}(X, \mathcal{A}, \mu)$ ou $\mathscr{L}^1_{\mathbb{K}}(\mu)$ l'ensemble des fonction de X dans $\mathbb{K}$ qui sont intégrables.

Définition 18. Pour $f \in \mathscr{L}^1_{\mathbb{R}}(X, \mathcal{A}, \mu)$, on note $f^+ = \max(0, f)$ et $f^- = -\min(0, f)$. On définit alors :

$$\int_X f d\mu = \int_X f^+ \, d\mu - \int_X f^- \, d\mu$$

Si $f \in \mathscr{L}^1_{\mathbb{C}}(X, \mathcal{A}, \mu)$, alors $\mathrm{Re}(f), \mathrm{Im}(f) \in \mathscr{L}^1_{\mathbb{R}}(X, \mathcal{A}, \mu)$, et on pose :

$$\int_X f d\mu = \int_X \mathrm{Re}(f) \, d\mu + i \int_X \mathrm{Im}(f) \, d\mu$$

Exemple 19. *Sur $(\mathbb{N}, \mathcal{P}(\mathbb{N}))$ muni de la mesure de comptage m, on a :*

$$\mathscr{L}^1_{\mathbb{K}}(\mathbb{N}, \mathcal{P}(\mathbb{N}), m) = \ell^1(\mathbb{N}) = \left\{ (u_n)_{n\in\mathbb{N}} \,\middle|\, \sum_{i=1}^{\infty} |u_n| < \infty \right\}$$

Théorème 20. *L'espace $\mathscr{L}^1_{\mathbb{K}}(X, \mathcal{A}, \mu)$ est un $\mathbb{K}$-espace vectoriel, où l'intégrale est une forme linéaire positive, et donc croissante.*

Proposition 21. *Pour $f \in \mathscr{L}^1_{\mathbb{K}}(\mu)$, on a $\left|\int_X f \, d\mu\right| \leqslant \int_X |f| \, d\mu$, avec égalité si, et seulement si, il existe $\alpha \in \mathbb{K}$ de Module 1 tel que $f = \alpha |f|$ p.p..*

4) Lien avec l'intégrale de Riemann

Théorème 22. *Soient $f : [a, b] \to \mathbb{K}$ intégrable au sens de Riemann. Il existe $g \in \mathscr{L}^1_{\mathbb{K}}([a, b], \mathscr{B}([a, b]), \lambda)$ égale presque partout à f et telle que $\int_a^b f(x) \, dx = \int_{[a,b]} g \, d\lambda$. En particulier, si $g : [a, b] \to \mathbb{K}$ est continue, alors g est Lebesgue-intégrable, et $\int_{[a,b]} g \, d\lambda = G(b) - G(a)$, où G est une primitive de g.*

Remarque 23. *Ce dernier théorème se généralise mal aux intégrales impropres. Le sinus cardinal est Riemann intégrable sur $\mathbb{R}$, mais pas au sens de Lebesgue.*

Exemple 24. $\lim_{n\to\infty} \int_0^n \left(1 - \frac{x}{n}\right)^n e^{\alpha x} \, dx = \int_0^{\infty} e^{(\alpha-1)x} \, dx$

II Théorèmes de convergence

1) Lemme de Fatou et convergence dominée

Théorème 25 (Lemme de Fatou)**.** *Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions mesurables positives, alors :*

$$0 \leqslant \int_X \liminf_{n\to\infty} f_n \, d\mu \leqslant \liminf_{n\to\infty} \int_X f_n \, d\mu \leqslant +\infty$$

Application 26. *Si $(f_n)_{n\in\mathbb{N}}$ est une suite de fonctions intégrables, et que $\sup \int |f_n| \, d\lambda < \infty$, alors $\lim_{n\to\infty} f_n$ est intégrable.*

Remarque 27. *Il faut la positivité, $\frac{-|x|}{n}$ contredit le lemme de Fatou.*

Théorème 28 (Convergence dominée)**.** *Soit $(f_n)_n$ une suite de fonctions intégrables et $f : X \to \mathbb{K}$ telles que :*

(i) $f_n(x) \to f(x)$ μ p.p.

(ii) $\exists\, g \in \mathscr{L}^1_{\mathbb{R}^+}(X, \mathcal{A}, \mu), \forall n \in \mathbb{N}, |f_n(x)| \leqslant g(x)$ μ p.p.

Alors $f \in \mathscr{L}^1_{\mathbb{K}}(X, \mathcal{A}, \mu)$ et $\lim_{n\to\infty} \int_X f_n d\mu = \int_X f d\mu$.

Application 29. *Soit f dérivable partout sur $[0, 1]$, de dérivée bornée. Alors $\int_0^1 f'(t)dt = f(1) - f(0)$.*

2) Application aux séries de fonctions

Théorème 30. *Soit $(\varphi_n)_{n\in\mathbb{N}}$ une suite de fonctions mesurables.*

(i) Si les φ_n sont positives, alors :

$$\int_X \left(\sum_{n\in\mathbb{N}} \varphi_n \right) d\mu = \sum_{n\in\mathbb{N}} \int_X \varphi_n d\mu$$

(ii) Si $\sum_{n\in\mathbb{N}} \int_X |\varphi_n| d\mu < +\infty$, alors les fonctions φ_n, $\sum_{n\in\mathbb{N}} |\varphi_n|$ et la fonction définie μ p.p. $\sum_{n\in\mathbb{N}} \varphi_n$ sont intégrables, et :

$$\int_X \left(\sum_{n\in\mathbb{N}} \varphi_n \right) d\mu = \sum_{n\in\mathbb{N}} \int_X \varphi_n d\mu$$

Application 31 (Lemme de Borel-Cantelli)**.** *Soit $(A_n)_{n\in\mathbb{N}}$ une famille de parties de $\mathcal{A}$, alors :*

$$\sum_{n\in\mathbb{N}} \mu(A_n) < +\infty \Rightarrow \mu\left(\limsup_{n\in\mathbb{N}} A_n \right) = 0$$

III Espaces L^p

1) Définitions et premières propriétés

Définition 32. Pour tout réel $p > 0$, on définit le $\mathbb{K}$-espace vectoriel :

$$\mathscr{L}^p_{\mathbb{K}}(X, \mathcal{A}, \mu) = \left\{ f : X \to \mathbb{K} \text{ mesurable} \,\middle|\, \int_X |f|^p \, d\mu < +\infty \right\}$$

Sauf situation ambiguë, on privilégiera la notation plus concise $\mathscr{L}^p_{\mathbb{K}}(\mu)$.

Exemple 33. *Dans le cas de la mesure de comptage, cette définition donne les espaces $\ell_{\mathbb{K}}(\mathbb{N})$ des suites de puissance p sommable.*

Proposition 34. *Soient $0 < p \leqslant q$ des réels.*

(i) Si μ est finie, alors $\mathscr{L}^p_{\mathbb{K}}(\mu) \supset \mathscr{L}^q_{\mathbb{K}}(\mu)$.

(ii) Si on considère la mesure de comptage sur $\mathbb{N}$, alors $\ell^p_{\mathbb{K}}(\mathbb{N}) \supset \ell^q_{\mathbb{K}}(\mathbb{N})$.

Remarque 35. *Il n'y a pas, en général, d'inclusion entre les espaces $\mathscr{L}^p$.*

Définition 36. Pour toute fonction $f : X \to \mathbb{K}$ et tout $p > 0$, on définit :

$$\|f\|_p = \left(\int_X |f|^p \, d\mu \right)^{\frac{1}{p}} \quad \left(\text{convention : } \infty^{\frac{1}{p}} = \infty \right)$$

Théorème 37 (Hölder)**.** *Soient $f \in \mathscr{L}^p_{\mathbb{K}}(\mu)$ et $g \in \mathscr{L}^q_{\mathbb{K}}(\mu)$, où $\frac{1}{p} + \frac{1}{q} = 1$. Alors $\|fg\|_1 \leqslant \|f\|_p \|g\|_q$.*

Théorème 38 (Minkowski)**.** *Soient $p \in [1, +\infty[$ et $f, g \in \mathscr{L}^p_{\mathbb{K}}(\mu)$. Alors $\|f + g\|_p \leqslant \|f\|_p + \|g\|_p$.*

Définition 39. Pour $1 \leqslant p < +\infty$, on définit $L^p_{\mathbb{K}}(\mu)$ comme l'espace vectoriel normé quotient de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ par les fonctions presque nulles. On associera par abus de langage un élément de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ à sa classe dans $L^p_{\mathbb{K}}(\mu)$.

Définition 40. On définit le supremum essentiel de $f : X \to \overline{\mathbb{R}^+}$ par :

$$\|f\|_\infty = \operatorname{supess}(f) = \inf \{ M > 0 \,|\, \mu(\{f > M\}) = 0 \} \geqslant 0$$

On note $\mathscr{L}^\infty_{\mathbb{K}}(\mu)$ l'ensemble des fonctions essentiellement bornées.

Définition 41. On définit $L^\infty_{\mathbb{K}}(\mu)$ comme l'espace vectoriel normé quotient de $\mathscr{L}^\infty_{\mathbb{K}}(\mu)$ par les fonctions presque nulles.

Remarque 42. *En considérant 1 et ∞ comme exposants conjugués, on retrouve les inégalités de Hölder et de Minkowski.*

Théorème 43 (Riesz-Fischer)**.** *Pour tout $1 \leqslant p \leqslant +\infty$, $L^p_{\mathbb{K}}(\mu)$ est un espace de Banach.*

2) Convolution, densité et régularisation

Définition 44. On appelle convolution de f et g la fonction $f * g$ définie par $f * g(x) = \int_{\mathbb{R}^d} f(y) g(x - y) \, dy$ lorsque celle-ci est bien définie.

Proposition 45. *(i) $f \in L^1$, $g \in L^p \Rightarrow \|f * g\|_p \leqslant \|f\|_1 \|g\|_p$.*

(ii) $f \in L^p$, $g \in L^q \Rightarrow \|f * g\|_\infty \leqslant \|f\|_p \|g\|_q$.

Proposition 46. *$(L^1, +, *)$ est une algèbre de Banach.*

Définition 47. Une suite $(\rho_n)_{n \in \mathbb{N}}$ de fonctions positives de L^1 d'intégrale 1 sur $\mathbb{R}^d$ est une approximation de l'unité si elles sont d'intégrale 1 sur $\mathbb{R}^d$, et si, pour tout $\varepsilon > 0$, $\lim_{n \to \infty} \int_{\{|x| > \varepsilon\}} \rho_n = 0$. Si les ρ_n sont $\mathcal{C}^\infty$ à support compact, on parle de suite régularisante.

Théorème 48. *Soient $f \in L^p(\mathbb{R}^d)$ et $(\rho_n)_n$ une approximation de l'identité ($p \in [1, +\infty[$), alors $\lim\limits_{n \to +\infty} (\rho_n * f) = f$ dans $L^p(\mathbb{R}^d)$.*

Théorème 49. *Pour tout $p \in [1, +\infty[$, $\mathcal{C}^\infty_c(\mathbb{R}^d)$ est dense dans $L^p(\mathbb{R}^d)$.*

3) Cas particulier de L^2

Définition 50. L'application $(f, g) \mapsto \langle f, g \rangle_{L^2_{\mathbb{K}}} = \int_X fg \, d\mu$ définit un produit scalaire. On note $\|.\|_{L^2_{\mathbb{K}}} = \|.\|_2$ la norme associée.

Corollaire 51. *$\left(L^2_{\mathbb{K}}(\mu), \langle ., . \rangle_{L^2_{\mathbb{K}}} \right)$ est un espace de Hilbert.*

Théorème 52. *Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. S'il existe $a > 0$ tel que $\int_I e^{a|x|} \rho(x) dx < \infty$, alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I, \rho)$.*

Développements

- Théorème de Riesz-Fischer (43) [Bre87]
- Densité des polynômes orthogonaux (52) [BMP05]

Références

[BP12] M. Briane et G. Pagès. *Théorie de l'intégration.* Vuilbert
[Bre87] H. Brezis. *Analyse fonctionelle.* Masson
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K

Cadre : $(X, \mathcal{A}, \mu)$ est un espace mesuré, E un espace vectoriel normé.

I Limites et intégration

1) Suites de fonctions

Définition 1. Soit $f : X \to E$ bornée. On introduit la norme uniforme $\|f\|_\infty = \sup_{x\in X} \|f(x)\|_E$. On dit que $(f_n)_n$ converge uniformément vers f si $\lim_{n\to\infty} \|f_n - f\|_\infty = 0$.

Théorème 2. *Soit $(f_n)_n$ une suite de fonctions continues d'un segment $[a, b] \subseteq \mathbb{R}$ dans un espace de Banach E, qui converge uniformément vers f sur $[a, b]$, alors on a :*

$$\lim_{x\to x_0} f(x) = \lim_{n\to\infty} f_n(x_0) \quad et \quad \int_a^b f(t)dt = \lim_{n\to\infty} \int_a^b f_n(t)dt$$

Exemple 3. *La suite $\left(x \mapsto \left(1 - \frac{x}{n}\right)^n\right)_n$ converge uniformément vers $(x \mapsto e^{-x})$ sur $[0, 1]$, donc :* $\lim_{n\to\infty} \int_0^1 \left(1 - \frac{x}{n}\right)^n dx = \int_0^1 e^{-x}dx = 1 - \frac{1}{e}$

Corollaire 4. *Si $\sum g_n$ est une série de fonctions continues de $[A, b] \subseteq \mathbb{R}$ dans un Banach E qui converge normalement vers g sur $[a, b]$, alors :*

$$\int_a^b \sum_{n\geqslant 0} g_n(t)dt = \sum_{n\geqslant 0} \int_a^b g_n(t)dt$$

Théorème 5 (Beppo Levi)**.** *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré et $(f_n)_n$ une suite croissante de fonctions mesurables positives, alors* $\lim_{n\to\infty} f_n$ *est mesurable et* $\int_X \lim_{n\to\infty} f_n d\mu = \lim_{n\to\infty} \int_X f_n d\mu$.

Application 6. *Soit $I_n(\alpha) = \int_0^n \left(1 - \frac{x}{n}\right)^n e^{\alpha x}dx$ pour $n \in \mathbb{N}$ et $\alpha \in \mathbb{R}$, alors* $\lim_{n\to\infty} I_n(\alpha) = \int_0^\infty e^{(\alpha-1)x}dx = \frac{1}{1-\alpha}$ *si $\alpha < 1$ et $+\infty$ sinon.*

Théorème 7 (Lemme de Fatou)**.** *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré et $(f_n)_n$ une suite de fonctions mesurables et positives, alors* $\int_X \liminf_{n\to\infty} f_n d\mu \leqslant \liminf_{n\to\infty} \int_X f_n d\mu$.

Application 8. *Soit $(f_n)_n$ une suite de fonctions intégrables simplement convergente vers f telle que* $\sup_n \int_X |f_n|d\mu < \infty$. *Alors f est intégrable.*

Application 9. *Soit f croissante sur $[0, 1]$, continue en 0 et 1, dérivable presque partout sur $[0, 1]$, alors* $\int_0^1 f'(t)dt \leqslant f(1) - f(0)$.

Théorème 10 (Convergence dominée)**.** *Soit $(f_n)_n$ une suite d'éléments de $L^1(X, \mathbb{C}, \mu)$ et $f : X \to \mathbb{C}$ telles que :*

(i) $f_n(x) \to f(x)$ *μ p.p.*

(ii) $\exists g \in L^1(X, \mathbb{R}^+, \mu), \forall n \in \mathbb{N}, |f_n(x)| \leqslant g(x)$ *μ p.p.*

Alors $f \in L^1(X, \mathbb{C}, \mu)$ et $\lim_{n\to\infty} \int_X f_n d\mu = \int_X f d\mu$.

Application 11. *Soit f dérivable partout sur $[0, 1]$, de dérivée bornée. Alors* $\int_0^1 f'(t)dt = f(1) - f(0)$.

Théorème 12 (Fubini-Tonelli)**.** *Soient $(X, \mathcal{A}, \mu)$, $(Y, \mathcal{B}, \nu)$ des espaces mesurés, $\lambda = \mu \otimes \nu$, et $f : X \times Y \to \mathbb{R}$ λ-mesurable positive, alors :*

(i) $x \mapsto \int_Y f(x, y)d\nu(y)$ *est μ-mesurable et positive.*

(ii) $y \mapsto \int_X f(x, y)d\mu(x)$ *est ν-mesurable et positive.*

De plus, on a :

$$\int_{X\times Y} f d\lambda = \int_X \left(\int_Y f(x, y)d\nu(y)\right) d\mu(x) = \int_Y \left(\int_X f(x, y)d\mu(x)\right) d\nu(y)$$

Théorème 13 (Fubini)**.** *Soient $(X, \mathcal{A}, \mu)$, $(Y, \mathcal{B}, \nu)$ des espaces mesurés, $\lambda = \mu \otimes \nu$, et $f : X \times Y \to \mathbb{R}$ λ-intégrable, alors :*

(i) La fonction $x \mapsto \int_Y f(x, y)d\nu(y)$ est définie pour μ-presque tout $x \in X$ et est intégrable.

(ii) La fonction $y \mapsto \int_X f(x, y)d\mu(x)$ est définie pour ν-presque tout $y \in Y$ et est intégrable.

De plus, on a :

$$\int_{X\times Y} f d\lambda = \int_X \left(\int_Y f(x, y)d\nu(y)\right) d\mu(x) = \int_Y \left(\int_X f(x, y)d\mu(x)\right) d\nu(y)$$

Théorème 14. *Soit $(f_n)_n$ une suite de fonctions mesurables à valeurs dans $\overline{\mathbb{R}}$ ou $\mathbb{C}$.*

(i) Si $\forall n \in \mathbb{N}$, $f_n \geqslant 0$, alors $\int_X \sum_{n\geqslant 0} f_n d\mu = \sum_{n\geqslant 0} \int_X f_n d\mu$.

(ii) Si $\sum_{n\geqslant 0} \int_X |f_n|d\mu < \infty$, *alors f_n,* $\sum_{n\geqslant 0} |f_n|$ *et* $\sum_{n\geqslant 0} f_n$ *sont intégrables, et* $\int_X \sum_{n\geqslant 0} f_n d\mu = \sum_{n\geqslant 0} \int_X f_n d\mu$.

Application 15 (Borel-Cantelli)**.** *Soit $(A_n)_n$ une suite de parties mesurables de X, alors :*

$$\sum_{n\geqslant 0} \mu(A_n) < +\infty \Rightarrow \mu(\limsup_{n\to\infty} A_n) = 0$$

2) Intégrale à paramètre

Soit $f : E \times X \to \mathbb{K}$.

Théorème 16. *Soit $u_0 \in E$. On suppose que :*

(i) Pour tout $u \in E$, $x \mapsto f(u,x)$ est mesurable.

(ii) Pour presque tout $x \in X$, $u \mapsto f(u,x)$ est continue en u_0.

(iii) $\exists\, g \in L^1(X, \mathbb{R}^+), \forall u \in E, |f(u,x)| \leqslant g(x)$ p.p.

Alors $u \mapsto \int_X f(u,x)d\mu(x)$ est définie pour tout $u \in E$ et continue en u_0.

Théorème 17. *On suppose que E est un intervalle non vide de $\mathbb{R}$, et :*

(i) Pour tout $u \in E$, $x \mapsto f(u,x)$ est μ-intégrable.

(ii) Pour presque tout $x \in X$, $u \mapsto f(u,x)$ est dérivable sur E.

(iii) $\exists\, g \in L^1(\mu), \forall u \in E, \left|\frac{\partial f}{\partial u}(u,x)\right| \leqslant g(x)$ p.p.

Alors $F(u) = \int_X f(u,x)d\mu(x)$ est définie pour tout $u \in E$ et dérivable sur E, de dérivée $F'(u) = \int_X \frac{\partial f}{\partial u}(u,x)d\mu(x)$.

Corollaire 18. *Soient $A \subseteq \mathbb{R}$ un intervalle et $]a,b[\subset \mathbb{R}$ un segment. Soit $f : A \times [a,b] \to E$, alors $F : x \mapsto \int_a^b f(x,t)dt$ est continue. Si de plus $\frac{\partial f}{\partial x}$ existe et est continue sur $A \times [a,b]$, alors F est $\mathcal{C}^1$ et pour tout $x \in A$, on a $F'(x) = \int_a^b \frac{\partial f}{\partial x}(x,t)dt$.*

Exemple 19. *Soit* $\Gamma : \left| \begin{array}{ccc} \mathbb{R}^{+\star} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \int_0^\infty t^{x-1}e^{-t}dt \end{array} \right.$, *alors Γ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}^{+\star}$, et on a :*

$$\forall\, n \in \mathbb{N},\ \forall x \in \mathbb{R}^{+\star},\ \Gamma^{(n)}(x) = \int_0^\infty (\ln t)^n e^{-t}t^{x-1}dt$$

II Limites et séries

On voit les séries comme des intégrales pour la mesure de comptage.

1) Séries de fonctions

Théorème 20. *Soit $(f_n)_n$ une suite de fonctions continues sur $A \subseteq \mathbb{R}$. Si $\sum f_n$ converge uniformément sur A, alors $\sum f_n$ est continue sur A.*

Exemple 21. *Sur $[0,1]$, on pose $f_n : x \mapsto x^n(1-x)$ continue. $\sum f_n$ converge simplement sur $[0,1]$ vers $f : x \mapsto \mathbb{1}_{[0,1[}$, qui est discontinue.*

Théorème 22. *Soient I un intervalle et $(f_n)_n$ une suite de fonctions dérivables sur I. On suppose que :*

(i) $\sum f_n$ converge simplement sur I

(ii) $\sum f_n'$ converge uniformément sur I

Alors $\sum f_n$ converge uniformément sur toute partie bornée de I, et $\sum f_n$ est dérivable sur I de dérivée $\sum f_n'$.

2) Séries entières

Définition 23. Soit $\sum a_n z^n$ une série entière. On appelle rayon de convergence de $\sum a_n z^n$ le réel R défini par :

$$R = \sup\left\{r \in \mathbb{R}^+ \,\middle|\, \exists M \in \mathbb{R}, \forall n \in \mathbb{N}, |a_n|r^n \leqslant M\right\}$$

$D(0,R)$ s'appelle le disque de convergence de $\sum a_n z^n$.

Proposition 24. *Soit $\sum a_n z^n$ série entière de rayon de convergence R.*

(i) Pour tout $z \in D(0,R)$, $\sum a_n z^n$ est absolument convergente.

(ii) Pour tout $z \in \mathbb{C} \setminus \overline{D(0,R)}$, $\sum a_n z^n$ diverge.

(iii) Pour tout $r \in]0,R[$, $\sum a_n z^n$ converge normalement sur $\overline{D(0,r)}$.

Remarque 25. *On ne peut rien dire si $|z| = R$.*

Théorème 26. *L'application f, appelée somme de la série entière $\sum a_n z^n$, définie par :*

$$f : \left| \begin{array}{ccc} D(0,R) & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \sum_{n=0}^n a_n z^n \end{array} \right.$$

est de classe $\mathcal{C}^1$. De plus, sa dérivée est donnée par :

$$f' : \left| \begin{array}{ccc} D(0,R) & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \sum_{n=1}^n n a_n z^{n-1} \end{array} \right.$$

Théorème 27 (Abel angulaire)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 telle que $\sum a_n$ converge. On note f sa somme et :*

$$\Delta_\theta = \left\{z \in \mathbb{C} \,\middle|\, 1 - z = \rho e^{i\varphi},\ \rho > 0,\ |\varphi| < \theta\right\} \quad \text{pour} \quad 0 \leqslant \theta < \frac{\pi}{2}$$

Alors :

$$\lim_{\substack{z \to 1 \\ z \in \Delta_\theta}} f(z) = \sum_{n \geqslant 0} a_n$$

Application 28. $\sum_{n\geqslant 0}\frac{(-1)^n}{2n+1}=\arctan(1)=\frac{\pi}{4}$ *et* $\sum_{n\geqslant 1}\frac{(-1)n-1}{n}=\ln(2)$

Théorème 29 (Taubérien faible)**.** *Soit f la somme d'une série entière $\sum a_n z^n$ de rayon de convergence 1. On suppose que $\lim_{x\to 1^-} f(z)=\ell$ existe, et $a_n=o\left(\frac{1}{n}\right)$. Alors $\sum a_n$ converge et $\ell=\sum_{n\geqslant 0}a_n$.*

III Applications

1) Holomorphie

Théorème 30. *Soient $(X,\mathcal{A},\mu)$ un espace mesuré, Ω un ouvert de $\mathbb{C}$, et $f:\Omega\times X\to\mathbb{C}$. Posons pour tout $z\in\Omega$ $F(z)=\int_X f(z,x)d\mu(x)$, et supposons que :*

(i) $\forall z\in\Omega$, $x\mapsto f(z,x)$ *est mesurable*

(ii) $\forall x\in X$, $z\mapsto f(z,x)$ *est holomorphe*

(iii) Pour tout compact K de Ω, il existe $g\in L^1(X)$ telle que pour tous $z\in K$ et $x\in X$, $|f(z,x)|\leqslant g(x)$

Alors F est holomorphe sur Ω, et pour tous $z\in\Omega$ et $n\in\mathbb{N}$:

$$F^{(n)}(z)=\int_X \frac{\partial^n f}{\partial z^n}(z,x)d\mu(x)$$

Application 31. *Soit $P=\{z\in\mathbb{C}\,|\,\mathrm{Re}(z)>0\}$. On définit sur P la fonction holomorphe :*

$$\Gamma(z)=\int_0^{+\infty}e^{-t}t^{z-1}dt$$

2) Séries de Fourier

Définition 32. Soit $f:\mathbb{R}\to\mathbb{C}$ continue par morceaux et 2π-périodique. Les coefficients exponentiels de Fourier de f sont :

$$c_n(f)=\frac{1}{2\pi}\int_0^{2\pi}f(t)e^{-int}\,dt\quad(n\in\mathbb{Z})$$

En posant $e_n:t\mapsto e^{int}$, la série de Fourier associée à f est la série trigonométrique $\sum_{n\in\mathbb{Z}}c_n(f)e_{-n}$.

Proposition 33 (Riemann-Lebesgue)**.** *Si f est continue par morceaux et 2π-périodique, alors $\lim_{|n|\to+\infty}c_n(f)=0$.*

Théorème 34. *La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de l'espace des fonctions 2π-périodiques de carré intégrable sur $[0,2\pi]$. On a en particulier :*

$$\frac{1}{2\pi}\|f\|_2^2=\sum_{n\in\mathbb{Z}}c_n(f)^2$$

Proposition 35. *Si f est $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge simplement vers la régularisation $\tilde{f}$ de f donnée pour $x\in\mathbb{R}$ par $\tilde{f}(x)=\frac{f(x^+)+f(x^-)}{2}$.*

Remarque 36. *L'hypothèse $\mathcal{C}^1$ par morceaux est nécessaire.*

Théorème 37. *Si f est continue, $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge normalement vers f.*

Théorème 38. *Pour $u_0\in L^2(\mathbb{T})$, on considère l'équation différentielle :*

$$\begin{cases}\frac{\partial u}{\partial t}-\frac{\partial^2 u}{\partial x^2}=0 & \text{sur } \mathbb{R}^{+\star}\times\mathbb{T}\\ u(0,.)=u_0 & \text{dans } L^2(\mathbb{T})\end{cases}\qquad(*)$$

Il existe une unique solution u de $(*)$ de classe $\mathcal{C}^2$ sur $\mathbb{R}^{+\star}\times\mathbb{T}$, avec $u(t,.)$ tendant vers u_0 dans $L^2(\mathbb{T})$ quand t tend vers 0.

Développements

— Théorèmes d'Abel angulaire et taubérien faible (27,29) [Gou08]
— Équation de la chaleur sur le cercle (38) [Can09]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[BP12] M. Briane et G. Pagès. *Théorie de l'intégration.* Vuilbert
[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions.* Ellipses
[Can09] B. Candelpergher. *Calcul intégral.* Cassini

I Méthodes de calcul directes

1) Calculs de primitives

Théorème 1. *Toute fonction continue $f : [a,b] \to \mathbb{R}$ admet des primitives. Si F est une primitive de f, on a $\int_a^b f(t)\,dt = F(b) - F(a)$.*

Exemple 2. *Pour $\alpha > 1$, on a $\int_1^{+\infty} \frac{1}{t^\alpha} dt = \frac{1}{1+\alpha}$.*

Exemple 3. *Pour $x \in \mathbb{R}$, on a $\int_0^x \frac{1}{1+t^2} dt = \arctan x$.*

Proposition 4. *Soit $f \in \mathbb{K}(X)$ non nulle ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$). Écrivons $f = \frac{N}{D}$, avec $N, D \in \mathbb{K}[X]$ premiers entre eux et D unitaires. Écrivons $D = \prod_{i=1}^n D_i^{\alpha_i}$ sa décomposition en facteurs irréductibles. Alors f s'écrit de manière unique sous la forme $f = E + \sum_{i=1}^n \sum_{j=1}^{\alpha_i} \frac{A_{i,j}}{D_i^j}$, avec $E \in \mathbb{K}[X]$, $A_{i,j} \in \mathbb{K}[X]$ et $\deg(A_{i,j}) < \deg(D_i)$.*

Application 5. *Pour calculer une intégrale d'une fraction rationnelle réelle, on la décompose en éléments simples. Il suffit alors de connaître les intégrales suivantes, pour $a, b, c, d \in \mathbb{N}$, $n \in \mathbb{N}$ et $c^2 - 4d < 0$:*

$$\int \frac{1}{(x-a)^n}\,dx \quad et \quad \int \frac{ax+b}{(x^2+cx+d)^n}\,dx$$

Exemple 6.

$$\begin{aligned}\int_0^x \frac{1}{t(t^2+1)}\,dx &= \int_0^x \frac{1}{x}\,dx - \int_0^x \frac{x}{x^2+1}\,dx - \int_0^x \frac{x}{(x^2+1)^2}\,dx \\ &= \ln|x| - \frac{1}{2}\ln(x^2+1) + \frac{1}{2}\frac{1}{1+x^2}\end{aligned}$$

2) Intégration par parties

Théorème 7 (Intégration par parties)**.** *Soient $u, v : [a,b] \to \mathbb{C}$ deux fonctions de classe $\mathcal{C}^1$. Alors :*

$$\int_a^b u(x)\,v'(x)\,dx = [u(x)\,v(x)]_a^b - \int_a^b u'(x)\,v(x)\,dx$$

Exemple 8 (Wallis)**.** *Si $I_n = \int_0^{\frac{\pi}{2}} \sin^n(x)\,dx$, alors $I_{n+2} = \frac{n+1}{n+2} I_n$.*

Exemple 9. *$\Gamma(x+1) = x\Gamma(x)$ pour $x \in \mathbb{R}^\star$, et $\Gamma(n+1) = n!$ pour $n \in \mathbb{N}$.*

3) Changement de variables

Théorème 10 (Changement de variable)**.** *Soient U et V deux ouverts de $\mathbb{R}^n$, et $\varphi : U \to V$ un $\mathcal{C}^1$-difféomorphisme. Alors, pour toute fonction borélienne $f : V \to \mathbb{R}$, on a :*

$$\int_V f(v)\,dv = \int_U f(\varphi(u))\,|J_\varphi(u)|\,du \quad où \quad J_\varphi(u) = \det(d\varphi_u)$$

De plus, toute fonction g mesurable et définie sur $\varphi(u)$ est intégrable si, et seulement si, $(g \circ \varphi)|J_\varphi|$ est intégrable sur U, et dans ce cas la formule précédente reste vraie pour g.

Application 11. *Pour $f : \mathbb{R}^2 \to \mathbb{R}^+$ borélienne, on a :*

$$\int_{\mathbb{R}^2} f(x,y)\,dx\,dy = \int_0^{2\pi} \int_{\mathbb{R}^{+\star}} f(r\cos\theta, r\sin\theta)\,r\,dr\,d\theta$$

Exemple 12. *$\int_{\mathbb{R}} e^{-x^2}\,dx = \sqrt{\pi}$*

Corollaire 13. *Soient $f : I \to \mathbb{R}$ continue par morceaux et $\varphi : [a,b] \to I$ de classe $\mathcal{C}^1$ dont la dérivée ne s'annule pas. Alors :*

$$\int_a^b f(\varphi(t))\,\varphi'(t)\,dt = \int_{\varphi(a)}^{\varphi(b)} f(u)\,du$$

Exemple 14. *$\int_0^1 \sqrt{1-x^2}\,dx = \frac{\pi}{4}$ et $\int_0^{\frac{\pi}{2}} \ln\sin t\,dt = \frac{\pi}{2}\ln 2$*

4) Théorèmes de Fubini

Soient $(X, \mathcal{A}, \mu)$, $(Y, \mathcal{B}, \nu)$ des espaces mesurés et $f : X \times Y \to \mathbb{R}$.

Théorème 15 (Fubini-Tonelli)**.** *Si f est $(\mu \otimes \nu)$-mesurable positive, alors $x \mapsto \int_Y f(x,y)d\nu(y)$ et $y \mapsto \int_X f(x,y)d\mu(x)$ sont mesurable. De plus :*

$$\int_{X\times Y} f d\lambda = \int_X \left(\int_Y f(x,y)d\nu(y)\right) d\mu(x) = \int_Y \left(\int_X f(x,y)d\mu(x)\right) d\nu(y)$$

Exemple 16. *Soit $D = \{x, y \geqslant 0, x + y \leqslant 1\}$. Alors $\int_D xy\,dx\,dy = \frac{1}{24}$.*

Théorème 17 (Fubini)**.** *Si f est $(\mu \otimes \nu)$-intégrable, alors la fonctions $x \mapsto \int_Y f(x,y)d\nu(y)$ et $y \mapsto \int_X f(x,y)d\mu(x)$ sont définies presque partout et intégrables. De plus :*

$$\int_{X\times Y} f d\lambda = \int_X \left(\int_Y f(x,y)d\nu(y)\right) d\mu(x) = \int_Y \left(\int_X f(x,y)d\mu(x)\right) d\nu(y)$$

II Méthodes de calcul indirectes

1) Suites et séries de fonctions

Théorème 18 (Beppo Levi)**.** *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré et $(f_n)_n$ une suite croissante de fonctions mesurables positives, alors $\lim\limits_{n\to\infty} f_n$ est mesurable et $\int_X \lim\limits_{n\to\infty} f_n d\mu = \lim\limits_{n\to\infty} \int_X f_n d\mu$.*

Théorème 19 (Convergence dominée)**.** *Soit $(f_n)_n$ une suite d'éléments de $L^1(X, \mathbb{C}, \mu)$ et $f : X \to \mathbb{C}$ telles que :*

(i) $f_n(x) \to f(x)$ μ p.p.

(ii) $\exists\, g \in L^1(X, \mathbb{R}^+, \mu), \forall n \in \mathbb{N}, |f_n(x)| \leqslant g(x)$ μ p.p.

Alors $f \in L^1(X, \mathbb{C}, \mu)$ et $\lim\limits_{n\to\infty} \int_X f_n d\mu = \int_X f d\mu$.

Exemple 20. *L'hypothèse de domination est cruciale (cf $f_n = n\mathbb{1}_{[0,\frac{1}{n}]}$).*

Application 21. *Lorsque l'on peut écrire f comme série de fonctions, on peut souvent appliquer le théorème de convergence dominée.*

Exemple 22. $\int_0^1 \frac{\ln x}{x-1} dx = \sum_{n\in\mathbb{N}^\star} \frac{1}{n^2} = \frac{\pi^2}{6}$

2) Somme de Riemann

Soient $f : [a, b] \to \mathbb{R}$ bornée, $\sigma = \{a = x_0 < x_1 < \ldots < x_n = b\}$ une subdivision de $[a, b]$ et $\xi = (\xi_i)_{1\leqslant i\leqslant n} \in \mathbb{R}^n$ tel que $\xi_i \in [x_{i-1}, x_i]$.

Définition 23. On appelle somme de Riemann de f la quantité :

$$S(f, \sigma, \xi) = \sum_{i=1}^{n} (x_i - x_{i-1}) f(\xi_i)$$

Théorème 24. *On suppose f continue par morceaux. Pour tout $\varepsilon > 0$, il existe $\alpha > 0$ tel que, pour tout σ de pas inférieur à α et tout ξ, on a :*

$$\left\| \int_a^b f(x)\, dx - S(f, \sigma, \xi) \right\| \leqslant \varepsilon$$

En particulier, on a :

$$\lim_{n\to+\infty} \frac{b-a}{n} \sum_{k=1}^{n} f\left(a + k\frac{b-a}{n}\right) = \int_a^b f(t)\, dt$$

Exemple 25. $\lim_{n\to+\infty} \sum_{k=1}^{n} \frac{1}{n+k} = \int_0^1 \frac{1}{1+t} dt = \ln 2$

3) Intégrales à paramètres

Soit $f : \Lambda \times I \to \mathbb{K}$, où Λ est un intervalle de $\mathbb{R}$.

Théorème 26. *On suppose que :*

(i) Pour tout $t \in I$, $\lambda \mapsto f(\lambda, t)$ est continue sur Λ.

(ii) Pour tout $\lambda \in \Lambda$, $t \mapsto f(\lambda, t)$ est intégrable sur I.

(iii) $\exists\, g \in L^1(I, \mathbb{R}^+), \forall \lambda \in \Lambda, |f(\lambda, t)| \leqslant g(t)$ p.p.

Alors $\lambda \mapsto \int_I f(\lambda, t) dt$ est continue sur Λ.

Théorème 27. *On suppose que :*

(i) Pour tout $t \in I$, $\lambda \mapsto f(\lambda, t)$ est dérivable sur Λ.

(ii) Pour tout $\lambda \in \Lambda$, $t \mapsto f(\lambda, t)$ est intégrable sur I.

(iii) $\exists\, g \in L^1(I, \mathbb{R}^+), \forall \lambda \in \Lambda, |f'(\lambda, t)| \leqslant g(t)$ p.p.

Alors $\lambda \mapsto \int_I f(\lambda, t) dt$ est dérivable sur Λ de dérivée $\lambda \mapsto \int_I f'(\lambda, t) dt$.

4) Analyse complexe

Soit Ω un ouvert connexe de $\mathbb{C}$ non vide.

Définition 28. Soit γ un lacet de $\mathbb{C}$ et $a \in \mathbb{C} \setminus \mathrm{Im}(\gamma)$. L'indice $\mathrm{Ind}_\gamma(a)$ de a par rapport à γ est l'entier défini par :

$$\mathrm{Ind}_\gamma(a) = \frac{1}{2i\pi} \int_\gamma \frac{1}{z-a} dz$$

Théorème 29 (Cauchy)**.** *Soient Ω un ouvert convexe et $z_0 \in \Omega$ et $f \in \mathcal{H}(\Omega \setminus \{z_0\})$, alors pour tout lacet γ de Ω, on a $\int_\gamma f = 0$.*

Exemple 30. *Si $\gamma_a(x) = e^{-ax^2}$ pour $a > 0$ et $x \in \mathbb{R}$, alors $\widehat{\gamma_a} = \sqrt{\frac{\pi}{a}} \gamma_{\frac{1}{4a}}$.*

Théorème 31 (Formule de Cauchy)**.** *Soient Ω est un ouvert convexe, $z \in \Omega$, γ un lacet de $\Omega \setminus \{z\}$ et $f \in \mathcal{H}(\Omega)$, alors on a :*

$$\mathrm{Ind}_\gamma(z) f(z) = \frac{1}{2i\pi} \int_\gamma \frac{f(\xi)}{\xi - z} d\xi$$

Théorème 32 (Théorème des résidus)**.** *Soient $S \subset \Omega$ fini, $f \in \mathcal{H}(\mathbb{C} \setminus S)$ et γ un lacet dans Ω ne rencontrant pas S, alors :*

$$\int_\gamma f(z) dz = 2i\pi \sum_{c\in S} \mathrm{Ind}_\gamma(c)\, \mathrm{Res}(f, c)$$

Exemple 33. $\int_0^{+\infty} \frac{\sin x}{x}\, dx = \frac{\pi}{2}$

Exemple 34. *Soit $\alpha \in]-1, 1[$. Alors $\int_0^{+\infty} \frac{x^\alpha \ln x}{x^2-1}\, dx = \frac{\pi^2}{4\cos^2(\frac{\alpha\pi}{2})}$.*

III Méthodes d'approximation numérique

1) Méthodes de quadrature

Soit $f : [a,b] \to \mathbb{R}$ une fonction continue. On cherche des formules pour approcher $I(f) = \int_a^b f(x)dx$. Fixons $a = x_0 < x_1 < \cdots < x_n = b$ une subdivision de $[a,b]$. On pose $h_i = x_{i+1} - x_i$.

Définition 35. Une méthode de quadrature consiste, pour $0 \leqslant i < n$ à approcher $I_i = \int_{x_i}^{x_{i+1}} f(x)dx$ par $A_i(f)$ défini par :

$$A_i(f) = h_i \sum_{j=0}^{n_i} \omega_{i,j} f(\zeta_{i,j}) \quad \text{où} \quad \zeta_{i,j} \in [\alpha_i, \alpha_{i+1}] \quad \text{et} \quad \sum_{i=0}^{n_i} \omega_{i,j} = 1$$

On note alors $E(f) = I(f) - \sum_{i=0}^{n-1} A_i(f)$ l'erreur de la méthode.

Définition 36. Une méthode de quadrature est d'ordre N si $E(f) = 0$ pour tout $f \in \mathbb{R}_N[X]$ et s'il existe $f \in \mathbb{R}_{N+1}[X]$ telle qu'elle soit inexacte.

Application 37. *En fixant $(\zeta_j)_{0\leqslant j\leqslant n}$ associé à une subdivision de $[x_i, x_{i+1}]$, on peut prendre pour fonction de poids $\omega_j = \frac{1}{h_i}\int_{[x_i,x_{i+1}]} \ell_j$, où $\ell_j = \prod_{k\neq j} \frac{X-\zeta_k}{\zeta_j-\zeta_k}$. Ce sont les méthodes par interpolation de Lagrange.*

(i) Méthode des rectangles : $I(f) \sim \sum_{i=0}^{n-1} h_i f(z_i)$ où $z_i = x_i$ ou x_{i+1}. Méthode d'ordre 0.

(ii) Méthode des points milieux : $I(f) \sim \sum_{i=0}^{n-1} h_i f(z_i)$ où $z_i = \frac{x_i+x_{i+1}}{2}$. Méthode d'ordre 1 et $E(f) \leqslant \frac{1}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iii) Méthode des trapèzes : $I(f) \sim \sum_{i=0}^{n-1} h_i \frac{f(x_i)+f(x_{i+1})}{2}$. Méthode d'ordre 1 et $E(f) \leqslant \frac{2}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iv) Méthode de Simpson : $I(f) \sim \sum_{i=0}^{n-1} h_i \frac{f(x_{i+1})+4f(\frac{x_i)+x_{i+1}}{2})+f(x_i)}{6}$. Méthode d'ordre 3 et $E(f) = \mathcal{O}\left(\left\|f^{(4)}\right\|_\infty\right)$ si f est $\mathcal{C}^4$.

2) Méthode de Monte-Carlo

Théorème 38 (Loi forte des grands nombres)**.** *Soit $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires réelles indépendantes et identiquement distribuées de même loi qu'une variable aléatoire réelle X. Alors :*

$$\mathbb{E}[|X|] < +\infty \quad \Leftrightarrow \quad \frac{1}{n}\sum_{i=1}^{n} X_i \xrightarrow{p.s.} \mathbb{E}[X]$$

Application 39 (Monte-Carlo)**.** *Soit $f : [0,1] \to \mathbb{R}$ intégrable par rapport à la mesure de Lebesgue, et $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires indépendantes, identiquement distribuées et de loi $\mathcal{U}([0,1])$. Alors :*

$$\frac{1}{n}\sum_{k=1}^{n} f(X_i) \xrightarrow[n\to+\infty]{} \int_0^1 f(t)dt \ p.s.$$

Théorème 40 (Théorème central limite)**.** *On suppose que les X_n sont indépendants, identiquement distribués et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n} \frac{X_i - \mathbb{E}[X_i]}{\sqrt{\mathrm{Var}(X_i)}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$$

Application 41. *On suppose que les X_n sont indépendants, identiquement distribués et de loi $\mathcal{B}(p)$ pour $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\widehat{p_n} = \frac{1}{n}\sum_{k=1}^{n} X_i$. Il s'agit de :*

$$IC_\alpha = \left[\widehat{p_n} \pm \frac{q_{1-\frac{\alpha}{2}}}{2\sqrt{n}}\right]$$

où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Application 42. *Dans Monte-Carlo, on a un intervalle de confiance de probabilité asymptotique $1-\alpha$ de longueur proportionnelle à $\frac{1}{\sqrt{n}}$.*

Développements

- Intégrale de Dirichlet (33) [Can09]
- Transformée de Fourier d'une gaussienne (30) [El 08]
- Calcul d'une intégrale par le théorème des résidus (34) [Tau06]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BP12] M. Briane et G. Pagès. *Théorie de l'intégration.* Vuilbert
[Dem06] J.-P. Demailly. *Analyse numérique et équations différentielles.* EDP Sciences
[Can09] B. Candelpergher. *Calcul intégral.* Cassini
[El 08] M. El Amrani. *Analyse de Fourier dans les espaces fonctionnels.* Ellipses
[Tau06] P. Tauvel. *Analyse complexe pour la licence 3.* Dunod

Cadre : $(X, \mathcal{A}, \mu)$ est un espace mesuré, E un espace vectoriel normé et $f : E \times X \to \mathbb{C}$ une application.

I Étude de la régularité

1) Continuité

Théorème 1. *Soit $u_0 \in E$. On suppose que :*

(i) Pour tout $u \in E$, $x \mapsto f(u,x)$ est mesurable.

(ii) Pour presque tout $x \in X$, $u \mapsto f(u,x)$ est continue en u_0.

(iii) $\exists\, g \in L^1(X, \mathbb{R}^+), \forall u \in E, |f(u,x)| \leqslant g(x)$ p.p.

Alors $u \mapsto \int_X f(u,x)d\mu(x)$ est définie pour tout $u \in E$ et continue en u_0.

Corollaire 2. *On suppose que :*

(i) Pour tout $u \in E$, $x \mapsto f(u,x)$ est mesurable.

(ii) Pour presque tout $x \in X$, $u \mapsto f(u,x)$ est continue sur E.

(iii) $\forall K \subset E$ compact , $\exists\, g \in L^1(X, \mathbb{R}^+)$, $\forall u \in K, |f(u,x)| \leqslant g(x)$ p.p.

Alors $u \mapsto \int_X f(u,x)d\mu(x)$ est définie pour tout $u \in E$ et continue en u_0.

Exemple 3. *On pose, pour $x > 0$, $\Gamma(x) = \int_0^{+\infty} e^{-t}t^{x-1}dt$. Γ est bien définie et continue sur $\mathbb{R}^{+\star}$.*

Exemple 4. *Soit f définie sur $\mathbb{R}^+ \times \mathbb{R}^+$ par $f(x,t) = xe^{-xt}$. La fonction $x \mapsto \int_0^{\infty} xe^{-xt}dt$ est bien définie, mais pas continue en 0.*

2) Dérivabilité

On suppose que E est un intervalle non vide de $\mathbb{R}$.

Théorème 5. *On suppose que :*

(i) Pour tout $u \in E$, $x \mapsto f(u,x)$ est μ-intégrable.

(ii) Pour presque tout $x \in X$, $u \mapsto f(u,x)$ est dérivable sur E.

(iii) $\exists\, g \in L^1(\mu), \forall u \in E, \left|\frac{\partial f}{\partial u}(u,x)\right| \leqslant g(x)$ p.p.

Alors $F(u) = \int_X f(u,x)d\mu(x)$ est définie pour tout $u \in E$ et dérivable sur E, de dérivée $F'(u) = \int_X \frac{\partial f}{\partial u}(u,x)d\mu(x)$.

Remarque 6. *Si $u \mapsto f(u,x)$ est $\mathcal{C}^1$ sur E, alors F aussi.*

Exemple 7. $\forall x \in \mathbb{R}^+, \int_0^{\infty} \frac{\sin(xt)}{t}e^{-t}dt = \arctan x$

Exemple 8. *Pour $(x,t) \in \mathbb{R} \times \mathbb{R}^+$, $f(x,t) = x^2e^{-t|x|}$, F est bien définie mais n'est pas dérivable.*

Théorème 9. *Soit $k \in \mathbb{N}$. On suppose que :*

(i) Pour tout $u \in E$, $x \mapsto f(u,x)$ est μ-intégrable.

(ii) Pour presque tout $x \in X$, $u \mapsto f(u,x)$ est $\mathcal{C}^k$ sur E.

(iii) Pour tout $j \in [\![1,k]\!]$, et tout $K \subset E$ compact, il existe $g \in L^1(X, \mathbb{R}^+)$, tel que pour tout $u \in K$, $|\frac{\partial^j f}{\partial t^j}(u,x)| \leqslant g(x)$ p.p.

Alors $F(u) = \int_X f(u,x)d\mu(x)$ est définie pour tout $u \in E$ et $\mathcal{C}^k$ sur E, avec $F^{(j)}(u) = \int_X \frac{\partial^j f}{\partial u^j}(u,x)d\mu(x)$ pour tout $j \in [\![1,k]\!]$.

Exemple 10. *La fonction Γ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}^{+\star}$.*

3) Holomorphie

Théorème 11. *Soient $(X, \mathcal{T}, \mu)$ un espace mesuré et $f : \Omega \times X \to \mathbb{C}$. Posons pour tout $z \in \Omega$ $F(z) = \int_X f(z,x)d\mu(x)$, et supposons que :*

(i) $\forall z \in \Omega$, $x \mapsto f(z,x)$ est mesurable

(ii) $\forall x \in X$, $z \mapsto f(z,x)$ est holomorphe

(iii) Pour tout compact K de Ω, il existe $g \in L^1(X)$ telle que pour tous $z \in K$ et $x \in X$, $|f(z,x)| \leqslant g(x)$

Alors F est holomorphe et pour tous $z \in \Omega$ et $n \in \mathbb{N}$:

$$F^{(n)}(z) = \int_X \frac{\partial^n f}{\partial z^n}(z,x)d\mu(x)$$

Proposition 12. *Soit $P = \{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > 0\}$. On définit sur P la fonction holomorphe :*

$$\Gamma(z) = \int_0^{+\infty} e^{-t}t^{z-1}dt$$

Théorème 13. *Soit $\sum f_n$ une série de fonctions méromorphes sur Ω. On suppose que cette série converge uniformément (resp. normalement) sur tout compact de Ω, alors :*

(i) La somme f de cette série est méromorphe sur Ω.

(ii) La série $\sum f_n^{(k)}$ converge uniformément (resp. normalement) sur tout compact de Ω et sa somme est $f^{(k)}$.

Proposition 14. *Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$.*

II Produit de convolution

1) Définition et premières propriétés

Définition 15. Soient $f, g : \mathbb{R}^n \to \mathbb{R}$. Quand ceci a un sens, on pose :

$$(f * g)(x) = \int_{\mathbb{R}^n} f(t)g(x-t)\,dt$$

le produit de convolution de f et g en $x \in \mathbb{R}^n$.

Remarque 16. *Si f et g sont positives, $f * g$ est toujours définie, à valeurs dans $\overline{\mathbb{R}^+}$.*

Proposition 17. *La convolution entre fonctions mesurables positives est commutative et associative.*

Exemple 18. *Soit $f \in L^1(\mathbb{R}^n)$ positive, alors $f*0 = 0$ et $f * \mathbb{1}_{\mathbb{R}^n} = \int_{\mathbb{R}^n} f$.*

Proposition 19. *Soit $f \in L^1_{loc}(\mathbb{R}^n)$ à support compact. Alors $f * g$ est bien définie sur $\mathbb{R}^n$.*

Théorème 20. *Soient $p, q \in [1, +\infty]$ tels que $\frac{1}{p} + \frac{1}{q} = 1$, $f \in L^p(\mathbb{R}^n)$ et $g \in L^q(\mathbb{R}^n)$. Alors $f * g$ est bien définie sur $\mathbb{R}^n$, uniformément continue, et bornée par $\|f\|_p \|g\|_q$. De plus, si $1 < p, q < +\infty$, alors $\lim\limits_{\|x\| \to \infty} (f * g)(x) = 0$.*

Théorème 21. *$(L^1(\mathbb{R}^n), +, \cdot, *)$ est une $\mathbb{R}$-algèbre commutative.*

Théorème 22. *Soient $f \in L^1(\mathbb{R}^n)$ et $g \in \mathcal{C}^k_c(\mathbb{R}^n)$, alors $(f*g) \in \mathcal{C}^k_c(\mathbb{R}^n)$, et $D(f * g) = f * D(g)$, où D est un opérateur différentiel.*

2) Approximations de l'unité

Définition 23. Une suite $(\rho_n)_{n \geqslant 1}$ d'éléments de $L^1(\mathbb{R}^d)$ est une approximation de l'unité si elle vérifie :

(i) $\forall\, n \geqslant 1,\ \int_{\mathbb{R}^d} \rho_n = 1$

(ii) $\sup\limits_{n \geqslant 1} \int_{\mathbb{R}^d} |\rho_n| < +\infty$

(iii) $\forall\, \varepsilon > 0,\ \int_{\{|x| > \varepsilon\}} \rho_n \xrightarrow[n \to +\infty]{} 0$

Exemple 24. *Soit $\rho \in L^1(\mathbb{R}^d)$ telle que $\int_{\mathbb{R}^d} \rho = 1$, alors $\rho_n : x \mapsto n\rho(nx)$ est une approximation de l'identité.*

Théorème 25. *Soit $(\rho_n)_n$ une approximation de l'identité.*

(i) Si $f \in L^\infty(\mathbb{R}^d)$ est continue en x, alors $\lim\limits_{n \to +\infty} (\rho_n * f)(x) = f(x)$.

(ii) Si $f \in L^\infty(\mathbb{R}^d)$ est uniformément continue sur $\mathbb{R}^d$, alors $\lim\limits_{n \to +\infty} (\rho_n * f) = f$ dans $L^\infty(\mathbb{R}^d)$.

(iii) Si $f \in L^p(\mathbb{R}^d)$ ($p \in [1, +\infty[$), alors $\lim\limits_{n \to +\infty} (\rho_n * f) = f$ dans $L^p(\mathbb{R}^d)$.

Théorème 26. *Pour tout $p \in [1, +\infty[$, $\mathcal{C}^\infty_c(\mathbb{R}^d)$ est dense dans $L^p(\mathbb{R}^d)$.*

Exemple 27. *On pose $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ et $F_n : x \mapsto \frac{1}{n+1} \sum\limits_{k=0}^{n} \frac{\sin(2\pi(k+1)x)}{\sin(\pi x)}$ le noyau de Fejer. Il s'agit d'une approximation de l'unité.*

Théorème 28. *Si f est continue et 1-périodique, $f * F_n$ converge uniformément vers f.*

III Transformée de Fourier

Définition 29. Soit $f \in L^1(\mathbb{R}^d)$. Sa transformée de Fourier $\widehat{f}$ est :

$$\widehat{f} : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{R}^d \\ \xi & \longmapsto & \displaystyle\int_{\mathbb{R}^d} f(x) e^{-i\langle x, \xi \rangle}\, dx \end{array} \right.$$

Proposition 30. *Si $f \in L^1(\mathbb{R}^d)$, $\widehat{f}$ est une fonction continue qui tend vers 0 à l'infini.*

Proposition 31. *Si $||x||^k f(x) \in L^1(\mathbb{R}^d)$, alors $\widehat{f} \in \mathcal{C}^k(\mathbb{R}^d)$ et pour tout $\alpha \in \mathbb{N}^d$ tel que $|\alpha| \leqslant k$, $\partial^\alpha \widehat{f} = \widehat{(-ix)^\alpha f}$.*

Proposition 32. *Soit $f \in \mathcal{C}^k(\mathbb{R}^d)$ dont les dérivées jusqu'à l'ordre k sont dans $L^1(\mathbb{R}^d)$. Alors, pour tout $\alpha \in \mathbb{N}^d$ tel que $|\alpha| \leqslant k$, $\widehat{\partial^\alpha f} = (i\xi)^\alpha \widehat{f}$.*

Théorème 33. *Soit $f \in L^1(\mathbb{R}^d)$ telle que $\widehat{f} \in L^1(\mathbb{R}^d)$. Alors $\widehat{\widehat{f}} = (2\pi)^d \check{f}$.*

Exemple 34. *Soit $a > 0$, et $\mathbb{1}_{[-a,a]} \in L^1(\mathbb{R}^d)$, mais sa transformée de Fourier n'est pas dans $L^1(\mathbb{R}^d)$.*

Application 35. *Soient I un intervalle de $\mathbb{R}$ et ρ une fonction poids. S'il existe $a > 0$ tel que $\int_I e^{a|x|} \rho(x) dx < \infty$, alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I, \rho)$.*

Définition 36. Soit X un vecteur aléatoire sur $(\Omega, \mathcal{A}, \mathbb{P})$, à valeurs dans $\mathbb{R}^d$. On définit la fonction caractéristique de X par :

$$\varphi : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C} \\ t & \longmapsto & \mathbb{E}\left[e^{i\langle t, X\rangle}\right] = \displaystyle\int_{\mathbb{R}^d} e^{i\langle t, X\rangle} d\mathbb{P}_X(x) \end{array} \right.$$

Remarque 37. *Si X a pour densité f, alors $\varphi_X = \overset{\vee}{f}$.*

Théorème 38. *La fonction caractéristique φ_X caractérise la loi de X.*

Développements

- Fonction Gamma (12,14) [Les14]
- Densité des polynômes orthogonaux (35) [BMP05]

Références

[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[Les14] A. Lesfari. *Variables complexes.* Ellipses

Cadre : On considère X un ensemble non vide et $(E, \|.\|)$ un espace vectoriel normé de dimension finie. Soient $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions de X dans E et $f : X \to E$.

I Modes de convergence

1) Suites de fonctions

Définition 1. On dit que $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f lorsque, pour tout $x \in X$, $(f_n(x))_{n\in\mathbb{N}}$ converge vers $f(x)$. On note $f_n \xrightarrow{CS} f$.

Remarque 2. *Il y a unicité de la limite simple.*

Exemple 3. *Soit $f_n : x \mapsto x^n$ sur $[0,1]$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ converge simplement vers $f = \mathbb{1}_{\{1\}}$ sur $[0,1]$. On note que la convergence simple ne préserve pas la régularité.*

Définition 4. On dit que $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f lorsque $(\|f - f_n\|_\infty)_{n\in\mathbb{N}}$ converge vers 0. On note $f_n \xrightarrow{CU} f$.

Remarque 5. *La convergence uniforme implique la convergence simple.*

Contre-exemple 6. *Soit $f_n : x \mapsto x^n$ sur $[0,1]$. Alors la suite $(f_n)_{n\in\mathbb{N}}$ ne converge pas uniformément sur $[0,1]$.*

Exemple 7. *Soit $f_n : x \mapsto \frac{\sin(nx)}{1+n^2x^2}$ sur $\mathbb{R}$. La suite $(f_n)_{n\in\mathbb{N}}$ converge simplement vers $f = 0$ sur $\mathbb{R}$, mais pas uniformément car $f_n\left(\frac{\pi}{2n}\right) = \frac{1}{1+\frac{\pi^2}{4}}$.*

Théorème 8 (Critère de Cauchy uniforme)**.** *La suite $(f_n)_{n\in\mathbb{N}}$ converge uniformément si, et seulement si, elle est uniformément de Cauchy :*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ \forall p \in \mathbb{N}^\star,\ \|f_n - f_{n+p}\|_\infty < \varepsilon$$

Application 9. *La limite uniforme sur $\mathbb{R}$ d'une suite de polynômes est un polynôme.*

Théorème 10 (Weierstrass)**.** *L'ensemble des polynômes sur $[a,b]$ est dense dans $(\mathcal{C}^0([a,b],\mathbb{R}), \|.\|_\infty)$.*

2) Séries de fonctions

Définition 11. On appelle série des fonctions $(f_n)_{n\in\mathbb{N}}$ la suite $(S_n)_{n\in\mathbb{N}}$ des sommes partielles définies pour tout $n \in \mathbb{N}$ par $S_n : x \mapsto \sum_{k=0}^{n} f_k(x)$. On la note $\sum f_n$, et on dit que la série $\sum f_n$ converge simplement vers f si la suite $(S_n)_{n\in\mathbb{N}}$ converge simplement vers f. On note alors $f = \sum_{n\in\mathbb{N}} f_n$.

Remarque 12. *Si $\sum f_n$ converge simplement, alors $(f_n)_{n\in\mathbb{N}}$ converge simplement vers 0.*

Définition 13. On dit que la série $\sum f_n$ converge uniformément vers f si la suite $(S_n)_{n\in\mathbb{N}}$ converge uniformément vers f.

Proposition 14. *Si $\sum f_n$ converge uniformément, alors $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers 0.*

Proposition 15. *Soit $\sum f_n$ une série simplement convergente vers f. La convergence est uniforme si, et seulement si, $(f - S_n)_{n\in\mathbb{N}}$ converge uniformément vers 0.*

Exemple 16. *Soit $f_n : x \mapsto xe^{-nx}$ sur $\mathbb{R}^+$. Alors la série $\sum f_n$ converge simplement vers $f : x \mapsto \frac{x}{1-e^{-x}}\mathbb{1}_{\mathbb{R}^{+\star}}(x)$, mais ne converge pas uniformément sur $\mathbb{R}^+$.*

Théorème 17. *$\sum f_n$ converge uniformément si, et seulement si :*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N,\ \forall p \in \mathbb{N}^\star,\ \|f_{n+1} + \ldots + f_{n+p}\|_\infty < \varepsilon$$

Définition 18. On dit que la série $\sum f_n$ converge normalement si la série $\sum \|f_n\|_\infty$ converge.

Exemple 19. *Si $f_n : x \mapsto \frac{x^n}{n^2}$, $\sum f_n$ converge normalement sur $[0,1]$.*

Théorème 20. *La convergence normale implique la convergence uniforme.*

3) Liens avec la continuité

On suppose que X est une partie d'un espace vectoriel F.

Théorème 21. *La convergence uniforme conserve la continuité.*

Théorème 22 (Double limite)**.** *Soit $a \in \overline{X}$ tel que, pour tout $n \in \mathbb{N}$, $b_n = \lim_{x\to a} f_n(x)$ existe. Alors la suite $(b_n)_{n\in\mathbb{N}}$ converge vers b et on a :*

$$\lim_{n\to\infty}\lim_{x\to a} f_n(x) = \lim_{x\to a}\lim_{n\to\infty} f_n(x)$$

Théorème 23 (Dini)**.** *Toute suite croissante de $\mathcal{C}^0([a,b],\mathbb{K})$ qui converge simplement dans $\mathcal{C}^0([a,b],\mathbb{K})$ converge uniformément.*

II Dérivation et intégration

1) Dérivabilité

Ici, $X = I \subseteq \mathbb{R}$ est un intervalle.

Théorème 24. *Si $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f, et si f_n est dérivable sur I, il suffit d'avoir la convergence uniforme de $(f_n')_{n\in\mathbb{N}}$ pour que f soit dérivable sur I.*

Exemple 25. *Si $f_n : x \mapsto \sqrt{x^2 + \frac{1}{n^2}}$ sur $\mathbb{R}$, $(f_n)_{n\in\mathbb{N}}$ converge simplement vers la fonction valeur absolue, non dérivable en 0.*

Théorème 26. *Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions dérivables sur I. Si $\sum f_n$ converge simplement, et si $\sum f_n'$ converge uniformément, alors $f = \sum_{n\in\mathbb{N}} f_n$ est dérivable de dérivée $f' = \sum_{n\in\mathbb{N}} f_n'$*

Remarque 27. *On peut réitérer le théorème précédent pour une plus grande régularité.*

Exemple 28. $\exp : \mathbb{R} \to \mathbb{R}^+$ *est de classe $\mathcal{C}^\infty$.*

2) Convergence dans un espace mesuré

Soit $(X, \mathcal{A}, \mu)$ un espace mesuré.

Définition 29. On dit que $(f_n)_{n\in\mathbb{N}}$ converge μ-presque partout vers f lorsqu'il existe $N \in \mathcal{A}$ tel que $\mu(N) = 0$ et que $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f sur $X \setminus N$.

Définition 30. On dit que $(f_n)_{n\in\mathbb{N}}$ converge vers f dans L^p lorsque la suite $(\|f_n - f\|_p)_{n\in\mathbb{N}}$ est de limite nulle.

Exemple 31. *Si $(X, \mathcal{A}, \mu) = ([0,1], \mathcal{B}([0,1]), \lambda)$, on pose, pour $n \geqslant 0$ et $k \in [\![0, 2^n - 1[\![$, $f_{2^n+k} = \mathbb{1}_{[\frac{k}{2n}, \frac{k+1}{2n}]}$. Ceci définit bien une suite $(f_n)_{n\in\mathbb{N}}$, avec $\|f_n\|_p = 2^{-\frac{n}{p}} \to 0$, mais $(f_n)_{n\in\mathbb{N}}$ ne converge pas μ-presque partout.*

Proposition 32. *Soient $(f_n)_{n\in\mathbb{N}}$ une suite de $L^p(\mu)$ et $f \in L^p(\mu)$. Si $f_n \xrightarrow{L^p} f$, alors on peut extraire de $(f_n)_{n\in\mathbb{N}}$ une sous-suite convergeant μ-presque partout.*

3) Théorèmes d'interversion

Soit $(X, \mathcal{A}, \mu)$ un espace mesuré.

Théorème 33 (Beppo Levi)**.** *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré et $(f_n)_n$ une suite croissante de fonctions mesurables positives, alors $\lim\limits_{n\to\infty} f_n$ est mesurable et $\int_X \lim\limits_{n\to\infty} f_n d\mu = \lim\limits_{n\to\infty} \int_X f_n d\mu$.*

Application 34. *Soit $I_n(\alpha) = \int_0^n \left(1 - \frac{x}{n}\right)^n e^{\alpha x} dx$ pour $n \in \mathbb{N}$ et $\alpha \in \mathbb{R}$, alors $\lim\limits_{n\to\infty} I_n(\alpha) = \int_0^\infty e^{(\alpha-1)x} dx = \frac{1}{1-\alpha}$ si $\alpha < 1$ et $+\infty$ sinon.*

Théorème 35 (Lemme de Fatou)**.** *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré et $(f_n)_n$ une suite de fonctions mesurables et positives, alors $\int_X \liminf\limits_{n\to\infty} f_n d\mu \leqslant \liminf\limits_{n\to\infty} \int_X f_n d\mu$.*

Application 36. *Soit $(f_n)_n$ une suite de fonctions intégrables simplement convergente vers f telle que $\sup_n \int_X |f_n| d\mu < \infty$. Alors f est intégrable.*

Application 37. *Soit f croissante sur $[0,1]$, continue en 0 et 1, dérivable presque partout sur $[0,1]$, alors $\int_0^1 f'(t)dt \leqslant f(1) - f(0)$.*

Théorème 38 (Convergence dominée)**.** *Soit $(f_n)_n$ une suite d'éléments de $L^1(X, \mathbb{C}, \mu)$ et $f : X \to \mathbb{C}$ telles que :*

(i) $f_n(x) \to f(x)$ μ *p.p.*

(ii) $\exists\, g \in L^1(X, \mathbb{R}^+, \mu), \forall n \in \mathbb{N}, |f_n(x)| \leqslant g(x)$ μ *p.p.*

Alors $f \in L^1(X, \mathbb{C}, \mu)$ et $\lim\limits_{n\to\infty} \int_X f_n d\mu = \int_X f d\mu$.

Application 39. *Soit f dérivable partout sur $[0,1]$, de dérivée bornée. Alors $\int_0^1 f'(t)dt = f(1) - f(0)$.*

Théorème 40. *Soit $f_n : [a,b] \to E$ intégrable. Supposons que $\sum f_n$ converge uniformément sur $[a,b]$. Alors sa somme f est intégrable, et $\int_{[a,b]} \sum_{n\in\mathbb{N}} f_n = \sum_{n\in\mathbb{N}} \int_{[a,b]} f_n$.*

Exemple 41. $\int_0^1 x^x\, dx = \sum_{n=1}^\infty \frac{(-1)^n}{n^n}$.

III Exemples de séries de fonctions

1) Séries entières

Définition 42. On appelle série entière toute série de fonctions de la forme $\sum_{n\geqslant 0} a_n z^n$ où z est une variable complexe, et $a_n \in \mathbb{C}$.

Définition 43. Soit $\sum a_n z^n$ une série entière. On appelle rayon de convergence de $\sum a_n z^n$ le réel R défini par :

$$R = \sup\left\{r \in \mathbb{R}^+ \,\middle|\, \exists M \in \mathbb{R}, \forall n \in \mathbb{N}, |a_n| r^n \leqslant M\right\}$$

Théorème 44 (Abel angulaire)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 telle que $\sum a_n$ converge. On note f sa somme et :*

$$\Delta_\theta = \left\{z \in \mathbb{C} \,\middle|\, 1 - z = \rho e^{i\varphi},\ \rho > 0,\ |\varphi| < \theta\right\} \quad \textit{pour} \quad 0 \leqslant \theta < \frac{\pi}{2}$$

Alors :

$$\lim_{\substack{z\to 1\\ z\in\Delta_\theta}} f(z) = \sum_{n\geqslant 0} a_n$$

Application 45. $\sum\limits_{n\geqslant 0} \frac{(-1)^n}{2n+1} = \arctan(1) = \frac{\pi}{4}$ *et* $\sum\limits_{n\geqslant 1} \frac{(-1)^n}{n} = \ln(2)$

Théorème 46 (Taubérien faible)**.** *Soit f la somme d'une série entière $\sum a_n z^n$ de rayon de convergence 1. On suppose que $\lim\limits_{x\to 1^-} f(z) = \ell$ existe, et $a_n = o\left(\frac{1}{n}\right)$. Alors $\sum a_n$ converge et $\ell = \sum\limits_{n\geqslant 0} a_n$.*

2) Séries de Fourier

Définition 47. Soit $f : \mathbb{R} \to \mathbb{C}$ continue par morceaux et 2π-périodique. Les coefficients exponentiels de Fourier de f sont :

$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}\,dt \quad (n \in \mathbb{Z})$$

En posant $e_n : t \mapsto e^{int}$, la série de Fourier associée à f est la série trigonométrique $\sum_{n\in\mathbb{Z}} c_n(f)e_{-n}$.

Proposition 48 (Riemann-Lebesgue)**.** *Si f est continue par morceaux et 2π-périodique, alors* $\lim_{|n|\to+\infty} c_n(f) = 0$.

Théorème 49. *La famille $(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de l'espace des fonctions 2π-périodiques de carré intégrable sur $[0, 2\pi]$. On a en particulier :*

$$\frac{1}{2\pi}\|f\|_2^2 = \sum_{n\in\mathbb{Z}} c_n(f)^2$$

Proposition 50. *Si f est $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge simplement vers la régularisation $\tilde{f}$ de f donnée pour $x \in \mathbb{R}$ par $\tilde{f}(x) = \frac{f(x^+)+f(x^-)}{2}$.*

Remarque 51. *L'hypothèse $\mathcal{C}^1$ par morceaux est nécessaire.*

Théorème 52. *Si f est continue, $\mathcal{C}^1$ par morceaux et 2π-périodique, alors la série de Fourier de f converge normalement vers f.*

Théorème 53. *Pour $u_0 \in L^2(\mathbb{T})$, on considère l'équation différentielle :*

$$\begin{cases} \frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 & \textit{sur } \mathbb{R}^{+\star}\times\mathbb{T} \\ u(0,.) = u_0 & \textit{dans } L^2(\mathbb{T}) \end{cases} \qquad (*)$$

Il existe une unique solution u de $(*)$ de classe $\mathcal{C}^2$ sur $\mathbb{R}^{+\star}\times\mathbb{T}$, avec $u(t,.)$ tendant vers u_0 dans $L^2(\mathbb{T})$ quand t tend vers 0.

Développements

- Théorèmes d'Abel angulaire et taubérien faible (44,46) [Gou08]
- Équation de la chaleur sur le cercle (53) [Can09]

Références

[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions.* Ellipses
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BP12] M. Briane et G. Pagès. *Théorie de l'intégration.* Vuilbert
[Hau07] B. Hauchecorne. *Les Contre-exemples en Mathématiques.* Ellipses
[Can09] B. Candelpergher. *Calcul intégral.* Cassini

I Généralités sur les séries entières

1) Définitions et premières propriétés

Définition 1. On appelle série entière toute série de fonctions de la forme $\sum_{n\geqslant 0} a_n z^n$ où z est une variable complexe, et $a_n \in \mathbb{C}$.

Exemple 2. *(i)* $\forall x \in \mathbb{R},\ e^x = \sum_{n\geqslant 0} \frac{x^n}{n!}$

(ii) $\forall x \in]-1,1[,\ \ln(1+x) = \sum_{n\geqslant 1} (-1)^n \frac{x^n}{n}$

Lemme 3 (Abel)**.** *Soit $\sum a_n z^n$ une série entière, et soit $z_0 \in \mathbb{C}$ tel que $(a_n z_0^n)_n$ soit bornée, alors :*

(i) Pour tout $z \in D(0,|z_0|)$, $\sum a_n z^n$ est absolument convergente.

(ii) Pour tout $r \in]0,|z_0|[$, $\sum a_n z^n$ converge normalement sur $\overline{D(0,r)}$.

Définition 4. Soit $\sum a_n z^n$ une série entière. On appelle rayon de convergence de $\sum a_n z^n$ le réel R défini par :

$$R = \sup\left\{ r \in \mathbb{R}^+ \,\middle|\, \exists M \in \mathbb{R}, \forall n \in \mathbb{N}, |a_n| r^n \leqslant M \right\}$$

$D(0,R)$ s'appelle le disque de convergence de $\sum a_n z^n$.

Corollaire 5. *Soit $\sum a_n z^n$ une série entière de rayon de convergence R.*

(i) Pour tout $z \in D(0,R)$, $\sum a_n z^n$ est absolument convergente.

(ii) Pour tout $z \in \mathbb{C} \setminus \overline{D(0,R)}$, $\sum a_n z^n$ diverge.

(iii) Pour tout $r \in]0,R[$, $\sum a_n z^n$ converge normalement sur $\overline{D(0,r)}$.

2) Détermination du rayon de convergence

Proposition 6 (Règle de d'Alembert)**.** *Soit $\sum a_n z^n$ une série entière. Si $\lim_{n\to+\infty} \left|\frac{a_{n+1}}{a_n}\right| = \lambda$, avec $\lambda \in \mathbb{R} \cup \{+\infty\}$, alors le rayon de convergence de la série entière $\sum a_n z^n$ est $R = \frac{1}{\lambda}$ (en convenant $\frac{1}{0} = +\infty$ et $\frac{1}{+\infty} = 0$).*

Proposition 7 (Règle de Cauchy)**.** *Soit $\sum a_n z^n$ une série entière. Si $\lim_{n\to+\infty} |a_n|^{\frac{1}{n}} = \lambda$, avec $\lambda \in \mathbb{R} \cup \{+\infty\}$, alors le rayon de convergence de la série entière $\sum a_n z^n$ est $R = \frac{1}{\lambda}$ (en convenant $\frac{1}{0} = +\infty$ et $\frac{1}{+\infty} = 0$).*

Proposition 8 (Règle d'Hadamard)**.** *Soit $\sum a_n z^n$ une série entière. Si $\limsup_{n\to+\infty} |a_n|^{\frac{1}{n}} = \lambda$, avec $\lambda \in \mathbb{R} \cup \{+\infty\}$, alors le rayon de convergence de la série entière $\sum a_n z^n$ est $R = \frac{1}{\lambda}$ (en convenant $\frac{1}{0} = +\infty$ et $\frac{1}{+\infty} = 0$).*

3) Opération sur les séries entières

Soient $\sum a_n z^n$ et $\sum b_n z^n$ deux séries entières de rayon de convergence respectivement égal à $R > 0$ et $R' > 0$.

Définition 9. La série entière $\sum c_n z^n$ définie par $c_n = a_n + b_n$ est appelée somme des séries entières $\sum a_n z^n$ et $\sum b_n z^n$. Son rayon de convergence R'' vérifie $R'' \geqslant \inf(R, R')$.

Définition 10. La série entière $\sum c_n z^n$ définie par $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ est appelée produit de Cauchy des séries entières $\sum a_n z^n$ et $\sum b_n z^n$. Son rayon de convergence R'' vérifie $R'' \geqslant \inf(R, R')$.

II Propriétés de la somme

1) Régularité

Théorème 11. *L'application f, appelée somme de la série entière $\sum a_n z^n$, définie par :*

$$f : \left| \begin{array}{ccc} D(0,R) & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \sum_{n=0}^{n} a_n z^n \end{array} \right.$$

est de classe $\mathcal{C}^1$. De plus, sa dérivée est donnée par :

$$f' : \left| \begin{array}{ccc} D(0,R) & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \sum_{n=1}^{n} n a_n z^{n-1} \end{array} \right.$$

Corollaire 12. *La somme de la série entière $\sum a_n z^n$ est en fait $\mathcal{C}^\infty$ sur son disque de convergence. De plus, pour tout $p \in \mathbb{N}$, $f^{(p)}$ est la somme d'une série entière. En outre :*

$$\forall\, z \in \mathbb{C},\ f(z) = \sum_{p=0}^{\infty} \frac{f^{(p)}(0)}{p!} z^p$$

2) Analycité

Définition 13. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et soit Ω un ouvert de $\mathbb{K}$. On dit que $f : \Omega \to \mathbb{K}$ est développable en série entière au voisinage de $a \in \Omega$ s'il existe une série entière $\sum a_n z^n$ et $r > 0$ tels que :

$$\forall\, z \in D(a,r),\ f(z) = \sum_{n\geqslant 0} a_n (z-a)^n$$

La foncion f est dite analytique sur Ω si elle est développable en série entire en chaque point de Ω.

Théorème 14. *Soit $\sum a_n z^n$ une série entière de rayon de convergence R. Alors la somme f de la série est analytique sur $D(0,R)$.*

Théorème 15 (Zéros isolés)**.** *Soit f une fonction analytique sur un ouvert connexe $\mathcal{U}$ non identiquement nulle. Alors les zéros de f sont isolés.*

Corollaire 16 (Prolongement analytique)**.** *Soit $\mathcal{U}$ un ouvert connexe. Si deux fonctions analytiques coïncident sur un sous-ensemble $D \subset \mathcal{U}$ ayant un point d'accumulation dans $\mathcal{U}$, alors elles sont égales sur $\mathcal{U}$.*

Théorème 17 (Formule de Cauchy)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence R, et soit f la somme de cette série entière sur son disque de convergence, alors :*

$$\forall\, r \in]0,R[,\ \forall\, n \in \mathbb{N},\ 2\pi r^n a_n = \int_0^{2\pi} f(re^{i\theta}) e^{-in\theta}\, d\theta$$

III Comportement au bord de $D(0,R)$

Exemple 18. *La série entière $\sum z^n$ a pour rayon de convergence 1, et cette série diverge sur tout le cercle unité.*

Exemple 19. *La série entière $\sum \frac{z^n}{n^2}$ a pour rayon de convergence 1, et cette série converge sur tout le cercle unité.*

Exemple 20. *La série entière $\sum \frac{z^n}{n}$ a pour rayon de convergence 1, et cette série diverge pour $z = 1$ et converge pour $z = -1$.*

Théorème 21 (Abel angulaire)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 telle que $\sum a_n$ converge. On note f sa somme et :*

$$\Delta_\theta = \left\{ z \in \mathbb{C} \,\middle|\, 1 - z = \rho e^{i\varphi},\ \rho > 0,\ |\varphi| < \theta \right\} \quad \textit{pour} \quad 0 \leqslant \theta < \frac{\pi}{2}$$

Alors :

$$\lim_{\substack{z\to 1 \\ z\in\Delta_\theta}} f(z) = \sum_{n\geqslant 0} a_n$$

Théorème 22 (Taubérien faible)**.** *Soit f la somme d'une série entière $\sum a_n z^n$ de rayon de convergence 1. On suppose que $\lim\limits_{x\to 1^-} f(z) = \ell$ existe, et $a_n = o\left(\frac{1}{n}\right)$. Alors $\sum a_n$ converge et $\ell = \sum\limits_{n\geqslant 0} a_n$.*

IV Applications

1) Suites récurrentes

Exemple 23. *On considère la suite $(a_n)_n$ définie par :*

$$\begin{cases} a_0 = 1 \\ \forall n \in \mathbb{N}, a_{n+1} = 2a_n + 2^n \end{cases}$$

Alors, pour tout $n \in \mathbb{N}$, on a $a_n = (n+2)2^{n-1}$.

Proposition 24 (Nombres de Bell)**.** *Pour $n \in \mathbb{N}^\star$, on pose B_n le nombre de partitions de l'ensemble $[\![1,n]\!]$ avec la convention $B_0 = 1$, alors :*

$$\forall\, k \in \mathbb{N},\ B_k = \frac{1}{e} \sum_{n\geqslant 0} \frac{n^k}{n}$$

2) Équation différentielles

Exemple 25. *L'équation $x^2 y'' + 4xy' + 2y = e^x$ admet $x \mapsto \frac{e^x - 1 - x}{x^2}$ comme solution développable en série entière.*

Exemple 26. *L'ensemble des solutions développables en séries entières de $xy'' + y' + y = 0$ est la droite vectorielle engendrée par :*

$$f : x \mapsto \sum_{n\geqslant 0} \frac{(-x)^n}{(n!)^2}$$

3) Construction de l'exponentielle complexe

Définition 27. On pose :

$$\exp : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \exp(z) = e^z = \sum_{n \geqslant 0} \frac{z^n}{n!} \end{array} \right.$$

Théorème 28. exp *est une surjection de* $\mathbb{C}$ *dans* $\mathbb{C}^\star$.

Définition 29. On pose :

$$\cos : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \frac{e^{iz}+e^{-iz}}{2} \end{array} \right. \quad \text{et} \quad \sin : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \frac{e^{iz}-e^{-iz}}{2i} \end{array} \right.$$

Corollaire 30. *(i)* $\forall z \in \mathbb{C},\ \cos z = \sum_{n \geqslant 0} (-1)^n \frac{x^{2n}}{(2n)!}$

(ii) $\forall z \in \mathbb{C},\ \sin z = \sum_{n \geqslant 0} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$

Développements

- Théorèmes d'Abel angulaire et taubérien faible (21,22) [Gou08]
- Nombres de Bell (24) [FGN13a]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Cadre : Ω est un ouvert de $\mathbb{C}$.

I $\mathbb{C}$-dérivabilité

Définition 1. Soient $f : \Omega \to \mathbb{C}$ et $a \in \mathbb{C}$. On dit que f est $\mathbb{C}$-dérivable en a lorsque $\lim\limits_{h\to 0} \frac{f(a+h)-f(a)}{h}$ existe. On note $f'(a)$ cette limite.

Proposition 2. *Si f est $\mathbb{C}$-dérivable en a, alors f est continue en a.*

Définition 3. f est dite holomorphe sur Ω si f est $\mathbb{C}$-dérivable en tout point de Ω. On note $\mathcal{H}(\Omega)$ l'ensemble des fonctions holomorphes sur Ω.

Exemple 4. $\forall n \in \mathbb{N}, (z \mapsto z^n) \in \mathcal{H}(\mathbb{C}),\ (z \mapsto \frac{1}{z}) \in \mathcal{H}(\mathbb{C}^\star)$

Contre-exemple 5. $(z \mapsto \overline{z}) \notin \mathcal{H}(\mathbb{C})$

Proposition 6. *(i) $\mathcal{H}(\Omega)$ est une sous-algèbre de $\mathbb{C}^\Omega$.*

(ii) Si $f \in \mathcal{H}(\Omega)$ est à valeurs dans $\mathbb{C}^\star$, alors $\frac{1}{f} \in \mathcal{H}(\Omega)$.

(iii) Si $f \in \mathcal{H}(\Omega)$ et $g \in \mathcal{H}(\Omega')$ avec $f(\Omega) \subseteq \Omega'$, alors $g \circ f \in \mathcal{H}(\Omega)$.

Corollaire 7. *Si $f(z) = \sum\limits_{n\geqslant 0} a_n z^n$ est une série entière de rayon de convergence $R > 0$, alors $f(z)$ est holomorphe sur $D(0, R)$.*

Théorème 8. *La fonction $f(z) = u(x, y) + iv(x, y)$ où $z = x + iy$, est holomorphe si, et seulement si, u et v sont différentiables sur Ω et vérifient les équations de Cauchy-Riemann :*

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \quad \text{et} \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

Corollaire 9. *Si $\frac{\partial}{\partial \overline{z}} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right)$, alors $f \in \mathcal{H}(\Omega) \Leftrightarrow \frac{\partial f}{\partial \overline{z}} = 0$.*

II Propriétés des fonctions holomorphes

1) Chemin

Définition 10. On appelle chemin dans $\mathbb{C}$ toute application $\gamma : [a, b] \to \mathbb{C}$ continue et $\mathcal{C}^1$ par morceaux. On parle de lacet si $\gamma(a) = \gamma(b)$.

Exemple 11. *Soient $z_0 \in \mathbb{C}$ et $r \in \mathbb{R}^+$, alors une paramétrisation du cercle de centre z_0 et de rayon r est donnée par :*

$$\gamma : \left| \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & z_0 + re^{2i\pi t} \end{array} \right.$$

Définition 12. Soient $\gamma : [a, b] \to \mathbb{C}$ un chemin et f une fonction continue sur $\mathrm{Im}(\gamma)$, alors on définit :

$$\forall\, z \in \mathrm{Im}(\gamma),\ \int_\gamma f = \int_\gamma f(z)\, dz = \int_a^b f(\gamma(t))\, \gamma'(t)\, dt$$

Exemple 13. *Si $\gamma(t) = z_0 + re^{2i\pi t}$, alors $\int \frac{1}{z-z_0}\, dz = 2i\pi$.*

2) Formule de Cauchy

Théorème 14. *Soient Ω un ouvert convexe et $z_0 \in \Omega$ et $f \in \mathcal{C}(\Omega) \cap \mathcal{H}(\Omega \setminus \{z_0\})$, alors pour tout lacet γ de Ω, on a $\int_\gamma f = 0$.*

Définition 15. Soit γ un lacet de $\mathbb{C}$ et $a \in \mathbb{C} \setminus \mathrm{Im}(\gamma)$. On définit l'indice $\mathrm{Ind}_\gamma(a)$ de a par rapport à γ par :

$$\mathrm{Ind}_\gamma(a) = \frac{1}{2i\pi} \int_\gamma \frac{1}{z-a} dz$$

Proposition 16. $\mathrm{Ind}_\gamma(a) \in \mathbb{Z}$

Théorème 17 (Formule de Cauchy)**.** *Soient Ω est un ouvert convexe, $z \in \Omega$, γ un lacet de $\Omega \setminus \{z\}$ et $f \in \mathcal{H}(\Omega)$, alors on a :*

$$\mathrm{Ind}_\gamma(z) f(z) = \frac{1}{2i\pi} \int_\gamma \frac{f(\xi)}{\xi - z} d\xi$$

Exemple 18. *Si γ décrit le cercle unité parcouru une fois dans le sens direct, alors $\int_\gamma \frac{\cos z}{z} dz = 0$ et $\int_\gamma \frac{\sin z}{z} dz = 2\pi$.*

3) Conséquence de la théorie de Cauchy

Définition 19. On dit que $f : \Omega \to \mathbb{C}$ est analytique si pour tout $z_0 \in \Omega$, il existe $r > 0$ et $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}^\mathbb{N}$ tels que pour tout $z \in D(z_0, r)$, $f(x) = \sum\limits_{n\geqslant 0} a_n (z - z_0)^n$.

Théorème 20. *Si f est holomorphe sur Ω, alors f est analytique sur Ω.*

Corollaire 21. *Une fonction holomorphe sur Ω est de classe $\mathcal{C}^\infty$ sur Ω.*

Proposition 22 (Inégalité de Cauchy). *Soit $f \in \mathcal{H}(\overline{D(a,r)})$ avec $a \in \mathbb{C}$ et $r > 0$, alors pour tout $n \in \mathbb{N}$, $|\frac{f^{(n)}(a)}{n!}| \leqslant \frac{M}{r^n}$, où $M = \max_{z \in \partial D(a,r)} (|f(z)|)$.*

Théorème 23 (Liouville). *Toute fonction holomorphe sur $\mathbb{C}$ et bornée est constante.*

Corollaire 24 (Théorème de d'Alembert). *Tout polynôme non constant à coefficients dans $\mathbb{C}$ admet au moins une racine.*

Théorème 25. *Soient $\Omega \subset \mathbb{C}$ connexe, $f \in \mathcal{H}(\mathbb{C})$ et $z_0 \in \Omega$. Les assertions suivantes sont équivalentes :*

(i) $\forall k \in \mathbb{N}, f^{(k)}(z_0) = 0$

(ii) *f est nulle sur un voisinage de z_0*

(iii) *f est nulle sur Ω*

Corollaire 26. *Soient f et g holomorphes sur Ω un connexe de $\mathbb{C}$. Si f et g coïncident sur un voisinage d'un point de Ω, alors $f = g$.*

Théorème 27 (Zéros isolés). *Soient Ω un connexe de $\mathbb{C}$ et f holomorphe sur Ω et non identiquement nulle, alors les zéros de f sont isolés.*

Corollaire 28. *Si deux fonctions holomorphes coïncident sur un ensemble admettant un point d'accumulation, alors elles sont égales.*

Exemple 29. *Il n'existe pas de fonction holomorphe sur $D(0,1)$ tel que pour tout $n \geqslant 1$, $f(\frac{1}{n}) = f(-\frac{1}{n}) = -\frac{1}{n^3}$.*

Corollaire 30. *$\mathcal{H}(\Omega)$ est intègre.*

Théorème 31 (Principe du maximum). *Soit $f \in \mathcal{H}(\Omega)$. Si $|f|$ atteint son maximum en un point de Ω, alors f est constante.*

Corollaire 32 (Lemme de Schwarz). *Soit $f \in \mathcal{H}(D(0,1))$ telle que $f(0) = 0$ et $\forall z \in D(0,1)$, $|f(z)| \leqslant 1$, alors $\forall z \in D(0,1)$, $|f(z)| \leqslant |z|$.*
S'il existe $z_0 \in D(0,1) \setminus \{0\}$ pour lequel $|f(z_0)| = |z_0|$, alors il existe une constante λ de module 1 telle que $\forall z \in D(0,1)$, $f(z) = \lambda z$.

Corollaire 33. *Les automorphismes (bijections biholomorphes) de $D(0,1)$ tels que $f(0) = 0$ sont de la forme : $z \mapsto e^{i\theta} z$, où $\theta \in \mathbb{R}$.*

Corollaire 34. $\mathrm{Aut}(D(0,1)) = \left\{ z \mapsto e^{i\theta} \left(\frac{z - z_0}{1 - \overline{z_0} z} \right) \,\middle|\, \theta \in \mathbb{R}, |z_0| < 1 \right\}$

4) Intégration à paramètre

Théorème 35. *Soient $(X, \mathcal{T}, \mu)$ un espace mesuré et $f : \Omega \times X \to \mathbb{C}$. Posons pour tout $z \in \Omega$ $F(z) = \int_X f(z,x) d\mu(x)$, et supposons que :*

(i) $\forall z \in \Omega$, $x \mapsto f(z,x)$ *est mesurable*

(ii) $\forall x \in X$, $z \mapsto f(z,x)$ *est holomorphe*

(iii) *Pour tout compact K de Ω, il existe $g \in L^1(X)$ telle que pour tous $z \in K$ et $x \in X$, $|f(z,x)| \leqslant g(x)$*

Alors F est holomorphe et pour tous $z \in \Omega$ et $n \in \mathbb{N}$:

$$F^{(n)}(z) = \int_X \frac{\partial^n f}{\partial z^n}(z,x) d\mu(x)$$

Corollaire 36. *Soit $P = \{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > 0\}$. On définit sur P la fonction holomorphe :*

$$\Gamma(z) = \int_0^{+\infty} e^{-t} t^{z-1} dt$$

III Fonctions méromorphes

1) Séries de Laurent

Définition 37. Une série de Laurent est une série de la forme :

$$\sum_{k \in \mathbb{Z}} a_k z^k \text{ où } (a_k)_{k \in \mathbb{Z}} \in \mathbb{C}^{\mathbb{Z}}$$

Théorème 38. *Soit f une fonction holomorphe sur une couronne centrée en $z_0 \in \mathbb{C}$, alors, pour un lacet γ de la couronne entourant z_0, on a :*

$$f(z) = \sum_{k \in \mathbb{Z}} a_k (z - z_0)^k \quad \text{où} \quad a_k = \frac{1}{2i\pi} \int_\gamma \frac{f(z)}{(z - z_0)^{k+1}} dz$$

Définition 39. Soit $a \in \mathbb{C}$. On dit qu'une fonction f admet une singularité en a si il existe un voisinage U de a telle que f est définie et holomorphe sur $U \setminus \{a\}$.

Théorème 40. *Soit $a \in \mathbb{C}$, et soit f une fonction holomorphe sur $\Omega \setminus \{a\}$. Alors f vérifie une, et une seule, des propriétés suivantes :*

(i) *a est une singularité artificielle : f se prolonge au voisinage de a en une fonction holomorphe.*

(ii) *a est un pôle d'ordre m : il existe un entier $m \geqslant 1$ minimal tel que $(z - a)^m f(z)$ est borné au voisinage de a.*

(iii) a est une sigularité essentielle : pour tout voisinage U de a dans Ω, $f(U \setminus \{a\})$ est dense dans $\mathbb{C}$.

Exemple 41. *(i) 2 est un pôle d'ordre 2 de $z \mapsto \frac{1}{(z-2)^2}$.*

(ii) 0 est une singularité essentielle de $z \mapsto e^{\frac{1}{z}}$.

Théorème 42. *Soit $a \in \mathbb{C}$, et soit f une fonction holomorphe sur $\Omega \setminus \{a\}$,. Alors f est développable en série de Laurent et :*

(i) a est une singularité artificielle $\Leftrightarrow \forall n < 0, a_n = 0$.

(ii) a est un pôle d'ordre $m \Leftrightarrow \forall n < m, a_n = 0$.

(iii) a est une singularité essentielle $\Leftrightarrow a_n \neq 0$ pour une infinité de n négatifs.

2) Théorème des résidus

Définition 43. On dit qu'une fonction f est méromorphe sur Ω s'il existe $A \subset \mathbb{C}$ discret et fermé tel que f est holomorphe sur $\Omega \setminus A$ et les points de A sont des pôles de f.

Exemple 44. *$f(z) = \frac{z}{(z-1)(z-2)^2}$ est méromorphe.*

Définition 45. Soit $z_0 \in \mathbb{C}$, U un voisinage de z_0, et soit f une fonction holomorphe sur $U \setminus \{z_0\}$. On appelle résidu de f au point z_0 le nombre $\mathrm{Res}(f, z_0) = a_{-1}$, où a_{-1} est le coefficient de $\frac{1}{z-z_0}$ dans le développement en série de Laurent de f au voisinage de z_0.

Proposition 46. *Si z_0 est un pôle d'ordre m de f, alors :*

$$\mathrm{Res}(f, z_0) = \frac{1}{(m-1)!} \lim_{z \to z_0} \frac{\partial^{m-1}}{\partial z^{m-1}} \left((z - z_0)^m f(z)\right)$$

Si z_0 est un pôle simple de $f(z) = \frac{P(z)}{Q(z)}$ avec $P(z_0) \neq 0$, alors :

$$\mathrm{Res}(f, z_0) = \frac{P(z_0)}{Q'(z_0)}$$

Exemple 47. *Pour $f(z) = \frac{z}{(z-1)(z-2)^2}$, $\mathrm{Res}(f, 1) = 1$ et $\mathrm{Res}(f, 2) = -1$.*

Théorème 48 (Théorème des résidus)**.** *Soient $S \subset \Omega$ fini, $f \in \mathcal{H}(\mathbb{C} \setminus S)$ et γ un lacet dans Ω ne rencontrant pas S, alors :*

$$\int_\gamma f(z)dz = 2i\pi \sum_{c \in S} \mathrm{Ind}_\gamma(c)\, \mathrm{Res}(f, c)$$

Exemple 49. $\int_0^{+\infty} \frac{\sin x}{x} dx = \frac{\pi}{2}$

Exemple 50. *Soit $\alpha \in]-1, 1[$. Alors $\int_0^{+\infty} \frac{x^\alpha \ln x}{x^2-1}\, dx = \frac{\pi^2}{4\cos^2(\frac{\alpha\pi}{2})}$.*

3) Suite de fonctions méromorphes

Définition 51. Soient $A \subset \Omega$ et $(f_n)_{n \in \mathbb{N}}$ une suite de fonctions méromorphes sur Ω. On dit que $\sum f_n$ converge uniformément (resp. normalement) sur A si :

(i) À partir d'un certain rang, f_n n'a pas de pôles dans A.

(ii) $\sum_{n>N} f_n$ converge uniformément (resp. normalement) sur A.

Théorème 52. *Soit $\sum f_n$ une série de fonctions méromorphes sur Ω. On suppose que cette série converge uniformément (resp. normalement) sur tout compact de Ω, alors :*

(i) La somme f de cette série est méromorphe sur Ω.

(ii) La série $\sum f_n^{(k)}$ converge uniformément (resp. normalement) sur tout compact de Ω et sa somme est $f^{(k)}$.

Corollaire 53. *Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$.*

Développements

- Les biholomorphismes du disque unité (32,33,34) [Les14]
- Fonction Gamma (36,53) [Les14]
- Calcul d'une intégrale par le théorème des résidus (50) [Tau06]

Références

[Cho20] M. Choulli. *Analyse complexe.* DeBoeck
[Tau06] P. Tauvel. *Analyse complexe pour la licence 3.* Dunod
[Les14] A. Lesfari. *Variables complexes.* Ellipses
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K
[Mai13] F. Maisonneuve. *Fonction d'une variable complexe.* Bréal

Cadre : On pose $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$, et on considère des fonction 2π-périodiques que l'on identifie à des fonctions $f : \mathbb{T} \to \mathbb{C}$.

I Définitions et premières propriétés

1) Définition des séries de Fourier

Définition 1. On pose $CM(\mathbb{T})$ l'espace vectoriel des fonctions $f : \mathbb{T} \to \mathbb{R}$ continues par morceaux, et $C(\mathbb{T})$ le sous-espace vectoriel formé des fonctions continues. On considère $L^p(\mathbb{T})$ comme identifié avec $L^p([0, 2\pi])$.

Définition 2. Les coefficients exponentiels de Fourier de $f \in L^1(\mathbb{T})$ sont :

$$c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}\,dt \quad (n \in \mathbb{Z})$$

Les coefficients trigonométriques de Fourier de $f \in L^1(\mathbb{T})$ sont :

$$a_n(f) = \frac{1}{\pi}\int_0^{\pi} f(t)\cos(nt)\,dt\ ,\ b_n(f) = \frac{1}{\pi}\int_0^{\pi} f(t)\sin(nt)\,dt \quad (n \in \mathbb{N})$$

Proposition 3. *Soient $f \in L^1(\mathbb{T})$ et $n \in \mathbb{N}$, alors :*

$$\left\{\begin{array}{rcl} c_n(f) &=& \frac{1}{2}(a_n(f) - ib_n(f)) \\ c_{-n}(f) &=& \frac{1}{2}(a_n(f) + ib_n(f)) \end{array}\right. \text{ et } \left\{\begin{array}{rcl} a_n(f) &=& c_n(f) + c_{-n}(f) \\ b_n(f) &=& i(c_n(f) - c_{-n}(f)) \end{array}\right.$$

Proposition 4. *Soient $f \in L^1(\mathbb{T})$ et $n \in \mathbb{N}$, alors :*

(i) Si f est paire, $a_n(f) = \frac{2}{\pi}\int_0^{\pi} f(t)\cos(nt)\,dt$ et $b_n(f) = 0$.

(ii) Si f est impaire, $b_n(f) = \frac{2}{\pi}\int_0^{\pi} f(t)\sin(nt)\,dt$ et $a_n(f) = 0$.

Exemple 5. *Soit $f_1 : \mathbb{R} \to \mathbb{R}$ impaire et 2π-périodique définie par $f_1(t) = \frac{\pi}{2} - |x - \frac{\pi}{2}|$ si $t \in [0, \pi]$. Alors, pour tout $n \in \mathbb{N}$:*

$$a_n(f_1) = 0\ ,\ b_{2n}(f_1) = 0\ ,\ b_{2n+1}(f_1) = \frac{4(-1)^n}{\pi(2n+1)^2}$$

Exemple 6. *Soit $f_2 : \mathbb{R} \to \mathbb{R}$ impaire et 2π-périodique définie par $f_2(t) = \sin^2(t)$ si $t \in [0, \pi]$. Alors, pour tout $n \in \mathbb{N}$:*

$$a_n(f_2) = 0\ ,\ b_{2n}(f_2) = 0\ ,\ b_{2n+1}(f_2) = \frac{-8}{\pi(2n-1)(2n+1)(2n+3)}$$

Exemple 7. *Soit $f_3 : \mathbb{R} \to \mathbb{R}$ paire et 2π-périodique définie par $f_3(t) = |t|$ si $t \in [-\pi, \pi]$. Alors, pour tout $n \in \mathbb{N}$:*

$$a_0(f_3) = \pi\ ,\ a_{2n}(f_3) = 0\ ,\ a_{2n+1}(f_3) = \frac{-4}{\pi(2n+1)^2}\ ,\ b_n(f_3) = 0$$

Définition 8. Soit $f \in L^1(\mathbb{T})$. On appelle série de Fourier de f la série :

$$S(f) = \sum_{n=-\infty}^{\infty} c_n(f)e^{int} = \frac{a_0(f)}{2} + \sum_{n=1}^{\infty}(a_n(f)\cos(nt) + b_n(f)\sin(nt))$$

Pour $N \in \mathbb{N}$, on appelle somme de Fourier d'ordre N :

$$S_N(f) = \sum_{n=-N}^{N} c_n(f)e^{int} = \frac{a_0(f)}{2} + \sum_{n=1}^{N}(a_n(f)\cos(nt) + b_n(f)\sin(nt))$$

Exemple 9. $S(f_1)(t) = \frac{4}{\pi}\sum_{n=0}^{\infty}\frac{(-1)^n\sin((2n+1)t)}{(2n+1)^2}$

Exemple 10. $S(f_2)(t) = \frac{-8}{\pi}\sum_{n=0}^{\infty}\frac{\sin((2n+1)t)}{(2n-1)(2n+1)(2n+3)}$

Exemple 11. $S(f_3)(t) = \frac{\pi}{2} - \frac{4}{\pi}\sum_{n=0}^{\infty}\frac{\cos((2n+1)t)}{(2n+1)^2}$

2) Premières propriétés

Proposition 12. *Soient $f \in L^1(\mathbb{T})$, $a \in \mathbb{R}$ et $k, n \in \mathbb{Z}$. Alors :*

(i) $c_n(\check{f}) = \overline{c_{-n}(f)}$ *(où $\check{f}(x) = f(-x)$)*

(ii) $c_n(\overline{f}) = \overline{c_{-n}(f)}$

(iii) $c_n(\tau_a f) = e^{-ina}c_n(f)$ *(où $(\tau_a f)(x) = f(x-a)$)*

(iv) $c_n(e_k f) = c_{n-k}(f)e_n$ *(où $e_k(t) = e^{ikt}$)*

Exemple 13. *Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(t) = \frac{1}{1+\cos^2 t}$, alors, pour tout $n \in \mathbb{Z}$, $c_{2n+1}(f) = 0$ et $c_{2n}(f) = \frac{1}{\pi}\int_0^{\pi}\frac{\cos(2nt)}{1+\cos^2 t}\,dt$.*

Proposition 14. *Soit $f \in C(\mathbb{T})$ de classe $\mathcal{C}^1$ par morceaux. Alors $f' \in CM(\mathbb{T})$ et, pour tout $n \in \mathbb{Z}$, on a $c_n(f') = in\,c_n(f)$.*

Théorème 15 (Riemann-Lebesgue)**.** *Soit $f \in L^1(\mathbb{T})$. Alors $c_n(f)$ tend vers 0 lorsque n tend vers $\pm\infty$.*

Corollaire 16. *Soient $k \in \mathbb{N}^\star$ et $f \in C(\mathbb{T})$ de classe $\mathcal{C}^{k-1}$ sur $\mathbb{R}$ et $\mathcal{C}^k$ par morceaux sur $\mathbb{R}$. Alors :*

$$c_n(f) = \underset{n\to\infty}{o}\left(\frac{1}{|n|^k}\right)\ ,\ a_n(f) = \underset{n\to\infty}{o}\left(\frac{1}{n^k}\right)\ ,\ b_n(f) = \underset{n\to\infty}{o}\left(\frac{1}{n^k}\right)$$

II Convolution et noyaux trigonométriques

1) Produit de convolution

Définition 17. Soient $f, g \in CM(\mathbb{T})$. On appelle produit de convolution de f et g la fonction $f * g : \mathbb{R} \to \mathbb{R}$ définie par :

$$\forall\, t \in \mathbb{R},\ (f*g)(t) = \frac{1}{2\pi}\int_0^{2\pi} f(t-x)g(x)\,dx$$

Proposition 18. *Soient $f, g \in CM(\mathbb{T})$, alors :*

(i) $f * g \in CM(\mathbb{T})$

(ii) $\forall\, n \in \mathbb{Z},\ c_n(f*g) = c_n(f)c_n(g)$

(iii) $\forall\, t \in \mathbb{R},\ (f*g)(t) = \sum_{n=-\infty}^{\infty} c_n(f)c_n(g)e^{int}$

(iv) $\forall\, n \in \mathbb{Z},\ f * e_n = c_n(f)e_n$

Proposition 19. *L'application $f \mapsto (c_n(f))_{n\in\mathbb{Z}}$ est un homomorphisme d'algèbre de $(L^1(\mathbb{T}), *, \|.\|_2)$ dans $(c_0(\mathbb{Z}), \cdot, \|.\|_\infty)$ continu et de norme 1.*

2) Noyaux trigonométriques

Définition 20. Soit $N \in \mathbb{N}$. La fonction $D_N = \sum_{n=-N}^{N} e_n$ est appelée noyau de Dirichlet d'ordre N.

Proposition 21. *(i) D_N est paire, 2π-périodique et vérifie :*

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} D_N(t)\,dt = 1$$

(ii) D_N est le prolongement par continuité à $\mathbb{R}$ de la fonction :

$$\begin{array}{ccc} \mathbb{T} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \frac{\sin((N+\frac{1}{2})t)}{\sin(\frac{t}{2})} \end{array}$$

(iii) Pour tout $f \in L^1(\mathbb{T})$, on a $S_N(f) = f * D_N$.

Définition 22. Soit $N \in \mathbb{N}$. La fonction $F_N = \frac{1}{N+1}\sum_{n=0}^{N} D_n$ est appelée noyau de Fejér d'ordre N.

Proposition 23. *Pour $N \in \mathbb{N}$ et $t \in \mathbb{T}$, on a :*

$$F_n(t) = \frac{1}{N+1}\left(\frac{\sin(\frac{N+1}{2}t)}{\sin(\frac{t}{2})}\right)^2$$

Corollaire 24. *$(F_N)_{N\in\mathbb{N}}$ est une approximation de l'identité.*

III Convergence et séries de Fourier

1) Convergence de Fejér

Théorème 25 (Fejér)**.** *Pour $f \in C(\mathbb{T})$, la moyenne de Cesàro des sommes partielles de la série de Fourier de f converge uniformément vers f sur $\mathbb{T}$.*

Corollaire 26. *Tout élément de $C(\mathbb{T})$ est limite uniforme d'une suite de polynômes trigonométriques.*

Corollaire 27. *Soit $f \in C(\mathbb{T})$. Si $(c_n(f))_{n\in\mathbb{Z}} = 0$, alors $f = 0$.*

2) Convergence dans L^2

Proposition 28. *Pour $f \in L^2(\mathbb{T})$, la somme $S_N(f)$ est la projection orthogonale de f sur l'ensemble des polynômes trigonométriques de degré inférieur ou égal à N.*

Théorème 29 (Bessel)**.** *Pour $f \in L^2(\mathbb{T})$ et $N \in \mathbb{N}$, on a :*

$$\|c_n(f)\|_2^2 = \sum_{n=-N}^{N} |c_n(f)|^2 \leqslant \frac{1}{2\pi}\int_0^{2\pi} |f(t)|^2\,dt = \|f\|_2^2$$

Théorème 30 (Parseval)**.** *Pour $f \in L^2(\mathbb{T})$, $\sum_{n=-\infty}^{\infty} |c_n(f)|^2 = \|f\|_2$.*

Corollaire 31. *Pour $f \in L^2(\mathbb{T})$, $S_N(f)$ converge vers f dans $L^2(\mathbb{T})$.*

3) Convergence de la série de Fourier

Théorème 32 (Dirichlet)**.** *Soit $f : \mathbb{T} \to \mathbb{C}$ de classe $\mathcal{C}^1$ par morceaux. Alors la série de Fourier de f converge simplement sur $\mathbb{R}$ vers $\tilde{f}$ la régularisée de f. ($\tilde{f}(x) = \frac{1}{2}(f(x^+) + f(x^-))$)*

Exemple 33. *$(S_N(f_2))_{N\in\mathbb{N}}$ converge simplement vers f_2, on a donc, pour tout $t \in \mathbb{T}$, que $f_2(t) = \frac{-8}{\pi}\sum_{n=0}^{\infty} \frac{\sin((2n+1)t)}{(2n-1)(2n+1)(2n+3)}$.*

Exemple 34. *$(S_N(f_3))_{N\in\mathbb{N}}$ converge simplement vers f_3, on a donc, pour tout $t \in \mathbb{T}$, que $f_3(t) = \frac{\pi}{2} - \frac{4}{\pi}\sum_{n=0}^{\infty} \frac{\cos((2n+1)t)}{(2n+1)^2}$.*

Théorème 35. *Soit $f : \mathbb{T} \to \mathbb{C}$ continue et de classe $\mathcal{C}^1$ par morceaux. Alors la série de Fourier de f converge normalement sur $\mathbb{R}$ vers f.*

Exemple 36. *$(S_N(f_1))_{N\in\mathbb{N}}$ converge normalement vers f_1, on a donc, pour tout $t \in \mathbb{T}$, que $f_1(t) = \frac{4}{\pi}\sum_{n=0}^{\infty} \frac{(-1)^n \sin((2n+1)t)}{(2n+1)^2}$.*

IV Applications

1) Calcul de sommes particulières

Exemple 37. *En évaluant f_1 en $\frac{\pi}{2}$, on obtient :*

$$\sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} = \frac{\pi^2}{8} \quad \textit{puis} \quad \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Exemple 38. *En appliquant la formule de Parseval à f_1, on obtient*

$$\sum_{n=0}^{\infty} \frac{1}{(2n+1)^4} = \frac{\pi^4}{96} \quad \textit{puis} \quad \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}$$

2) Formule sommatoire de Poisson

Théorème 39. *Soit $F : L^1(\mathbb{R}) \cap \mathcal{C}^0(\mathbb{R})$. On note, pour tout $n \in \mathbb{N}$, $\widehat{F}(n) = \int_{\mathbb{R}} F(t)e^{-int}\,dt$. On suppose :*

$$\exists M > 0,\ \exists \alpha > 1,\ \forall x \in \mathbb{R},\ |F(x)| \leqslant M(1+|x|)^{-\alpha} \quad \textit{et} \quad \sum_{n\in\mathbb{Z}} |\widehat{F}(n)| < +\infty$$

Alors on a la relation :

$$2\pi \sum_{n\in\mathbb{Z}} F(2\pi n) = \sum_{n\in\mathbb{Z}} \widehat{F}(n)$$

Application 40. *Pour tout $s > 0$, on a :*

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi k^2}{s}}$$

3) Équation de la chaleur sur le cercle

Pour $u_0 \in L^2(\mathbb{T})$, on considère l'équation différentielle :

$$\begin{cases} \frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 & \text{sur } \mathbb{R}^{+\star} \times \mathbb{T} \\ u(0,.) = u_0 & \text{dans } L^2(\mathbb{T}) \end{cases} \qquad (*)$$

Théorème 41. *Il existe une unique solution u de $(*)$ de classe $\mathcal{C}^2$ sur $\mathbb{R}^{+\star} \times \mathbb{T}$, avec $u(t,.)$ tendant vers u_0 dans $L^2(\mathbb{T})$ quand t tend vers 0.*

Développements

- Formule sommatoire de Poisson (39,40) [Gou08]
- Équation de la chaleur sur le cercle (41) [Can09]

Références

[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions.* Ellipses
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Can09] B. Candelpergher. *Calcul intégral.* Cassini

Cadre : Soit $d \in \mathbb{N}^\star$. On considère $\langle ., . \rangle$ le produit scalaire usuel sur $\mathbb{R}^d$.

I Transformée de Fourier dans $L^1(\mathbb{R}^d)$

1) Définition et premières propriétés

Définition 1. On définit la transformée de Fourier de $f \in L^1(\mathbb{R}^d)$ par :

$$\mathcal{F}(f) = \widehat{f} : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{C} \\ \xi & \longmapsto & \displaystyle\int_{\mathbb{R}^d} f(x) e^{-i\langle x, \xi \rangle}\, dx \end{array} \right.$$

Remarque 2. *Cette définition a un sens car* $\left| f(x) e^{-i\langle x,\xi\rangle} \right| = |f(x)|$.

Proposition 3. *Pour* $f \in L^1(\mathbb{R}^d)$, $\widehat{f}$ *est une fonction continue.*

Théorème 4 (Riemann-Lebesgue)**.** *Si* $f \in L^1(\mathbb{R}^d)$, $\lim_{\|\xi\| \to \infty} \widehat{f}(\xi) = 0$.

Proposition 5. *Pour* $f \in L^1(\mathbb{R}^d)$, *on a* $\widehat{f} \in L^\infty(\mathbb{R}^d)$ *avec* $\left\| \widehat{f} \right\|_\infty \leqslant \|f\|_1$.

Proposition 6. *L'application* $\mathcal{F} : L^1(\mathbb{R}^d) \to \mathcal{C}^0(\mathbb{R}^d, \mathbb{C})$ *est bien définie, linéaire et continue.*

Exemple 7. *Si* $f = \mathbb{1}_{[-b,b]}$, *on a* $\widehat{f} : \xi \mapsto \frac{\sin(b\xi)}{\xi}$ *(prolongée par* b *en 0).*

Exemple 8. *Si* $\gamma_a(x) = e^{-ax^2}$ *pour* $a > 0$ *et* $x \in \mathbb{R}$, *alors* $\widehat{\gamma_a} = \sqrt{\frac{\pi}{a}} \gamma_{\frac{1}{4a}}$.

Proposition 9. *Soient* $f \in L^1(\mathbb{R}^d)$, $\alpha \in \mathbb{R}^d$ *et* $\lambda > 0$.

(i) Si $g(x) = f(x) e^{i\langle \alpha, x \rangle}$, *alors* $\widehat{g}(\xi) = \widehat{f}(\xi - \alpha)$.

(ii) Si $g(x) = f(x - \alpha)$, *alors* $\widehat{g}(\xi) = \widehat{f}(\xi) e^{-i\langle \alpha, \xi \rangle}$.

(iii) Si $g = \overline{\check{f}}$, *alors* $\widehat{g} = \overline{\widehat{f}}$.

(iv) Si $g(x) = f(\lambda x)$, *alors* $\widehat{g}(\xi) = \frac{1}{\lambda^d} \widehat{f}\left(\frac{\xi}{\lambda}\right)$.

Proposition 10. *Soient* $f \in L^1(\mathbb{R}^d)$ *et* $j \in [\![1, d]\!]$.

(i) Si $f \in \mathcal{C}^1(\mathbb{R}^d)$ *et* $\partial_j f \in L^1(\mathbb{R}^d)$, *alors* $\widehat{\partial_j f}(\xi) = i\xi_j \widehat{f}(\xi)$ *pour* $\xi \in \mathbb{R}^d$.

(ii) Si $x_j f \in L^1(\mathbb{R}^d)$, *alors* $\partial_j \widehat{f}$ *existe et* $\partial_j \widehat{f} = -i\widehat{x_j f}$.

2) Produit de convolution

Définition 11. Soient $f, g : \mathbb{R}^d \to \mathbb{R}$. Quand ceci a un sens, on pose :

$$(f * g)(x) = \int_{\mathbb{R}^d} f(t) g(x - t)\, dt$$

le produit de convolution de f et g en $x \in \mathbb{R}^d$.

Proposition 12. *La convolution entre fonctions mesurables positives est commutative et associative.*

Exemple 13. *Soit* $f \in L^1(\mathbb{R}^d)$ *positive, alors* $f * 0 = 0$ *et* $f * \mathbb{1}_{\mathbb{R}^d} = \int_{\mathbb{R}^d} f$.

Proposition 14. *Soit* $f \in L^1_{loc}(\mathbb{R}^d)$ *à support compact. Alors* $f * g$ *est bien définie sur* $\mathbb{R}^d$.

Théorème 15. $(L^1(\mathbb{R}^d), +, \cdot, *)$ *est une* $\mathbb{R}$*-algèbre commutative.*

Proposition 16. *Soient* $f, g \in L^1(\mathbb{R}^d)$. *Alors* $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$.

Application 17. *L'algèbre* $(L^1(\mathbb{R}^d), +, \cdot, *)$ *est sans unité.*

Application 18. *Si* $f = f * f$ *dans* $L^1(\mathbb{R}^d)$, *alors* $f = 0$.

3) Inversion de Fourier

Théorème 19. *Soit* $f \in L^1(\mathbb{R}^d)$ *telle que* $\widehat{f} \in L^1(\mathbb{R}^n)$. *Alors :*

$$\widehat{\widehat{f}} = (2\pi)^d \check{f} \qquad i.e. \quad \forall\, x \in \mathbb{R}^d,\ f(x) = \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} \widehat{f}(\xi) e^{i\langle x, \xi \rangle}\, d\xi$$

Corollaire 20. *La transformée de Fourier est injective.*

Corollaire 21. *Si* $f \in L^1(\mathbb{R}^d)$ *n'est pas continue,* $\widehat{f}$ *n'est pas intégrable.*

Définition 22. Soit $\rho : I \to \mathbb{R}$ une fonction mesurable et strictement positive, vérifiant $\forall\, n \in \mathbb{N},\ \int_I |x|^n \rho(x)\, dx < +\infty$. On dit alors que ρ est une fonction poids.

Théorème 23. *Soient* I *un intervalle de* $\mathbb{R}$ *et* ρ *une fonction poids. S'il existe* $a > 0$ *tel que* $\int_I e^{a|x|} \rho(x) dx < \infty$, *alors les polynômes orthogonaux associés à* ρ *forment une base hilbertienne de* $L^2(I, \rho)$.

II Extension de la transformée de Fourier

1) Prolongement à $L^2(\mathbb{R}^d)$

Remarque 24. *Pour $f \in L^2(\mathbb{R}^d)$, on ne peut pas définir $\widehat{f}$ comme dans $L^1(\mathbb{R}^d)$ puisque $x \mapsto f(x)e^{-i\langle \xi, x\rangle}$ n'est en général pas intégrable.*

Exemple 25. *Si $f : x \mapsto \frac{1}{x}\mathbb{1}_{[1,100[}(x) \in L^2(\mathbb{R})$, $x \mapsto f(x)e^{-i\xi x} \notin L^1(\mathbb{R})$.*

Lemme 26. *Si $\varphi \in \mathcal{C}_c^\infty(\mathbb{R}^d)$, alors $\widehat{\varphi} \in L^2(\mathbb{R}^d)$, et $\|\widehat{\varphi}\|_2 = \|\varphi\|_2$.*

Définition 27. Soit $f \in L^2(\mathbb{R}^d)$. Par densité de $\mathcal{C}_c^\infty(\mathbb{R}^d)$ dans $L^2(\mathbb{R}^d)$, on écrit f comme limite de $\varphi_n \in \mathcal{C}_c^\infty(\mathbb{R}^d)$. Posons $\mathcal{F}(f) = \lim_{n\to\infty} \mathcal{F}(\varphi_n)$. Cette limite existe et est indépendante de la suite choisie, et définit un élément de $L^2(\mathbb{R}^d)$.

Proposition 28. *L'application $\mathcal{F} : L^2(\mathbb{R}^d) \to L^2(\mathbb{R}^d)$ est linéaire et continue telle que pour tout $f \in L^2(\mathbb{R}^d)$ on a $\|\mathcal{F}(f)\|_2 = \|f\|_2$. Pour $f, g \in L^2(\mathbb{R}^d)$, on a $\langle \mathcal{F}(f), \mathcal{F}(g)\rangle = \langle f, g\rangle$, et $\int_{\mathbb{R}} (\mathcal{F}(f))g = \int_{\mathbb{R}} f(\mathcal{F}(g))$.*

Théorème 29. *Pour $f \in L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$, on a deux définitions de la transformée de Fourier. Ces deux définitions sont équivalentes.*

Théorème 30 (Plancherel)**.** *La transformation de Fourier su $L^2(\mathbb{R}^d)$ est un isomorphisme. En notant J l'opérateur défini sur $L^2(\mathbb{R}^d)$ par $Jf(x) = f(-x)$, l'inverse de $\mathcal{F}$ et donné par $\mathcal{F}^{-1} = \mathcal{F} \circ J = J \circ \mathcal{F}$, ce que l'on peut traduire sous la forme $\mathcal{F} \circ \mathcal{F} = J$. L'opérateur $\mathcal{F}$ est unitaire : $\mathcal{F}^\star = \mathcal{F}^{-1}$.*

2) Espace de Schwartz

Définition 31. Pour $x \in \mathbb{R}^d$ et $\alpha \in \mathbb{N}^d$, on pose $x^\alpha = x_1^{\alpha_1} \cdots x_d^{\alpha_d}$, et pour f de classe $\mathcal{C}^{|\alpha|}$, on pose $\partial^\alpha f = \partial_{x_1}^{\alpha_1} \cdots \partial_{x_d}^{\alpha_d} f$. Pour f de classe $\mathcal{C}^n$ et $\alpha, \beta \in \mathbb{N}^d$ avec $|\alpha| \leqslant n$, on pose $N_{\alpha,\beta}(f) = \left\|x^\beta \partial^\alpha f\right\|_\infty$.

Définition 32. On appelle espace de Schwartz sur $\mathbb{R}^d$ l'ensemble :

$$\mathcal{S}(\mathbb{R}^d) = \left\{ f \in \mathcal{C}^\infty(\mathbb{R}^d, \mathbb{R}) \,\middle|\, \forall\, \alpha, \beta \in \mathbb{N}^d, N_{\alpha,\beta}(f) < \infty \right\}$$

Proposition 33. *Pour tout $p \geqslant 1$, on a $\mathcal{C}_c^\infty(\mathbb{R}^d, \mathbb{R}) \subset \mathcal{S}(\mathbb{R}^d) \subset L^p(\mathbb{R}^d)$.*

Proposition 34. *L'espace de Schwartz est stable par produit avec les polynômes, dérivation et produit.*

Proposition 35. *Pour $\alpha, \beta \in \mathbb{N}^d$ et $f \in \mathcal{S}(\mathbb{R}^d)$, on a, pour $\xi \in \mathbb{R}^d$:*

$$\mathcal{F}(\partial^\alpha f)(\xi) = i^{|\alpha|}\xi^\alpha \mathcal{F}(f)(\xi) \quad \text{et} \quad \mathcal{F}\left(x^\beta f\right)(\xi) = i^{|\beta|}\partial^\beta \mathcal{F}(f)(\xi)$$

Théorème 36. *La transformée de Fourier est un homéomorphisme linéaire de l'espace de Schwartz dans lui-même.*

3) Distributions tempérées

Définition 37. On définit l'espace vectoriel $\mathcal{D}'(\mathbb{R}^d)$ des distributions dans $\mathbb{R}^d$ comme le dual topologique de $\mathcal{C}_0^\infty(\mathbb{R}^d, \mathbb{R})$, l'espace vectoriel $\mathcal{S}'(\mathbb{R}^d)$ des distributions tempérées dans $\mathbb{R}^d$ comme le dual topologique de $\mathcal{S}(\mathbb{R}^d)$, et l'espace vectoriel $\mathcal{E}'(\mathbb{R}^d)$ des distributions à support compact dans $\mathbb{R}^d$ comme le dual topologique de $\mathcal{C}^\infty(\mathbb{R}^d, \mathbb{R})$.

Proposition 38. *Comme on a une injection continue $\mathcal{C}_K^\infty(\mathbb{R}^d, \mathbb{R}) \hookrightarrow \mathcal{S}(\mathbb{R}^d)$, on a une injection continue $\mathcal{S}'(\mathbb{R}^d) \hookrightarrow \mathcal{D}'(\mathbb{R}^d)$.*

Définition 39. Pour $T \in \mathcal{S}'(\mathbb{R}^d)$, on définit $\widehat{T} : \mathcal{S}(\mathbb{R}^d) \to \mathbb{R}$ par $\left\langle \widehat{T}, \varphi \right\rangle = \langle T, \widehat{\varphi}\rangle$ pour tout $\varphi \in \mathcal{S}(\mathbb{R}^d)$. L'application $\widehat{T}$ est une distribution tempérée, appelée transformée de Fourier de T.

Théorème 40. *La transformée de Fourier des distributions tempérées donne un homéomorphisme linéaire de $\mathcal{S}'(\mathbb{R}^d)$ dans lui-même.*

Proposition 41. *Soient $T \in \mathcal{S}'(\mathbb{R}^d)$ et $\alpha \in \mathbb{N}^d$. On a :*

(i) $\mathcal{F}(\mathcal{F}(T)) = (2\pi)^d \check{T}$, *où* $\left\langle \check{T}, \varphi \right\rangle = \langle T, \check{\varphi}\rangle$.

(ii) $\mathcal{F}(\partial^\alpha T) = i^{|\alpha|}\xi^\alpha \mathcal{F}(T)$, *où* $\langle \partial^\alpha T, \varphi\rangle = (-1)^{|\alpha|}\langle T, \partial^\alpha \varphi\rangle$.

(iii) $\mathcal{F}(x^\alpha T) = i^{|\alpha|}\partial^\alpha \mathcal{F}(T)$.

Exemple 42. *On a $\widehat{\delta_0} = 1$, $\widehat{\sin} = \delta_1 - \delta_{-1}$, $(x \mapsto \frac{\sin(bx)}{x}) \xrightarrow[b\to+\infty]{\mathcal{S}'(\mathbb{R}^d)} \delta_0$.*

Définition 43. Soient $T \in \mathcal{D}'(\mathbb{R}^d)$ et $S \in \mathcal{E}'(\mathbb{R}^d)$. On définit la convolution de T et S par $\langle T * S, \varphi\rangle = \left\langle T, \check{S} * \varphi \right\rangle$, où $\check{S} * \varphi : x \mapsto \langle S(y), \varphi(y - x)\rangle$.

Proposition 44. *Soient $T \in \mathcal{D}'(\mathbb{R}^d)$, $S \in \mathcal{E}'(\mathbb{R}^d)$ et $\alpha \in \mathbb{N}^d$. Alors :*

$$T * \delta_0 = \delta_0 * T = T \quad \text{et} \quad \partial^\alpha(T * S) = (\partial^\alpha T) * S = T * (\partial^\alpha S)$$

Théorème 45. *Soient $T \in \mathcal{S}'(\mathbb{R}^d)$ et $S \in \mathcal{E}'(\mathbb{R}^d)$. Alors $T * S \in \mathcal{S}'(\mathbb{R}^d)$, et $\mathcal{F}(T * S) = \mathcal{F}(T)\mathcal{F}(S)$.*

III Applications

1) Formule sommatoire de Poisson

Théorème 46. *Soit $F : L^1(\mathbb{R}) \cap \mathcal{C}^0(\mathbb{R})$. On note, pour tout $n \in \mathbb{N}$, $\widehat{F}(n) = \int_{\mathbb{R}} F(t)e^{-int}\,dt$. On suppose :*

$$\exists M > 0,\ \exists \alpha > 1,\ \forall x \in \mathbb{R},\ |F(x)| \leqslant M(1+|x|)^{-\alpha} \quad \text{et} \quad \sum_{n\in\mathbb{Z}} |\widehat{F}(n)| < +\infty$$

Alors on a la relation :

$$2\pi \sum_{n\in\mathbb{Z}} F(2\pi n) = \sum_{n\in\mathbb{Z}} \widehat{F}(n)$$

Application 47. *Pour tout $s > 0$, on a :*

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi k^2}{s}}$$

2) Équations aux dérivées partielles

Pour $u_0 \in \mathcal{C}^2(\mathbb{R})$, on considère l'équation différentielle :

$$\begin{cases} \frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 & \text{sur } \mathbb{R}^{+\star} \times \mathbb{R} \\ u(0,.) = u_0 & \text{dans } \mathcal{C}^2(\mathbb{R}) \end{cases} \qquad (*)$$

Théorème 48. *Il existe une unique solution u au problème de Cauchy $(*)$ donnée pour $x \in \mathbb{R}$ et $t > 0$ par :*

$$u(t,x) = \frac{1}{2\sqrt{\pi t}} \int_{\mathbb{R}} u_0(y) e^{-\frac{(x-y)^2}{4t}}\,dy$$

3) Application en probabilités

Définition 49. Soit $f(x) = \frac{1}{\sqrt{\pi}} e^{-\frac{x^2}{2}}$ définie sur $\mathbb{R}$. La fonction f est la densité d'une loi de probabilité, appelée loi normale centrée réduite et notée $\mathcal{N}(0,1)$. Si X suit la loi $\mathcal{N}(0,1)$, on notera $\mathcal{N}(m,\sigma^2)$ la loi de $Y = \sigma X + m$, pour $m \in \mathbb{R}$ et $\sigma > 0$.

Proposition 50. *Soient $X \hookrightarrow \mathcal{N}(0,1)$ et $Y \hookrightarrow \mathcal{N}(m,\sigma^2)$. Alors $\mathbb{E}[X] = 0$, $\mathbb{E}[Y] = m$, $\mathrm{Var}(X) = 1$ et $\mathrm{Var}(Y) = \sigma^2$.*

Définition 51. Soit X une variable aléatoire à valeurs dans $E = \mathbb{R}^d$. On définit la fonction caractéristique φ_X de X par :

$$\varphi_X : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{C} \\ \lambda & \longmapsto & \mathbb{E}\left[e^{i\langle \lambda, X\rangle}\right] \end{array} \right.$$

Exemple 52. *Si $X \hookrightarrow \mathcal{N}(0,1)$, alors $\varphi_X(t) = e^{-\frac{t^2}{2}}$.*

Remarque 53. *Si X a pour densité f, alors $\varphi_X = \overset{\vee}{f}$.*

Proposition 54. *φ_X caractérise $\mathbb{P}_X$.*

Proposition 55. *Si X est réelle et $\mathbb{E}[|X|^p] < +\infty$, alors φ_X est p fois dérivable et $\varphi_X^{(p)}(\lambda) = i^p \mathbb{E}\left[X^p e^{i\lambda X}\right]$. En particulier, $\varphi_X^{(p)}(0) = i^p \mathbb{E}[X^p]$.*

Théorème 56 (Lévy). *$X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si et seulement si $\varphi_{X_n} \xrightarrow[n\to+\infty]{} \varphi_X$.*

Théorème 57 (Théorème central limite)**.** *On suppose que les X_n sont indépendants, identiquement distribués et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} \frac{X_i - \mathbb{E}[X_i]}{\sqrt{\mathrm{Var}(X_i)}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$$

Développements

- Formule sommatoire de Poisson (46,47) [Gou08]
- Transformée de Fourier d'une gaussienne (8) [El 08]
- Densité des polynômes orthogonaux (23) [BMP05]

Références

[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod
[El 08] M. El Amrani. *Analyse de Fourier dans les espaces fonctionnels.* Ellipses
[Rud09] W. Rudin. *Analyse réelle et complexe.* Dunod
[BP12] M. Briane et G. Pagès. *Théorie de l'intégration.* Vuilbert
[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K

Cadre : I est un intervalle de $\mathbb{R}$ non réduit à un singleton, et C une partie d'un espace vectoriel E.

I Généralités autour de la convexité

1) Définition et premières propriétés

Définition 1. C est convexe si : $\forall\, a, b \in C,\ \forall\, t \in [0,1],\ (1-t)a + tb \in C$.

Exemple 2. *Un intervalle de $\mathbb{R}$ est convexe, une boule de E est convexe.*

Définition 3. On dit que la fonction $f : C \to \mathbb{R}$ est convexe lorsque, pour tous $a, b \in C$ et tout $\lambda \in [0,1]$, on a :

$$f((1-\lambda)a + \lambda b) \leqslant (1-\lambda)f(a) + \lambda f(b)$$

On dit que f concave si $-f$ est convexe. Lorsque l'inégalité est stricte pour $a \neq b$ et $0 < \lambda < 1$, f est strictement convexe. Pour $\alpha > 0$, on dit que f est α-convexe si pour tous $a, b \in C$ distincts et tout $\lambda \in]0,1[$, on a :

$$f((1-\lambda)a + \lambda b) \leqslant (1-\lambda)f(a) + \lambda f(b) - \frac{\alpha}{2}\|a-b\|^2 \lambda(1-\lambda)$$

Remarque 4. *L'α-convexité implique la stricte convexité, qui implique la convexité.*

Remarque 5. *Une fonction $f : C \to \mathbb{R}$ est convexe si l'ensemble $\{(x,y) \in C \times \mathbb{R} \,|\, y \geqslant f(x)\}$ est convexe.*

Exemple 6. *L'application $x \mapsto \|x\|$ est convexe*

Théorème 7. *Une fonction $f : C \to \mathbb{R}$ est convexe si, et seulement si, pour tous $x, y \in C$, $t \mapsto f((1-t)x + ty)$ est convexe sur $[0,1]$.*

Proposition 8.
(i) Une combinaison linéaire à coefficients réels positifs de fonctions convexes est convexe.
(ii) La composée d'une fonction convexe croissante avec une fonction convexe est convexe.
(iii) Une limite simple de fonctions convexes est convexe.
(iv) Le maximum de deux fonctions convexes est convexe.

Remarque 9. *Le produit de deux fonctions convexes n'est pas nécessairement convexe ($-x \cdot x^2 = x^3$), et leur composition non plus ($(x \mapsto -x) \circ (x \mapsto x^2) = (x \mapsto -x^2)$).*

Proposition 10. *Une fonction convexe sur I est continue sur $\mathring{I}$.*

2) Caractérisation des fonctions convexes

En dimension 1

Théorème 11. *Pour $f : I \to \mathbb{R}$, il y a équivalence entre :*
(i) f est convexe sur I.
(ii) Pour $a < b < c$ dans I, on a : $\frac{f(b)-f(a)}{b-a} \leqslant \frac{f(c)-f(a)}{c-a} \leqslant \frac{f(c)-f(b)}{c-b}$
(iii) Pour $a \in I$, la fonction $x \mapsto \frac{f(x)-f(a)}{x-a}$ est croissante sur $I \setminus \{a\}$.

Corollaire 12. *Une fonction de $\mathbb{R}$ dans $\mathbb{R}$ est affine si, et seulement si, elle est convexe et concave.*

Théorème 13. *Soit $f : I \to \mathbb{R}$ dérivable. Il y a équivalence entre :*
(i) f est (strictement) convexe sur I.
(ii) La fonction dérivée f' est (strictement) croissante.
(iii) La courbe représentative de f est située (strictement) au-dessus de sa tangente en tout point de I.

Proposition 14. *Si f est deux fois dérivable sur I, elle est alors convexe si, et seulement si, $f'' \geqslant 0$.*

En dimension $n \geqslant 1$

Théorème 15. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*
(i) J est convexe sur C.
(ii) $\forall\, x, y \in C,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geqslant 0$.
(iii) $\forall\, x, y \in C,\ J(x) \geqslant J(y) + \langle \nabla J(y), x - y\rangle$.
Si J est deux fois différentiable, on a aussi : $\left\langle d^2J(x)\cdot y, y\right\rangle \geqslant 0$.

Théorème 16. *Soit $J : C \to \mathbb{R}$ différentiable. Il y a équivalence entre :*
(i) J est α-convexe sur C.
(ii) $\forall\, x, y \in C,\ \langle \nabla J(x) - \nabla J(y), x - y\rangle \geqslant \alpha\|x-y\|^2$.
(iii) $\forall\, x, y \in C,\ J(x) \geqslant J(y) + \langle \nabla J(y), x - y\rangle + \frac{\alpha}{2}\|x-y\|^2$.
Si J est deux fois différentiable, on a aussi : $\left\langle d^2J(x)\cdot y, y\right\rangle \geqslant \alpha\|y\|^2$.

Exemple 17. *Si A est une matrice symétrique définie positive, alors la fonctionnelle quadratique $J : X \mapsto \langle AX, X\rangle - \langle B, X\rangle$ est λ_1-convexe, où λ_1 est la plus petite valeur propre de A.*

3) Inégalités de convexité

Proposition 18. *Soient $n \in \mathbb{N}^\star$ et $a_1, \dots, a_n \in \mathbb{R}^+$, alors :*

$$\sqrt[n]{\prod_{i=1}^{n} a_i} \leqslant \frac{1}{n} \sum_{i=1}^{n} a_i$$

Il y a égalité si, et seulement si, tous les a_i sont égaux.

Proposition 19 (Young)**.** *Soient $p, q > 0$ tels que $\frac{1}{p} + \frac{1}{q} = 1$ et $a, b \in \mathbb{R}^+$:*

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

Il y a égalité si, et seulement si, $a^p = b^q$.

II Applications dans certains espaces

1) Espaces de Hilbert

Soit $(H, \langle ., . \rangle)$ un espace de Hilbert. Soit $K \subset E$ un convexe fermé non vide.

Théorème 20. *Pour tout $f \in H$, il existe un unique élément de K, noté $P_K(f)$, et appelé projection de f sur K, tel que :*

$$\|P_K(f) - f\| = \inf_{v \in K} \|v - f\|$$

De plus, $P_K(f)$ est caractérisée par :

$$\forall v \in K,\ \mathrm{Re}\left(\langle f - P_K(f), v - P_K(f) \rangle\right) \leqslant 0$$

Remarque 21. *L'application $x \mapsto P_K(x)$ est 1-lipschitzienne.*

Corollaire 22. *Soient M un sous-espace vectoriel fermé de H et $f \in H$. Alors $P_M(f)$ est caractérisé par :*

$$P_M(f) \in M \qquad et \qquad \forall\, v \in M,\ \mathrm{Re}\left(\langle f - P_M(f), v \rangle\right) = 0$$

De plus, P_M est un opérateur linéaire.

Théorème 23 (Riesz-Fréchet)**.** *Soit $\varphi \in H'$. Alors :*

$$\exists!\, f \in H,\ \forall\, v \in H,\ \langle \varphi, v \rangle = \langle f, v \rangle$$

Théorème 24 (Lax-Milgram)**.** *Soient H un espace de Hilbert, a une forme bilinéaire continue et coercive sur H, et $\ell \in H'$. Alors il existe un unique $u \in H$ tel que, pour tout $v \in H$, $a(u, v) = \ell(v)$. Si de plus a est symétrique, u réalise le minimum sur H de $v \mapsto \frac{1}{2} a(v, v) - \ell(v)$.*

Application 25 (Dirichlet)**.** *Pour $f \in L^2$, on considère le problème :*

$$\begin{cases} -u'' + u = f & sur\ ]0, 1[\\ u(0) = u(1) = 0 \end{cases}$$

Il existe une unique solution faible $u \in H_0^1([0, 1])$ à ce problème.

2) Espaces L^p

Soient $(E, \mathcal{A}, \mu)$ un espace mesuré, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $p, q > 0$ conjugués.

Définition 26. Pour tout réel $p > 0$, on définit le $\mathbb{K}$-espace vectoriel :

$$\mathscr{L}^p_{\mathbb{K}}(X, \mathcal{A}, \mu) = \left\{ f : X \to \mathbb{K} \text{ mesurable} \,\middle|\, \int_X |f|^p \, d\mu < +\infty \right\}$$

Sauf situation ambiguë, on privilégiera la notation plus concise $\mathscr{L}^p_{\mathbb{K}}(\mu)$.

Définition 27. Pour toute fonction $f : X \to \mathbb{K}$ et tout $p > 0$, on définit :

$$\|f\|_p = \left(\int_X |f|^p \, d\mu \right)^{\frac{1}{p}} \quad \left(\text{convention : } \infty^{\frac{1}{p}} = \infty \right)$$

Proposition 28 (Hölder et Minkowski)**.** *Soient $a, b \in \mathbb{R}^+$ et $f, g : E \to \mathbb{K}$ mesurables, alors :*

$$\|fg\|_1 \leqslant \|f\|_p \|g\|_q \quad et \quad \|f + g\|_p \leqslant \|f\|_p + \|g\|_p$$

Définition 29. Pour $1 \leqslant p < +\infty$, on définit $L^p_{\mathbb{K}}(\mu)$ comme l'espace vectoriel normé quotient de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ par les fonctions presque nulles. On associera par abus de langage un élément de $\mathscr{L}^p_{\mathbb{K}}(\mu)$ à sa classe dans $L^p_{\mathbb{K}}(\mu)$.

Théorème 30. *$(L^p, \|.\|_p)$ est un espace vectoriel normé.*

3) Espaces de probabilité

Soient $(\Omega, \mathcal{A}, \mathbb{P})$ un espace de probabilité et X une variable aléatoire.

Proposition 31 (Jensen)**.** *Si $X \in L^1$ et ϕ est convexe, alors $\phi(\mathbb{E}[X]) \leqslant \mathbb{E}[\phi(X)]$. De plus, si ϕ est strictement convexe, on a égalité si, et seulement si, X est constante presque sûrement.*

Remarque 32. *En particulier, $|\mathbb{E}[X]| \leqslant \mathbb{E}[|X|]$ et $\mathbb{E}[X]^2 \leqslant \mathbb{E}[X^2]$.*

III Recherche d'extrema et de points fixes

1) Optimisation

Théorème 33. *Si $J : C \to \mathbb{R}$ est différentiable en $u \in C$ et admet un minimum local en u, alors :*

$$\forall\, v \in C,\ \langle \nabla J(u), v - u\rangle \geqslant 0$$

Théorème 34. *On considère $J : C \to \mathbb{R}$.*

(i) Si J est convexe, tout minimum local est global.

(ii) Si J est strictement convexe, J admet au plus un minimum global.

(iii) Si J est α-convexe, J admet un unique minimum global.

(iv) Si J est définie sur un ouvert contenant C et différentiable en $u \in C$, alors le théorème précédent donne en fait une équivalence.

(v) Si C est ouvert, le théorème précédent équivaut à $\nabla J(u) = 0$.

2) Méthodes de gradient

Soit $J : \mathbb{R}^n \to \mathbb{R}$. On suppose J différentiable. On cherche, s'il existe, un élément $u \in \mathbb{R}^n$ tel que :

$$J(u) = \inf_{v \in \mathbb{R}^n} J(v)$$

Pour cela, on utilise les méthodes de gradient. On considère la suite :

$$u_0 \in \mathbb{R}^n \quad \text{et} \quad \forall\, k \in \mathbb{N},\ u^{k+1} = u^k - \rho^k \nabla J(u^k)$$

Il existe plusieurs possibilités pour choisir les ρ^k, par exemple :

(i) Gradient à pas fixe : $\rho^k = \rho$ une constante positive fixée.

(ii) Gradient à pas optimal : ρ^k minimise $\rho \mapsto J\left(u^k - \rho \nabla J(u^k)\right)$.

Théorème 35. *Si J est α-convexe et différentiable, et que ∇J est L-lipschitzienne, alors la méthode de gradient à pas optimal converge vers l'unique minimum de J.*

Application 36. *Soient $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. On considère la fonctionnelle quadratique $J : \mathbb{R}^n \to \mathbb{R}$ définie par :*

$$J(X) = \langle AX, X\rangle - \langle b, X\rangle + c$$

Cette fonctionnelle satisfait les conditions du théorème précédent. De plus, son minimum est atteint en $X_0 \in \mathbb{R}^n$ qui vérifie $\nabla J(X_0) = AX - b = 0$. On a donc une méthode itérative pour approcher la solution de $AX = b$.

3) Méthode de Newton

La méthode de Newton consiste à approcher une solution d'une équation $f(x) = 0$ en partant d'une approximation plus grossière. L'idée est de remplacer la courbe de f par sa tangente.

Théorème 37 (Méthode de Newton)**.** *Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f : [a, b] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ telle que $f(a) < 0 < f(b)$ et $f' > 0$ sur $[a, b]$. On considère la suite $(x_n)_{n\in\mathbb{N}}$ définie par :*

$$x_0 \in [a, b] \quad \text{et} \quad \forall\, n \in \mathbb{N},\ x_{n+1} = \phi(x_n) = x_n - \frac{f(x_n)}{f'(x_n)}$$

La fonction f admet un unique zéro $\alpha \in]a, b[$, et on a :

(i) Il existe $\varepsilon > 0$ tel que, pour $x_0 \in I =]\alpha - \varepsilon, \alpha + \varepsilon[$, la suite $(x_n)_{n\in\mathbb{N}}$ converge quadratiquement vers α, et il existe $C > 0$ tel que :

$$\forall\, n \in \mathbb{N},\ |x_{n+1} - \alpha| \leqslant C|x_n - \alpha|^2$$

(ii) Si de plus $f'' > 0$ sur $[\alpha, b]$, alors, pour $x \in]\alpha, b]$, la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante, et pour tout $n \in \mathbb{N}$ on a :

$$0 \leqslant x_{n+1} - \alpha \leqslant C(x_n - \alpha)^2 \quad \text{et} \quad x_{n+1} - \alpha \sim \frac{f''(\alpha)}{2f'(\alpha)}(x_n - \alpha)^2$$

Développements

— Projection sur un convexe fermé et théorème de Riesz (20,22,23) [Bre87]

— Algorithme de gradient à pas optimal (35) [Cia88]

Références

[RDO91] E. Ramis, C. Deschamps, et J. Odoux. *Cours de Mathématiques, Topologie et éléments d'analyse.* Masson

[Rom19] J.-E. Rombaldi. *Éléments d'analyse réelle.* EDP Sciences

[BP12] M. Briane et G. Pagès. *Théorie de l'intégration.* Vuilbert

[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

[Bre87] H. Brezis. *Analyse fonctionelle.* Masson

Annexes

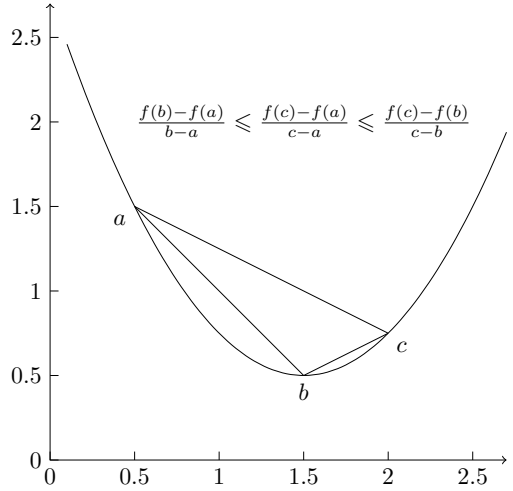


FIGURE 1 – Inégalité des trois pentes

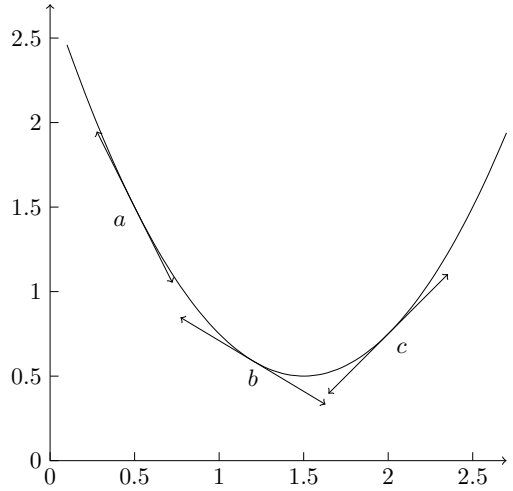


FIGURE 2 – Tangentes d'une fonction convexe

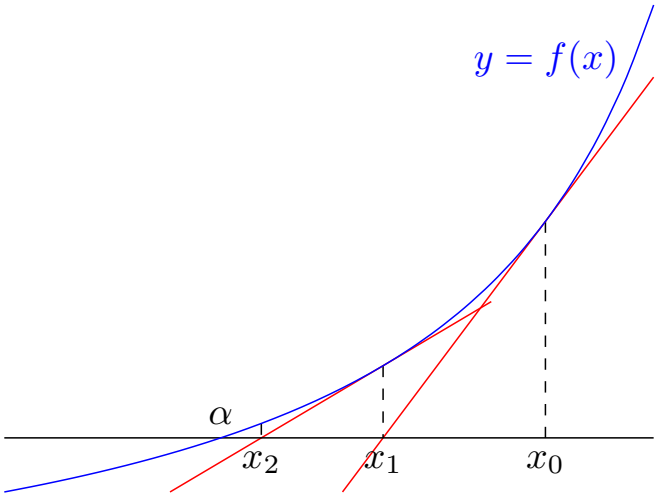


FIGURE 3 – Méthode de Newton

Cadre : Soient $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé, $(E, \mathcal{E})$ un espace probabilisable et $d \in \mathbb{N}^\star$.

I Loi d'une variable aléatoire

1) Définitions et premières conséquences

Définition 1. (i) Une fonction mesurable $X : (\Omega, \mathcal{A}) \to (E, \mathcal{E})$ est appelée variable aléatoire.

(ii) On note $\mathbb{P}_X$ la mesure image de $\mathbb{P}$ par X, que l'on appelle loi de X.

(iii) Si $(E, \mathcal{E}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$, X est dite réelle.

(iv) Si $X(\Omega)$ est dénombrable presque sûrement, X est dite discrète.

(v) Si $\mathbb{P}_X$ est absolument continue par rapport à la mesure de Lebesgue λ, on dit que X est à densité de densité $d\mathbb{P}_X/d\lambda$.

Exemple 2. *(i) Résultat du lancer d'une pièce : $E = \{P, F\}$.*

(ii) Couleur d'une boule tirée dans une urne : $E = \{couleurs\}$.

Soit X une variable aléatoire discrète à valeurs dans E.

Proposition 3. *Soient I au plus dénombrable et $E' = (e_i)_{i\in I} \subset E$ tel que $X(\Omega) \subset E'$. Alors $\mathbb{P}_X$ est caractérisée par $(p_i)_{i\in I}$, où $p_i = \mathbb{P}(X = e_i)$ avec $\sum_{i\in I} p_i = 1$ et $\mathbb{P}_X = \sum_{i\in I} p_i \delta_{e_i}$.*

Remarque 4. *Réciproquement, si $f : E' \to [0,1]$ est telle que $\sum_{i\in I} f(e_i) = 1$, alors il existe une unique probabilité $\mathbb{P}$ sur $(E, \mathcal{E})$ telle que $\mathbb{P}(e_i) = f(e_i)$. Une variable aléatoire suivant cette loi est alors discrète.*

Exemple 5. *$\mathcal{B}(p)$, $\mathcal{B}(n,p)$, $\mathcal{U}([\![1,n]\!])$, $\mathcal{P}(\lambda)$, $\mathcal{G}(q)$ et leur loi. (cf Annexe)*

2) Caractérisation par l'espérance de fonctions

Soit X une variable aléatoire à valeurs dans $E = \mathbb{R}^d$.

Remarque 6. *$\mathbb{P}_X$ est déterminé par son image sur les boréliens.*

Définition 7. Si X est réelle et intégrable, on définit l'espérance de X par $\mathbb{E}[X] = \int_\Omega X(\omega) d\mathbb{P}(\omega)$. Sinon, on écrit $X = (X_1, \dots, X_d)$, et si $\|X\|$ est intégrable, on définit l'espérance de X par $\mathbb{E}[X] = (\mathbb{E}[X_1], \dots, \mathbb{E}[X_d])$.

Exemple 8. *(i) Espérance des lois classiques (cf Annexe).*

(ii) Les lois de Cauchy n'admettent pas d'espérance.

Remarque 9. *L'espérance ne dépend que de la loi de la variable aléatoire.*

Définition 10. Si X est de carré intégrable, on définit la variance de X par $\mathrm{Var}(X) = \mathbb{E}\left[(X - \mathbb{E}[X])^2\right]$.

Proposition 11 (Formule de transfert)**.** *Soit $f : \mathbb{R}^d \to \mathbb{R}$ borélienne. Alors $f(X) \in L^1(\Omega, \mathcal{A}, \mathbb{P})$ si, et seulement si, $f \in L^1(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d), \mathbb{P}_X)$. Dans ce cas, on a :*

$$\mathbb{E}[X] = \int_\Omega f(X(\omega)) d\mathbb{P}(\omega) = \int_{\mathbb{R}^d} f(x) d\mathbb{P}_X(x)$$

Application 12. *Si $X \hookrightarrow \mathcal{E}(\lambda)$ avec $\lambda > 0$ et $\theta > 0$, alors $\theta X \hookrightarrow \mathcal{E}\left(\frac{\lambda}{\theta}\right)$.*

Proposition 13. *La donnée de $\mathbb{E}[f(X)]$ pour toutes les fonctions f continues positives à support compact caractérise la loi de X.*

Remarque 14. *On peut aussi prendre les fonctions continues bornées ou les fonctions $\mathcal{C}^\infty$ à support compact.*

Application 15. *Si $U_1, U_2 \hookrightarrow \mathcal{N}(0,1)$ sont indépendantes $\frac{U_1}{U_2} \hookrightarrow \mathcal{C}(0,1)$.*

II Caractérisation par des fonctions

1) Fonction de répartition

Soit X une variable aléatoire réelle.

Définition 16. On définit la fonction de répartition F_X de X par :

$$F_X : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & [0,1] \\ x & \longmapsto & \mathbb{P}_X(]-\infty, x]) = \mathbb{P}(X \leqslant x) \end{array} \right.$$

Exemple 17. *Fonctions de répartition des lois classiques (cf Annexe).*

Proposition 18. *(i) F_X est croissante, continue à droite, tend vers 0 en $-\infty$ et vers 1 en $+\infty$.*

(ii) Réciproquement, toute fonction satisfaisant le point précédent est la fonction de répartition d'une variable aléatoire.

(iii) Si f est une densité de probabilité, alors $F : x \mapsto \int_{-\infty}^x f(t)dt$ est la fonction de répartition d'une variable aléatoire Y telle que $\mathbb{P}_Y$ admette pour densité f.

Proposition 19. *F_X caractérise $\mathbb{P}_X$.*

Remarque 20. *On peut généraliser la fonction de répartition pour une variable aléatoire à valeurs dans $\mathbb{R}^d$. Le résultat reste valable.*

2) Fonction caractéristique

Soit X une variable aléatoire à valeurs dans $E = \mathbb{R}^d$.

Définition 21. On définit la fonction caractéristique φ_X de X par :

$$\varphi_X : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{C} \\ \lambda & \longmapsto & \mathbb{E}\left[e^{i\langle \lambda, X\rangle}\right] \end{array} \right.$$

Exemple 22. *Fonctions caractéristiques des lois classiques (cf Annexe).*

Proposition 23. *φ_X caractérise $\mathbb{P}_X$.*

Proposition 24. *Si X est réelle et $\mathbb{E}[|X|^p] < +\infty$, alors φ_X est p fois dérivable et $\varphi_X^{(p)}(\lambda) = i^p \mathbb{E}\left[X^p e^{i\lambda X}\right]$. En particulier, $\varphi_X^{(p)}(0) = i^p \mathbb{E}[X^p]$.*

Remarque 25. *Réciproquement, si p est pair et φ_X p fois dérivable en 0, alors $\mathbb{E}[|X|^p] < +\infty$. On peut construire X n'admettant pas d'espérance, mais telle que φ_X est dérivable en 0 (admis).*

3) Fonction génératrice

Soit X une variable aléatoire à valeurs dans $E = \mathbb{N}$.

Définition 26. On définit la fonction génératrice G_X de X par :

$$G_X : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ s & \longmapsto & \mathbb{E}\left[s^X\right] \end{array} \right.$$

Remarque 27. *Le rayon de convergence de cette série est au moins égal à 1 et $G_X(1) = 1$.*

Exemple 28. *Fonctions génératrices des lois classiques (cf Annexe).*

Proposition 29. *G_X caractérise $\mathbb{P}_X$. En particulier $\mathbb{P}(X = k) = \frac{G_X^{(k)}(0)}{k!}$.*

Proposition 30. *$\mathbb{E}[|X|^p] < +\infty$ si, et seulement si, G_X est p fois dérivable et dans ce cas $G_X^{(p)}(1) = \mathbb{E}[X(X-1)\cdots(X-p+1)]$.*

Application 31. *$\mathbb{E}[X] = G_X'(1)$ et $\mathrm{Var}(X) = G_X''(1) + G_X'(1) - G_X'(1)^2$.*

III Vecteurs aléatoires et indépendance

Soient X, Y des variables aléatoires à valeurs dans E, F des espaces probabilisables.

Définition 32. La loi du couple (X, Y) est appelée loi conjointe. Les lois de X et de Y sont appelées lois marginales.

Remarque 33. *La donnée de la loi conjointe permet de retrouver les lois marginales. La réciproque est fausse : si $X, Y \hookrightarrow \mathcal{B}\left(\frac{1}{2}\right)$ et sont indépendantes, alors (X, X) et (X, Y) ont même lois marginales, mais pas même loi conjointe.*

Proposition 34. *X et Y sont indépendantes si, et seulement si :*

(i) $\mathbb{P}_{(X,Y)} = \mathbb{P}_X \otimes \mathbb{P}_Y$

(ii) $\mathbb{E}[f_1(X) f_2(Y)] = \mathbb{E}[f_1(X)]\,\mathbb{E}[f_2(X)]$ *pour toutes fonctions boréliennes f_1 et f_2.*

(iii) Pour tous $\lambda_1, \lambda_2 \in \mathbb{R}$, $\varphi_{(X,Y)}(\lambda_1, \lambda_2) = \varphi_X(\lambda_1)\varphi_Y(\lambda_2)$.

Définition 35. On définit la covariance de X et Y par :

$$\mathrm{Cov}(X, Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])]$$

Proposition 36. *Si X et Y sont indépendantes, alors $\mathrm{Cov}(X, Y) = 0$, $\mathbb{P}_{X+Y} = \mathbb{P}_X \times \mathbb{P}_Y$ et $G_{X+Y} = G_X G_Y$ lorsque ces quantités existent.*

Remarque 37. *On peut généraliser ces propositions à des familles quelconques de variables aléatoires.*

IV Convergence en loi

Soit $(X_n)_{n\in\mathbb{N}^*}$ et X des variables aléatoires à valeurs dans $\mathbb{R}^d$.

Définition 38. On dit que (X_n) converge en loi vers X si, pour tout $\varphi \in \mathcal{C}_b(\mathbb{R}, \mathbb{R})$, $\lim_n \mathbb{E}[\varphi(X_n)] = \mathbb{E}[\varphi(X)]$. On note alors $X_n \xrightarrow{\mathcal{L}} X$.

Exemple 39. *Si $X_n \hookrightarrow \mathcal{N}\left(0, \sigma_n^2\right)$ avec $\lim_{n\to+\infty} \sigma_n = \sigma$, alors X_n converge en loi vers $X \hookrightarrow \mathcal{N}\left(0, \sigma^2\right)$.*

Théorème 40 (Lévy). *$X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si et seulement si $\varphi_{X_n} \xrightarrow[n\to+\infty]{} \varphi_X$.*

On se place maintenant dans le cas réel, où $d = 1$.

Proposition 41. *Si les X_n sont à valeurs dans $\mathbb{N}$, alors $X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si, et seulement si, pour tout $k \in \mathbb{N}$, $\mathbb{P}(X_n = k) \xrightarrow[n\to+\infty]{} \mathbb{P}(X = k)$.*

Proposition 42. *$X_n \xrightarrow{\mathcal{L}} X$ si, et seulement si, $F_{X_n} \to F_X$ en tout point de continuité de F_X.*

Théorème 43 (Théorème central limite)**.** *On suppose que les X_n sont indépendants, identiquement distribués et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} \frac{X_i - \mathbb{E}[X_i]}{\sqrt{\mathrm{Var}(X_i)}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$$

Application 44. *On suppose que les X_n sont indépendants, identiquement distribués et de loi $\mathcal{B}(p)$ pour $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\widehat{p_n} = \frac{1}{n}\sum_{k=1}^{n} X_i$. Il s'agit de :*

$$IC_\alpha = \left[\widehat{p_n} \pm \frac{q_{1-\frac{\alpha}{2}}}{2\sqrt{n}}\right]$$

où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Application 45 (Monte-Carlo)**.** *Soit $f : [0,1] \to \mathbb{R}$ intégrable par rapport à la mesure de Lebesgue, et $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires indépendantes, identiquement distribuées et de loi $\mathcal{U}([0,1])$. Alors :*

$$\frac{1}{n}\sum_{k=1}^{n} f(X_i) \xrightarrow[n\to+\infty]{} \int_0^1 f(t)dt \text{ p.s.}$$

Théorème 46. *Soit $(X_{n,j})_{n\in\mathbb{N}^\star, j\in[\![1,M_n]\!]}$ une suite de variables aléatoires indépendantes à valeurs dans $\{0,1\}$, avec $(M_n)_{n\in\mathbb{N}^\star}$ une suite croissante de $\mathbb{N}^\star$ qui tend vers $+\infty$. On pose $\mathbb{P}(X_{n,j} = 1) = p_{n,j}$ et $S_n = \sum_{j=1}^{M_n} X_{n,j}$. On suppose de plus que :*

$$\lim_{n\to+\infty} \max_{1\leqslant j\leqslant M_n} p_{n,j} = 0 \quad \text{et} \quad \lim_{n\to+\infty} \sum_{j=1}^{M_n} p_{n,j} = \lambda > 0$$

Alors la suite $(S_n)_{n\in\mathbb{N}^\star}$ converge en loi vers la loi de Poisson $\mathcal{P}(\lambda)$.

Développements

- Théorème central limite et intervalle de confiance (43,44) [BL07]
- Loi des évènements rares de Poisson (46) [Ouv09]

Références

[BL07] P. Barbe et M. Ledoux. *Probabilité.* EDP Sciences
[Ouv08] J.-Y. Ouvrard. *Probabilités : Tome 1.* Cassini
[Ouv09] J.-Y. Ouvrard. *Probabilités : Tome 2.* Cassini

Annexes

Nom	Paramètres	Notation	$\mathbb{P}_X$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$\varphi_X(t)$	$G_X(t)$
Uniforme	$n \in \mathbb{N}^\star$	$\mathcal{U}([\![1,n]\!])$	$\sum_{k=1}^{n} \frac{1}{n}\delta_k$	$\frac{n+1}{2}$	$\frac{n^2-1}{12}$	$\frac{1}{n}\sum_{k=1}^{n} e^{ikt}$	$\frac{1}{n}\frac{t-t^{n+1}}{1-t}$ $(t \neq 1)$
Bernoulli	$p \in [0,1]$	$\mathcal{B}(p)$	$p\delta_1 + (1-p)\delta_0$	p	$p(1-p)$	$pe^{it} + (1-p)$	$1-p+pt$
Binomiale	$n \in \mathbb{N}^\star, p \in [0,1]$	$\mathcal{B}(n,p)$	$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k}\delta_k$	np	$np(1-p)$	$pe^{it} + (1-p)^n$	$(1-p+pt)^n$
Géométrique	$q \in [0,1]$	$\mathcal{G}(q)$	$\sum_{k=0}^{\infty} q(1-q)^{k-1}\delta_k$	$\frac{1}{q}$	$\frac{1-q}{q^2}$	$\frac{qe^{it}}{1-(1-q)e^{it}}$	$\frac{(1-q)t}{1-qt}$
Poisson	$\lambda > 0$	$\mathcal{P}(\lambda)$	$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!}\delta_k$	λ	λ	$e^{\lambda(e^{it}-1)}$	$e^{(\lambda-1)t}$

FIGURE 1 – Lois de probabilités discrètes

Nom	Paramètres	Notation	$f(t)$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$\varphi_X(t)$
Uniforme	$a,b \in \mathbb{R},\ a<b$	$\mathcal{U}([a,b])$	$\frac{1}{b-a}\mathbb{1}_{[a,b]}(t)$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$	$\frac{e^{itb}-e^{ita}}{it(b-a)}$
Normale	$m \in \mathbb{R},\ \sigma^2 > 0$	$\mathcal{N}(m,\sigma^2)$	$\frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(t-m)^2}{2\sigma^2}}$	m	σ^2	$e^{imt-\frac{t^2\sigma^2}{2}}$
Exponentielle	$\lambda > 0$	$\mathcal{E}(\lambda)$	$\lambda e^{-\lambda t}\mathbb{1}_{\mathbb{R}^+}(t)$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	$\frac{\lambda}{\lambda - it}$
Cauchy	$m \in \mathbb{R},\ a > 0$	$\mathcal{C}(m,a)$	$\frac{1}{\pi}\frac{1}{a+(t-m)^2}$			$e^{-\lvert t\rvert}$
Gamma	$\lambda > 0,\ n \in \mathbb{N}^\star$	$\Gamma(\lambda,n)$	$\frac{\lambda^n}{\Gamma(n)} e^{-\lambda t} t^{n-1}\mathbb{1}_{\mathbb{R}^+}(t)$	$\frac{n}{\lambda}$	$\frac{n}{\lambda^2}$	$\frac{\lambda^n}{(\lambda - it)^n}$

FIGURE 2 – Lois de probabilités continues

Cadre : On se place dans l'espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$, sur lequel sont définies $(X_n)_{n\in\mathbb{N}^\star}$ et X des variables aléatoires réelles.

I Modes de convergence

1) Convergence presque sûre

Définition 1. On dit que (X_n) converge presque sûrement vers X si :

$$\mathbb{P}\left(\left\{\omega\in\Omega \,\middle|\, \lim_{n\to+\infty} X_n(\omega) = X(\omega)\right\}\right) = 1$$

Autrement dit, si l'ensemble où X_n ne converge pas vers X est négligeable. On note alors $X_n \xrightarrow{\text{p.s.}} X$.

Remarque 2. *La condition de convergence presque sûre équivaut à :*

$$\forall\,\varepsilon>0,\ \mathbb{P}\left(\limsup_{n\to+\infty}\{|X_n - X| \geqslant \varepsilon\}\right) = 0$$

Exemple 3. *Dans $([0,1], \mathcal{B}([0,1]), \lambda)$, où λ est la mesure de Lebesgue sur $[0,1]$, $X_n = \mathbb{1}_{[0,\frac{1}{n}[}$ converge presque sûrement vers 0.*

Exemple 4. *Supposons que $X_n \hookrightarrow \mathcal{B}(p)$, et posons $U_n = \sum_{i=1}^n 2^{-i} X_i$. Alors $U_n \xrightarrow{p.s.} U$, où U est une variable aléatoire à valeurs dans $[0,1]$.*

Théorème 5 (Borel-Cantelli)**.** *Soit $(A_n)_{n\in\mathbb{N}^\star}$ une suite d'évènements.*

(i) Si $\sum \mathbb{P}(A_n) < \infty$, $\mathbb{P}(\limsup A_n) = 0$.

(ii) Si $\sum \mathbb{P}(A_n) = \infty$ et les A_n sont indépendants, $\mathbb{P}(\limsup A_n) = 1$.

Exemple 6. *On lance une infinité de fois une pièce équilibrée, on obtiendra presque sûrement une infinité de fois 42 piles consécutifs.*

Exemple 7. *Supposons que $X_n \hookrightarrow \mathcal{E}(1)$ et sont indépendantes. Alors $\frac{\max_{1\leqslant i\leqslant n} X_i}{\ln n}$ converge presque sûrement vers 1.*

2) Convergence en probabilités

Définition 8. On dit que (X_n) converge en probabilité vers X si :

$$\forall\,\varepsilon>0,\ \lim_{n\to+\infty}\mathbb{P}(|X_n - X| \geqslant \varepsilon) = 0$$

On note alors $X_n \xrightarrow{\mathbb{P}} X$.

Exemple 9. *Dans $([0,1], \mathcal{B}([0,1]), \lambda)$, où λ est la mesure de Lebesgue sur $[0,1]$, $X_n = \mathbb{1}_{[0,\frac{1}{n}[}$ converge en probabilités vers 0.*

Proposition 10. *Soient $f:\mathbb{R}\to\mathbb{R}$ continue, $X_n \xrightarrow{\mathbb{P}} X$ et $Y_n \xrightarrow{\mathbb{P}} Y$.*

$$(X_n, Y_n) \xrightarrow{\mathbb{P}} (X,Y) \qquad X_n + Y_n \xrightarrow{\mathbb{P}} X+Y \qquad f(X_n) \xrightarrow{\mathbb{P}} f(X)$$

3) Convergence dans L^p

Définition 11. Si les $(X_n)_{n\in\mathbb{N}^\star}$ et X sont dans L^p, pour $p\in[1,+\infty[$. On dit que $(X_n)_{n\in\mathbb{N}^\star}$ converge vers X dans L^p si $\lim_{n\to+\infty}\|X_n - X\|_p = 0$, ou de manière équivalente $\lim_{n\to+\infty}\mathbb{E}[|X_n - X|^p] = 0$. On note $X^n \xrightarrow{L^p} X$.

Exemple 12. *Supposons que $X_n \hookrightarrow \mathcal{B}\left(\frac{1}{n}\right)$ et sont indépendantes. Alors $\mathbb{E}[|X^p|] = \mathbb{E}[X] = \frac{1}{n} \xrightarrow[n\to+\infty]{} 0$. Donc X_n converge dans L^p.*

Proposition 13 (Markov)**.** *Soit X est positive.*

$$\forall\, t>0,\ \mathbb{P}(X \geqslant t) \leqslant \frac{\mathbb{E}[X]}{t}$$

Corollaire 14 (Bienaymé-Tchébychev)**.** *Soit X est de carré intégrable.*

$$\forall\, t>0,\ \mathbb{P}(|X - \mathbb{E}[X]| \geqslant t) \leqslant \frac{\mathbb{E}[(X-\mathbb{E}[X])^n]}{t^n}$$

Proposition 15 (Hölder)**.** *Soient $X\in L^p$ et $Y\in L^q$ tels que $\frac{1}{p}+\frac{1}{q}=1$.*

$$\mathbb{E}[|XY|] \leqslant \mathbb{E}[|X|^p]^{\frac{1}{p}}\,\mathbb{E}[|Y|^q]^{\frac{1}{q}}$$

Définition 16. On dit que $(X_n)_{n\in\mathbb{N}^\star}$ est équi-intégrable si les X_n sont intégrables et que :

$$\lim_{c\to+\infty}\sup_{n\in\mathbb{N}^\star}\int_{\{|X_i|>c\}}|X_i|d\mathbb{P} = 0$$

Exemple 17. *Une famille finie de variables aléatoires intégrables est équi-intégrable.*

4) Convergence en loi

Définition 18. On dit que (X_n) converge en loi vers X si, pour tout $\varphi \in \mathcal{C}_b(\mathbb{R},\mathbb{R})$, $\lim_n \mathbb{E}[\varphi(X_n)] = \mathbb{E}[\varphi(X)]$. On note alors$X_n \xrightarrow{\mathcal{L}} X$.

Remarque 19. *On peut prendre les $(X_n)_{n\in\mathbb{N}^\star}$ et X définies sur des espace probabilisés différents.*

Exemple 20. *Si $X \hookrightarrow \mathcal{N}(0,\sigma_n^2)$ avec $\lim_{n\to+\infty}\sigma_n = \sigma$, alors X_n converge en loi vers $X \hookrightarrow \mathcal{N}(0,\sigma^2)$.*

Théorème 21 (Lévy)**.** *$X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si et seulement si $\varphi_{X_n} \xrightarrow[n\to+\infty]{} \varphi_X$.*

Proposition 22. *Si les X_n sont à valeurs dans $\mathbb{N}$, alors $X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si, et seulement si, pour tout $k\in\mathbb{N}$, $\mathbb{P}(X_n=k) \xrightarrow[n\to+\infty]{} \mathbb{P}(X=k)$.*

Proposition 23. *$X_n \xrightarrow{\mathcal{L}} X$ si, et seulement si, $F_{X_n} \to F_X$ en tout point de continuité de F_X.*

II Liens entre les modes de convergence

Proposition 24. *Soient $1 \leqslant p \leqslant q \leqslant +\infty$. On a :*

$$X_n \xrightarrow{L^\infty} X \quad\Rightarrow\quad X_n \xrightarrow{L^q} X \quad\Rightarrow\quad X_n \xrightarrow{L^p} X$$

Proposition 25. $X_n \xrightarrow{p.s.} X \;\Rightarrow\; X_n \xrightarrow{\mathbb{P}} X$

Contre-exemple 26. *Supposons que $X_n \hookrightarrow \mathcal{B}\left(\frac{1}{n}\right)$ et sont indépendantes. Alors X_n converge en probabilités et dans L^p vers 0, mais ne converge pas presque sûrement.*

Proposition 27. $X_n \xrightarrow{L^p} X \;\Rightarrow\; X_n \xrightarrow{\mathbb{P}} X$

Théorème 28. *La convergence en probabilité implique la convergence presque sûre d'une sous-suite vers la même limite.*

Corollaire 29. *La convergence dans L^p implique la convergence presque sûre d'une sous-suite vers la même limite.*

Théorème 30. $X_n \xrightarrow{\mathbb{P}} X \;\Rightarrow\; X_n \xrightarrow{\mathcal{L}} X$

Remarque 31. *La réciproque est vraie si la variable limite est constante, mais pas en général : si $X \hookrightarrow \mathcal{B}\left(\frac{1}{2}\right)$, alors $1-X \xrightarrow{\mathcal{L}} X$, mais pas en probabilités.*

Théorème 32. *Si les X_n sont intégrables, on a équivalence entre :*

(i) $X_n \xrightarrow{\mathbb{P}} X$ et $(X_n)_{n\in\mathbb{N}^\star}$ est équi-intégrable.

(ii) $X_n \xrightarrow{L^1} X$ et X est intégrable.

Contre-exemple 33. *Dans $([0,1],\mathcal{B}([0,1]),\lambda)$, où λ est la mesure de Lebesgue sur $[0,1]$, $X_n = n\mathbb{1}_{[0,\frac{1}{n}[}$ converge en probabilités vers 0, mais pas dans L^p.*

III Théorèmes limites

1) Lois des grands nombres

Théorème 34 (Loi faible des grands nombres)**.** *Soit $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires réelles indépendantes et identiquement distribuées de même loi qu'une variable aléatoire réelle X. Alors :*

$$\mathbb{E}[|X|] < +\infty \quad\Rightarrow\quad \frac{1}{n}\sum_{i=1}^{n} X_i \xrightarrow{\mathbb{P}} \mathbb{E}[X]$$

Théorème 35 (Loi forte des grands nombres)**.** *Soit $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires réelles indépendantes et identiquement distribuées de même loi qu'une variable aléatoire réelle X. Alors :*

$$\mathbb{E}[|X|] < +\infty \quad\Leftrightarrow\quad \frac{1}{n}\sum_{i=1}^{n} X_i \xrightarrow{p.s.} \mathbb{E}[X]$$

Application 36 (Monte-Carlo)**.** *Soit $f:[0,1]\to\mathbb{R}$ intégrable par rapport à la mesure de Lebesgue, et $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires indépendantes, identiquement distribuées et de loi $\mathcal{U}([0,1])$. Alors :*

$$\frac{1}{n}\sum_{k=1}^{n} f(X_i) \xrightarrow[n\to+\infty]{} \int_0^1 f(t)dt \text{ p.s.}$$

2) Théorème central limite

Théorème 37 (Théorème central limite)**.** *On suppose que les X_n sont indépendants, identiquement distribués et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}\frac{X_i-\mathbb{E}[X_i]}{\sqrt{\mathrm{Var}(X_i)}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$$

Application 38. *On suppose que les X_n sont indépendants, identiquement distribués et de loi $\mathcal{B}(p)$ pour $p\in[0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\widehat{p_n}=\frac{1}{n}\sum_{k=1}^{n}X_i$. Il s'agit de :*

$$IC_\alpha=\left[\widehat{p_n}\pm\frac{q_{1-\frac{\alpha}{2}}}{2\sqrt{n}}\right]$$

où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Application 39. *Dans la méthode de Monte-Carlo, on obtient un intervalle de confiance de probabilité asymptotique $1-\alpha$ de longueur proportionnelle à $\frac{1}{\sqrt{n}}$.*

Théorème 40. *Soit $(X_{n,j})_{n\in\mathbb{N}^\star,j\in[\![1,M_n]\!]}$ une suite de variables aléatoires indépendantes à valeurs dans $\{0,1\}$, avec $(M_n)_{n\in\mathbb{N}^\star}$ une suite croissante de $\mathbb{N}^\star$ qui tend vers $+\infty$. On pose $\mathbb{P}(X_{n,j}=1)=p_{n,j}$ et $S_n=\sum_{j=1}^{M_n}X_{n,j}$. On suppose de plus que :*

$$\lim_{n\to+\infty}\max_{1\leqslant j\leqslant M_n}p_{n,j}=0 \quad et \quad \lim_{n\to+\infty}\sum_{j=1}^{M_n}p_{n,j}=\lambda>0$$

Alors la suite $(S_n)_{n\in\mathbb{N}^\star}$ converge en loi vers la loi de Poisson $\mathcal{P}(\lambda)$.

Développements

- Théorème central limite et intervalle de confiance (37,38) [BL07]
- Loi des évènements rares de Poisson (40) [Ouv09]

Références

[BL07] P. Barbe et M. Ledoux. *Probabilité.* EDP Sciences
[Ouv08] J.-Y. Ouvrard. *Probabilités : Tome 1.* Cassini
[Ouv09] J.-Y. Ouvrard. *Probabilités : Tome 2.* Cassini

Annexes

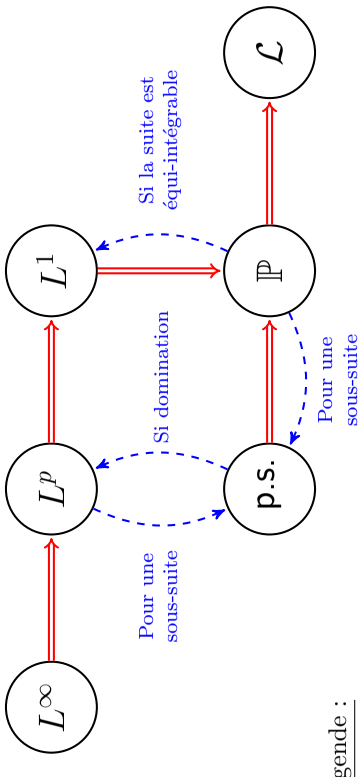


FIGURE 1 – Liens entre les modes de convergence

Cadre : On considère $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé et $(E, \mathcal{E})$ un espace probabilisable.

I Variables aléatoires discrètes, généralités

1) Loi d'une variable aléatoire discrète

Définition 1. (i) Une fonction mesurable $X : (\Omega, \mathcal{A}) \to (E, \mathcal{E})$ est appelée variable aléatoire.

(ii) On note $\mathbb{P}_X$ la mesure image de $\mathbb{P}$ par X, que l'on appelle loi de X.

(iii) Si $(E, \mathcal{E}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$, X est dite réelle.

(iv) Si $X(\Omega)$ est dénombrable presque sûrement, X est dite discrète.

Exemple 2. *(i) Résultat du lancer d'une pièce : $E = \{P, F\}$.*

(ii) Couleur d'une boule tirée dans une urne : $E = \{couleurs\}$.

Soit X une variable aléatoire discrète à valeurs dans E.

Proposition 3. *Soient I au plus dénombrable et $E' = (e_i)_{i\in I} \subset E$ tel que $X(\Omega) \subset E'$. Alors $\mathbb{P}_X$ est caractérisée par $(p_i)_{i\in I}$, où $p_i = \mathbb{P}(X = e_i)$ avec $\sum_{i\in I} p_i = 1$ et $\mathbb{P}_X = \sum_{i\in I} p_i \delta_{e_i}$.*

Remarque 4. *Réciproquement, si $f : E' \to [0,1]$ est telle que $\sum_{i\in I} f(e_i) = 1$, alors il existe une unique probabilité $\mathbb{P}$ sur $(E, \mathcal{E})$ telle que $\mathbb{P}(e_i) = f(e_i)$. Une variable aléatoire suivant cette loi est alors discrète.*

2) Lois discrètes usuelles

Les variables aléatoires discrètes les plus classiques sont à valeurs dans $\mathbb{N}$. On trouvera en annexe les propriétés de ces lois.

Application 5 (Modélisation par des variables aléatoires discrètes)**.**

(i) On lance une pièce équilibrée et on note $X = 1$ si le résultat est "face", 0 sinon. Alors $X \hookrightarrow \mathcal{B}\left(\frac{1}{2}\right)$.

(ii) Si on lance n fois la pièce de manière indépendante, le nombre X de succès suit $\mathcal{B}\left(n, \frac{1}{2}\right)$.

(iii) Le résultat du jet d'un dé à 6 faces équilibré suit $\mathcal{U}(\llbracket 1, 6 \rrbracket)$.

(iv) Soit ℓ le nombre moyen de personnes se présentant à un guichet chaque minute. Le nombre de personnes se présentant pendant N minutes peut se modéliser par $\mathcal{P}(N\ell)$.

(v) On lance une pièce équilibrée et on note X le nombre de lancers nécessaires avant d'obtenir "face". Alors $X \hookrightarrow \mathcal{G}\left(\frac{1}{2}\right)$.

3) Espérance, variance

Soient X et Y deux variables aléatoires réelles discrètes.

Définition 6. Lorsque cela a un sens, on définit :

(i) L'espérance de X : $\mathbb{E}[X] = \sum_{x\in\mathbb{R}} x\mathbb{P}(X = x)$

(ii) La covariance de X et Y : $\mathrm{Cov}(X, Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])]$

(iii) La variance de X : $\mathrm{Var}(X) = \mathrm{Cov}(X, X) = \mathbb{E}\left[(X - \mathbb{E}[X])^2\right]$

Proposition 7. Cov *est une forme bilinéaire symétrique positive, et on a* $\mathrm{Cov}(X, Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$ *et* $\mathrm{Var}(X) = \mathbb{E}\left[X^2\right] - \mathbb{E}[X]^2$.

Proposition 8. *Si X et Y sont indépendantes, alors* $\mathrm{Cov}(X, Y) = 0$, *et* $\mathrm{Var}(X + Y) = \mathrm{Var}(X) + \mathrm{Var}(Y)$.

4) Indépendance

Définition 9. Soient I un ensemble et $(X_i)_{i\in I}$ des variables aléatoires à valeurs dans $(E_i, \mathcal{E}_i)$. Les X_i sont indépendantes si, pour tout $J \subset I$ fini :

$$\forall (A_i)_{i\in J} \in \prod_{i\in J} \mathcal{E}_i,\ \mathbb{P}\left(\bigcap_{i\in J} X_i \in A_i\right) = \prod_{i\in J} \mathbb{P}(X_i \in A_i)$$

Proposition 10. *Soient I un ensemble et $(X_i)_{i\in I}$ des variables aléatoires à valeurs dans $(E_i, \mathcal{E}_i)$. Soient $(E'_i)_{i\in I}$ dénombrables tels que $X_i \in E'_i$ presque sûrement. Les $(X_i)_{i\in I}$ sont indépendantes si, et seulement si, pour tout $J \subset I$ fini, on a :*

$$\forall (e_i)_{i\in J} \in \prod_{i\in J} E'_i,\ \mathbb{P}\left(\bigcap_{i\in J} \{X_i = e_i\}\right) = \prod_{i\in J} \mathbb{P}(X_i = e_i)$$

Exemple 11. *Soient X et Y les résultats de deux lancers indépendants d'un dé à 6 faces équilibré. Soit $Z = \mathbb{1}_{\{X+Y \text{ est pair}\}}$. Alors (X, Y), (X, Z) et (Y, Z) sont indépendantes, mais pas (X, Y, Z).*

Proposition 12. *Soient X et Y réelles discrètes indépendantes. Alors :*

$$\mathbb{P}_{X+Y} = \mathbb{P}_X * \mathbb{P}_Y \quad où \quad \mathbb{P}_X * \mathbb{P}_Y(z) = \sum_{x+y=z} \mathbb{P}_X(x)\mathbb{P}_Y(y)$$

Application 13 (Marche aléatoire sur $\mathbb{Z}^d$)**.** *Soit (e_i) la base canonique de $\mathbb{R}^d$. Soient $(X_i)_{i\in\mathbb{N}^\star}$ des variables aléatoires indépendantes identiquement distribuées telles que $\mathbb{P}(X_k = e_i) = \mathbb{P}(X_k = -e_i) = \frac{1}{2d}$. On pose $S_0 = 0$ et $S_n = \sum_{k=1}^n X_i$ pour $n \in \mathbb{N}^\star$. Alors $\mathbb{P}(S_n = 0$ infiniment souvent$) = 1$ si $d \leqslant 2$ et $\mathbb{P}(|S_n| \to \infty) = 1$ si $d > 2$.*

II Caractérisation des lois discrètes

1) Fonction de répartition

Soit X une variable aléatoire réelle discrète.

Définition 14. On définit la fonction de répartition F_X de X par :

$$F_X : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & [0,1] \\ x & \longmapsto & \mathbb{P}_X(]-\infty, x]) = \mathbb{P}(X \leqslant x) \end{array} \right.$$

Exemple 15. *Fonctions de répartition des lois classiques (cf Annexe).*

Proposition 16. *(i) F_X est croissante, continue à droite, tend vers 0 en $-\infty$ et vers 1 en $+\infty$.*

(ii) Réciproquement, toute fonction satisfaisant le point précédent est la fonction de répartition d'une variable aléatoire.

Proposition 17. *F_X caractérise $\mathbb{P}_X$.*

Remarque 18. *On peut généraliser la fonction de répartition pour une variable aléatoire à valeurs dans $\mathbb{R}^d$. Le résultat reste valable.*

2) Fonction génératrice

Soit X une variable aléatoire à valeurs dans $E = \mathbb{N}$.

Définition 19. On définit la fonction génératrice G_X de X par :

$$G_X : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ s & \longmapsto & \mathbb{E}\left[s^X\right] \end{array} \right.$$

Remarque 20. *Le rayon de convergence de cette série est au moins égal à 1 et $G_X(1) = 1$.*

Exemple 21. *Fonctions génératrices des lois classiques (cf Annexe).*

Proposition 22. *G_X caractérise $\mathbb{P}_X$. En particulier $\mathbb{P}(X = k) = \frac{G_X^{(k)}(0)}{k!}$.*

Proposition 23. *$\mathbb{E}[|X|^p] < +\infty$ si, et seulement si, G_X est p fois dérivable et dans ce cas $G_X^{(p)}(1) = \mathbb{E}[X(X-1)\cdots(X-p+1)]$.*

Application 24. *$\mathbb{E}[X] = G_X'(1)$ et $\mathrm{Var}(X) = G_X''(1) + G_X'(1) - G_X'(1)^2$.*

Proposition 25. *Si X et Y sont deux variables aléatoires discrètes indépendantes, alors $G_{X+Y} = G_X G_Y$.*

Application 26. *On ne peut pas truquer deux dés de sorte que leur somme suivent une loi uniforme sur $[\![2, 12]\!]$.*

Corollaire 27. *Soient $\lambda, \mu > 0$, $X \hookrightarrow \mathcal{P}(\lambda)$ et $Y \hookrightarrow \mathcal{P}(\mu)$ indépendants. Alors $X + Y \hookrightarrow \mathcal{P}(\lambda + \mu)$.*

Théorème 28 (Galton-Watson)**.** *Soient $(X_i^j)_{i,j\in\mathbb{N}^\star}$ des variables aléatoires indépendantes et identiquement distribuées à valeurs dans $\mathbb{N}$. On note μ leur loi et m leur espérance. On définit le processus $(Z_n)_{n\in\mathbb{N}}$ par $Z_0 = 1$ et $Z_{n+1} = \sum_{i=1}^{Z_n} X_i^{n+1}$ pour $n \in \mathbb{N}$. On note $\pi_\infty = \mathbb{P}(\exists\, n \in \mathbb{N},\ Z_n = 0)$. Alors si $\mu \neq \delta_1$, on a :*

(i) Si $m \leqslant 1$, alors $\pi_\infty = 1$: Il y a extinction presque sûre du processus.

(ii) Si $m > 1$, alors $\pi_\infty < 1$: Il y a une probabilité non nulle de survie.

3) Fonction caractéristique

Soit X une variable aléatoire à valeurs dans $\mathbb{R}^d$.

Définition 29. On définit la fonction caractéristique φ_X de X par :

$$\varphi_X : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{C} \\ \lambda & \longmapsto & \mathbb{E}\left[e^{i\langle\lambda, X\rangle}\right] \end{array} \right.$$

Exemple 30. *Fonctions caractéristiques des lois classiques (cf Annexe).*

Proposition 31. *φ_X caractérise $\mathbb{P}_X$.*

Proposition 32. *Si X est réelle et $\mathbb{E}[|X|^p] < +\infty$, alors φ_X est p fois dérivable et $\varphi_X^{(p)}(\lambda) = i^p \mathbb{E}\left[X^p e^{i\lambda X}\right]$. En particulier, $\varphi_X^{(p)}(0) = i^p \mathbb{E}[X^p]$.*

Remarque 33. *Réciproquement, si p est pair et φ_X p fois dérivable en 0, alors $\mathbb{E}[|X|^p] < +\infty$. On peut construire X n'admettant pas d'espérance, mais telle que φ_X est dérivable en 0 (admis).*

III Convergence en loi

Définition 34. On dit que (X_n) converge en loi vers X si, pour tout $\varphi \in \mathcal{C}_b(\mathbb{R},\mathbb{R})$, $\lim_n \mathbb{E}[\varphi(X_n)] = \mathbb{E}[\varphi(X)]$. On note alors $X_n \xrightarrow{\mathcal{L}} X$.

Exemple 35. *Si $X_n \hookrightarrow \mathcal{G}\left(\frac{p}{n}\right)$ avec $p>0$, alors $\frac{1}{n}X_n \xrightarrow{\mathcal{L}} \mathcal{E}(p)$.*

Théorème 36 (Lévy)**.** *$X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si et seulement si $\varphi_{X_n} \xrightarrow[n\to+\infty]{} \varphi_X$.*

Proposition 37. *$X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si, et seulement si, pour tout $x \in E$, $\mathbb{P}(X_n = E) \xrightarrow[n\to+\infty]{} \mathbb{P}(X=k)$.*

Proposition 38. *$X_n \xrightarrow{\mathcal{L}} X$ si, et seulement si, $F_{X_n} \to F_X$ en tout point de continuité de F_X.*

Théorème 39 (Théorème central limite)**.** *On suppose que les X_n sont indépendants, identiquement distribués et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}\frac{X_i - \mathbb{E}[X_i]}{\sqrt{\mathrm{Var}(X_i)}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$$

Application 40. *On suppose que les X_n sont indépendants, identiquement distribués et de loi $\mathcal{B}(p)$ pour $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\widehat{p_n} = \frac{1}{n}\sum_{k=1}^{n} X_i$. Il s'agit de :*

$$IC_\alpha = \left[\widehat{p_n} \pm \frac{q_{1-\frac{\alpha}{2}}}{2\sqrt{n}}\right]$$

où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Application 41 (Monte-Carlo)**.** *Soit $f : [0,1] \to \mathbb{R}$ intégrable par rapport à la mesure de Lebesgue, et $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires indépendantes, identiquement distribuées et de loi $\mathcal{U}([0,1])$. Alors :*

$$\frac{1}{n}\sum_{k=1}^{n} f(X_i) \xrightarrow[n\to+\infty]{} \int_0^1 f(t)dt \text{ p.s.}$$

Théorème 42. *Soit $(X_{n,j})_{n\in\mathbb{N}^\star, j\in[\![1,M_n]\!]}$ une suite de variables aléatoires indépendantes à valeurs dans $\{0,1\}$, avec $(M_n)_{n\in\mathbb{N}^\star}$ une suite croissante de $\mathbb{N}^\star$ qui tend vers $+\infty$. On pose $\mathbb{P}(X_{n,j}=1) = p_{n,j}$ et $S_n = \sum_{j=1}^{M_n} X_{n,j}$. On suppose de plus que :*

$$\lim_{n\to+\infty}\max_{1\leqslant j\leqslant M_n} p_{n,j} = 0 \quad \text{et} \quad \lim_{n\to+\infty}\sum_{j=1}^{M_n} p_{n,j} = \lambda > 0$$

Alors la suite $(S_n)_{n\in\mathbb{N}^\star}$ converge en loi vers la loi de Poisson $\mathcal{P}(\lambda)$.

Développements

- Processus de Galton-Watson (28) [App13]
- Loi des évènements rares de Poisson (42) [Ouv09]

Références

[BL07] P. Barbe et M. Ledoux. *Probabilité.* EDP Sciences
[Ouv08] J.-Y. Ouvrard. *Probabilités : Tome 1.* Cassini
[Ouv09] J.-Y. Ouvrard. *Probabilités : Tome 2.* Cassini
[App13] W. Appel. *Probabilités pour les non probabilistes.* H&K

Annexes

Nom	Paramètres	Notation	$\mathbb{P}_X$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$\varphi_X(t)$	$G_X(t)$
Uniforme	$n \in \mathbb{N}^\star$	$\mathcal{U}([\![1,n]\!])$	$\sum_{k=1}^{n} \frac{1}{n}\delta_k$	$\frac{n+1}{2}$	$\frac{n^2-1}{12}$	$\frac{1}{n}\sum_{k=1}^{n} e^{ikt}$	$\frac{1}{n}\frac{t-t^{n+1}}{1-t}$ $(t \neq 1)$
Bernoulli	$p \in [0,1]$	$\mathcal{B}(p)$	$p\delta_1 + (1-p)\delta_0$	p	$p(1-p)$	$pe^{it} + (1-p)$	$1-p+pt$
Binomiale	$n \in \mathbb{N}^\star, p \in [0,1]$	$\mathcal{B}(n,p)$	$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k}\delta_k$	np	$np(1-p)$	$pe^{it} + (1-p)^n$	$(1-p+pt)^n$
Géométrique	$q \in [0,1]$	$\mathcal{G}(q)$	$\sum_{k=0}^{\infty} q(1-q)^{k-1}\delta_k$	$\frac{1}{q}$	$\frac{1-q}{q^2}$	$\frac{qe^{it}}{1-(1-q)e^{it}}$	$\frac{(1-q)t}{1-qt}$
Poisson	$\lambda > 0$	$\mathcal{P}(\lambda)$	$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!}\delta_k$	λ	λ	$e^{\lambda(e^{it}-1)}$	$e^{(\lambda-1)t}$

FIGURE 1 – Lois de probabilités discrètes

I Exemples de fonctions usuelles

1) Fonction exponentielle

Définition 1. On définit la série entière suivante sur $\mathbb{C}$:

$$\exp(z) = e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Proposition 2. *(i) Pour tout $z_1, z_2 \in \mathbb{C}$, on a $e^{z_1+z_2} = e^{z_1}e^{z_2}$.*
(ii) Pour tout $z \in \mathbb{C}$, on a $e^z \neq 0$, $\frac{1}{e^z} = e^{-z}$, $\overline{e^z} = e^{\overline{z}}$ et $|e^z| = e^{\mathrm{Re}\, z}$.
(iii) exp *est un morphisme de groupe surjectif de $(\mathbb{C}, +)$ dans $(\mathbb{C}^\star, \times)$.*
(iv) exp *est holomorphe sur $\mathbb{C}$, et* exp *est sa propre dérivée.*

Théorème 3. *La restriction de* exp *à $\mathbb{R}$ est positive et croissante, avec, pour tout $n \in \mathbb{N}$, $\lim_{x\to-\infty} x^n e^x = 0$ et $\lim_{x\to+\infty} \frac{e^x}{x^n} = +\infty$.*

Application 4. *La restriction de la fonction* exp *à $\mathbb{R}$ est l'unique solution du problème de Cauchy $y' = y$ avec $y(0) = 1$.*

2) Fonctions trigonométriques

Définition 5. On définit les séries entières suivantes sur $\mathbb{C}$:

$$\cos(z) = \sum_{n\in\mathbb{N}} \frac{(-1)^n z^{2n}}{(2n)!} \qquad \sin(z) = \sum_{n\in\mathbb{N}} \frac{(-1)^n z^{2n+1}}{(2n+1)!}$$

Proposition 6. *Pour tout $z \in \mathbb{C}$, on a $\exp(iz) = \cos(z) + i\sin(z)$.*

Proposition 7. cos *et* sin *sont holomorphes,* $\cos' = -\sin$ *et* $\sin' = \cos$.

Proposition 8. *Pour $\theta \in \mathbb{R}$, $\cos\theta$ et $\sin\theta$ sont réels.*

Corollaire 9 (Moivre)**.** *Pour $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$, on a :*

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Corollaire 10 (Euler)**.** *Pour $\theta \in \mathbb{R}$, on a :*

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad et \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

Application 11. *On peut exprimer $\cos(n\theta)$ comme un polynôme en $\cos\theta$: ce sont les polynômes de Tchebychev.*

Proposition 12. *Pour $x, y \in \mathbb{R}$, on a $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$ et $\sin(x+y) = \cos(x)\sin(y) + \sin(x)\cos(y)$.*

3) Fonctions hyperboliques

Définition 13. On définit les séries entières suivantes sur $\mathbb{C}$:

$$\cosh(z) = \sum_{n\in\mathbb{N}} \frac{z^{2n}}{(2n)!} \qquad \sinh(z) = \sum_{n\in\mathbb{N}} \frac{z^{2n+1}}{(2n+1)!}$$

Proposition 14. *Elles sont holomorphes,* $\cosh' = \sinh$, $\sinh' = \cosh$.

Proposition 15. *Pour $x \in \mathbb{R}$, on a :*

$$\cosh x = \frac{e^x + e^{-x}}{2} \quad et \quad \sinh x = \frac{e^x - e^{-x}}{2}$$

4) Fonctions réciproques dérivées

Théorème 16. *Soit $f : I \to \mathbb{R}$ strictement croissante et dérivable, où I est un intervalle de $\mathbb{R}$. Alors f est bijective de I sur $J = f(I)$, et sa réciproque f^{-1} est dérivable sur J et vérifie :*

$$\forall\, y \in J,\ (f^{-1})'(y) = \frac{1}{f'(f^{-1}(y))}$$

Exemple 17. *L'exponentielle réelle donne* $\ln : \mathbb{R}^{+\star} \to \mathbb{R}$, *dérivable de dérivée $x \mapsto \frac{1}{x}$.*

Exemple 18. *Le cosinus sur $]0, \pi[$ donne* $\arccos :]-1, 1[\to]0, \pi[$, *dérivable de dérivée $x \mapsto -\frac{1}{\sqrt{1-x^2}}$.*

Exemple 19. *Le sinus sur $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ donne* $\arcsin :]-1, 1[\to \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$, *dérivable de dérivée $x \mapsto \frac{1}{\sqrt{1-x^2}}$.*

Exemple 20. *La tangente* $\tan = \frac{\sin}{\cos}$ *sur $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ donne* $\arctan : \mathbb{R} \to \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$, *dérivable de dérivée $x \mapsto \frac{1}{1+x^2}$.*

Exemple 21. *Le cosinus hyperbolique sur $\mathbb{R}$ donne* $\mathrm{argch} :]1, +\infty[\to \mathbb{R}$, *dérivable de dérivée $x \mapsto \frac{1}{x^2-1}$. On a* $\mathrm{argch} : x \mapsto \ln\left(x + \sqrt{x^2-1}\right)$.

Exemple 22. *Le sinus hyperbolique sur $\mathbb{R}$ donne* $\mathrm{argsh} : \mathbb{R} \to \mathbb{R}$, *dérivable de dérivée $x \mapsto \frac{1}{x^2+1}$. On a* $\mathrm{argsh} : x \mapsto \ln\left(x + \sqrt{x^2+1}\right)$.

Exemple 23. *La tangente hyperbolique* $\tanh = \frac{\sinh}{\cosh}$ *sur $\mathbb{R}$ donne* $\mathrm{argth} :]-1, 1[\to \mathbb{R}$, *dérivable de dérivée $x \mapsto \frac{1}{1-x^2}$. On a* $\mathrm{argth} : x \mapsto \frac{1}{2}\ln\left(\frac{1+x}{1-x}\right)$.

II Fonctions spéciales à variables complexes

1) Fonction Γ d'Euler

Définition 24. La fonction Γ d'Euler est définie sur le demi-plan complexe $P = \{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > 0\}$ par :

$$\Gamma : \left| \begin{array}{ccc} P & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \displaystyle\int_0^{+\infty} e^{-t} t^{z-1} dt \end{array} \right.$$

Proposition 25. *La fonction Γ est holomorphe sur P.*

Proposition 26. *(i) On a $\Gamma(1) = 1$.*

(ii) La fonction Γ vérifie $\Gamma(z+1) = z\Gamma(z)$ pour $z \in P$.

(iii) Pour tout $n \in \mathbb{N}^\star$, on a $\Gamma(n) = (n-1)!$.

Théorème 27. *La fonction Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$ dont ses pôles sont les entiers négatifs ou nuls et sont tous simples.*

2) Fonction ζ de Riemann

Définition 28. La fonction ζ de Riemann est définie sur le demi-plan complexe $G = \{s \in \mathbb{C} \,|\, \mathrm{Re}(s) > 1\}$ par :

$$\zeta : \left| \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ s & \longmapsto & \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^s} \end{array} \right.$$

Exemple 29. *On a $\zeta(2) = \frac{\pi^2}{6}$ et $\zeta(4) = \frac{\pi^4}{90}$.*

Proposition 30. *La fonction ζ est holomorphe sur G.*

On s'intéresse maintenant aux propriétés de la restriction de ζ à $]1, +\infty[$.

Proposition 31. *La fonction ζ est de classe $\mathcal{C}^\infty$ sur $]1, +\infty[$.*

Proposition 32. $\lim_{s\to+\infty} \zeta(s) = 1$, $\lim_{s\to 1} \zeta(s) = +\infty$

Proposition 33. $\zeta(s) = \frac{1}{s-1} + \gamma + \mathrm{o}_{1^+}(1)$, *où γ est la constante d'Euler.*

3) Applications

Définition 34. Soit X une variable aléatoire. On dit que X suit la loi gamma de paramètres $a > 0$ et $\lambda > 0$, notée $\Gamma(a, \lambda)$, si sa densité est :

$$f(x) = \frac{\lambda^a}{\Gamma(a)} e^{-\lambda x} x^{a-1} \mathbb{1}_{\mathbb{R}^+}(x)$$

Proposition 35. *Soit $X \hookrightarrow \Gamma(a, \lambda)$. Alors $\mathbb{E}[X] = \frac{a}{\lambda}$ et $\mathrm{Var}(X) = \frac{a}{\lambda^2}$.*

Proposition 36. *Soit $X \hookrightarrow \Gamma(a, \lambda)$. Alors $\varphi_X : t \mapsto \frac{\lambda^a}{(\lambda - it)^a}$.*

Remarque 37. *L'hypothèse de Riemann dit : Les zéros de la fonction ζ qui ne sont pas des entiers négatifs sont de partie réelle $\frac{1}{2}$. Cette hypothèse à ce jour non démontrée forme un lien avec la répartition des nombres premiers.*

III Fonctions pathologiques

On parle de fonctions pathologiques pour désigner des fonctions particulières qui ont eu une importance historique dans leur introduction ou qui fournissent des contre-exemples a des propriétés que l'on pourrait naïvement considérer comme vraies.

(i) Fonction de Dirichlet : L'indicatrice de l'ensemble $\mathbb{Q} \subset \mathbb{R}$ n'est continue en aucun point de $\mathbb{R}$, car $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$. Il s'agit également d'une fonction intégrable au sens de Lebesgue, mais pas au sens de Riemann. De plus, la fonction $t \mapsto t\mathbb{1}_{\mathbb{Q}}(t)$ est continue en un unique point : 0.

(ii) Fonction de Takagi : Pour $x \in \mathbb{R}$, on pose $s(x) = d(x, \mathbb{Z})$. La fonction $f : x \mapsto \sum_{n=0}^{\infty} \frac{s(2^n x)}{2^n}$ est continue sur $[0, 1]$, et 1-périodique donc continue sur $\mathbb{R}$. Elle n'est cependant dérivable en aucun point.

(iii) La fonction $\sum_{n=0}^{\infty} u_n$, où $u_n : x \mapsto \frac{h(nx)}{2^n}$ et $h : x \mapsto x - \lfloor x \rfloor$, est continue sur $\mathbb{R} \setminus \mathbb{Q}$, mais discontinue en tout point de $\mathbb{Q}$.

(iv) La fonction $x \mapsto x^2 \sin\left(\frac{1}{x^2}\right)$ est dérivable sur $\mathbb{R}$, mais n'est pas de classe $\mathcal{C}^1$.

(v) La fonction $x \mapsto \frac{\sin x}{x}$ prolongée par 1 en 0 est intégrable sur $\mathbb{R}$ au sens de Riemann, mais pas au sens de Lebesgue.

(vi) La fonction $x \mapsto e^{-\frac{1}{x}} \mathbb{1}_{\mathbb{R}}(x)$ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$, mais ne coïncide pas avec sa série de Taylor en 0.

IV Transformée de Fourier

1) Généralités

Soit $f \in L^1(\mathbb{R}^d)$, pour $d \in \mathbb{N}^\star$.

Définition 38. On définit la transformée de Fourier de f par :

$$\mathcal{F}(f) = \widehat{f} : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{C} \\ \zeta & \longmapsto & \displaystyle\int_{\mathbb{R}^d} f(x) e^{-i\langle x,\zeta\rangle}\, dx \end{array} \right.$$

Exemple 39. *Si $\gamma_a(x) = e^{-ax^2}$ pour $a > 0$ et $x \in \mathbb{R}$, alors $\widehat{\gamma_a} = \sqrt{\frac{\pi}{a}}\gamma_{\frac{1}{4a}}$.*

Proposition 40. *L'application $\mathcal{F} : L^1(\mathbb{R}^d) \to \mathcal{C}^0(\mathbb{R}^d, \mathbb{C})$ est bien définie, linéaire et continue.*

Théorème 41 (Riemann-Lebesgue)**.** $\lim_{|\zeta|\to\infty} \widehat{f}(\zeta) = 0$

Proposition 42. *Soient $f, g \in L^1(\mathbb{R}^d)$. Alors $\widehat{fg} = \widehat{f * g}$.*

Proposition 43. *Soit $n \in \mathbb{N}^\star$ tel que $f_k : t \mapsto t^k f(t) \in L^1(\mathbb{R}^d)$ pour tout $k \in [\![1, n]\!]$. Alors $\widehat{f} \in \mathcal{C}^{\mathbb{R}^d}(n)$ et on a $\widehat{f}^{(k)} = (-2i\pi)^k \widehat{f_k}$.*

Proposition 44. *Soit $n \in \mathbb{N}^\star$ tel que $f \in L^1(\mathbb{R}^d) \cap \mathcal{C}^n(\mathbb{R}^d, \mathbb{C})$ et que $f^{(k)} \in L^1(\mathbb{R}^d)$ pour tout $k \in [\![1, n]\!]$. Alors $\widehat{f^{(k)}}(\zeta) = (2i\pi\zeta)^k \widehat{f}(\zeta)$.*

2) Applications en probabilités

Définition 45. Soit $f(x) = \frac{1}{\sqrt{\pi}} e^{-\frac{x^2}{2}}$ définie sur $\mathbb{R}$. La fonction f est la densité d'une loi de probabilité, appelée loi normale centrée réduite et notée $\mathcal{N}(0,1)$. Si X suit la loi $\mathcal{N}(0,1)$, on notera $\mathcal{N}(m, \sigma^2)$ la loi de $Y = \sigma X + m$, pour $m \in \mathbb{R}$ et $\sigma > 0$.

Proposition 46. *Soient $X \hookrightarrow \mathcal{N}(0,1)$ et $Y \hookrightarrow \mathcal{N}(m, \sigma^2)$. Alors $\mathbb{E}[X] = 0$, $\mathbb{E}[Y] = m$, $\mathrm{Var}(X) = 1$ et $\mathrm{Var}(Y) = \sigma^2$.*

Définition 47. Soit X une variable aléatoire à valeurs dans $E = \mathbb{R}^d$. On définit la fonction caractéristique φ_X de X par :

$$\varphi_X : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{C} \\ \lambda & \longmapsto & \mathbb{E}\left[e^{i\langle \lambda, X\rangle}\right] \end{array} \right.$$

Exemple 48. *Si $X \hookrightarrow \mathcal{N}(0,1)$, alors $\varphi_X(t) = e^{-\frac{t^2}{2}}$.*

Remarque 49. *Si X a pour densité f, alors $\varphi_X = \check{\widehat{f}}$.*

Proposition 50. *φ_X caractérise $\mathbb{P}_X$.*

Proposition 51. *Si X est réelle et $\mathbb{E}[|X|^p] < +\infty$, alors φ_X est p fois dérivable et $\varphi_X^{(p)}(\lambda) = i^p \mathbb{E}\left[X^p e^{i\lambda X}\right]$. En particulier, $\varphi_X^{(p)}(0) = i^p \mathbb{E}[X^p]$.*

Théorème 52 (Lévy)**.** *$X_n \xrightarrow[n\to+\infty]{\mathcal{L}} X$ si et seulement si $\varphi_{X_n} \xrightarrow[n\to+\infty]{} \varphi_X$.*

Théorème 53 (Théorème central limite)**.** *On suppose que les X_n sont indépendants, identiquement distribués et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} \frac{X_i - \mathbb{E}[X_i]}{\sqrt{\mathrm{Var}(X_i)}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$$

Application 54. *On suppose que les X_n sont indépendants, identiquement distribués et de loi $\mathcal{B}(p)$ pour $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\widehat{p_n} = \frac{1}{n}\sum_{k=1}^{n} X_i$. Il s'agit de :*

$$IC_\alpha = \left[\widehat{p_n} \pm \frac{q_{1-\frac{\alpha}{2}}}{2\sqrt{n}}\right]$$

où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Développements

- Fonction Gamma (25,27) [Les14]
- Transformée de Fourier d'une gaussienne (39) [El 08]
- Théorème central limite et intervalle de confiance (53,54) [BL07]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[Rud09] W. Rudin. *Analyse réelle et complexe.* Dunod
[Hau07] B. Hauchecorne. *Les Contre-exemples en Mathématiques.* Ellipses
[BL07] P. Barbe et M. Ledoux. *Probabilité.* EDP Sciences
[El 08] M. El Amrani. *Analyse de Fourier dans les espaces fonctionnels.* Ellipses
[Les14] A. Lesfari. *Variables complexes.* Ellipses

Cadre : Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé.

I Notion d'indépendance

1) Indépendance d'évènements

Définition 1. Deux évènements A et B sont dits indépendants si $\mathbb{P}(A \cap B) = \mathbb{P}(A)\,\mathbb{P}(B)$.

Définition 2. Une famille $(A_i)_{i\in I}$ d'évènements est dite indépendante dans son ensemble si, pour tout $J \subset I$ fini, on a :

$$\mathbb{P}\left(\bigcap_{j\in J} A_j\right) = \prod_{j\in J} \mathbb{P}(A_j)$$

Remarque 3. *(i) Si $I = \{1,2\}$, on retrouve la définition de deux évènements indépendants.*

(ii) Si n évènements sont indépendants dans leur ensemble, alors ils sont indépendants deux à deux, mais la réciproque est fausse.

Exemple 4. *On considère $\Omega = [\![1,4]\!]$ muni de la tribu discrète et de la probabilité uniforme. Soient $A = \{1,2\}$, $B = \{3,4\}$ et $C = \{1,4\}$. Alors A, B, C sont indépendants dans leur ensemble mais pas deux à deux.*

Proposition 5. *Soit $(A_i)_{i\in I}$ une famille d'évènements indépendants. On suppose que $I = I_1 \cup I_2$ avec $I_1 \cap I_2 = \varnothing$. Soit $(B_i)_{i\in I}$ la famille d'évènements définis par $B_i = A_i$ si $i \in I_1$ et $B_i = A_i^c$ si $i \in I_2$. Alors les B_i sont indépendants dans leur ensemble.*

2) Indépendance de variables aléatoire

Soit $(X_i)_{i\in I}$ une famille de variables aléatoires définies sur $(\Omega, \mathcal{A}, \mathbb{P})$ à valeurs dans des espaces probabilisables $(E_i, \mathcal{E}_i)$.

Définition 6. Les variables aléatoires X_i sont dites indépendantes si, pour toute famille d'évènements $(A_i)_{i\in I}$ avec $A_i \in \mathcal{E}_i$, les évènements $(X_i \in A_i)$ sont indépendants dans leur ensemble.

Proposition 7. *Les variables aléatoires X_i sont indépendantes si, et seulement si, pour toute famille d'évènements $(A_i)_{i\in I}$ avec $A_i \in \mathcal{E}_i$:*

$$\mathbb{P}\left(\bigcap_{i\in I}(X_i \in A_i)\right) = \prod_{i\in I} \mathbb{P}(X_i \in A_i)$$

Proposition 8. *On suppose que les X_i sont des variables aléatoires discrètes et que $I = [\![1,n]\!]$. Les variables aléatoires X_i sont indépendantes si, et seulement si, pour tout n-uplet $(x_1,\dots,x_n) \in X_1(\Omega)\times\ldots\times X_n(\Omega)$:*

$$\mathbb{P}(X_1 = x_1, \dots, X_n = x_n) = \mathbb{P}(X_1 = x_1)\dots\mathbb{P}(X_n = x_n)$$

Proposition 9. *On suppose que les X_i sont indépendantes. Soit $(f_i)_{i\in I}$ une famille de variables aléatoires définies sur $(E_i, \mathcal{E}_i)$ à valeurs dans des espaces probabilisables $(F_i, \mathcal{F}_i)$. Alors les variables aléatoires $f_i \circ X_i$ sont indépendantes.*

Corollaire 10. *On suppose que les X_i sont des variables aléatoires discrètes indépendantes et que $I = [\![1,n]\!]$. Pour $k \in [\![1, n-1]\!]$, soient $f_1 : E_1\times\ldots\times E_k \to F_1$ et $f_2 : E_{k+1}\times\ldots\times E_n \to F_2$. Alors les variables aléatoires $f_1(X_1,\dots,X_k)$ et $f_2(X_{k+1},\dots,X_n)$ sont indépendantes.*

Exemple 11. *Si X_1, X_2, X_3 et X_4 sont des variables aléatoires indépendantes à valeurs dans $\mathbb{Z}$, les variables aléatoires $X_i + X_j$ et $X_k + X_l$ sont indépendantes pour $i,j,k,l \in [\![1,4]\!]$ distincts.*

Exemple 12 (Box-Muller)**.** *Soient U et V deux variables aléatoires indépendantes de loi $\mathcal{U}(]0,1[)$, et posons $X = \sqrt{-2\ln(V)}\cos(2\pi U)$ et $Y = \sqrt{-2\ln(V)}\sin(2\pi U)$. Alors X et Y sont indépendantes et suivent une loi $\mathcal{N}(0,1)$.*

3) Indépendance de sous-tribus

Définition 13. Une famille de sous-tribus $\mathcal{A}_i \subset \mathcal{A}$ pour $i \in I$ est indépendante dans son ensemble si toute famille d'évènements $A_i \in \mathcal{A}_i$ pour $i \in I$ est indépendante dans son ensemble.

Exemple 14. *On considère $\Omega = [0,1]$ muni de sa tribu borélienne et $\mathbb{P}$ la mesure de Lebesgue sur $[0,1]$. Soient, pour tout $n \in \mathbb{N}^\star$, $A_n = \bigcup_{1\leqslant k\leqslant 2^{n-1}} \left]\frac{2k-2}{2^n}, \frac{2k-1}{2^n}\right]$. La famille $(A_n)_{n\in\mathbb{N}^\star}$ est indépendante.*

Proposition 15. *Soit $(\mathcal{A}_i)_{i\in I}$ une famille de sous-tribus de $\mathcal{A}$. Soit $(I_l)_{l\in L}$ une partition de I. La famille des tribus $(\sigma(\mathcal{A}_i | i \in I_l))_{l\in L}$ est une famille indépendante.*

II Indépendance et caractérisation de loi

1) Fonction de répartition

Soit X une variable aléatoire réelle.

Définition 16. On définit la fonction de répartition F_X de X par :

$$F_X : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & [0,1] \\ x & \longmapsto & \mathbb{P}_X(]-\infty, x]) = \mathbb{P}(X \leqslant x) \end{array} \right.$$

Proposition 17. *F_X caractérise $\mathbb{P}_X$.*

Proposition 18. *(i) F_X est croissante, continue à droite, tend vers 0 en $-\infty$ et vers 1 en $+\infty$.*

(ii) Réciproquement, toute fonction satisfaisant le point précédent est la fonction de répartition d'une variable aléatoire.

(iii) Si f est une densité de probabilité, alors $F : x \mapsto \int_{-\infty}^{x} f(t)dt$ est la fonction de répartition d'une variable aléatoire Y telle que $\mathbb{P}_Y$ admette pour densité f.

Proposition 19. *Soient $X_1, \ldots, X_n$ des variables aléatoires indépendantes et identiquement distribuées de fonction de répartition F. Alors $F_{\max(X_i)}(t) = F(t)^n$ et $F_{\min(X_i)}(t) = 1 - (1 - F(t))^n$.*

Corollaire 20. *Soient $X_1, \ldots, X_n$ des variables aléatoires indépendantes et identiquement distribuées de loi $\mathcal{U}(]0,1[)$. Posons $M_n = \max_{1 \leqslant i \leqslant n} X_i$. Alors $M_n \xrightarrow{\mathcal{L}} 1$ et $n(1 - M_n) \xrightarrow{\mathcal{L}} \mathcal{E}(1)$.*

2) Fonction caractéristique

Soit X une variable aléatoire à valeurs dans $\mathbb{R}^d$.

Définition 21. On définit la fonction caractéristique φ_X de X par :

$$\varphi_X : \left| \begin{array}{ccc} \mathbb{R}^d & \longrightarrow & \mathbb{C} \\ \lambda & \longmapsto & \mathbb{E}\left[e^{i\langle \lambda, X \rangle}\right] \end{array} \right.$$

Proposition 22. *φ_X caractérise $\mathbb{P}_X$.*

Proposition 23. *Si X est réelle et $\mathbb{E}[|X|^p] < +\infty$, alors φ_X est p fois dérivable et $\varphi_X^{(p)}(\lambda) = i^p \mathbb{E}\left[X^p e^{i\lambda X}\right]$. En particulier, $\varphi_X^{(p)}(0) = i^p \mathbb{E}[X^p]$.*

Proposition 24. *Soient X et Y deux variables aléatoires indépendantes à valeurs dans $\mathbb{R}^d$. Alors :*

(i) $\varphi_{X+Y} = \varphi_X \varphi_Y$

(ii) Pour tout $(t_1, t_2) \in \mathbb{R}^n \times \mathbb{R}^n$, on a $\varphi_{(X,Y)}(t_1, t_2) = \varphi_X(t_1)\varphi_Y(t_2)$

Application 25. *Soient $X_1, \ldots, X_n$ des variables aléatoires à valeurs dans $\mathbb{R}^d$ indépendantes.*

(i) Si $X_1, \ldots, X_n \hookrightarrow \mathcal{E}(\lambda)$, alors $X_1 + \ldots + X_n \hookrightarrow \Gamma(n, \lambda)$.

(ii) Si $X_1, \ldots, X_n \hookrightarrow \mathcal{N}(0,1)$, alors $X_1^2 + \ldots + X_n^2 \hookrightarrow \Gamma\left(\frac{1}{2}, \frac{n}{2}\right)$.

3) Fonction génératrice

Soit X une variable aléatoire à valeurs dans $\mathbb{N}$.

Définition 26. On définit la fonction génératrice G_X de X par :

$$G_X : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ s & \longmapsto & \mathbb{E}\left[s^X\right] \end{array} \right.$$

Remarque 27. *Le rayon de convergence de cette série est au moins égal à 1 et $G_X(1) = 1$.*

Proposition 28. *G_X caractérise $\mathbb{P}_X$. En particulier, on a $\mathbb{P}(X = k) = \frac{1}{k!} G_X^{(k)}(0)$.*

Proposition 29. *$\mathbb{E}[|X|^p] < +\infty$ si, et seulement si, G_X est p fois dérivable et dans ce cas $G_X^{(p)}(1) = \mathbb{E}[X(X-1)\cdots(X-p+1)]$.*

Application 30. *$\mathbb{E}[X] = G_X'(1)$ et $\mathrm{Var}(X) = G_X''(1) + G_X'(1) - G_X'(1)^2$.*

Proposition 31. *Soient X et Y deux variables aléatoires indépendantes à valeurs dans $\mathbb{N}$. Alors :*

(i) $G_{X+Y} = G_X G_Y$

(ii) Pour tout $(t_1, t_2) \in \mathbb{R}^2$, on a $G_{(X,Y)}(t_1, t_2) = G_X(t_1) G_Y(t_2)$.

(iii) Pour tout $s \in \mathbb{R}$, on a $G_{(X,Y)}(s, s) = G_X(s) G_Y(s)$.

Application 32. *Soient $X_1, \ldots, X_n$ des variables aléatoires à valeurs dans $E = \mathbb{N}$ indépendantes.*

(i) Si $X_i \hookrightarrow \mathcal{P}(\lambda_i)$, alors $X_1 + \ldots + X_n \hookrightarrow \mathcal{P}\left(\sum_{i=1}^n \lambda_i\right)$.

(ii) Si $X_1, \ldots, X_n \hookrightarrow \mathcal{B}(p)$, alors $X_1^2 + \ldots + X_n^2 \hookrightarrow \mathcal{B}(n, p)$.

III Applications

1) Loi du 0-1 et lemme de Borel-Cantelli

Définition 33. Soit $(T_n)_{n\in\mathbb{N}}$ une famille indépendante de tribus sur $(\Omega,\mathcal{A},\mathbb{P})$. On désigne par $\mathcal{A}_n$ la tribu engendrée par $T_n, T_{n+1},\dots$ et on pose $\mathcal{A}_\infty = \bigcap_{n\in\mathbb{N}} \mathcal{A}_n$. La tribu $\mathcal{A}_\infty$ est appelée tribu des évènements terminaux, ou tribu terminale de la suite $(T_n)_{n\in\mathbb{N}}$.

Théorème 34 (Loi du 0-1)**.** *Soit $\mathcal{A}_\infty$ une tribu terminale. Alors, pour tout $A\in\mathcal{A}_\infty$, on a $\mathbb{P}(A)=0$ ou $\mathbb{P}(A)=1$.*

Exemple 35. *Soit $(A_n)_{n\in\mathbb{N}}$ une suite d'évènements indépendants de $(\Omega,\mathcal{A},\mathbb{P})$. Alors $A=\bigcap_{n\in\mathbb{N}}\bigcup_{m\geqslant n} A_m$ est un évènement terminal pour la suite de tribus $T_n=\{\varnothing,\Omega,A_n,A_n^c\}$, donc $\mathbb{P}(A)=0$ ou $\mathbb{P}(A)=1$.*

Théorème 36 (Borel-Cantelli)**.** *Soit $(A_n)_{n\in\mathbb{N}^\star}$ une suite d'évènements.*

(i) Si $\sum\mathbb{P}(A_n)<\infty$, $\mathbb{P}(\limsup A_n)=0$.

(ii) Si $\sum\mathbb{P}(A_n)=\infty$ et les A_n sont indépendants, $\mathbb{P}(\limsup A_n)=1$.

Application 37. *On lance une infinité de fois une pièce équilibrée, on obtiendra presque sûrement une infinité de fois 42 piles consécutifs.*

2) Théorème central limite

Théorème 38 (Théorème central limite)**.** *On suppose que les X_n sont indépendants, identiquement distribués et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}\frac{X_i-\mathbb{E}[X_i]}{\sqrt{\mathrm{Var}(X_i)}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$$

Application 39. *On suppose que les X_n sont indépendants, identiquement distribués et de loi $\mathcal{B}(p)$ pour $p\in[0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\widehat{p_n}=\frac{1}{n}\sum_{k=1}^{n}X_i$. Il s'agit de :*

$$IC_\alpha=\left[\widehat{p_n}\pm\frac{q_{1-\frac{\alpha}{2}}}{2\sqrt{n}}\right]$$

où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Théorème 40. *Soit $(X_{n,j})_{n\in\mathbb{N}^\star,j\in[\![1,M_n]\!]}$ une suite de variables aléatoires indépendantes à valeurs dans $\{0,1\}$, avec $(M_n)_{n\in\mathbb{N}^\star}$ une suite croissante de $\mathbb{N}^\star$ qui tend vers $+\infty$. On pose $\mathbb{P}(X_{n,j}=1)=p_{n,j}$ et $S_n=\sum_{j=1}^{M_n}X_{n,j}$. On suppose de plus que :*

$$\lim_{n\to+\infty}\max_{1\leqslant j\leqslant M_n}p_{n,j}=0 \quad et \quad \lim_{n\to+\infty}\sum_{j=1}^{M_n}p_{n,j}=\lambda>0$$

Alors la suite $(S_n)_{n\in\mathbb{N}^\star}$ converge en loi vers la loi de Poisson $\mathcal{P}(\lambda)$.

3) Processus de Galton-Watson

Théorème 41 (Galton-Watson)**.** *Soient $(X_i^j)_{i,j\in\mathbb{N}^\star}$ des variables aléatoires indépendantes et identiquement distribuées à valeurs dans $\mathbb{N}$. On note μ leur loi et m leur espérance. On définit le processus $(Z_n)_{n\in\mathbb{N}}$ par $Z_0=1$ et $Z_{n+1}=\sum_{i=1}^{Z_n}X_i^{n+1}$ pour $n\in\mathbb{N}$. On note $\pi_\infty=\mathbb{P}(\exists\, n\in\mathbb{N},\ Z_n=0)$. Alors si $\mu\neq\delta_1$, on a :*

(i) Si $m\leqslant 1$, alors $\pi_\infty=1$: Il y a extinction presque sûre du processus.

(ii) Si $m>1$, alors $\pi_\infty<1$: Il y a une probabilité non nulle de survie.

Développements

- Théorème central limite et intervalle de confiance (38,39) [BL07]
- Loi des évènements rares de Poisson (40) [Ouv09]
- Processus de Galton-Watson (41) [App13] [Ouv09]

Références

[BL07] P. Barbe et M. Ledoux. *Probabilité.* EDP Sciences
[App13] W. Appel. *Probabilités pour les non probabilistes.* H&K
[Ouv08] J.-Y. Ouvrard. *Probabilités : Tome 1.* Cassini
[Ouv09] J.-Y. Ouvrard. *Probabilités : Tome 2.* Cassini

I Propriétés métriques des courbes

On considère $\mathcal{E}$ un espace affine dirigé par un espace vectoriel E de dimension n muni de la norme $\|.\|$. Soient $I = [a, b] \subset \mathbb{R}$ et $\gamma : I \to \mathcal{E}$ un arc de courbe paramétrée.

1) Longueur d'un arc de courbe

Définition 1. Soit $\sigma = \{a_0, a_1, \ldots, a_n\}$ une subdivision de I, avec $a = a_0 < a_1 < \ldots < a_n = b$. On pose $L_\sigma(\gamma) = \sum_{i=0}^{n+1} \left\|\overrightarrow{\gamma(a_i)\gamma(a_{i+1})}\right\|$ et $L(\gamma) = \sup_\sigma(L_\sigma(\gamma))$. Si $L(\gamma) < +\infty$, on dit que γ est rectifiable. Dans ce cas, le nombre $L(\gamma)$ sera appelé longueur de γ.

Théorème 2. *Soit $\gamma : I \to \mathcal{E}$ un arc de courbe de classe $\mathcal{C}^1$. Alors γ est rectifiable, et on a $L(\gamma) = \int_a^b \|\gamma'(t)\|\ dt$.*

Corollaire 3. *On suppose $\mathcal{E}$ affine euclidien muni d'un repère orthonormal $\mathcal{R} = (0, e_1, \ldots, e_n)$. Soit $\gamma : I \to \mathcal{E}$ un arc de courbe de classe $\mathcal{C}^1$, on note $\gamma = (\gamma_1, \ldots, \gamma_n)$ les fonctions coordonnées de γ dans $\mathcal{R}$. Alors $L(\gamma) = \int_a^b \left(\sum_{i=1}^n \gamma_i'(t)^2\right)^{\frac{1}{2}}\ dt$*

Exemple 4 (Longueur d'un arc de cercle)**.** *Dans $\mathbb{R}^2$, on considère $\gamma : t \mapsto (R\cos t, R\sin t)$ avec $R > 0$. Alors $L(\gamma) = R(b - a)$.*

Exemple 5 (Longueur d'un arc de parabole)**.** *Dans $\mathbb{R}^2$, on considère $\gamma : t \mapsto (t, t^2)$. Alors :*

$$L(\gamma) = \frac{1}{2}\left(b\sqrt{1+b^2} - a\sqrt{1+a^2} + \operatorname{argsh}(b) - \operatorname{argsh}(a)\right)$$

2) Régularité d'une courbe paramétrée

Définition 6. Soit $\gamma : I \to \mathcal{E}$ un arc de courbe paramétrée. Pour $t_0 \in I$, on dit que $\gamma(t_0)$ est un point singulier si $\gamma'(t_0) = 0$, sinon on dit que c'est un point régulier. La courbe est dite régulière si elle ne possède aucun point singulier, donc si $\gamma'(t) \neq 0$ pour tout $t \in I$.

Exemple 7. *(i) Dans $\mathbb{R}^2$, on considère $\gamma : t \mapsto (t, t^2)$. La courbe associée (parabole) est régulière.*

(ii) Dans $\mathbb{R}^2$, on considère $\gamma : t \mapsto (t - \sin t, 1 - \cos t)$. La courbe associée n'est pas régulière.

Définition 8. Soient $\gamma_1 : I \to \mathcal{E}$ et $\gamma_2 : J \to \mathcal{E}$ avec $J = [\alpha, \beta] \subset \mathbb{R}$. On dit que γ_1 et γ_2 sont $\mathcal{C}^k$-équivalentes s'il existe un $\mathcal{C}^k$-difféomorphisme $\varphi : I \to J$ tel que $\gamma_1 = \gamma_2 \circ \varphi$.

Exemple 9. *La courbe $\gamma_1 : t \mapsto (\cos t, \sin t)$ sur $]-\pi, \pi[$ et la courbe $\gamma_2 : t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ sur $\mathbb{R}^\star$ sont équivalentes.*

Définition 10. Soit $\gamma : I \to \mathcal{E}$ un arc de courbe paramétrée. On dit que γ est paramétrée par une abscisse curviligne, ou normale, si $\|\gamma'(t)\| = 1$ pour tout $t \in I$.

Proposition 11. *Soit $\gamma : I \to \mathcal{E}$ un arc de courbe paramétrée. Si γ est paramétrée par une abscisse curviligne, alors $L(\gamma) = b - a$.*

Théorème 12. *Toute courbe paramétrée régulière peut être paramétrée par une abscisse curviligne.*

3) Tangente à une courbe paramétrée régulière

Définition 13. Soit $\gamma : I \to \mathcal{E}$ un arc de courbe paramétrée de classe $\mathcal{C}^1$. La droite vectorielle $\operatorname{Vect}(\gamma'(t_0))$ est appelée droite vectorielle tangente à γ en t_0. La droite affine $\gamma(t_0) + \operatorname{Vect}(\gamma'(t_0))$ est appelée droite affine tangente à γ en t_0.

Exemple 14. *Dans $\mathbb{R}^2$, on considère $\gamma : t \mapsto (\cos t, \sin t)$. Pour $t_0 \in I$, la droite vectorielle tangente à γ en t_0 est $\operatorname{Vect}(-\sin t_0, \cos t_0)$, et la droite affine tangente à γ en t_0 est $(\cos t_0, \sin t_0) + \operatorname{Vect}(-\sin t_0, \cos t_0)$,*

4) Courbure d'une courbe paramétrée régulière

Définition 15. Soit $\gamma : I \to \mathcal{E}$ un arc de courbe paramétrée par une abscisse curviligne. On définit le courbure de γ en le paramètre $t \in I$ par $\kappa(t) = \|\gamma''(t)\|$.

Proposition 16. *Si $\mathcal{E}$ est euclidien de dimension 2, alors :*

$$\kappa(t) = \frac{|\det(\gamma'(t), \gamma''(t))|}{\|\gamma'(t)\|^3}$$

Exemple 17 (Courbure d'un arc de cercle)**.** *Dans $\mathbb{R}^2$, on considère $\gamma : t \mapsto (R\cos t, R\sin t)$ avec $R > 0$. Alors $\kappa(t) = \frac{1}{R}$ pour tout $t \in I$.*

Exemple 18 (Courbure d'un arc de parabole)**.** *Dans $\mathbb{R}^2$, on considère $\gamma : t \mapsto (t, t^2)$. Alors $\kappa(t) = (1 + t^2)^{-\frac{3}{2}}$.*

II Courbes en topologie

On considère (E, d) un espace métrique.

1) Connexité et connexité par arcs

Proposition 19. *Les assertions suivantes sont équivalentes :*

(i) Il n'existe pas de partition de E en deux ouverts disjoints non vides.

(ii) Il n'existe pas de partition de E en deux fermés disjoints non vides.

(iii) Les seules parties ouvertes et fermées de E sont $\varnothing$ et E.

(iv) Toute fonction continue de E dans $\{0,1\}$ est constante.

Définition 20. Un espace métrique vérifiant l'une des assertions de la proposition précédente est dit connexe.

Remarque 21. *La connexité est une notion topologique.*

Exemple 22. *$\mathbb{R}$ est connexe, $\{0,1\}$ n'est pas connexe.*

Définition 23. On appelle chemin de E toute application continue $\gamma : [0,1] \to E$. Son image $\gamma([0,1])$ est appelée un arc, $\gamma(0)$ son origine et $\gamma(1)$ son but. On dit que γ lie $\gamma(0)$ et $\gamma(1)$.

Définition 24. L'espace E est dit connexe par arcs si, pour tous $a, b \in E$, il existe un chemin liant a et b.

Théorème 25. *La connexité par arcs entraîne la connexité.*

Exemple 26. *La réciproque est fausse : l'adhérence du graphe de la fonction $x \mapsto \sin(\frac{1}{x})$ définie sur $\mathbb{R}^{+\star}$ est connexe non connexe par arcs.*

Proposition 27. *Pour un ouvert d'un espace vectoriel normé, la connexité est équivalente à la connexité par arcs.*

2) Connexité par lignes brisées

On considère (E, d) un espace métrique.

Définition 28. Soient $a, b \in E$. On appelle segment d'extrémités a et b l'ensemble $[a,b] = \{\lambda a + (1-\lambda b) \,|\, \lambda \in [0,1]\}$.

Définition 29. On appelle ligne brisée de E joignant deux points a et b de E tout ensemble de la forme $\bigcup_{i=1}^{n} [x_{i-1}, x_i]$, où $n \in \mathbb{N}^\star$ et $a = x_0, x_1, \ldots, b = x_n \in E$.

Définition 30. Une partie A de E est dite connexe par lignes brisée si, pour tout $a, b \in A$, il existe une ligne brisée dans A joignant a et b.

Remarque 31. *Une partie connexe par ligne brisée est connexe par arcs.*

Théorème 32. *Une partie ouverte de E est connexe si, et seulement si, elle est connexe par lignes brisées.*

Corollaire 33. *Tout ouvert connexe d'un espace vectoriel normé est connexe par arcs.*

3) Homotopie des chemins et des lacets

On considère X un espace topologique. On appelle chemin dans X toute application continue $\gamma : [0,1] \to X$.

Définition 34. On appelle chemin dans X toute application continue $\gamma : [0,1] \to X$. Si $\gamma(0) = \gamma(1)$, on dit que γ est un lacet.

Définition 35. Soient γ_1 et γ_2 deux chemins dans X. Une homotopie de γ_1 à γ_2 est une application continue $H : [0,1] \times [0,1] \to X$ telle que, pour tout $t \in [0,1]$, on a $H(t,0) = \gamma_1(t)$ et $H(t,1) = \gamma_2(t)$. On dira que γ_1 et γ_2 sont homotopes.

Remarque 36. *L'homotopie est une relation d'équivalence.*

Exemple 37. *Soient $\gamma_1(t) = r_1 e^{2i\pi t}$ et $\gamma_2(t) = r_2 e^{2i\pi t}$. Alors l'application $(t,u) \mapsto (ur_2 + (1-u)r_1)e^{2i\pi t}$ est une homotopie de γ_1 à γ_2.*

Définition 38. Soit γ_1 un chemin dans X de x à y, et soit γ_2 un chemin dans X de y à z. On définit $\gamma_1\gamma_2$, appelé composée de γ_1 et γ_2, par :

$$\gamma_1\gamma_2(t) = \begin{cases} \gamma_1(2t) & \text{si } 0 \leqslant t \leqslant \frac{1}{2} \\ \gamma_2(2t-1) & \text{si } \frac{1}{2} \leqslant t \leqslant 1 \end{cases}$$

Définition 39. L'ensemble $\pi_1(X,x)$ des classes d'homotopies des lacets dans X de base x muni de la composition des chemins est un groupe, appelé groupe fondamental.

Proposition 40. *Si x et y sont dans la même composante connexe par arcs de X, les groupes $\pi_1(X,x)$ et $\pi_1(X,y)$ sont isomorphes.*

Exemple 41. *$\pi_1(\mathbb{S}^1) \cong \mathbb{Z}$, $\pi_1(\mathbb{R}^n) \cong \pi_1(\mathbb{S}^2) \cong \{1\}$ et $\pi_1(\mathbb{T}^2) \cong \mathbb{Z}^2$.*

Définition 42. Si X est connexe par arcs, on dit qu'il est simplement connexe si $\pi_1(X) \cong \{e\}$.

Exemple 43. *$\mathbb{R}^n$ et $\mathbb{S}^2$ est simplement connexe.*

III Courbes en analyse complexe

1) Intégration sur un chemin

Définition 44. On appelle chemin dans $\mathbb{C}$ toute application $\gamma : [a,b] \to \mathbb{C}$ continue et $\mathcal{C}^1$ par morceaux. On parle de lacet si $\gamma(a) = \gamma(b)$.

Exemple 45. *Soient $z_0 \in \mathbb{C}$ et $r \in \mathbb{R}^+$, alors une paramétrisation du cercle de centre z_0 et de rayon r est donnée par :*

$$\gamma : \left| \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{C} \\ t & \longmapsto & z_0 + re^{2i\pi t} \end{array} \right.$$

Définition 46. Soient $\gamma : [a,b] \to \mathbb{C}$ un chemin et f une fonction continue sur $\mathrm{Im}(\gamma)$, alors on définit :

$$\forall\, z \in \mathrm{Im}(\gamma),\ \int_\gamma f = \int_\gamma f(z)\,dz = \int_a^b f(\gamma(t))\,\gamma'(t)\,dt$$

Exemple 47. *Si $\gamma(t) = z_0 + re^{2i\pi t}$, alors $\int \frac{1}{z-z_0}\,dz = 2i\pi$.*

2) Théorème de Cauchy

Théorème 48 (Cauchy)**.** *Soient Ω un ouvert convexe et $z_0 \in \Omega$ et $f \in \mathcal{H}(\Omega \setminus \{z_0\})$, alors pour tout lacet γ de Ω, on a $\int_\gamma f = 0$.*

Exemple 49. *Si $\gamma_a(x) = e^{-ax^2}$ pour $a > 0$ et $x \in \mathbb{R}$, alors $\widehat{\gamma_a} = \sqrt{\frac{\pi}{a}}\gamma_{\frac{1}{4a}}$.*

Définition 50. Soit γ un lacet de $\mathbb{C}$ et $a \in \mathbb{C} \setminus \mathrm{Im}(\gamma)$. On définit l'indice $\mathrm{Ind}_\gamma(a)$ de a par rapport à γ par :

$$\mathrm{Ind}_\gamma(a) = \frac{1}{2i\pi}\int_\gamma \frac{1}{z-a}dz$$

Proposition 51. $\mathrm{Ind}_\gamma(a) \in \mathbb{Z}$

Théorème 52 (Formule de Cauchy)**.** *Soient Ω est un ouvert convexe, $z \in \Omega$, γ un lacet de $\Omega \setminus \{z\}$ et $f \in \mathcal{H}(\Omega)$, alors on a :*

$$\mathrm{Ind}_\gamma(z) f(z) = \frac{1}{2i\pi}\int_\gamma \frac{f(\xi)}{\xi - z}d\xi$$

Exemple 53. *Si γ décrit le cercle unité parcouru une fois dans le sens direct, alors $\int_\gamma \frac{\cos z}{z}dz = 0$ et $\int_\gamma \frac{\sin z}{z}dz = 2\pi$.*

3) Théorème des résidus

Définition 54. On dit qu'une fonction f est méromorphe sur Ω s'il existe $A \subset \mathbb{C}$ discret et fermé tel que f est holomorphe sur $\Omega \setminus A$ et les points de A sont des pôles de f.

Exemple 55. *$f(z) = \frac{z}{(z-1)(z-2)^2}$ est méromorphe.*

Définition 56. Soit $z_0 \in \mathbb{C}$, U un voisinage de z_0, et soit f une fonction holomorphe sur $U \setminus \{z_0\}$. On appelle résidu de f au point z_0 le nombre $\mathrm{Res}(f, z_0) = a_{-1}$, où a_{-1} est le coefficient de $\frac{1}{z-z_0}$ dans le développement en série de Laurent de f au voisinage de z_0.

Proposition 57. *Si z_0 est un pôle simple de $f(z) = \frac{P(z)}{Q(z)}$ avec P, Q des polynômes tels que $P(z_0) \neq 0$, alors :*

$$\mathrm{Res}(f, z_0) = \frac{P(z_0)}{Q'(z_0)}$$

Exemple 58. *Pour $f(z) = \frac{z}{(z-1)(z-2)^2}$, $\mathrm{Res}(f,1) = 1$ et $\mathrm{Res}(f,2) = -1$.*

Théorème 59 (Théorème des résidus)**.** *Soient $S \subset \Omega$ fini, $f \in \mathcal{H}(\mathbb{C} \setminus S)$ et γ un lacet dans Ω ne rencontrant pas S, alors :*

$$\int_\gamma f(z)dz = 2i\pi \sum_{c \in S} \mathrm{Ind}_\gamma(c)\,\mathrm{Res}(f, c)$$

Exemple 60. *Soit $\alpha \in]-1, 1[$. Alors $\int_0^{+\infty} \frac{x^\alpha \ln x}{x^2-1}\,dx = \frac{\pi^2}{4\cos^2(\frac{\alpha\pi}{2})}$.*

Développements

- Transformée de Fourier d'une gaussienne (49) [El 08]
- Calcul d'une intégrale par le théorème des résidus (60) [Tau06]

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod
[Rud09] W. Rudin. *Analyse réelle et complexe.* Dunod
[El 08] M. El Amrani. *Analyse de Fourier dans les espaces fonctionnels.* Ellipses
[Tau06] P. Tauvel. *Analyse complexe pour la licence 3.* Dunod

Partie III

Développements

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\sum_{k=0}^{\infty} a_0 q^k = \lim_{n\to\infty} \sum_{k=0}^{n} a_0 q^k = \lim_{n\to\infty} a_0 \frac{1-q^{n+1}}{1-q} = \frac{a_0}{1-q}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\frac{\partial^2 \Phi}{\partial x^2} + \frac{\partial^2 \Phi}{\partial y^2} + \frac{\partial^2 \Phi}{\partial z^2} = \frac{1}{c^2} \frac{\partial^2 \Phi}{\partial t^2}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{ab}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\frac{\sqrt[n]{a}}{\sqrt[n]{b}} = \sqrt[n]{\frac{a}{b}}$$

Qu'est que c'est?. C'est une phrase français avant le lorem ipsum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Répartition des développements d'analyse

Répartition des développements d'algèbre

Répartition des développements mixtes

Développements non utilisés

Leçons d'algèbre et leurs développements

101 - Groupe opérant sur un ensemble. Exemples et applications.
- (i) Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$
- (ii) Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

102 - Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
- (i) Étude des polynômes cyclotomiques
- (ii) Forme faible de la progression arithmétique de Dirichlet
- (iii) Structure des groupes abéliens finis

103 - Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.
- (i) Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$
- (ii) Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

104 - Groupes abéliens et non abéliens finis. Exemples et applications.
- (i) Structure des groupes abéliens finis
- (ii) Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

105 - Groupe des permutations d'un ensemble fini. Applications.
- (i) Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$
- (ii) Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathcal{GL}(E)$. Applications.
- (i) Décomposition polaire
- (ii) Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$

107 - Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel. Exemples.
- (i) Structure des groupes abéliens finis
- (ii) Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

108 - Exemples de parties génératrices d'un groupe. Applications.
- (i) Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$
- (ii) Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$

120 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- (i) Forme faible de la progression arithmétique de Dirichlet
- (ii) Loi de réciprocité quadratique
- (iii) Théorème de Sophie Germain

121 - Nombres premiers. Applications.
- (i) Forme faible de la progression arithmétique de Dirichlet
- (ii) Loi de réciprocité quadratique
- (iii) Théorème de Sophie Germain

122 - Anneaux principaux. Applications.
- (i) Critère d'Eisenstein
- (ii) Théorème des deux carrés

123 - Corps finis. Applications.
- (i) Étude des polynômes cyclotomiques
- (ii) Loi de réciprocité quadratique
- (iii) Polynômes irréductibles unitaires sur $\mathbb{F}_q$

125 - Extensions de corps. Exemples et applications.
- (i) Étude des polynômes cyclotomiques
- (ii) Polynômes irréductibles unitaires sur $\mathbb{F}_q$

126 - Exemples d'équations en arithmétiques.
- (i) Loi de réciprocité quadratique
- (ii) Théorème de Sophie Germain
- (iii) Théorème des deux carrés

141 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- (i) Critère d'Eisenstein
- (ii) Étude des polynômes cyclotomiques

142 - PGCD et PPCM, algorithmes de calcul. Applications.
- (i) Critère d'Eisenstein
- (ii) Étude des polynômes cyclotomiques
- (iii) Théorème de Sophie Germain

144 - Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.
- (i) Polynômes irréductibles unitaires sur $\mathbb{F}_q$
- (ii) Étude des polynômes cyclotomiques

150 - Exemples d'actions de groupes sur les espaces de matrices.

(i) Décomposition polaire

(ii) Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$

(iii) Réduction des endomorphismes normaux

151 - Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

(i) Réduction de Jordan (par la dualité)

(ii) Réduction des endomorphismes normaux

152 - Déterminant. Exemples et Applications.

(i) Déterminant de Gram et inégalité de Hadamard

(ii) Ellipsoïde de John-Loewner

153 - Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

(i) Décomposition de Dunford

(ii) Réduction de Jordan (par la dualité)

154 - Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

(i) Décomposition de Dunford

(ii) Réduction de Jordan (par la dualité)

(iii) Réduction des endomorphismes normaux

155 - Endomorphismes diagonalisables en dimension finie.

(i) Décomposition de Dunford

(ii) Réduction des endomorphismes normaux

156 - Exponentielle de matrices. Applications.

(i) Décomposition de Dunford

(ii) Un homéomorphisme induit par l'exponentielle

157 - Endomorphismes trigonalisables. Endomorphismes nilpotents.

(i) Décomposition de Dunford

(ii) Réduction de Jordan (par la dualité)

158 - Matrices symétriques réelles, matrices hermitiennes.

(i) Décomposition polaire

(ii) Un homéomorphisme induit par l'exponentielle

(iii) Ellipsoïde de John-Loewner

159 - Formes linéaires et dualité en dimension finie. Exemples et applications.

(i) Réduction de Jordan (par la dualité)

(ii) Extrema liés

160 - Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

(i) Décomposition polaire

(ii) Réduction des endomorphismes normaux

(iii) Un homéomorphisme induit par l'exponentielle

161 - Distances et isométries d'un espace affine euclidien.

(i) Décomposition polaire

(ii) Déterminant de Gram et inégalité de Hadamard

(iii) Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

162 - Systèmes d'équations linéaires. Opérations élémentaires, aspects algorithmiques et conséquences théoriques.

(i) Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$

(ii) Algorithme de gradient à pas optimal

170 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

(i) Ellipsoïde de John-Loewner

(ii) Lemme de Morse

171 - Formes quadratiques réelles. Coniques. Exemples et applications.

(i) Ellipsoïde de John-Loewner

(ii) Lemme de Morse

181 - Barycentres dans un espace affine réel de dimension finie, convexité. Applications.

(i) Théorème de Carathéodory

(ii) Ellipsoïde de John-Loewner

190 - Méthodes combinatoires, problèmes de dénombrement.

(i) Polynômes irréductibles unitaires sur $\mathbb{F}_q$

(ii) Nombres de Bell

191 - Exemples d'utilisation des techniques d'algèbre en géométrie.

(i) Déterminant de Gram et inégalité de Hadamard

(ii) Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

Leçons d'analyse et leurs développements

201 - Espaces de fonctions. Exemples et applications.
- (i) Densité des polynômes orthogonaux
- (ii) Théorème de Riesz-Fischer
- (iii) Théorème de Weierstrass

203 - Utilisation de la notion de compacité.
- (i) Connexité des valeurs d'adhérence d'une suite
- (ii) Théorème de Weierstrass
- (iii) Ellipsoïde de John-Loewner

204 - Connexité. Exemples et applications.
- (i) Calcul d'une intégrale par le théorème des résidus
- (ii) Connexité des valeurs d'adhérence d'une suite

205 - Espaces complets. Exemples et applications.
- (i) Projection sur un convexe fermé et théorème de Riesz
- (ii) Théorème de Lax-Milgram et application
- (iii) Théorème de Riesz-Fischer

207 - Prolongement de fonctions. Exemples et applications.
- (i) Fonction Gamma
- (ii) Théorèmes d'Abel angulaire et taubérien faible

208 - Espaces vectoriels normés, applications linéaires continues. Exemples.
- (i) Projection sur un convexe fermé et théorème de Riesz
- (ii) Théorème de Lax-Milgram et application
- (iii) Théorème de Riesz-Fischer

209 - Approximation d'une fonction par des fonctions régulières. Exemples et applications.
- (i) Densité des polynômes orthogonaux
- (ii) Théorème de Weierstrass

213 - Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.
- (i) Densité des polynômes orthogonaux
- (ii) Projection sur un convexe fermé et théorème de Riesz
- (iii) Théorème de Lax-Milgram et application

214 - Théorème d'inversion locale. Théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.
- (i) Extrema liés
- (ii) Lemme de Morse

215 - Applications différentiables sur un ouvert de $\mathbb{R}^n$. Exemples et applications.
- (i) Extrema liés
- (ii) Lemme de Morse

219 - Extremums : existence, caractérisation, recherche. Exemples et applications.
- (i) Méthode de Newton
- (ii) Projection sur un convexe fermé et théorème de Riesz
- (iii) Algorithme de gradient à pas optimal
- (iv) Extrema liés

220 - Équations différentielles ordinaires. Exemples de résolution et d'études de solutions en dimension 1 et 2.
- (i) Équation de Bessel
- (ii) Équation de Hill-Mathieu

221 - Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.
- (i) Équation de Bessel
- (ii) Équation de Hill-Mathieu

222 - Exemples d'équations aux dérivées partielles linéaires.
- (i) Équation de la chaleur sur le cercle
- (ii) Théorème de Lax-Milgram et application

223 - Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.
- (i) Connexité des valeurs d'adhérence d'une suite
- (ii) Méthode de Newton

226 - Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.
- (i) Connexité des valeurs d'adhérence d'une suite
- (ii) Méthode de Newton
- (iii) Algorithme de gradient à pas optimal

228 - Continuité, dérivabilité, dérivation faible des fonctions fonctions réelles d'une variable réelle. Exemples et applications.
(i) Méthode de Newton
(ii) Théorème de Weierstrass

229 - Fonctions monotones. Fonctions convexes. Exemples et applications.
(i) Algorithme de gradient à pas optimal
(ii) Ellipsoïde de John-Loewner

230 - Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.
(i) Théorèmes d'Abel angulaire et taubérien faible
(ii) Nombres de Bell

233 - Analyse numérique matricielle. Résolution approchée de systèmes linéaires, recherche d'éléments propres, exemples.
(i) Algorithme de gradient à pas optimal
(ii) Méthode QR

234 - Fonctions et espaces de fonctions Lebesgue-intégrables.
(i) Densité des polynômes orthogonaux
(ii) Théorème de Riesz-Fischer

235 - Problèmes d'interversion de limites et d'intégrales.
(i) Fonction Gamma
(ii) Théorèmes d'Abel angulaire et taubérien faible

236 - Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.
(i) Calcul d'une intégrale par le théorème des résidus
(ii) Transformée de Fourier d'une gaussienne

239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.
(i) Densité des polynômes orthogonaux
(ii) Fonction Gamma

241 - Suites et séries de fonctions. Exemples et contre-exemples.
(i) Équation de la chaleur sur le cercle
(ii) Théorèmes d'Abel angulaire et taubérien faible

243 - Séries entières, propriétés de la somme. Exemples et applications.
(i) Théorèmes d'Abel angulaire et taubérien faible
(ii) Nombres de Bell

245 - Fonctions d'une variable complexe. Exemples et applications.
(i) Calcul d'une intégrale par le théorème des résidus
(ii) Fonction Gamma

246 - Séries de Fourier. Exemples et applications.
(i) Équation de la chaleur sur le cercle
(ii) Formule sommatoire de Poisson

250 - Transformation de Fourier. Applications.
(i) Densité des polynômes orthogonaux
(ii) Formule sommatoire de Poisson
(iii) Transformée de Fourier d'une gaussienne

253 - Utilisation de la notion de convexité en analyse.
(i) Projection sur un convexe fermé et théorème de Riesz
(ii) Algorithme de gradient à pas optimal

261 - Loi d'une variable aléatoire : caractérisations, exemples, applications.
(i) Loi des évènements rares de Poisson
(ii) Théorème central limite et intervalle de confiance

262 - Convergences d'une suite de variables aléatoires. Théorèmes limite. Exemples et applications.
(i) Loi des évènements rares de Poisson
(ii) Théorème central limite et intervalle de confiance

264 - Variables aléatoires discrètes. Exemples et applications.
(i) Loi des évènements rares de Poisson
(ii) Processus de Galton-Watson

265 - Exemples d'études et d'applications de fonctions usuelles et spéciales.
(i) Fonction Gamma
(ii) Théorème central limite et intervalle de confiance
(iii) Transformée de Fourier d'une gaussienne

266 - Illustration de la notion d'indépendance en probabilités.
(i) Loi des évènements rares de Poisson
(ii) Processus de Galton-Watson
(iii) Théorème central limite et intervalle de confiance

267 - Exemples d'utilisation de courbes en dimension 2 ou supérieure.
(i) Calcul d'une intégrale par le théorème des résidus
(ii) Transformée de Fourier d'une gaussienne

Liste des développements

Algorithme de gradient à pas optimal

Leçons concernées : 162 219 226 229 233 253

Rappelons que, pour $J : \mathbb{R} \to \mathbb{R}$ différentiable, l'algorithme du gradient à pas optimal est défini par la suite :

$$u_0 \in \mathbb{R}^n \quad \text{et} \quad \forall\, k \in \mathbb{N},\ u^{k+1} = u^k - \rho^k \nabla J(u^k) \quad \text{où} \quad J\left(u^k - \rho^k \nabla J(u^k)\right) = \inf_{\rho \in \mathbb{R}^n} J\left(u^k - \rho \nabla J(u^k)\right)$$

Théorème 1. *Si J est α-convexe et différentiable, et que ∇J est L-lipschitzienne, alors la méthode de gradient à pas optimal converge vers l'unique minimum de J.*

Démonstration.

Étape 1 : Montrons que le problème de minimisation est bien posé.

Commençons par noter que l'α-convexité de J assure l'existence d'un unique minimum global $u \in \mathbb{R}^n$, caractérisé par l'équation d'Euler $\nabla J(u) = 0$, le problème de minimisation est donc bien posé.

Étape 2 : Montrons que le problème de minimisation intermédiaire est bien posé.

On peut supposer que, pour tout $k \in \mathbb{N}$, $\nabla J(u^k) \neq 0$. En effet, si $\nabla J(u^k) = 0$ alors la suite est stationnaire, et donc convergente en un nombre fini d'itérations. On considère maintenant la fonction suivante, que l'on cherche à minimiser à chaque étape :

$$\varphi_k : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ \rho & \longmapsto & J(u^k - \rho \nabla J(u^k)) \end{array} \right.$$

Cette fonction est dérivable, et on a :

$$\varphi_k'(\rho) = -\left\langle \nabla J(u^k - \rho \nabla J(u^k)), \nabla J(u^k) \right\rangle$$

De plus, pour tous $\rho, \sigma \in \mathbb{R}$, on a :

$$\begin{aligned}
(\varphi_k'(\rho) - \varphi_k'(\sigma))(\rho - \sigma) &= \left\langle \nabla J(u^k - \sigma \nabla J(u^k)) - \nabla J(u^k - \rho \nabla J(u^k)), \nabla J(u^k) \right\rangle (\rho - \sigma) \\
&= \left\langle \nabla J(u^k - \sigma \nabla J(u^k)) - \nabla J(u^k - \rho \nabla J(u^k)), (u^k - \sigma \nabla J(u^k)) - (u^k - \rho \nabla J(u^k)) \right\rangle \\
&\geqslant \alpha \left\| (u^k - \sigma \nabla J(u^k)) - (u^k - \rho \nabla J(u^k)) \right\|^2 \\
&\geqslant \alpha |\rho - \sigma|^2 \left\| \nabla J(u^k) \right\|^2
\end{aligned}$$

Donc φ_k est $\alpha \left\| \nabla J(u^k) \right\|^2$-convexe, et le problème de minimisation intermédiaire admet une unique solution ρ^k caractérisée par l'équation d'Euler :

$$\varphi_k'(\rho) = -\left\langle \nabla J(u^k - \rho \nabla J(u^k)), \nabla J(u^k) \right\rangle = \left\langle \nabla J(u^{k+1}), \nabla J(u^k) \right\rangle = 0$$

En particulier, deux directions de descente successives $\nabla J(u^k)$ et $\nabla J(u^{k+1})$ son orthogonales.

Étape 3 : Montrons que la suite $(J(u^k))_{k \in \mathbb{N}}$ est convergente.

Par α-convexité de J, on a :

$$\begin{aligned}
J(u^k) &\geqslant J(u^{k+1}) + \left\langle \nabla J(u^{k+1}), u^k - u^{k+1} \right\rangle + \frac{\alpha}{2} \left\| u^k - u^{k+1} \right\|^2 \\
&\geqslant J(u^{k+1}) + \rho^k \left\langle \nabla J(u^{k+1}), \nabla J(u^k) \right\rangle + \frac{\alpha}{2} \left\| u^k - u^{k+1} \right\|^2 \\
&\geqslant J(u^{k+1}) + \frac{\alpha}{2} \left\| u^k - u^{k+1} \right\|^2
\end{aligned}$$

La suite $(J(u^k))_{k \in \mathbb{N}}$ est donc décroissante et minorée par $J(u)$ par définition : elle est convergente.

Étape 4 : Montrons que la suite $(u^k)_{k\in\mathbb{N}}$ converge vers u.

Comme la suite $(J(u^k))_{k\in\mathbb{N}}$ est convergente, $J(u^k) - J(u^{k+1})$ tend vers 0 quand k tends vers $+\infty$, et donc $u^k - u^{k+1}$ également par l'inégalité précédente. Par α-convexité de J, on a :

$$\begin{aligned}\alpha \left\|u^k - u\right\|^2 &\leqslant \left\langle \nabla J(u^k) - \nabla J(u), u^k - u\right\rangle \\ &= \left\langle \nabla J(u^k), u^k - u\right\rangle \\ &\leqslant \left\|\nabla J(u^k)\right\| \left\|u^k - u\right\|\end{aligned}$$

Ainsi $\alpha \left\|u^k - u\right\| \leqslant \left\|\nabla J(u^k)\right\|$. Pour montrer la convergence de $(u^k)_{k\in\mathbb{N}}$ vers u, il suffit donc de montrer celle de $(\nabla J(u^k))_{k\in\mathbb{N}}$ vers 0. Or, on a :

$$\begin{aligned}\left\|\nabla J(u^k)\right\|^2 &= \left\langle \nabla J(u^k), \nabla J(u^k)\right\rangle \\ &= \left\langle \nabla J(u^k) - \nabla J(u^{k+1}), \nabla J(u^k)\right\rangle \\ &\leqslant \left\|\nabla J(u^k) - \nabla J(u^{k+1})\right\| \left\|\nabla J(u^k)\right\| \\ &\leqslant L \left\|u^k - u^{k+1}\right\| \left\|\nabla J(u^k)\right\|\end{aligned}$$

Donc $\left\|\nabla J(u^k)\right\| \leqslant L \left\|u^k - u^{k+1}\right\|$, et $(\nabla J(u^k))_{k\in\mathbb{N}}$ tend vers 0 lorsque k tend vers $+\infty$. On en déduit alors que la suite $(u^k)_{k\in\mathbb{N}}$ converge vers u.

□

Références

[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

Calcul d'une intégrale par le théorème des résidus

Leçons concernées : 204 236 245 267

Lemme 1. *Soient $\alpha, \beta \in [0, 2\pi]$ et $a \in \mathbb{C}$. On pose $\gamma_{a,r} : t \mapsto a + re^{it}$ sur $[\alpha, \beta]$. Soit f holomorphe sur $B(a, R) \setminus \{a\}$ pour $R > 0$, tel que a soit un pôle simple de f. Alors :*

$$\lim_{r \to 0} \int_{\gamma_{a,r}} f(z)\, dz = (\beta - \alpha) i \operatorname{Res}(f, a)$$

Démonstration.

Posons $g : z \mapsto f(z) - \frac{\operatorname{Res}(f,a)}{z-a}$. Ainsi g est holomorphe en a, et il existe $\rho > 0$ et $M > 0$ tels que $|g| \leqslant M$ sur $B(a, \rho) \setminus \{a\}$. On obtient ainsi :

$$\left| \int_{\gamma_{a,r}} g(z)\, dz \right| \leqslant M(\beta - \alpha) r \qquad \text{et} \qquad \int_{\gamma_{a,r}} \frac{\operatorname{Res}(f,a)}{z-a}\, dz = \int_{\alpha}^{\beta} \operatorname{Res}(f,a) i\, dz = (\beta - \alpha) i \operatorname{Res}(f,a)$$

Le résultat vient alors par linéarité de l'intégrale. □

Théorème 2. *Soit $\alpha \in]-1, 1[$. Alors $I_\alpha = \displaystyle\int_0^{+\infty} \frac{x^\alpha \ln x}{x^2 - 1}\, dx = \frac{\pi^2}{4 \cos^2(\frac{\alpha\pi}{2})}$.*

Démonstration.

Étape 1 : Vérifions que I_α est bien définie.

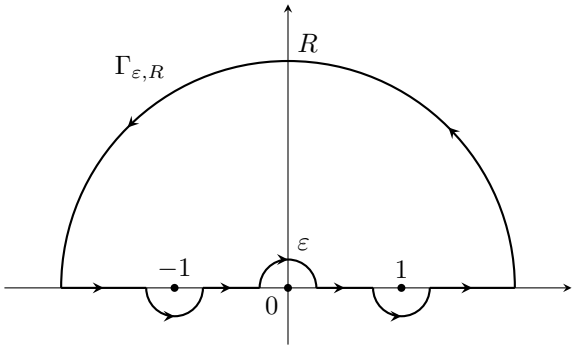
Puisque, pour tout $\varepsilon > 0$, on a $\ln x = \mathrm{o}\left(\frac{1}{x^\varepsilon}\right)$ en 0^+, et $\ln x = \mathrm{o}\left(x^\varepsilon\right)$ en $+\infty$, on a :

$$\frac{x^\alpha \ln x}{x^2 - 1} \underset{0^+}{\sim} x^\alpha \ln x = \mathrm{o}\left(\frac{1}{x^{\varepsilon - \alpha}}\right) \qquad \text{et} \qquad \frac{x^\alpha \ln x}{x^2 - 1} \underset{+\infty}{\sim} x^{\alpha - 2} \ln x = \mathrm{o}\left(\frac{1}{x^{2 - (\alpha + \varepsilon)}}\right)$$

Ainsi, en prenant $0 < \varepsilon < 1 - \alpha$, on a que la fonction est bien intégrable en 0 et en $+\infty$. De plus, en 1, on a $\ln x = \ln(1 + x - 1) \sim x - 1$, donc $\frac{x^\alpha \ln x}{x^2 - 1} \sim \frac{x^\alpha}{(x+1)} \sim \frac{1}{2}$. Ainsi, la fonction est continue en 1, donc sur $\mathbb{R}$.

Étape 2 : Cherchons à appliquer le théorème des résidus.

Considérons Log une détermination du logarithme complexe définie sur $U = \mathbb{C} \setminus i\mathbb{R}^-$ telle que $\operatorname{Log}(1) = 0$, et définissons $z^\alpha = \exp(\alpha \operatorname{Log}(z))$ pour $z \in U$. Posons également la fonction $f : U \to \mathbb{C}$ définie pour $z \in U$ par $f(z) = \frac{z^\alpha \operatorname{Log}(z)}{z^2 - 1}$. C'est une fonction méromorphe ayant pour pôles -1 et 1 qui sont au plus simples. Pour $\varepsilon > 0$ et $R > 0$, on peut donc considérer le chemin $\Gamma_{\varepsilon,R}$ suivant :



Étape 3 : Étude sur $\gamma_{0,r}$.

Soient $r > 0$ et $t \in [0, \pi]$. On a :

$$|\operatorname{Log}(re^{it})| = |\ln r + it| \leqslant |\ln r| + \pi \qquad \text{et} \qquad |(re^{it})^2 - 1| \geqslant \big||r^2 e^{2it}| - |-1|\big| = |r^2 - 1|$$

On obtient ainsi :

$$\left|\int_{\gamma_{0,r}} f(z)dz\right| = \left|\int_0^\pi ire^{it} f(re^{it})dt\right| \leqslant \int_0^\pi r\frac{|(re^{it})^\alpha||\operatorname{Log}(re^{it})|}{|(re^{it})^2 - 1|}dt \leqslant \int_0^\pi r\frac{r^\alpha(|\ln r| + \pi)}{|r^2-1|}dt = \frac{\pi r^{\alpha+1}(|\ln r| + \pi)}{|r^2-1|}$$

L'intégrale tend alors vers 0 en faisant tendre r vers 0 ou $+\infty$.

Étape 4 : Calculs des résidus de f en -1, 0 et 1.

On a :

$$\operatorname{Res}(f, -1) = \lim_{z\to -1}(z+1)\frac{z^\alpha \operatorname{Log}(z)}{z^2+1} = \lim_{z\to -1}\frac{z^\alpha \operatorname{Log}(z)}{z-1} = \frac{(-1)^\alpha \operatorname{Log}(-1)}{-2} = \frac{-i\pi}{2}e^{i\pi\alpha}$$

$$\operatorname{Res}(f, 1) = \lim_{z\to 1}(z-1)\frac{z^\alpha \operatorname{Log}(z)}{z^2+1} = \lim_{z\to 1}\frac{z^\alpha \operatorname{Log}(z)}{z+1} = 0$$

Étape 5 : Conclusion.

On a vu que les intégrales de f sur $\gamma_{0,R}$ et $\gamma_{0,\varepsilon}$ tendent vers 0 lorsque ε tend vers 0 et R tend vers $+\infty$. De plus, par le théorème des résidus et passage à la limite, on a :

$$\frac{\pi^2 e^{i\pi\alpha}}{2} + \int_{-\infty}^{+\infty}\frac{x^\alpha \ln x}{x^2-1}\,dx = \pi^2 e^{i\pi\alpha} \quad \text{donc} \quad \int_{-\infty}^{+\infty}\frac{x^\alpha \ln x}{x^2-1}\,dx = \frac{\pi^2}{2}e^{i\pi\alpha}$$

Or, on a par définition de Log :

$$\int_{-\infty}^0 \frac{x^\alpha \operatorname{Log}(x)}{x^2-1}\,dx = (-1)^\alpha \int_{-\infty}^0 \frac{|x|^\alpha \ln|x|}{x^2-1}\,dx + (-1)^\alpha i\pi \int_{-\infty}^0 \frac{|x|^\alpha}{x^2-1}\,dx = e^{i\pi\alpha} I_\alpha + e^{i\pi\alpha} i\pi \int_0^{+\infty}\frac{x^\alpha}{x^2-1}\,dx$$

Il vient alors que :

$$\int_{-\infty}^{+\infty}\frac{x^\alpha \ln x}{x^2-1}\,dx = e^{i\pi\alpha} I_\alpha + e^{i\pi\alpha} i\pi \int_0^{+\infty}\frac{x^\alpha}{x^2-1}\,dx + I_\alpha = \frac{\pi^2}{2}e^{i\pi\alpha}$$

On a donc :

$$\frac{1+e^{i\pi\alpha}}{e^{i\pi\alpha}} I_\alpha + i\pi\int_0^{+\infty}\frac{x^\alpha}{x^2-1}\,dx = (1+e^{-i\pi\alpha})I_\alpha + i\pi\int_0^{+\infty}\frac{x^\alpha}{x^2-1}\,dx = \frac{\pi^2}{2}$$

En prenant la partie réelle, on obtient finalement :

$$I_\alpha = \frac{\pi^2}{2}\frac{1}{\operatorname{Re}(1+e^{-i\pi\alpha})} = \frac{\pi^2}{2}\frac{1}{1+\cos(\pi\alpha)} = \frac{\pi^2}{4\cos^2(\frac{\pi}{2}\alpha)}$$

□

Références

[Tau06] P. Tauvel. *Analyse complexe pour la licence 3.* Dunod

Connexité des valeurs d'adhérence d'une suite

Leçons concernées : 203 204 223 226

Proposition 1. *Soit (E,d) un espace métrique compact et $(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de E telle que $\lim_{n\to+\infty} d(u_n,u_{n+1})=0$. Alors l'ensemble des valeurs d'adhérence de $(u_n)_{n\in\mathbb{N}}$ est connexe.*

Démonstration.

On note Γ l'ensemble des valeurs d'adhérence de $(u_n)_{n\in\mathbb{N}}$. Pour tout $p\in\mathbb{N}$, on note $A_p=\{u_n\,|\,n\geqslant p\}$. On sait que l'ensemble Γ est égal à l'intersection des $\overline{A_p}$. C'est donc un fermé, et comme E est compact, Γ est compact.

Supposons Γ non connexe, de sorte que l'on peut écrire $\Gamma=A\cup B$ où A et B sont deux fermés non vides disjoints de Γ. Comme Γ est compact, A et B sont même compacts et donc $\alpha=d(A,B)>0$ puisque A et B sont disjoints. On note alors :

$$A'=\left\{x\in E\,\middle|\,d(x,A)<\frac{\alpha}{3}\right\}\quad\text{et}\quad B'=\left\{x\in E\,\middle|\,d(x,B)<\frac{\alpha}{3}\right\}$$

Les ensembles A' et B' sont ouverts, donc $K=E\backslash(A'\cup B')$ est fermé dans le compact E, donc compact. Montrons que $(u_n)_{n\in\mathbb{N}}$ admet au moins une valeur d'adhérence dans K, ce qui sera une absurdité car $\Gamma\cap K=\varnothing$.

Par hypothèse, $\lim_{n\to+\infty} d(u_n,u_{n+1})=0$, donc il existe $N_0\in\mathbb{N}$ tel que, pour tout $n\geqslant N_0$, on a $d(u_n,u_{n+1})<\frac{\alpha}{3}$. Soient $N\geqslant N_0$, $x_0\in A$ et $y_0\in B$. Le point x_0 est dans A, donc dans Γ, ainsi x_0 est point d'adhérence de la suite $(u_n)_{n\in\mathbb{N}}$. Il existe alors $n_1\geqslant N$ tel que $d(x_0,u_{n_1})<\frac{\alpha}{3}$, donc $u_{n_1}\in A'$. De même, le point y_0 est dans B, donc dans Γ, ainsi y_0 est point d'adhérence de la suite $(u_n)_{n\in\mathbb{N}}$. Il existe alors $n_2>n_1$ tel que $d(y_0,u_{n_2})<\frac{\alpha}{3}$, donc $u_{n_2}\in B'$.

Notons maintenant n_0 le premier entier supérieur à n_1 tel que $u_{n_0}\notin A'$. En effet, un tel entier existe car $u_{n_2}\notin A'$. On a alors $u_{n_0-1}\in A'$, donc :

$$d(u_{n_0},B)\geqslant d(u_{n_0-1},B)-d(u_{n_0-1},u_{n_0})\geqslant d(A,B)-d(u_{n_0-1},A)-d(u_{n_0-1},u_{n_0})>\frac{\alpha}{3}$$

Cela prouve que $u_{n_0}\notin B'$. Comme de plus $u_{n_0}\notin A'$, on a $u_{n_0}\in K$.

Résumons. Nous venons de montrer que pour tout $N\geqslant N_0$ il existe $n_0\geqslant N$ tel que $u_{n_0}\in K$. On peut donc construire une sous-suite $(u_{\varphi(n)})_{n\in\mathbb{N}}$ de $(u_n)_{n\in\mathbb{N}}$ qui prend ses valeurs dans K. Comme K est compact, $(u_{\varphi(n)})_{n\in\mathbb{N}}$ admet au moins une valeur d'adhérence dans K, donc $(u_n)_{n\in\mathbb{N}}$ admet au moins une valeur d'adhérence dans K. Ceci est impossible, car $\Gamma\cap K=\varnothing$. L'ensemble Γ est donc connexe. □

Application 2. *Soient $f:[0,1]\to[0,1]$ une fonction continue et $(x_n)_{n\in\mathbb{N}}$ la suite définie par $x_0\in[0,1]$ et $x_{n+1}=f(x_n)$ pour tout $n\in\mathbb{N}$. Alors $(x_n)_{n\in\mathbb{N}}$ converge si, et seulement si, $\lim_{n\to+\infty} x_{n+1}-x_n=0$.*

Démonstration.

Bien évidemment, si $(x_n)_{n\in\mathbb{N}}$ converge vers ℓ, alors :

$$\lim_{n\to+\infty} x_{n+1}-x_n=\ell-\ell=0$$

Réciproquement, supposons que $\lim_{n\to\infty} x_{n+1}-x_n=0$. On note Γ l'ensemble des valeurs d'adhérence de $(x_n)_{n\in\mathbb{N}}$. Comme $[0,1]$ est compact, la proposition précédente donne que Γ est connexe : c'est un intervalle

fermé de $[0,1]$. Montrons qu'alors tout élément $\ell \in \Gamma$ est point fixe de f. Puisque ℓ est valeur d'adhérence, il existe une sous-suite $(x_{\varphi(n)})_{n\in\mathbb{N}}$ qui converge vers ℓ. Par continuité de f, et puisque $\lim_{n\to+\infty} x_{n+1} - x_n = 0$, on a :

$$\ell = \lim_{n\to+\infty} x_{\varphi(n)} = \lim_{n\to+\infty} (x_{\varphi(n)} - x_{\varphi(n)+1}) + x_{\varphi(n)+1} = \lim_{n\to+\infty} x_{\varphi(n)+1} = \lim_{n\to+\infty} f(x_{\varphi(n)}) = f(\ell)$$

Ainsi, si $(x_n)_{n\in\mathbb{N}}$ possède au moins deux valeurs d'adhérence $\ell < \ell'$, alors $[\ell, \ell'] \subset \Gamma$. En particulier, $\frac{\ell+\ell'}{2}$ est une valeur d'adhérence de $(x_n)_{n\in\mathbb{N}}$. Ainsi, il existe $n_0 \in \mathbb{N}$ tel que $x_{n_0} \in [\ell, \ell']$. Mais alors on a $x_n = x_{n_0}$ pour tout $n \geqslant n_0$, et $(x_n)_{n\in\mathbb{N}}$ converge, ce qui contredit l'hypothèse sur le nombre de valeurs d'adhérence. Ainsi, $(x_n)_{n\in\mathbb{N}}$ n'a qu'une valeur d'adhérence, donc converge. □

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses
[FGN13d] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 1.* Cassini

Critère d'Eisenstein

Leçons concernées : 122 141 142

On se place dans un anneau factoriel A, et on note $\mathbb{K} = \mathrm{Frac}(A)$.

Lemme 1. *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Démonstration.

Supposons d'abord P et Q primitifs. On suppose par l'absurde que PQ n'est pas primitif. Comme A est factoriel, il existe donc $p \in A$ irréductible qui divise $c(PQ)$. Ainsi (p) est un idéal premier, donc $A/(p)$ est intègre, et $A/(p)[X]$ aussi. Or $c(P) = c(Q) = 1$, donc $\overline{P}$ et $\overline{Q}$ ne sont pas nuls dans $A/(p)[X]$. Alors $\overline{PQ}$ n'est pas nul sur $A/(p)[X]$, et p ne divise pas PQ. Contradiction. Donc PQ est primitif.

Dans le cas général, on écrit $PQ = c(P)c(Q)\frac{P}{c(P)}\frac{Q}{c(Q)}$, où les polynômes $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ sont primitifs, et leur produit également. On obtient alors, en passant au contenu, que $c(PQ) = c(P)c(Q)$. □

Théorème 2. *Soit $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

Démonstration.

Supposons P primitif et irréductible dans $\mathbb{K}[X]$. Si $P = QR$ dans $A[X]$, c'est vrai aussi dans $\mathbb{K}[X]$. Quitte à échanger Q et R, comme P est irréductible dans $\mathbb{K}[X]$, on suppose que $Q \in \mathbb{K}[X]^\times$. On a alors $Q = a \in A \setminus \{0\}$. On en déduit que $P = aR$, donc $a \mid c(P)$. Mais $c(P) = 1$, donc $a \in A^\times$, et P est irréductible dans $A[X]$.

Réciproquement, supposons P irréductible dans $A[X]$. On a $c(P) = 1$, car sinon $P = pP'$ avec p un irréductible de A divisant $c(P)$. Écrivons $P = QR$ avec $Q, R \in \mathbb{K}[X]$. Soient $q, r \in A$ tels que $Q' = qQ, R' = rR \in A[X]$. Alors $qrP = Q'R'$, donc $qr = c(Q')c(R')$. On a donc $P = \frac{Q'}{q}\frac{R'}{r} = \frac{Q'}{c(Q')}\frac{R'}{c(R')}$ dans $A[X]$. Ainsi, un terme est de degré 0 par irréductibilité de P, et de même pour Q ou R. Donc P est irréductible dans $\mathbb{K}[X]$. □

Théorème 3 (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_k sauf a_n et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{K}[X]$.*

Démonstration.

Supposons P non irréductible dans $\mathbb{K}[X]$. Par le théorème précédent, P est non irréductible dans $A[X]$. Il existe alors $Q, R \in A[X]$ non constants tels que $P = QR$. Posons alors $Q(X) = \sum_{k=0}^{q} b_k X^k$ et $R(X) = \sum_{k=0}^{r} c_k X^k$ avec $b_k, c_k \in A$ et $0 < q, r < n$. Comme A est factoriel et p irréductible, l'idéal (p) est premier, donc $B = A/(p)$ est intègre. Projetons l'égalité $P = QR$ dans $B[X]$:

$$\overline{P}(X) = \overline{a_n} X^n = \left(\sum_{k=0}^{q} \overline{b_k} X^k\right)\left(\sum_{k=0}^{r} \overline{c_k} X^k\right) = \overline{Q}(X)\overline{R}(X)$$

En effet, comme $\overline{a_n} \neq 0$, on a $\overline{b_q} \neq 0 \neq \overline{c_r}$. Cette égalité est encore vraie dans $\mathbb{L}[X]$, où $\mathbb{L} = \mathrm{Frac}(B)$. Comme $\mathbb{L}[X]$ est principal et X irréductible, l'unicité de la décomposition en facteurs irréductibles dans $\mathbb{L}[X]$ montre que X divise $\overline{Q}$ et $\overline{R}$. Ainsi, $\overline{b_0} = \overline{c_0} = 0$ dans B, mais alors p^2 divise $b_0 c_0 = a_0$. Contradiction. □

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses

Décomposition de Dunford

Leçons concernées : 153 154 155 156 157
On se place dans un $\mathbb{K}$-espace vectoriel E, où $\mathbb{K}$ est un corps.

Proposition 1. *Soient $f \in \mathcal{L}(E)$ et $F \in \mathbb{K}[X]$ un polynôme annulateur de f. Soit $F = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ la décomposition en facteurs irréductibles dans $\mathbb{K}[X]$ du polynôme F. Pour tout i, on note $N_i = \operatorname{Ker} M_i^{\alpha_i}(f)$. Alors $E = \bigoplus_{i=1}^s N_i$, et, pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j\neq i} N_j$ est un polynôme en f.*

Démonstration.

Étape 1 : Premier point.

Le fait que $E = \bigoplus_{i=1}^s N_i$ résulte du théorème des noyaux.

Étape 2 : Mise en avant de projecteurs.

Pour tout i, notons $Q_i = \prod_{j\neq i} M_j^{\alpha_j}$. Aucun facteur n'est commun à tous les Q_i, c'est-à-dire que les Q_i sont premiers entre eux dans leur ensemble. En appliquant l'égalité de Bézout, on voit qu'il existe $U_1, \ldots, U_s \in \mathbb{K}[X]$ tels que $U_1Q_1 + \ldots + U_sQ_s = 1$, de sorte que :

$$Id_E = U_1(f) \circ Q_1(f) + \ldots + U_s(f) \circ Q_s(f)$$

Pour tout i, on note $P_i = U_iQ_i$ est $p_i = P_i(f)$. Par ce qui précède, on a :

$$Id_E = \sum_{i=1}^{s} p_i \tag{$\star$}$$

Par ailleurs, pour tout $j \neq i$, F divise Q_iQ_j, donc :

$$\forall j \neq i,\ p_i \circ p_j = Q_iQ_j(f) \circ U_iU_j(f) = 0 \tag{$\star\star$}$$

On déduit de ($\star$) que $p_i = \sum_{j=1}^s p_i \circ p_j$ pour tout i, donc $p_i = p_i^2$ d'après ($\star\star$). Les p_i sont donc des projecteurs.

Étape 3 : Montrons que, pour tout i, $\operatorname{Im} p_i = N_i$.

Soit $y = p_i(x) \in \operatorname{Im} p_i$. On a :

$$M_i^{\alpha_i}(f)(y) = M_i^{\alpha_i}(f) \circ P_i(f)(x) = U_i(f) \circ F(f)(x) = 0$$

Ainsi, $\operatorname{Im} p_i \subseteq \operatorname{Ker} M_i^{\alpha_i}(f) = N_i$. Il reste à montrer l'inclusion réciproque. Soit $x \in N_i = \operatorname{Ker} M_i^{\alpha_i}(f)$. D'après ($\star$), $x = p_1(x) + \ldots + p_s(x)$. Or, pour tout $j \neq i$, $p_j(x) = U_j(f) \circ Q_j(f)(x) = 0$, car $M_i^{\alpha_i}$ divise Q_j, donc finalement $x = p_i(x) \in \operatorname{Im} p_i = N_i$.

Étape 4 : Montrons que, pour tout i, $\operatorname{Ker} p_i = \bigoplus_{j\neq i} N_j$.

Pout tout $j \neq i$, on a $N_j \subseteq \operatorname{Ker} p_i$, car si $x \in N_j$, alors $p_i(x) = U_i(f) \circ Q_i(f)(x) = 0$ car $M_j^{\alpha_j}$ divise Q_i. On en déduit que $\bigoplus_{j\neq i} N_j \subseteq \operatorname{Ker} p_i$. Soit maintenant $x \in \operatorname{Ker} p_i$. D'après ($\star$), $x = \sum_{j\neq i} p_j(x)$ donc $x \in \bigoplus_{j\neq i} N_j$. Finalement, $\operatorname{Ker} p_i = \bigoplus_{j\neq i} N_j$. La démonstration est terminée puisque, par construction, les projecteurs p_i sont des polynômes en f.

□

Théorème 2 (Décomposition de Dunford)**.** *Soit $f \in \mathcal{L}(E)$ dont le polynôme caractéristique χ_f est scindé sur $\mathbb{K}$. Alors il existe un unique couple (n, d) d'endomorphismes tels que :*

(i) d est diagonalisable, n est nilpotent

(ii) $f = d + n$ et n et d commutent

De plus, d et n sont des polynômes en f

Démonstration.

Étape 1 : Existence

Écrivons $\chi_f = \prod_{i=1}^{s}(X - \lambda_i)^{\alpha_i}$ et notons $N_i = \mathrm{Ker}(f - \lambda_i)^{\alpha_i}$ pour tout i. La proposition précédente s'applique avec $F = \chi_f$ et $M_i = X - \lambda_i$ pour tout i. En utilisant les notations précédentes, pour tout i, $p_i = P_i(f)$ est le projecteur sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$. Posons $d = \sum_{i=1}^{s} \lambda_i p_i$ et $n = f - d$. Alors d est diagonalisable en tant que combinaison linéaire de projecteurs. De plus, comme les p_i sont des projecteurs tels que $p_i \circ p_j = 0$ si $j \neq i$, et que les p_i commutent avec f en tant que polynômes en f, on a :

$$\forall q \in \mathbb{N},\ n^q = \left(\sum_{i=1}^{s}(f - \lambda_i Id_E)p_i\right)^q = \sum_{i=1}^{s}(f - \lambda_i Id_E)^q p_i$$

Si $q = \sup_j \alpha_j$, alors χ_f divise $(X - \lambda)^q Q_i$, donc $n^q = \sum_{i=1}^{s}((X - \lambda_i)^q Q_i U_i)(f) = 0$ et n est nilpotent. Ainsi construits, d et n sont des polynômes en f vérifiant les propriétés voulues.

Étape 2 : Unicité

Soit (d', n') un autre couple vérifiant les propriétés voulues. Alors f, d, n , d' et n' commutent en tant que polynômes en f. Ainsi, d et d' sont diagonalisables dans une même base, ce qui entraîne que $d - d'$ est diagonalisable. De plus, comme $d - d' = n' - n$ est nilpotente, on en déduit que $d - d' = n - n' = 0$, d'où l'unicité.

□

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

Décomposition polaire

Leçons concernées : 106 150 158 160 161

Théorème 1 (Décomposition polaire)**.** *On a les homéomorphismes :*

$$\begin{array}{ccccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) & \quad \mathcal{U}_n(\mathbb{R}) \times H_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O,S) & \longmapsto & OS & (U,H) & \longmapsto & UH \end{array}$$

Démonstration.

On ne démontrera ici que le premier homéomorphisme, la démonstration du second étant similaire.
On note μ cette application. Elle est bien définie et elle est continue.

Étape 1 : Montrons que μ est surjective.

Soit $M \in \mathcal{GL}_n(\mathbb{R})$. La matrice ${}^tMM$ est symétrique. De plus $\langle X, {}^tMMX\rangle = \langle MX, MX\rangle = \|MX\|^2 \geqslant 0$, pour tout $X \in \mathbb{R}^n$. Et puisque $\langle X, {}^tMMX\rangle = 0 \Leftrightarrow MX = 0 \Leftrightarrow X = 0$ on a que ${}^tMM$ est dans $\mathcal{S}_n^{++}(\mathbb{R})$.

On peut ainsi diagonaliser ${}^tMM$ dans une base orthonormée. Il existe alors $P \in \mathcal{O}_n(\mathbb{R})$ et $D = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$ avec $\lambda_i > 0$ pour tout i tels que ${}^tMM = PDP^{-1}$. On pose $S = P\,\mathrm{Diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_n})P^{-1}$. C'est une matrice symétrique, puisque P est orthogonale, et définie positive, car ses valeurs propres sont strictement positives.

On a $S^2 = {}^tMM$ et, si l'on pose $O = MS^{-1}$, il vient que :

$${}^tOO = {}^tMS^{-1}MS^{-1} = {}^tS^{-1}\,{}^tMMS^{-1} = {}^tS^{-1}S^2S^{-1} = I_n$$

Ainsi $M = OS$, où $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$, donc μ est surjective.

Étape 2 : Montrons que μ est injective.

Supposons que l'on ait $M = OS = O'S'$, avec $O \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$. Il vient alors :

$$S^2 = {}^tMM = {}^t(O'S')O'S' = {}^tS'\,{}^tO'O'S' = S'^2$$

Soit Q un polynôme interpolateur tel que, pour tout $i \in [\![1, n]\!]$, $Q(\lambda_i) = \sqrt{\lambda_i}$. Alors :

$$S = PQ\left(\begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix}\right)P^{-1} = Q\left(P\begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix}P^{-1}\right) = Q(S^2) = Q(S'^2)$$

Or, S' commute avec S'^2, donc avec $Q(S'^2) = S$, et donc S' et S sont diagonalisables dans une base commune. Il existe ainsi une matrice de passage P_0 qui permet de les diagonaliser simultanément. On a alors $S' = P_0\,\mathrm{Diag}(\mu'_1, \dots, \mu'_n)P_0^{-1}$ et $S = P_0\,\mathrm{Diag}(\mu_1, \dots, \mu_n)P_0^{-1}$. Alors :

$$\begin{aligned} S'^2 = S^2 &\Longrightarrow P_0\,\mathrm{Diag}(\mu_1'^2, \dots, \mu_n'^2)P_0^{-1} = P_0\,\mathrm{Diag}(\mu_1^2, \dots, \mu_n^2)P_0^{-1} \\ &\Longrightarrow \forall\, i \in [\![1, n]\!],\ \mu_i'^2 = \mu_i^2 \\ &\Longrightarrow \forall\, i \in [\![1, n]\!],\ \mu'_i = \mu_i \\ &\Longrightarrow S' = S \end{aligned}$$

Ainsi, on a $S = S'$, puis $O = O'$, d'où l'injectivité de μ.

Étape 3 : Montrons que μ^{-1} est continue.

Soit $(M_p)_{p\in\mathbb{N}}$ une suite de $\mathcal{GL}_n(\mathbb{R})$ qui converge vers M. On note, pour tout $p \in \mathbb{N}$, $(O_p, S_p) = \mu^{-1}(M_p)$, de sorte que $M_p = O_pS_p$, avec $O_p \in \mathcal{O}_n(\mathbb{R})$ et $S_p \in \mathcal{S}_n^{++}(\mathbb{R})$. On va montrer que les suites $(O_p)_{p\in\mathbb{N}}$ et $(S_p)_{p\in\mathbb{N}}$ convergent respectivement vers O et S.

Comme $\mathcal{O}_n(\mathbb{R})$ est compact, soit $\overline{O}$ une valeur d'adhérence de $(O_p)_{p\in\mathbb{N}}$, et soit $(O_{p_k})_{k\in\mathbb{N}}$ une sous-suite de $(O_p)_{p\in\mathbb{N}}$ qui converge vers $\overline{O}$. Alors la sous-suite $(S_{p_k})_{k\in\mathbb{N}}$ converge vers $\overline{O}^{-1}M = \overline{S}$, et on a :

$$\overline{S} = \overline{O}^{-1}M \in \mathcal{GL}_n(\mathbb{R}) \cap \overline{\mathcal{S}_n^{++}(\mathbb{R})} = \mathcal{GL}_n(\mathbb{R}) \cap \mathcal{S}_n^{+}(\mathbb{R}) = \mathcal{S}_n^{++}(\mathbb{R})$$

On a donc $M = \overline{OS}$ par injectivité de μ, puis $\overline{O} = O$ et $\overline{S} = S$. D'où la continuité de μ^{-1}.

□

Corollaire 2. *Pour $A \in \mathcal{GL}_n(\mathbb{R})$, on a $\|A\|_2^2 = \rho({}^tAA)$.*

Démonstration.

Soit $A = OS$ la décomposition polaire de A. Comme $\|OSx\|_2 = \|Sx\|_2$ pour tout vecteur $x \in \mathbb{R}^n$, on a $\|A\|_2 = \|S\|_2$. Comme S est symétrique réelle, elle est diagonalisable dans une base orthonormée $(e_1, \dots, e_n)$, ordonnée de sorte que les valeurs propres correspondantes soient dans l'ordre décroissant en module.

Maintenant, si $x = \sum_{i=1}^n x_ie_i$ est de norme 1, on a :

$$\|Sx\|_2 = \left\|\sum_{i=1}^n \lambda_i x_i e_i\right\|_2 \leqslant |\lambda_1| \left\|\sum_{i=1}^n x_i e_i\right\|_2 = |\lambda_1| = \rho(S)$$

La borne étant atteinte pour $x = e_1$. On a ainsi montré que $\|S\|_2 = \rho(S)$, et on a ensuite :

$$\|A\|_2^2 = \|S\|_2^2 = \rho(S)^2 = |\lambda_1|^2 = \rho(S^2) = \rho({}^tAA)$$

□

Références

[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet

Densité des polynômes orthogonaux

Leçons concernées : 201 207 209 213 234 235 239 245 250

Pour $I \subset \mathbb{R}$ un intervalle, on appelle fonction poids toute $\rho : I \to \mathbb{R}$ mesurable strictement positive telle que :

$$\forall\, n \in \mathbb{N},\ \int_I |x|^n \rho(x)\, dx < +\infty$$

De plus, l'espace $L^2(I,\rho) = \left\{ f : I \to \mathbb{R} \,\middle|\, \int_I |f(x)|^2 \rho(x) dx < +\infty \right\}$ est de Hilbert pour le produit scalaire :

$$\forall\, f, g \in L^2(I,\rho),\quad \langle f, g \rangle_\rho = \int_I f(x) g(x) \rho(x)\, dx$$

Théorème 1. *Soit ρ une fonction poids. On suppose qu'il existe $a > 0$ tel que $\int_I e^{a|x|} \rho(x) dx < \infty$. Alors les polynômes orthogonaux associés à ρ forment une base hilbertienne de $L^2(I,\rho)$.*

Démonstration.

Étape 1 : Montrons l'existence d'une famille de polynômes orthogonaux.

Remarquons que, comme $(x \mapsto x^n) \in L^1(I,\rho)$ pour tout $n \in \mathbb{N}$, alors :

$$\|x^n\|_2^2 = \int_I |x^n|^2 \rho(x)\, dx = \int_I |x^{2n}| \rho(x)\, dx = \left\|x^{2n}\right\|_1 < +\infty$$

Les polynômes appartiennent donc à $L^2(I,\rho)$, et nous pouvons bien appliquer l'algorithme de Gram-Schmidt pour avoir une famille de polynômes $(P_n)_{n\in\mathbb{N}}$ de degrés échelonné et orthogonaux dans $L^2(I,\rho)$.

Étape 2 : Introduisons une fonction auxiliaire.

On pose, pour tout $n \in \mathbb{N}$, $g_n : x \mapsto x^n$. Soit $f \in L^2(I,\rho)$ telle que, pour tout $n \in \mathbb{N}$, $\langle f, g_n \rangle_\rho = 0$. Soit $\varphi = f\rho \mathbb{1}_I$. Alors, par l'inégalité de Cauchy-Schwarz :

$$\int_{\mathbb{R}} |\varphi(t)|\, dt = \int_I |f(t)| \rho(t)\, dt \leqslant \left(\int_I |f(t)|^2 \rho(t)\, dt \right)^{\frac{1}{2}} \left(\int_I \rho(t)\, dt \right)^{\frac{1}{2}} = \|f\|_\rho \, \|1\|_\rho < +\infty$$

Donc $\varphi \in L^1(\mathbb{R})$, et on peut alors considérer sa transformée de Fourier :

$$\forall\, t \in \mathbb{R},\ \widehat{\varphi}(t) = \int_{\mathbb{R}} e^{-itx} \varphi(x)\, dx = \int_I e^{-itx} f(x) \rho(x)\, dx$$

Étape 3 : Montrons que $\widehat{\varphi}$ se prolonge en une fonction holomorphe.

On considère $B_\alpha = \left\{ z \in \mathbb{C} \,\middle|\, |\operatorname{Im}(z)| < \frac{\alpha}{2} \right\}$, où $\alpha > 0$. Pour $x \in I$ et tout $z \in B_\alpha$, on pose $g(z,x) = e^{-itx} f(x) \rho(x)$ et $F(z) = \int_I g(z,x)\, dx$, alors :

(i) Pour tout $z \in B_\alpha$, $x \mapsto g(z,x)$ est mesurable.

(ii) Pour presque tout $x \in I$, $z \mapsto g(z,x)$ est holomorphe sur B_α.

(iii) Pour tout $z \in B_\alpha$, $|g(z,x)| = e^{\operatorname{Im}(z)x} |f(x)| \rho(x) \leqslant e^{\frac{\alpha}{2}x} |f(x)| \rho(x)$. L'inégalité de Cauchy-Schwarz donne :

$$\int_I e^{\frac{\alpha}{2}x} |f(x)| \rho(x)\, dx \leqslant \left(\int_I e^{\alpha x} \rho(x)\, dx \right)^{\frac{1}{2}} \left(\int_I |f(x)|^2 \rho(x)\, dx \right)^{\frac{1}{2}} < +\infty$$

$|g(z,x)|$ est donc bien dominée par une fonction indépendante de z et intégrable sur I.

Par le théorème d'holomorphie sous le signe intégrale, F est bien définie et holomorphe sur B_α, et coïncide avec $\widehat{\varphi}$ sur $\mathbb{R}$. De plus, on a également :

$$F^{(n)}(z) = \int_I \frac{\partial^n}{\partial z^n} g(z,x)\, dx = (-i)^n \int_I x^n e^{-ixz} f(x) \rho(x)\, dx$$

Étape 4 : Conclusion.

Évaluons en 0 :

$$F^{(n)}(0) = (-i)^n \int_I x^n f(x)\rho(x)\,dx = (-i)^n \langle f, g_n \rangle_\rho = 0$$

Tous les coefficients du développement en série entière de F au voisinage de 0 sont donc nuls. Par unicité du développement en série entière, F est nulle sur un voisinage de 0.

Le théorème du prolongement analytique implique alors que $F = 0$ sur le connexe B_α tout entier, et en particulier sur $\mathbb{R}$. Donc, pour tout $t \in \mathbb{R}$, $\widehat{\varphi}(t) = 0$.

Or $\varphi \in L^1(\mathbb{R})$, donc, par injectivité de la transformée de Fourier sur $L^1(\mathbb{R})$, on en déduit que $\varphi = f\rho\mathbb{1}_I = 0$. Comme, sur I, on a $\rho > 0$ et $\mathbb{1}_I = 1 > 0$, il vient que $f = 0$.

On a donc finalement que $\mathrm{Vect}((P_n)_n)^\perp = \mathrm{Vect}((X^n)_n)^\perp = \{0\}$, et donc que les polynômes orthogonaux forment bien une base hilbertienne de $L^2(I, \rho)$.

□

Références

[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K

Déterminant de Gram et inégalité de Hadamard

Leçons concernées : 152 161 191

Soient $(E, \langle .,. \rangle)$ un espace pré-hilbertien (réel ou complexe) et $(x_i)_{1\leqslant i\leqslant n}$ une famille de vecteurs de E. On appelle matrice de Gram de $(x_i)_{1\leqslant i\leqslant n}$ la matrice $M_G(x_1,\dots,x_n) = (\langle x_i, x_j\rangle)_{1\leqslant i,j\leqslant n}$, et déterminant de Gram le déterminant de cette matrice, noté $G(x_1,\dots,x_n)$.

Lemme 1. *Le déterminant de Gram d'une famille de vecteurs est nul si, et seulement si, elle est liée.*

Démonstration.

Soit $(e_i)_{1\leqslant i\leqslant n}$ une famille de vecteurs de E. Si $(e_i)_{1\leqslant i\leqslant n}$ est liée, son déterminant de Gram est nul, par linéarité du produit scalaire. Réciproquement, si le déterminant de Gram de $(e_i)_{1\leqslant i\leqslant n}$ est nul, les vecteurs colonnes des produits scalaires sont liés, donc il existe $k \in [\![1,n]\!]$ et $(\lambda_\ell)_{\ell\neq k}$ des coefficients non tous nuls tels que :

$$\forall\, i \in [\![1,n]\!],\ \langle e_i, e_k\rangle = \sum_{\ell\neq k} \lambda_\ell \langle e_i, e_\ell\rangle = \left\langle e_i, \sum_{\ell\neq k} \overline{\lambda_\ell} e_\ell \right\rangle \quad \Rightarrow \quad e_k - \sum_{\ell\neq k} \overline{\lambda_\ell} e_\ell \in \mathrm{Vect}(e_1,\dots,e_n)^\perp$$

Or $e_k - \sum_{\ell\neq k} \overline{\lambda_\ell} e_\ell \in \mathrm{Vect}(e_1,\dots,e_n)$, donc $e_k = \sum_{\ell\neq k} \overline{\lambda_\ell} e_\ell$, et $(e_i)_{1\leqslant i\leqslant n}$ est liée. □

Théorème 2. *Soit F un sous-espace vectoriel de E de dimension finie $n \in \mathbb{N}^\star$ muni d'une base $(e_i)_{1\leqslant i\leqslant n}$. Alors, pour tout $x \in E$, on a :*

$$d(x,F)^2 = \frac{G(e_1,\dots,e_n,x)}{G(e_1,\dots,e_n)}$$

Démonstration.

Comme F est de dimension finie, $d(x,F)$ est atteint en la projection $f \in F$ de x.
On a ainsi $d(x,F) = \|x-f\|$, et, par définition de f :

$$\forall\, i \in [\![1,n]\!],\ \langle x, e_i\rangle = \langle f, e_i\rangle \quad \text{et} \quad \|x\|^2 = \|f\|^2 + \|x-f\|^2$$

Calculons la matrice de Gram de $(e_1,\dots,e_n,x)$:

$$M_G(e_1,\dots,e_n,x) = \left(\begin{array}{ccc|c} & M_G(e_1,\dots,e_n) & & \begin{matrix}\langle e_1,x\rangle\\ \vdots \\ \langle e_n,x\rangle\end{matrix} \\ \hline \langle x,e_1\rangle & \cdots & \langle x,e_n\rangle & \|x\|^2 \end{array}\right)$$

On peut alors calculer le déterminant de Gram G de $(e_1,\dots,e_n,x)$:

$$G = \left|\begin{array}{ccc|c} & M_G(e_1,\dots,e_n) & & \begin{matrix}\langle e_1,f\rangle\\ \vdots \\ \langle e_n,f\rangle\end{matrix} \\ \hline \langle f,e_1\rangle & \cdots & \langle f,e_n\rangle & \|f\|^2 \end{array}\right| + \left|\begin{array}{ccc|c} & M_G(e_1,\dots,e_n) & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline \langle f,e_1\rangle & \cdots & \langle f,e_n\rangle & \|x-f\|^2 \end{array}\right|$$
$$= G(e_1,\dots,e_n,f) + \|x-f\|^2\, G(e_1,\dots,e_n) = d(x,F)^2 G(e_1,\dots,e_n)$$

Comme la famille $(e_i)_{1\leqslant i\leqslant n}$ est libre, son déterminant de Gram est non nul, et on a bien :

$$d(x,F)^2 = \frac{G(e_1,\dots,e_n,x)}{G(e_1,\dots,e_n)}$$

□

Théorème 3 (Hadamard). *(i) Soient $x_1, \dots, x_n \in E$. Alors $G(x_1, \dots, x_n) \leqslant \prod_{i=1}^n \|x_i\|^2$.*
(ii) Soient $x_1, \dots, x_n \in \mathbb{C}^n$. Alors $|\det(x_1, \dots, x_n)| \leqslant \prod_{i=1}^n \|x_i\|_2$.
Dans les deux cas, on a égalité si, et seulement si, $(x_i)_{1 \leqslant i \leqslant n}$ est orthogonale ou l'un des vecteurs est nul.

Démonstration.

(i) Si la famille $(x_1, \dots, x_n)$ est liée, alors $G(x_1, \dots, x_n) = 0$, et l'inégalité sont évidentes.
On va montrer par récurrence sur $n \in \mathbb{N}^\star$ qu'une famille de n vecteurs libres de E vérifie l'inégalité, avec égalité si, et seulement si, ils sont orthogonaux.

Si $n = 1$, on a $G(x_1) = \|x_1\|^2$. Supposons la propriété vraie au rang n. Soient $x_1, \dots, x_{n+1}$ des vecteurs libres de E. Notons $F = \mathrm{Vect}(x_1, \dots, x_n)$, et considérons f la projection orthogonale de x_{n+1} sur F. En remarquant que $\|x_{n+1} - f\|^2 \leqslant \|x_{n+1} - f\|^2 + \|f\|^2 = \|x_{n+1}\|^2$, on obtient par hypothèse de récurrence :

$$G(x_1, \dots, x_{n+1}) = G(x_1, \dots, x_n) \|x_{n+1} - f\|^2 \leqslant \prod_{i=1}^n \|x_i\|^2 \times \|x_{n+1} - f\|^2 \leqslant \prod_{i=1}^n \|x_i\|^2 \times \|x_{n+1}\|^2$$

La première inégalité est une égalité si, et seulement si, la famille $(x_1, \dots, x_n)$ est orthogonale. De plus, la deuxième inégalité est une égalité si, et seulement si, $\|x_{n+1} - f\|^2 = \|x_{n+1}\|^2$, c'est-à-dire $\|f\|^2 = 0$ donc x_{n+1} est orthogonal aux $(x_1, \dots, x_n)$. On a donc montré l'hypothèse de récurrence au rang $n+1$, d'où le résultat par récurrence.

(ii) Notons que $M_G(x_1, \dots, x_n) = N^\star N$, où N est la matrice de vecteurs colonnes des $(x_1, \dots, x_n)$. On applique alors le point précédent avec $G(x_1, \dots, x_n) = |\det N|^2$.

□

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

Différentiabilité de l'exponentielle de matrices

Leçons concernées : 156 215 220 221

Théorème 1. *Pour $X, H \in \mathcal{M}_n(\mathbb{K})$, $d_X \exp(H) = e^X \sum_{k=0}^{\infty} \frac{(-ad\,X)^k}{(k+1)!} H$, où $ad\,X(H) = XH - HX$.*

Démonstration.

Soient $X, H \in \mathcal{M}_n(\mathbb{K})$.

(i) Tout d'abord, résolvons les deux problèmes de Cauchy suivant, pour $A \in \mathcal{L}(\mathcal{M}_n(\mathbb{K}))$:

$$S_1 : \begin{cases} f'(t) &= Af(t) \\ f(0) &= H \end{cases} \qquad \text{et} \qquad S_2 : \begin{cases} g'(t) &= e^{tA}H \\ g(0) &= 0 \end{cases}$$

Le premier système entraîne :

$$(e^{-tA}f(t))' = e^{-tA}f'(t) - e^{-tA}Af(t) = 0$$

Donc $e^{-tA}f(t) = e^0 f(0) = H$, puis $f(t) = e^{tA}H$. La réciproque est immédiate.

Maintenant, pour obtenir g, on doit intégrer terme à terme la série de l'exponentielle, d'où :

$$g(t) = \left(\sum_{k=0}^{\infty} \frac{t^{k+1}A^k}{(k+1)!} \right) H$$

En effet, les fonctions des deux membres ont même dérivée et s'annulent toutes deux en 0.

(ii) On pose ici $ad\,X(H) = XH - HX$, et $f(t) = e^{tX}He^{-tX}$.
Alors $f'(t) = Xe^{tX}He^{-tX} - e^{tX}He^{-tX}X = ad\,X(f(t))$ et $f(0) = H$, donc $f(t) = e^{t\,ad\,X}H$.
Pour $t = 1$, on obtient $e^X He^{-X} = e^{ad\,X}H$.

(iii) Soit maintenant la fonction $g : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ t & \longmapsto & \partial_{u=0}\left(e^{-tX}e^{t(X+uH)}\right) \end{array} \right.$, où u est une variable réelle.
On remarque que $g(0) = \partial_{u=0}(e^0 e^0) = 0$.
De plus, comme exp est de classe $\mathscr{C}^\infty$, alors il en est de même pour :

$$\varphi : \left| \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ (t,u) & \longmapsto & e^{-tX}e^{t(X+uH)} \end{array} \right.$$

Par le théorème de Schwarz, on peut donc permuter les dérivées secondes, d'où :

$$\begin{aligned} g'(t) &= \partial_t \partial_{u=0}\left(e^{-tX}e^{t(X+uH)}\right) \\ &= \partial_{u=0}\partial_t\left(e^{-tX}e^{t(X+uH)}\right) \\ &= \partial_{u=0}\left(-e^{-tX}Xe^{t(X+uH)} + e^{-tX}(X+uH)e^{t(X+uH)}\right) \\ &= \partial_{u=0}\left(ue^{-tX}He^{t(x+uH)}\right) \\ &= e^{-tX}He^{tX} \\ &= e^{-t\,ad\,X}H \end{aligned}$$

(iv) On sait que $g(0) = 0$ et que $g'(t) = e^{-t\,ad\,X}H$, alors :

$$g(t) = \partial_{u=0}\left(e^{-tX}e^{t(X+uH)}\right) = \left(\sum_{k=0}^{\infty}\frac{t^{k+1}(-ad\,X)^k}{(k+1)!}\right)H$$

En prenant $t = 1$, on obtient :

$$g(1) = \partial_{u=0}\left(e^{-X}e^{X+uH}\right) = \left(\sum_{k=0}^{\infty}\frac{(-ad\,X)^k}{(k+1)!}\right)H$$

Mais comme exp est différentiable en X, on a par ailleurs :

$$\partial_{u=0}\left(e^{-X}e^{X+uH}\right) = e^{-X}d_X\exp(H)$$

Finalement :

$$d_X\exp(H) = e^X\sum_{k=0}^{\infty}\frac{(-ad\,X)^k}{(k+1)!}H$$

□

Références

[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

Différentielle du déterminant

Leçons concernées : 152 215

Lemme 1. *Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $\mathcal{GL}_n(\mathbb{K})$ est un ouvert dense dans $\mathcal{M}_n(\mathbb{R})$.*

Démonstration.

Montrons que $\mathcal{GL}_n(\mathbb{R})$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.

$$\mathcal{GL}_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \,|\, \det M \neq 0\} = \overset{-1}{\det}(\mathbb{R}*)$$

Comme det est continue, $\mathcal{GL}_n(\mathbb{K})$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.

Soit $M \in \mathcal{M}_n(\mathbb{K})$, et $\lambda_1, \dots, \lambda_n$ ses valeurs propres (complexes).
Soit $(\varepsilon_k)_k$ une suite de complexes qui converge vers 0.
Il existe $N \in \mathbb{N}$ tel que pour tout $k \geqslant N$, $|\varepsilon_k| < \min(|\lambda_1|, \dots, |\lambda_n|)$.
Alors, pour tout $k \geqslant N$, on a :

$$\det(M + \varepsilon_k I_n) = \prod_{i=1}^{n} (\lambda_i + \varepsilon_k) \neq 0$$

Les matrices $X_k = M + \varepsilon_k I_n$ sont inversibles et convergent vers M, d'où la densité. □

Théorème 2. *La fonction* $\det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ *est de classe* $\mathscr{C}^1$ *et de différentielle* $d_X \det(H) = \operatorname{tr}({}^{\mathrm{t}}\mathrm{Com}(X)H)$.

Démonstration.

La fonction det est une fonction polynomiale en les coefficients de la matrice, donc elle est de classe $\mathscr{C}^1$.
On munit $\mathcal{M}_n(\mathbb{R})$ d'une norme.

Soit H une matrice, et $\lambda_1, \dots, \lambda_n$ ses valeurs propres. On a, pour $t \in \mathbb{R}$:

$$\det(I_n + tH) = \prod_{i=1}^{n} (1 + t\lambda_i) = 1 + t \operatorname{tr} H + \mathcal{O}(t^2)$$

Alors on a $d_{I_n} \det(H) = \operatorname{tr} H$.

Soient $X \in \mathcal{GL}_n(\mathbb{R})$ et $H \in \mathcal{M}_n(\mathbb{R})$. Alors :

$$\begin{aligned} \det(X + H) &= \det(X) \det(I_n + X^{-1}H) = \det(X) \left(1 + \operatorname{tr}(X^{-1}H) + o(\|H\|\,)\right) \\ &= \det(X) + \operatorname{tr}({}^{\mathrm{t}}\mathrm{Com}(X)H) + o(\|H\|\,) \end{aligned}$$

Donc $d_X \det(H) = \operatorname{tr}({}^{\mathrm{t}}\mathrm{Com}(X)H)$.

Les fonctions $X \mapsto d_X \det$ et $X \mapsto (H \mapsto \operatorname{tr}({}^{\mathrm{t}}\mathrm{Com}(X)H)$ coïncident sur $\mathcal{GL}_n(\mathbb{K})$ qui est un ouvert dense de $\mathcal{M}_n(\mathbb{K})$. On en conclut que pour tout $X, H \in \mathcal{M}_n(\mathbb{R})$, on a $d_X \det(H) = \operatorname{tr}({}^{\mathrm{t}}\mathrm{Com}(X)H)$. □

Application 3. *Pour $A \in \mathcal{M}_n(\mathbb{R})$, $\det(e^A) = e^{\operatorname{tr} A}$*

Démonstration.

Soient $y_1, \dots, y_n$ les solutions du système différentiel $y'(t) = A(t)y(t)$, où $A(t) \in \mathcal{M}_n(\mathbb{R})$ est une fonction continue et soit $w(t) = \det(y_1(t), \dots, y_n(t))$ leur wronskien.

Soit Y la matrice colonne de $(y_1, \dots, y_n)$, ainsi $Y' = AY$.

$$\begin{aligned} w'(t) &= d_{Y(t)} \det(Y'(t)) = \operatorname{tr}({}^{\mathrm{t}}\mathrm{Com}(Y(t))Y'(t)) = \operatorname{tr}({}^{\mathrm{t}}\mathrm{Com}(Y(t))A(t)Y(t)) \\ &= \operatorname{tr}(A(t)Y(t)\,{}^{\mathrm{t}}\mathrm{Com}(Y(t))) = \operatorname{tr}(A(t)\det(Y(t))) = \operatorname{tr}(A(t))w(t) \end{aligned}$$

On obtient donc $w'(t) = \operatorname{tr}(A(t))w(t)$ et, par conséquent :

$$w(t) = w(0)\exp\left(\int_0^t \operatorname{tr}(A(s))ds\right)$$

Si de plus, A est constant, alors, revenant au système initial, on a $Y'(t) = AY(t)$, donc $Y(t) = Y(0)e^{tA}$. On applique le déterminant à cette égalité et on obtient $w(t) = w(0)\det(e^{tA})$. Utilisons maintenant le résultat dans le cas où A n'est pas constant, on obtient alors $w(t) = w(0)e^{t\operatorname{tr}(A)}$. Ainsi, on obtient le résultat. □

Références

[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

Ellipsoïde de John-Loewner

Leçons concernées : 152 158 170 171 181 203 219 229 253

Lemme 1. *Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ symétriques définies positives distinctes, et $\alpha, \beta > 0$ tels que $\alpha + \beta = 1$, alors :*

$$\det(\alpha A + \beta B) > \det(A)^\alpha \det(B)^\beta$$

Démonstration.

On utilise le théorème de pseudo-réduction simultanée :
Il existe $P \in \mathcal{GL}_n(\mathbb{R})$ tel que $A = {}^tPP$ et $B = {}^tPDP$, avec $D = Diag(\lambda_1, \dots, \lambda_n)$, alors :

$$(\det A)^\alpha (\det B)^\beta = (\det P^2)^\alpha (\det P^2 \det D)^\beta = \det P^2 (\det D)^\beta$$

$$\det(\alpha A + \beta B) = \det({}^tP(\alpha I_n + \beta D)P) = \det P^2 \det(\alpha I_n + \beta D)$$

On est donc ramenés à montrer que $\det(\alpha I_n + \beta D) > (\det D)^\beta$. Par la stricte concavité du logarithme, on a :

$$\ln(\alpha + \beta\lambda_i) > \alpha \ln 1 + \beta \ln \lambda_i = \beta \ln \lambda_i \quad \Rightarrow \quad \sum_{i=1}^n \ln(\alpha + \beta\lambda_i) > \beta \sum_{i=1}^n \ln \lambda_i$$

En prenant l'exponentielle, on obtient :

$$\prod_{i=1}^n (\alpha + \beta\lambda_i) > \left(\prod_{i=1}^n \lambda_i \right)^\beta \quad \Leftrightarrow \quad \det(\alpha I_n + \beta D) > (\det D)^\beta$$

□

Théorème 2. *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe un unique ellipsoïde de centre 0 et de volume minimal contenant K.*

Démonstration.

On munit $\mathbb{R}^n$ de sa structure euclidienne usuelle. Un ellipsoïde $\mathbb{R}^n$ centré en 0 de a une équation du type $q(x) \leqslant 1$, où $q \in Q^{++}$. On note $\mathcal{E}_q = \{x \in \mathbb{R}^n \,|\, q(x) \leqslant 1\}$. Il existe une base $\mathcal{B}$ dans laquelle q s'écrit $q(x) = \sum_{i=1}^n a_i x_i^2$.

Étape 1 : Reformulons le problème comme un problème d'optimisation avec contrainte.

On note V_q le volume de $\mathcal{E}_q$, alors :

$$V_q = \int \int \cdots \int_{q(x) \leqslant 1} dx_1 \cdot dx_n$$

On effectue le changement de variable $x_i = \frac{t_i}{\sqrt{a_i}}$ de jacobien $\frac{1}{\sqrt{a_1 \dots a_n}}$. En notant $D(q) = a_1 \dots a_n$, qui est aussi le déterminant de la matrice de q, on obtient alors :

$$V_q = \int \int \cdots \int_{\|x\| \leqslant 1} \frac{dx_1 \dots dx_n}{\sqrt{D(q)}} = \frac{V_0}{\sqrt{D(q)}}$$

où V_0 est le volume de la boule unité pour la norme euclidienne canonique.

Le problème se reformule alors comme un problème d'optimisation avec contrainte. On cherche q qui maximise $D(q)$ et tel que $q(x) \leqslant 1$ pour tout $x \in K$. On munit Q de la norme $N(q) = \sup_{\|x\| \leqslant 1} |q(x)|$, et on considère l'ensemble $\mathcal{A} = \{q \in Q^+ \,|\, \forall x \in K, q(x) \leqslant 1\}$. Montrons que $\mathcal{A}$ est un compact convexe non vide de Q.

Étape 2 : Montrons que K est convexe.

Soit q et q' dans $\mathcal{A}$, et soit $\lambda \in [0,1]$.

$$q_\lambda = \lambda q + (1-\lambda)q'$$

Alors on a bien $q_\lambda(x) \geqslant 0$ pour tout $x \in \mathbb{R}^n$, et $q_\lambda(x) \leqslant 1$ pour tout $x \in K$. Donc $\mathcal{A}$ est convexe.

Étape 3 : Montrons que K est fermé.

Soit $(q_n)_n$ une suite de $\mathcal{A}$ convergente dans Q vers q. On a pour tout $x \in \mathbb{R}^n$, $|q(x) - q_n(x)| \leqslant N(q-q_n)\|x\|$, donc $\lim_{n\to+\infty} q_n(x) = q(x)$. On en déduit que :

$$\forall\, x \in \mathbb{R}^n,\ q(x) = \lim_{n\to+\infty} q_n(x) \geqslant 0 \qquad \text{et} \qquad \forall\, x \in K,\ q(x) = \lim_{n\to+\infty} q_n(x) \leqslant 1$$

Donc $q \in \mathcal{A}$, et $\mathcal{A}$ est fermé.

Étape 4 : Montrons que K est borné et non vide.

Soient a dans l'intérieur de K et $r > 0$ tel que $B(a,r) \subset K$. Si $\|x\| \leqslant r$, alors $a + x \in K$, donc on a :

$$\sqrt{q(x)} = \sqrt{q(x+a-a)} \leqslant \sqrt{q(x+a)} + \sqrt{q(-a)} \leqslant 2$$

Donc $q(x) \leqslant 4$. Si $\|x\| \leqslant 1$, $|q(x)| = q(x) = \frac{q(rx)}{r^2} \leqslant \frac{4}{r^2}$, ainsi $N(q) \leqslant \frac{4}{r^2}$, et $\mathcal{A}$ est borné.

De plus, K étant borné, il existe $M > 0$ tel que pour $x \in K$, $\|x\| \leqslant M$. Donc $x \mapsto \frac{\|x\|^2}{M^2}$ est dans $\mathcal{A}$.

Étape 6 : Existence.

Comme det est continue, D est continue sur $\mathcal{A}$. On en déduit que D atteint sont maximum sur $\mathcal{A}$ en q_0. De plus, comme $x \mapsto \frac{\|x\|^2}{M^2}$ est dans $\mathcal{A}$ et est de déterminant strictement positif, on a $D(q_0) > 0$, donc $q_0 \in Q^{++}$.

Étape 7 : Unicité.

Soit $q \in \mathcal{A}$. Par l'absurde, on suppose que $D(q) = D(q_0)$ avec $q \neq q_0$. Soient S et S_0 les matrices de q et q_0.

$$D\left(\frac{1}{2}(q+q_0)\right) = \det\left(\frac{1}{2}(S+S_0)\right) > (\det S)^{\frac{1}{2}}(\det S_0)^{\frac{1}{2}} \geqslant \det S_0 = D(q_0)$$

Cela contredit la maximalité de $D(q_0)$, puisque $\frac{1}{2}(q+q_0) \in \mathcal{A}$ par convexité.

□

Références

[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3.* Cassini

Équation de Bessel

Leçons concernées : 220 221 243

Théorème 1. *On considère l'équation différentielle de Bessel $xy'' + y' + xy = 0$. Sa solution f_0 valant 1 en 0 se développe en série entière sur $\mathbb{R}$. De plus, si f est une autre solution sur un intervalle $]0, a[$, alors (f, f_0) est libre si, et seulement si, f n'est pas bornée au voisinage de 0.*

Démonstration.

Étape 1 : Premier point - Analyse

Soit f_0 une série entière. Il existe donc une suite $(a_n)_{n\in\mathbb{N}}$ et un réel $R > 0$ tels que, sur $]-R, R[$, on ait :

$$f_0(x) = \sum_{n=0}^{\infty} a_n x^n \qquad f_0'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1} \qquad f_0''(x) = \sum_{n=2}^{\infty} n(n-1) a_n x^{n-2}$$

Si f_0 est solution de l'équation de Bessel sur $]-R, R[$, on a :

$$\begin{aligned} 0 = x f_0''(x) + f_0'(x) + x f_0(x) &= \sum_{n=2}^{\infty} n(n-1) a_n x^{n-1} + \sum_{n=1}^{\infty} n a_n x^{n-1} + \sum_{n=0}^{\infty} a_n x^{n+1} \\ &= a_1 + \sum_{n=1}^{\infty} (n+1) n a_{n+1} x^n + \sum_{n=1}^{\infty} (n+1) a_{n+1} x^n + \sum_{n=1}^{\infty} a_{n-1} x^n \\ &= a_1 + \sum_{n=1}^{\infty} \left((n+1)^2 a_{n+1} + a_{n-1} \right) x^n \end{aligned}$$

Par unicité du développement en série entière, on obtient donc les conditions suivantes :

$$\begin{cases} a_1 = 0 \\ \forall\, n \in \mathbb{N},\ (n+2)^2 a_{n+2} = -a_n \end{cases}$$

Ainsi, pour tout $n \in \mathbb{N}$, on a $a_{2n+1} = 0$ et :

$$a_{2n} = \frac{-1}{(2n)^2} \frac{-1}{(2(n-1))^2} \cdots \frac{-1}{2^2} a_0 = \frac{(-1)^n}{4^n (n!)^2} a_0$$

Comme $a_0 = f_0(0) = 1$, on obtient :

$$f_0(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{4^n (n!)^2} x^{2n}$$

Étape 2 : Premier point - Synthèse

La série entière ci-dessus a un rayon de convergence infini par le critère de d'Alembert. En effet :

$$\forall\, x \in \mathbb{R}, \quad \left| \frac{(-1)^{n+1}}{4^{n+1}((n+1)!)^2} \frac{4^n (n!)^2}{(-1)^n} \right| = \frac{1}{4(n+1)^2} \xrightarrow[n\to+\infty]{} 0$$

Alors, les calculs précédents assurent que f_0 est solution de l'équation de Bessel.

Étape 3 : Deuxième point

Soit f une autre solution sur un intervalle $]0, a[$ avec $a > 0$.

Comme f_0 est définie sur $\mathbb{R}$ et continue, elle est bornée au voisinage de 0, ainsi que tous ses multiples. Donc si la famille (f, f_0) est liée, alors f est bornée au voisinage de 0.

Réciproquement, supposons que (f, f_0) est libre. Comme on se place sur un intervalle de $\mathbb{R}^{+\star}$, on peut écrire l'équation de Bessel comme $y'' + \frac{1}{x}y' + y = 0$. L'ensemble des solutions de cette équation est un $\mathbb{R}$-espace vectoriel de dimension 2, dont (f, f_0) est une base. Soit maintenant $W = ff_0' - f'f_0$ le wronskien de (f, f_0). Pour tout $x \in]0, a[$, on a :

$$W'(x) = f(x)f_0''(x) - f''(x)f_0(x) = -\frac{1}{x}f(x)f_0'(x) - f(x)f_0(x) + \frac{1}{x}f'(x)f_0(x) + f(x)f_0'(x) = -\frac{1}{x}W(x)$$

Ainsi, il existe une constante C telle que $W(x) = Ce^{-\ln(x)} = \frac{C}{x}$. De plus, $C \neq 0$, car sinon (f, f_0) serait liée. Par l'absurde, supposons f bornée au voisinage de 0. Comme $\lim_{x\to 0^+} f_0(x) = 1$ et $\lim_{x\to 0^+} f_0'(x) = 0$, on a :

$$\frac{C}{x} = f(x)f_0'(x) - f'(x)f_0(x) \underset{x\to 0^+}{\sim} -f'(x)$$

Soit $b \in]0, a[$. Comme $(x \mapsto -\frac{C}{x})$ est de signe constant sur $]0, b]$ et n'est pas intégrable, on obtient :

$$f(x) - f(b) = \int_b^x f'(t)dt \underset{x\to 0^+}{\sim} -C\int_b^x \frac{1}{t}dt = -C(\ln x - \ln b)$$

Ainsi, $f(x)$ est équivalent en 0^+ à $-C\ln x + C\ln b + f(b)$, et f n'est effectivement pas bornée. □

Références

[FGN13e] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 4*. Cassini

Équation de Hill-Mathieu

Leçons concernées : 220 221

On considère l'équation différentielle d'ordre 2 suivante :

$$y'' + qy = 0 \tag{E}$$

où $q : \mathbb{R} \to \mathbb{R}$ est une fonction continue, paire et π-périodique.
On note W l'espace des solutions de cette équation, qui est un $\mathbb{C}$-espace vectoriel de dimension 2. Par le théorème de Cauchy-Lipschitz, on peut identifier W à $\mathbb{C}^2$ en associant $(y(0), y'(0))$ à une solution y. On notera alors (y_1, y_2) une base de W définie par :

$$\begin{cases} y_1(0) = 1 \\ y_1'(0) = 0 \end{cases} \quad \text{et} \quad \begin{cases} y_2(0) = 0 \\ y_2'(0) = 1 \end{cases}$$

Ensuite, si y est une solution de (E), alors on a :

$$(\tau_{-\pi} y'') + q(\tau_{-\pi} y) = (\tau_{-\pi} y'') + (\tau_{-\pi} qy) = (\tau_{-\pi} y'' + qy) = \tau_{-\pi}(0) = 0$$

Ainsi, $\tau_{-\pi} y \in W$, et $A = \tau_{-\pi}$ est un endomorphisme de W. Si on note également A sa matrice, on a :

$$A = \begin{pmatrix} y_1(\pi) & y_2(\pi) \\ y_1'(\pi) & y_2'(\pi) \end{pmatrix}$$

En effet, comme $W \ni A(y_1)(x) = y_1(x+\pi) = ay_1(x) + by_2(x)$, dériver donne $y_1'(x+\pi) = ay_1'(x) + by_2'(x)$, et évaluer en 0 donne $a = y_1(\pi)$ et $b = y_1'(\pi)$. D'où la première colonne de A, et on fait de même pour la seconde.

Lemme 1.
(i) y_1 *est paire,* y_2 *est impaire*
(ii) $\det A = 1$
(iii) $y_1(\pi) = y_2'(\pi)$

Démonstration.

(i) Soit $z_1(x) = y_1(-x)$. Alors, par parité de q, on a :

$$z_1''(x) + q(x)z_1(x) = y_1''(-x) + q(x)y_1(-x) = y_1''(-x) + q(-x)y_1(-x) = 0$$

Donc z_1 est solution de (E). D'autre part, on a :

$$z_1(0) = y_1(0) = 1 \quad \text{et} \quad z_1'(0) = -y_1'(0) = 0$$

Alors $z_1 = y_1$, et donc y_1 et paire. On montre de même, avec $z_2(x) = -y_2(-x)$ que y_2 est impaire.

(ii) En notant $w = y_1y_2' - y_1'y_2$, on obtient :

$$w' = (y_1y_2' - y_1'y_2)' = y_1'y_2' + y_1y_2'' - y_1''y_2 - y_1'y_2' = y_1y_2'' - y_1''y_2 = -y_1qy_2 + qy_1y_2 = 0$$

Ainsi w est constante égale à $w(0) = y_1(0)y_2'(0) - y_1'(0)y_2(0) = 1$. Donc $\det A = w(\pi) = 1$.

(iii) L'endomorphisme inverse de A est donné par $A^{-1}(y)(x) = y(x-\pi)$, qui a pour matrice :

$$A^{-1} = \begin{pmatrix} y_1(-\pi) & y_2(-\pi) \\ y_1'(-\pi) & y_2'(-\pi) \end{pmatrix} = \begin{pmatrix} y_1(\pi) & -y_2(\pi) \\ -y_1'(\pi) & y_2'(\pi) \end{pmatrix}$$

Or, par le théorème de Cayley-Hamilton, on a $A^2 - (\operatorname{tr} A)A + I_2 = 0$.
En multipliant par A^{-1}, on obtient $A + A^{-1} = (\operatorname{tr} A)I_2$. Alors :

$$\begin{pmatrix} y_1(\pi) & y_2(\pi) \\ y_1'(\pi) & y_2'(\pi) \end{pmatrix} + \begin{pmatrix} y_1(\pi) & -y_2(\pi) \\ -y_1'(\pi) & y_2'(\pi) \end{pmatrix} = \begin{pmatrix} 2y_1(\pi) & 0 \\ 0 & 2y_2'(\pi) \end{pmatrix} = \begin{pmatrix} y_1(\pi)+y_2'(\pi) & 0 \\ 0 & y_1(\pi)+y_2'(\pi) \end{pmatrix}$$

On en déduit que $y_1(\pi) = y_2'(\pi)$.

□

Théorème 2 (Hill-Mathieu)**.**

(i) Si $|\operatorname{tr}(A)| < 2$*, alors toutes les solutions sont bornées.*

(ii) Si $|\operatorname{tr}(A)| = 2$*, alors il existe une solution non nulle bornée.*

(iii) On a $|\operatorname{tr}(A)| < 2$ *si, et seulement si,* $y_1'(\pi)y_2(\pi) = 0$*.*

(iv) Si $|\operatorname{tr}(A)| > 2$*, alors aucune solution non triviale n'est bornée.*

Démonstration.

On commence par noter :

$$\chi_A(X) = X^2 - (\operatorname{tr} A)X + 1 \qquad \text{et} \qquad \Delta = \Delta(\chi_A) = (\operatorname{tr} A)^2 - 4$$

(i) Si $|\operatorname{tr}(A)| < 2$, alors $\Delta < 0$, et χ_A admet deux racines complexes conjuguées ρ et $\overline{\rho}$. La matrice A est ainsi diagonalisable, il existe donc une base (u, v) de W telle que :

$$\tau_{-\pi}u = \rho u \qquad \text{et} \qquad \tau_{-\pi}v = \overline{\rho}v$$

Comme $|\rho|^2 = \rho\overline{\rho} = 1$, $|u|$ et $|v|$ sont continues et π-périodiques, donc u et v sont bornées, d'où le résultat.

(ii) Si $|\operatorname{tr}(A)| = 2$, alors $\Delta = 0$, et χ_A admet une racine double réelle r. Comme $r^2 = 1$, on a $r = \pm 1$. Il existe donc $u \in W$ tel que $\tau_{-\pi}u = ru$, ce qui entraîne encore une fois que u est bornée.

(iii) Comme $y_1(\pi) = y_2'(\pi)$, on a $|T| = 2$ si, et seulement si, $y_1(\pi) = y_2'(\pi) = \pm 1$, ce qui équivaut à $y_1(\pi)y_2'(\pi) = 1$, donc à $y_1'(\pi)y_2(\pi) = 1$ car $\det A = 1$.

(iv) Si $|\operatorname{tr}(A)| > 2$, alors $\Delta > 0$, et χ_A admet deux racines réelles, qui sont inverses l'une de l'autre, car $\det A = 1$. Notons les r et r^{-1}. Quitte à les échanger, on suppose $|r| > 1$. Soient $u, v \in W$ telles que $\tau_{-\pi}u = ru$ et $\tau_{-\pi}v = r^{-1}v$, et soit $y = au + bv$, avec $a \neq 0$ ou $b \neq 0$, une solution non nulle de (E).
Si $a \neq 0$, soit $x \in \mathbb{R}$ n'annulant pas u. Alors $y(x + n\pi) = ar^n u(x) + br^{-n}v(x) \sim_{n\to+\infty} ar^n u(x)$.
Si $a = 0$, alors $b \neq 0$, soit $x \in \mathbb{R}$ n'annulant pas v. Alors $y(x - n\pi) = br^n v(x)$.
Dans les deux cas, y n'est pas bornée.

□

Références

[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation*. Dunod

Équation de la chaleur sur le cercle

Leçons concernées : 222 239 241 246

On pose $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$. Pour $u_0 \in L^2(\mathbb{T})$, on considère l'équation différentielle :

$$\begin{cases} \frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 & \text{sur } \mathbb{R}^{+\star} \times \mathbb{T} \\ u(0,.) = u_0 & \text{dans } L^2(\mathbb{T}) \end{cases} \tag{$*$}$$

Théorème 1. *Il existe une unique solution u de ($*$) de classe $\mathcal{C}^2$ sur $\mathbb{R}^{+\star} \times \mathbb{T}$, avec $u(t,.)$ tendant vers u_0 dans $L^2(\mathbb{T})$ quand t tend vers 0.*

Démonstration.

Étape 1 : Analyse

Soit u une solution de ($*$) de classe $\mathcal{C}^2$ sur $\mathbb{R}^{+\star} \times \mathbb{T}$, avec $u(t,.)$ tendant vers u_0 dans $L^2(\mathbb{T})$ quand t tend vers 0. On peut alors écrire sa série de Fourier, qui converge normalement :

$$\forall\, (t,x) \in \mathbb{R}^{+\star} \times \mathbb{T},\ u(t,x) = \sum_{n\in\mathbb{Z}} c_n(t)\, e^{inx} \quad \text{où} \quad \forall\, n \in \mathbb{Z},\ c_n(t) = \frac{1}{2\pi}\int_0^{2\pi} u(t,x)\, e^{-inx}\, dx$$

Comme $(t,x) \mapsto u(t,x)\, e^{-inx}$ est de classe $\mathcal{C}^1$ en t, par dérivation sous l'intégrale, on obtient :

$$c_n'(t) = \frac{1}{2\pi}\int_0^{2\pi} \frac{\partial u}{\partial t}(t,x)\, e^{-inx}\, dx = \frac{1}{2\pi}\int_0^{2\pi} \frac{\partial^2 u}{\partial x^2}(t,x)\, e^{-inx}\, dx$$

Par intégration par partie et périodicité de $u(t,.)$ et $\frac{\partial u}{\partial t}(t,x)$, on a :

$$c_n'(t) = \frac{in}{2\pi}\int_0^{2\pi} \frac{\partial u}{\partial x}(t,x)\, e^{-inx}\, dx = \frac{-n^2}{2\pi}\int_0^{2\pi} u(t,x)\, e^{-inx}\, dx = -n^2 c_n(t)$$

On en déduit alors que $c_n(t) = c_n^0 e^{-n^2 t}$ avec $c_n^0 \in \mathbb{R}$. Fixons $t > 0$, et appliquons la formule de Parseval à $x \mapsto |u(0,x) - u(t,x)|$, en notant $c_n(u_0)$ le n-ième coefficient de Fourier de u_0 :

$$\sum_{n\in\mathbb{Z}} |c_n(u_0) - c_n(t)|^2 = \frac{1}{2\pi}\int_0^{2\pi} |u(0,x) - u(t,x)|^2\, dx$$

Or, comme $|u(0,x) - u(t,x)|$ est bornée, on a la convergence de l'intégrale vers 0 par convergence dominée. On en déduit alors que $c_n(t)$ converge vers $c_n(u_0)$. On a donc $c_n^0 = c_n(u_0)$ par unicité de la limite. On peut écrire :

$$u(t,x) = \sum_{n\in\mathbb{Z}} c_n(u_0) e^{-n^2 t} e^{inx}$$

Une potentielle solution serait donc unique et donnée par la forme ci-dessus.

Étape 2 : Synthèse

Définissons u par l'expression trouvée précédemment, et vérifions que u est bien solution de ($*$).

Pour $n \in \mathbb{Z}$, on a $|c_n(u_0) e^{-n^2 t} e^{inx}| \leqslant |c_n(u_0)|$, qui est le terme général d'une série convergente, puisque $u_0 \in L^2(\mathbb{T}) \subset L^1(\mathbb{T})$. On a donc la convergence normale de u, et u est bien définie et est continue. De plus, u et clairement 2π-périodique en x.

Pour $n \in \mathbb{Z}$, $k, l \in \mathbb{N}$ et $0 < a < t$ on a alors :

$$\left| \frac{\partial^{k+l}}{\partial t^k \partial x^l}(c_n(u_0)e^{-n^2 t}e^{inx}) \right| = \left| c_n(u_0)(-n^2)^k (in)^l e^{-n^2 t} e^{inx} \right| \leqslant \|u_0\|_1 \, |n|^{2k+l} e^{-n^2 a}$$

Ainsi, par convergence normale, u est de classe $\mathcal{C}^\infty$, et pour $k, l \in \mathbb{N}$, on a :

$$\frac{\partial^{k+l}}{\partial t^k \partial x^l} u(t,x) = \sum_{n \in \mathbb{Z}} \frac{\partial^{k+l}}{\partial t^k \partial x^l}(c_n(u_0)e^{-n^2 t}e^{inx}) = \sum_{n \in \mathbb{Z}} c_n(u_0)(-1)^k i^l n^{2k+l} e^{-n^2 t} e^{inx}$$

Pour finir, on a $u(0,.) = u_0$ en prenant $t = 0$, et que u vérifie $(*)$ en prenant $(k,l) = (0,2)$ puis $(k,l) = (1,0)$. □

Références

[Can09] B. Candelpergher. *Calcul intégral*. Cassini

Étude des polynômes cyclotomiques

Leçons concernées : 102 123 125 141 144

Proposition 1. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Démonstration.

On raisonne par récurrence sur n.
Le résultat étant clair pour $\Phi_1(X) = X - 1$, on suppose le résultat vrai pour un diviseur d de $n \geqslant 2$. On pose :

$$F(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$$

F est un polynôme unitaire de $\mathbb{Z}[X]$. On effectue alors la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$:

$$X^n - 1 = F(X)P(X) + R(X) \qquad \text{avec} \qquad P, R \in \mathbb{Z}[X] \qquad \text{et} \qquad \deg R < \deg F$$

Or, on sait que $X^n - 1 = F(X)\Phi_n(X)$ est dans $\mathbb{C}$[X], donc $F(X)(\Phi_n(X) - P(X)) = R(X)$. Par comparaison des degrés, on a donc $\Phi_n(X) = P(X) \in \mathbb{Z}[X]$.

□

Proposition 2. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Z}[X]$.*

Démonstration.

Soit $\zeta \in \mu_n^\star$. Soit p un nombre premier ne divisant pas n. Alors $\zeta^p \in \mu_n^\star$. Posons f et g les polynômes minimaux de ζ et ζ^p sur $\mathbb{Q}$.

Étape 1 : Montrons que f et g sont dans $\mathbb{Z}[X]$.

L'anneau $\mathbb{Z}[X]$ est factoriel, on peut donc écrire une décomposition de Φ_n en produit de facteurs irréductibles :

$$\Phi_n(X) = \prod_{i=1}^{r} P_i$$

Comme Φ_n est unitaire, on peut supposer que les P_i le sont également. Or, ζ est racine de Φ_n, donc de l'un des P_i, qui est alors égal à f par irréductibilité. Ainsi, $f = P_i \in \mathbb{Z}[X]$ et $f \mid \Phi_n$, et de même $g \in \mathbb{Z}[X]$ et $g \mid \Phi_n$.

Étape 2 : Montrons que $f = g$.

On suppose par l'absurde que $f \neq g$.
Comme f et g sont irréductibles et distincts, on a $fg \mid \Phi_n$ dans $\mathbb{Z}[X]$. De plus, comme $g(\zeta^p) = 0$, ζ est racine du polynôme $g(X^p)$, donc $f(X) \mid g(X^p)$ dans $\mathbb{Q}[X]$, et donc dans $\mathbb{Z}[X]$ car $f(X)$ et $g(X^p)$ sont unitaires. Soit $h \in \mathbb{Z}[X]$ tel que $g(X^p) = f(X)h(X)$. On pose :

$$g(X) = \sum_{k=0}^{r} a_k X^k \quad \text{avec} \quad \forall\, k \in [\![0, r]\!],\ a_k \in \mathbb{Z}$$

Projetons l'égalité $g(X^p) = f(X)h(X)$ dans $\mathbb{F}_p$. Grâce au morphisme de Frobenius, on obtient :

$$\overline{g}(X^p) = \sum_{k=0}^{r} \overline{a_k} X^{kp} = \left(\sum_{k=0}^{r} \overline{a_k} X^k \right)^p = \overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$$

Soit φ un facteur irréductible de $\overline{f}$ dans $\mathbb{F}_p[X]$. Par le lemme d'Euclide, φ divise $\overline{g}$. Comme fg divise Φ_n dans $\mathbb{Z}[X]$, fg divise $X^n - 1$ dans $\mathbb{Z}[X]$, donc φ^2 divise $X^n - 1$ dans $\mathbb{F}_p[X]$. Or, φ^2 admet une racine double dans $\mathbb{F}_p$, donc $X^n - 1$ aussi. Cette dernière proposition est fausse, donc $f = g$.

Étape 3 : Montrons que Φ_n est irréductible sur $\mathbb{Z}[X]$.

Soit $\zeta' \in \mu_n^\star$. On a $\zeta' = \zeta^m$ avec $m \in \mathbb{Z}$, que l'on décompose comme $m = \prod_{i=1}^{r} p_i^{\alpha_i}$. Par itération des étapes précédentes, on sait que ζ et ζ' ont même polynôme minimal sur $\mathbb{Q}$. On a donc $f(\zeta') = 0$, ainsi f admet toutes les racines primitives n-ièmes de l'unité comme racine. Alors $\deg f \geqslant \varphi(n) = \deg \Phi_n$, mais comme $f \mid \Phi_n$, on a $f = \Phi_n$. Il en résulte que Φ_n est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$ puisque Φ_n est unitaire.

□

Références

[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses

Exemple d'anneau principal et non-euclidien

Leçons concernées : 122

On notera pour tout ce développement $\alpha = \dfrac{1+i\sqrt{19}}{2}$.
On remarque que $\alpha + \overline{\alpha} = 1$, $\alpha\overline{\alpha} = 5$ et que $\alpha^2 - \alpha + 5 = 0$. On a donc : $\mathbb{Z}[\alpha] = \{z = a + b\alpha \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$.
On définit alors la norme $N : \left| \begin{array}{ccc} \mathbb{Z}[\alpha] & \longrightarrow & \mathbb{N} \\ z = a + b\alpha & \longmapsto & z\overline{z} = a^2 + ab + 5b^2 \end{array} \right.$.

Lemme 1. *Soit A un anneau euclidien. Il existe $x \in A \setminus A^\times$ tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective.*

Démonstration du lemme 1.

Si A est un corps, $x = 0$ convient.
Sinon, parmi les éléments de A non nuls et non inversibles, on choisit x tel que $\nu(x)$ soit minimal.
Alors, si $a \in A$, on a $a = xq + r$ avec $r = 0$ ou $\nu(r) = \nu(x)$, donc $a \equiv r \mod x$.
Mais, si $r \neq 0$, comme $\nu(r) < \nu(x)$, r est inversible, et a est bien égal, modulo (x), à 0 ou à un élément de $A^\star$.
□

Théorème 2. *$\mathbb{Z}[\alpha]$ n'est pas euclidien.*

Démonstration du théorème 2.

(i) Montrons que $(\mathbb{Z}[\alpha])^\times = \{1, -1\}$.
Soit $z = a + b\alpha \in (\mathbb{Z}[\alpha])^\times$. On a $N(z)N(z^{-1}) = N(zz^{-1}) = N(1) = 1$.
Comme $N(z), N(z^{-1}) \in \mathbb{N}$, on a $N(z) = a^2 + ab + 5b^2 = 1$.
Or, $b^2 + a^2 + ab \geqslant b^2 + a^2 - |ab| \geqslant (|b| - |a|)^2 \geqslant 0$, donc $1 = a^2 + ab + 5b^2 \geqslant 4b^2$.
On en déduit que $b = 0$, puis que $a = \pm 1$. Donc $(\mathbb{Z}[\alpha])^\times = \{1, -1\}$.

(ii) Supposons que $\mathbb{Z}[\alpha]$ est euclidien.
Alors par la propositon, il existe $x \in \mathbb{Z}[\alpha] \setminus \{1, -1\}$ tel que la restriction à $\{1, -1, 0\}$ de la projection canonique de $\mathbb{Z}[\alpha]$ sur $\mathbb{Z}[\alpha]/(x)$ soit surjective.
$\mathbb{Z}[\alpha]/(x)$ est donc un corps de cardinal inférieur ou égal à 3. Donc $\mathbb{Z}[\alpha]/(x) = \mathbb{K}$, avec $\mathbb{K} \cong \mathbb{F}_2$ ou $\mathbb{F}_3$.
On en déduit l'existence d'un morphisme d'anneaux surjectif $\varphi : \mathbb{Z}[\alpha] \to \mathbb{K}$.
Alors $\beta = \varphi(a)$ vérifie $\beta^2 - \beta + 5 = 0$. Mais cette équation ne possède de solution ni dans $\mathbb{F}_2$ ni dans $\mathbb{F}_3$.
On aboutit donc à une contradiction, et $\mathbb{Z}[\alpha]$ n'est donc pas euclidien.

□

Lemme 3 (Pseudo division euclidienne)**.** *Soient $a, b \in \mathbb{Z}[\alpha] \setminus \{0\}$. Alors il existe $q, r \in \mathbb{Z}[\alpha]$ tels que :*
- *$a = bq + r$ ou $2a = bq + r$*
- *$r = 0$ ou $N(r) < N(b)$*

Démonstration du lemme 3.

Soit $x = \frac{a}{b} = \frac{a\overline{b}}{b\overline{b}} \in \mathbb{C}$, que l'on écrit $x = u + v\alpha$, avec $u, v \in \mathbb{Q}$. Soit $n = \lfloor v \rfloor$. On a $v \in [n, n+1[$.

— Supposons que $v \notin \left]n+\frac{1}{3}, n+\frac{2}{3}\right[$.
Soient alors s et t les entiers les plus proches de u et v respectivement. On a $|s-u| \leqslant \frac{1}{2}$ et $|t-v| \leqslant \frac{1}{3}$.
On pose alors $q = s + t\alpha$, de sorte que q est dans A et on a :

$$N(x-q) = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leqslant \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1$$

Si on pose $r = a - bq = b(x-q)$, on a bien $N(r) < N(b)$.

— Supposons que $v \in \left]n+\frac{1}{3}, n+\frac{2}{3}\right[$.
On considère alors $2x = 2u + 2v\alpha$ et $m = \lfloor 2v \rfloor$, et on a :

$$2v \in \left]2n+1-\frac{1}{3}, 2n+1+\frac{1}{3}\right[\text{ puis } 2v \notin \left]m+\frac{1}{3}, m+\frac{2}{3}\right[$$

On est ramené au cas précédent, et on a $2a = bq + r$ avec $N(r) < N(b)$.

□

Théorème 4. *$\mathbb{Z}[\alpha]$ est principal.*

Démonstration du théorème 4.

(i) L'idéal (2) est maximal dans $\mathbb{Z}[\alpha]$. Comme on a $\mathbb{Z}[\alpha]/(2) \cong (\mathbb{Z}[X]/(X^2 - X + 5))/(2)$, on en déduit que :

$$\mathbb{Z}[\alpha]/(2) \cong \mathbb{Z}[X]/(2, X^2 - X + 5) \cong (\mathbb{Z}[X]/(2))/(X^2 + X + 1) \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1)$$

Or le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{Z}/2\mathbb{Z}$, donc $\mathbb{Z}[\alpha]/(2)$ est un corps, donc (2) est maximal.

(ii) Soit I un idéal non trivial de $\mathbb{Z}[\alpha]$, et soit $a \in I \setminus \{0\}$ tel que $N(a)$ soit minimal.
Si $I = (a)$, on a terminé. Sinon, soit $x \in I \setminus (a)$, et appliquons le lemme :
— Si $x = aq + r$, avec $N(r) < N(a)$ ou $r = 0$.
Comme $r \in I$, on a $r = 0$ par minimalité de $N(a)$, donc $x \in (a)$, c'est une contradiction.
— Si $2x = aq + r$, avec $N(r) < N(a)$ ou $r = 0$, on a de la même manière $r = 0$ puis $2x = aq$.
Comme (2) est maximal, donc premier, on a soit $a \in (2)$ soit $q \in (2)$.
Si $q \in (2)$, $q = 2q'$ et $x \in (a)$, contradiction.
On a donc $q \notin (2)$ et $a \in (2)$. On note $a = 2a'$, d'où $x = a'q \in (a')$.
Comme (2) est maximal et ne contient pas q, on a $(2, q) = \mathbb{Z}[\alpha]$.
On a donc l'existence de $\lambda, \mu \in \mathbb{Z}[\alpha]$ tels que $2\lambda + q\mu = 1$.
On en déduit $a' = 2\lambda a' + q\mu a' = \lambda a + \mu x$, donc $a' \in I$, ce qui contredit la minimalité de $N(a)$.

Ainsi forcément $I = (a)$, donc $\mathbb{Z}[\alpha]$ est principal.

□

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses

Extrema liés

Leçons concernées : 159 214 215 219

Lemme 1. *Soit $\ell_1, \dots, \ell_k$ des formes linéaires sur $\mathbb{R}^n$ qui sont linéairement indépendantes. Alors :*

$$\dim \bigcap_{i=1}^{k} \operatorname{Ker} \ell_i = n - k$$

Démonstration.

On complète la famille $(\ell_1, \dots, \ell_k)$ en une base $(\ell_1, \dots, \ell_n)$ de $(\mathbb{R}^n)^\star$. On considère la base antéduale $(e_1, \dots, e_n)$ de $\mathbb{R}^n$ associée. Alors $x \in \bigcap_{i=1}^{k} \operatorname{Ker} \ell_i$ si, et seulement si, $x \in \operatorname{Vect}(e_{k+1}, \dots, e_n)$. Ainsi :

$$\dim \bigcap_{i=1}^{k} \operatorname{Ker} \ell_i = \dim \operatorname{Vect}(e_{k+1}, \dots, e_n) = n - k$$

□

Proposition 2. *Soit M une sous-variété de dimension d de $\mathbb{R}^n$. Soient $a \in M$ et U un voisinage de a dans $\mathbb{R}^n$. Soient $g_1, \dots, g_{n-d} : U \to \mathbb{R}$ des fonctions de classe $\mathcal{C}^k$ telles que :*

(i) Les formes linéaires $d_x g_1, \dots, d_x g_{n-d}$ sont linéairement indépendantes pour tout $x \in U$.

(ii) $U \cap M = \{x \in U \mid \forall\, i \in [\![1, n-d]\!],\ g_i(x) = 0\}$

Alors :

$$T_a M = \bigcap_{i=1}^{n-d} \operatorname{Ker} d_a g_i$$

Démonstration.

Soit $v \in T_a M$, et soit $\gamma :]-\varepsilon, \varepsilon[\to M$, où $\varepsilon > 0$ est tel que $\gamma(]-\varepsilon, \varepsilon[) \subset U$, avec $\gamma(0) = a$ et $\gamma'(0) = v$. Pour tout $i \in [\![1, n-d]\!]$, et pour tout $t \in]-\varepsilon, \varepsilon[$, on a $g_i \circ \gamma(t) = 0$, donc $d_{\gamma(t)} g_i \circ \gamma'(t) = 0$. En particulier, pour $t = 0$ on a $d_a g_i(v) = 0$. Donc, pour tout $i \in [\![1, n-d]\!]$, on a $v \in \operatorname{Ker} d_a g_i$. Ainsi, $v \in \bigcap_{i=1}^{n-d} \operatorname{Ker} d_a g_i$, et $T_a M \subseteq \bigcap_{i=1}^{n-d} \operatorname{Ker} d_a g_i$. Or, par le lemme, $\dim \bigcap_{i=1}^{n-d} \operatorname{Ker} d_a g_i = d = \dim T_a M$. Finalement, on a $T_a M = \bigcap_{i=1}^{n-d} \operatorname{Ker} d_a g_i$. □

Théorème 3 (Extrema liés)**.** *Soit U un ouvert de $\mathbb{R}^n$. Soient $g_1, \dots, g_k$ des fonctions de classe $\mathcal{C}^1$ de U dans $\mathbb{R}$ telles que les formes linéaires $d_x g_1, \dots, d_x g_k$ sont linéairement indépendantes pour tout $x \in U$. Posons :*

$$M = \{x \in U \mid \forall\, i \in [\![1, k]\!],\ g_i(x) = 0\}$$

Alors, si f a un extremum lié en $a \in M$, il existe $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ tels que :

$$d_a f = \sum_{i=1}^{k} \lambda_k\, d_a g_i$$

Ces réels $\lambda_1, \dots, \lambda_k$ sont appelés multiplicateurs de Lagrange.

Démonstration.

On a tout d'abord que M est une sous-variété de $\mathbb{R}^n$ de dimension $n-k$ et de classe $\mathcal{C}^1$, car on reconnait la définition par submersion des sous-variétés dans les hypothèses.

Soient $a \in M$ et $v \in T_aM$. Soit $\gamma :]-\varepsilon, \varepsilon[\to M$, où $\varepsilon > 0$, telle que $\gamma(0) = a$ et $\gamma'(0) = v$. Si f admet un extremum lié en a sur M, alors $f \circ \gamma$ admet un extremum en 0. Ainsi, $(f \circ \gamma)'(0) = d_{\gamma(0)} f \circ \gamma'(0) = d_a f(v) = 0$, donc $v \in \operatorname{Ker} d_a f$ et $T_aM \subseteq \operatorname{Ker} d_a f$.

La famille $(d_x g_1, \dots, d_x g_k)$ étant libre par hypothèse, on la complète en une base $(d_x g_1, \dots, d_x g_k, \ell_{k+1}, \dots, \ell_n)$ de $(\mathbb{R}^n)^\star$. On considère la base antéduale $(e_1, \dots, e_n)$ de $\mathbb{R}^n$ associée. Alors, pour tout $j \in [\![k+1, n]\!]$ et tout $i \in [\![1, k]\!]$, on a $d_a g_i(e_j) = 0$. Donc $\operatorname{Vect}(e_{k+1}, \dots, e_n) \subseteq \bigcap_{i=1}^k \operatorname{Ker} d_a g_i$. Or, par la proposition 2, on a $\dim \operatorname{Vect}(e_{k+1}, \dots, e_n) = n - k = \dim \bigcap_{i=1}^k \operatorname{Ker} d_a g_i$. Donc :

$$T_aM = \bigcap_{i=1}^k \operatorname{Ker} d_a g_i = \operatorname{Vect}(e_{k+1}, \dots, e_n)$$

Comme $(d_x g_1, \dots, d_x g_k, \ell_{k+1}, \dots, \ell_n)$ est une base de $(\mathbb{R}^n)^\star$, il existe $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ tels que :

$$d_a f = \sum_{i=1}^k \lambda_i d_a g_i + \sum_{i=k+1}^n \lambda_i \ell_i$$

Or, si $a \in M$ est un extremum lié de f sur M, alors $T_aM \subseteq \operatorname{Ker} d_a f$. Donc, pour tout $i \in [\![k+1, n]\!]$, on a $d_a f(e_i) = \lambda_i = 0$, et il reste :

$$d_a f = \sum_{i=1}^k \lambda_i d_a g_i$$

□

Références

[Ave83] A. Avez. *Calcul différentiel.* Masson

Familles libres d'applications

Leçons concernées : 151 228

Proposition 1. *Soient $f_1, \dots, f_n$ des applications de $\mathbb{K}$ dans $\mathbb{K}$. Alors la famille $(f_1, \dots, f_n)$ est libre dans $\mathscr{F}(\mathbb{K}, \mathbb{K})$ si, et seulement si, il existe $x_1, \dots, x_n$ dans $\mathbb{K}$ tels que la matrice $(f_i(x_j))_{i,j}$ est inversible.*

Démonstration.

— On suppose que la famille $(f_1, \dots, f_n)$ est liée, les lignes de la matrice $(f_i(x_j))_{1 \leqslant i,j \leqslant n}$ sont alors liées, quel que soit le choix des scalaires $x_1, \dots x_n$.
La contraposée fournit donc une des deux implications.

— Supposons que $\mathcal{B} = (f_1, \dots, f_n)$ est libre. Soit F le sous-espace de dimension n qu'elle engendre.
Pour tout $a \in K$, l'application e_a d'évaluation en a est une forme linéaire sur F.
L'ensemble A des formes linéaires e_a, pour $a \in K$, constitue une partie génératrice de $F^\star$. En effet, si $f \in A^\circ$, on a $f(a) = e_a(f) = 0$ pour tout $a \in K$, donc $f = 0$. Ainsi, on a $A^\circ = \{0\}$ et $\operatorname{Vect} A = ((\operatorname{Vect} A)^\circ)^\perp = 0^\perp = F$, puisqu'on est en dimension finie.
On peut donc choisir des scalaires $x_1, \dots, x_n$ tels que les formes linéaires $e_{x_1}, \dots, e_{x_n}$ constituent une base de $F^\star$. Montrons que le n-uplet $(x_1, \dots, x_n)$ répond à la question.

Considérons la matrice $M = (f_i(x_j))_{1 \leqslant i,j \leqslant n}$.
Montrons que les lignes $L_1, \dots, L_n$ de M forment une famille libre.
Soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}n$ tel que $\sum_{i=1}^{n} \lambda_i L_i = 0$.
On a alors, pour tout $j \in [\![1, n]\!]$, $\sum_{i=1}^{n} \lambda_i f_i(x_j) = 0$, c'est-à-dire $e_{x_j}\left(\sum_{i=1}^{n} \lambda_i f_i\right) = 0$.
La famille $(e_{x_1}, \dots, e_{x_n})$ étant une base de $F^\star$, on a donc $\sum_{i=1}^{n} \lambda_i f_i \in (F^\star)^\circ = \{0\}$.
La famille $(f_1, \dots, f_n)$ étant une base de F, on en déduit que $\lambda_1 = \dots = \lambda_n = 0$.
La matrice M est donc inversible.

□

Théorème 2. *Les translatées $f_a : h \mapsto f(a + h)$ d'applications $f : \mathbb{R} \to \mathbb{R}$ dérivables engendrent un sous-espace vectoriel de dimension finie de $\mathscr{C}(\mathbb{R}, \mathbb{R})$ si, et seulement si, f est solution d'une équation différentielle linéaire homogène à coefficients constants.*

Démonstration.

Soit $f : \mathbb{R} \to \mathbb{R}$ dérivable dont les translatées engendrent un $\mathbb{R}$-espace vectoriel F de dimension n.
On considère des réels $a_1, \dots, a_n$ tels que la famille $(f_{a_1}, \dots, f_{a_n})$ soit une base de F.
D'après la Proposition 1, il existe $x_1, \dots, x_n \in \mathbb{R}$ tels que la matrice $M = (f_i(x_j))_{1 \leqslant i,j \leqslant n}$ soit inversible.
La fonction f étant dérivable, les fonctions f_{a_i} le sont également, ainsi que tout élément de F.

Soit g un élément quelconque de F. Montrons que g' est encore dans F.
Il est clair que, pour tout $a \in \mathbb{R}$, la fonction g_a est dans F.
En effet, on a $g_a \in \operatorname{Vect}(f_{a_1+a}, \dots, f_{a_n+a}) \subset F$.

Il existe donc des réels $\lambda_1(a), \dots, \lambda_n(a)$ tels que $g_a = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}$.
Montrons que les fonctions λ_i sont dérivables. On a pour $1 \leqslant j \leqslant n$:

$$g(a + x_j) = g_a(x_j) = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}(x_j)$$

Matriciellement, cela s'écrit $\begin{pmatrix} g(a+x_1) \\ \vdots \\ g(a+x_n) \end{pmatrix} = {}^{\mathrm{t}}M \begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix}$. On en déduit que $\begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix} = ({}^{\mathrm{t}}M)^{-1} \begin{pmatrix} g(a+x_1) \\ \vdots \\ g(a+x_n) \end{pmatrix}$.
Les coefficients de la matrice $({}^{\mathrm{t}}M)^{-1}$ étant indépendants de a, on en déduit que les fonctions $\lambda_1, \dots, \lambda_n$ sont des combinaisons linéaires des fonctions $g_{x_1}, \dots, g_{x_n}$. Elles sont dérivables comme ces dernières.

On a, pour tout réel x, $g(x + a) = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}(x)$.
En dérivant par rapport à a, on obtient $g'(x + a) = \sum_{i=1}^{n} \lambda_i'(a) f_{a_i}(x)$.
On obtient en particulier, en prenant $a = 0$, on a $g' = \sum_{i=1}^{n} \lambda_i(0) f_{a_i} \in F$.
On en déduit immédiatement que tout élément g de F est $\mathscr{C}^\infty$, et que, pour tout $k \in \mathbb{N}$, on a $g^{(k)} \in F$.
C'est vrai en particulier pour la fonction f. L'espace vectoriel F étant de dimension finie n, il existe un entier $p \in [\![1, n]\!]$ tel que $f^{(p)} \in \mathrm{Vect}(f, f', \dots, f^{(p-1)})$. La fonction f est donc solution d'une équation différentielle linéaire homogène à coefficients constants d'ordre p.

Réciproquement, si f est solution d'une équation différencielle linéaire homogène à coefficients constants d'ordre p, il est clair que, pour tout $a \in \mathbb{R}$, la fonction f_a esst solution de la même équation différentielle. L'ensemble des solutions de cette équation différentielle étant un espace vectoriel de dimension p, les fonctions f_a engendrent un espace vectoriel de dimension finie inférieure ou égale à p.

□

Références

[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Fonction Gamma

Leçons concernées : 207 235 239 241 245 265

Proposition 1. *Soit $P = \{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > 0\}$. On définit sur P la fonction holomorphe :*

$$\Gamma(z) = \int_0^{+\infty} e^{-t} t^{z-1} dt$$

Démonstration.

On pose $f(z,t) = e^{-t}t^{z-1}$. On va appliquer le théorème d'holomorphie des intégrales à paramètres. La fonction $z \mapsto f(z,t)$ est holomorphe, et la fonction $t \mapsto f(z,t)$ est mesurable. Soit $K \subset P$ un compact. Il existe δ_1 et δ_2 tels que, pour tout $z \in K$, $0 < \delta_1 < \mathrm{Re}\, z < \delta_2 < +\infty$. Alors :

$$|e^{-t}t^{z-1}| \leqslant \begin{cases} t^{\delta_1 - 1} & \text{si} \quad 0 < t \leqslant 1 \\ e^{-t}t^{\delta_2 - 1} & \text{si} \quad t > 1 \end{cases}$$

Or $(t \mapsto t^{\delta_1 - 1}) \in L^1([0,1])$ et $(t \mapsto e^{-t}t^{\delta_2 - 1}) \in L^1([1, +\infty[)$, on en conclut que Γ est holomorphe sur P. □

Proposition 2. *Γ se prolonge en une fonction méromorphe sur $\mathbb{C}$, dont l'ensemble des pôles est $\mathbb{Z}^{\leqslant 0}$.*

Démonstration.

On écrit :

$$\Gamma(z) = \underbrace{\int_0^1 e^{-t}t^{z-1}dt}_{f(z)} + \underbrace{\int_1^{+\infty} e^{-t}t^{z-1}dt}_{g(z)}$$

On va montrer d'une part que f est méromorphe sur $\mathbb{C}$ dont les pôles sont les entiers négatifs, et d'autre part que g est holomorphe sur $\mathbb{C}$. Ainsi, on aura que Γ est méromorphe sur $\mathbb{C}$ dont les pôles sont les entiers négatifs.

Étape 1 : Montrons que f est méromorphe sur $\mathbb{C}$ dont les pôles sont les entiers négatifs.

On se place d'abord sur P. Comme $e^{-t} = \sum_{n=0}^{\infty} \frac{(-1)^n t^n}{n!}$, alors $e^{-t}t^{+z-1} = \sum_{n=0}^{\infty} \frac{(-1)^n t^{n+z-1}}{n!}$. On en déduit :

$$|e^{-t}t^{+z-1}| \leqslant \sum_{n=0}^{\infty} \left| \frac{(-1)^n t^{n+z-1}}{n!} \right| = \sum_{n=0}^{\infty} \frac{t^{n+\mathrm{Re}\, z - 1}}{n!} = e^t t^{\mathrm{Re}\, z - 1} \in L^1([0,1])$$

Donc, par le théorème de Fubini, on obtient :

$$f(z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \int_0^1 t^{n+z-1} dt = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(z+n)}$$

On pose $f_n(z) = \frac{(-1)^n}{n!(z+n)}$, qui a pour pôle $-n$. Soit K un compact de $\mathbb{C}$. Il existe $N \in \mathbb{N}$ tel que $K \subset \overline{D(0,N)}$, et pour tout $n \geqslant N$, f_n n'a pas de pôle dans K. Comme $|z+n| \geqslant n - |z| > n - N$, on a $|f_n(z)| \leqslant \frac{1}{n!(n+N)}$. De plus, $\sum \frac{1}{n!(n+N)}$ converge, donc $\sum_{n \geqslant N} f_n$ converge normalement. On en déduit que f est méromorphe sur $\mathbb{C}$, et que ses pôles sont simples et sont les entiers négatifs.

Étape 2 : Montrons que g est holomorphe sur $\mathbb{C}$.

On va appliquer le théorème d'holomorphie des intégrales à paramètres pour montrer que g est holomorphe. La fonction $z \mapsto e^{-t}t^{z-1}$ est holomorphe, et la fonction $t \mapsto e^{-t}t^{z-1}$ est mesurable. Soit $\tilde{K}$ un compact de $\mathbb{C}$. Alors il existe δ tel que pour tout $z \in \tilde{K}$, $\operatorname{Re} z \leqslant \delta$. Alors :

$$|e^{-t}t^{z-1}| \leqslant e^{-t}t^{\delta-1} \in L^1([1,+\infty[)$$

On en déduit que g est holomorphe sur $\mathbb{C}$. □

Références

[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation.* H&K

Forme faible de la progression arithmétique de Dirichlet

Leçons concernées : 102 120 121

Lemme 1. *Soit $a \in \mathbb{Z}$ et p premier tel que $p|\Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour $d|n$ et $d < n$. Alors $p \equiv 1[n]$.*

Démonstration.

Soit p premier vérifiant l'hypothèse. Comme p divise $\Phi_n(a)$, il divise aussi $a^n - 1$. Ainsi, l'ordre de $\overline{a}$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ divise n. Montrons que cet ordre est exactement n. Si d divise n, $d < n$, on a dans $\mathbb{Z}/p\mathbb{Z}$:

$$\overline{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}(a)}$$

Or, si d' divise d, d' divise aussi n, et par hypothèse p ne divise pas $\Phi_{d'}(a)$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le produit de ces éléments non nuls est également non nul, si bien que $\overline{a}^d \neq 1$. L'ordre de $\overline{a}$ est donc n. Comme cet ordre divise $p - 1$ d'après le théorème de Lagrange, $p \equiv 1[n]$. □

Théorème 2 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

Démonstration.

Supposons qu'il n'existe qu'un nombre fini de premiers $p_1, \ldots, p_q$ de la forme $\lambda n + 1$. On pose $N = np_1 \ldots p_q$.

Étape 1 : Montrons le résultat en supposant qu'il existe a et p vérifiant les hypothèses du lemme.

On suppose qu'il existe $a \in \mathbb{Z}$ et p un nombre premier tel que $p|\Phi_N(a)$ mais $p \nmid \Phi_d(a)$ pour $d|N$ et $d < N$. Par le lemme, $p \equiv 1[N]$. Alors $p \equiv 1[n]$, et $p \equiv 1[p_i]$. p est donc de la forme $\lambda n + 1$ et distinct des p_i. On en conclut qu'il existe une infinité de nombres premiers de la forme $\lambda n + 1$.

Étape 2 : Montrons l'existence de tels a et p.

En notant $B = \prod_{d|N, d<N} \Phi_d$, on cherche donc $a \in \mathbb{Z}$ et p premier tels que p divise $\Phi_N(a)$ et ne divise pas $B(a)$.

Les polynômes B et Φ_N sont premiers entre eux dans $\mathbb{C}[X]$, car ils n'ont pas de racine commune. Ils sont également premiers entre eux dans $\mathbb{Q}[X]$, puisque leurs coefficients sont rationnels et que l'algorithme d'Euclide s'écrit de la même manière dans $\mathbb{C}[X]$ et dans $\mathbb{Q}[X]$. Par le théorème de Bézout, il existe donc $U, V \in \mathbb{Q}[X]$ tels que $U\Phi_N + VB = 1$.

Soit $a \in \mathbb{Z}$ tel que $U' = aU$ et $V' = aV$ appartiennent à $\mathbb{Z}[X]$. On choisit a tel que $|\Phi_N(a)| \geqslant 2$, ce qui est possible puisque Φ_N n'est pas constant. Alors $a = U'\Phi_N + V'B$, et en particulier $a = U'(a)\Phi_N(a) + V'(a)B(a)$.

Soit p un nombre premier divisant $\Phi_N(a)$. Alors p divise $a^N - 1$, car Φ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$. Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = 1$, donc $\overline{a}$ est inversible, et a est premier avec p. Si p divisait $B(a)$, il diviserait a, ce qui est exclu. On a donc trouvé $a \in \mathbb{Z}$ et p premier comme on les cherchait. □

Références

[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Formule sommatoire de Poisson

Leçons concernées : 246 250

Théorème 1. *Soit $F \in L^1(\mathbb{R}) \cap \mathcal{C}^0(\mathbb{R})$. On note, pour tout $n \in \mathbb{N}$, $\widehat{F}(n) = \int_{\mathbb{R}} F(t)e^{-int}\,dt$. On suppose :*

$$\exists M > 0,\ \exists \alpha > 1,\ \forall x \in \mathbb{R},\ |F(x)| \leqslant M(1+|x|)^{-\alpha} \quad \text{et} \quad \sum_{n\in\mathbb{Z}} |\widehat{F}(n)| < +\infty$$

Alors on a la relation :

$$2\pi \sum_{n\in\mathbb{Z}} F(2\pi n) = \sum_{n\in\mathbb{Z}} \widehat{F}(n)$$

Démonstration.

On considère la fonction :

$$f(x) = \sum_{n\in\mathbb{Z}} F(x+2n\pi)$$

Étape 1 : Montrons que cette fonction est continue et 2π-périodique.

Cette série est normalement convergente sur tout compact de $\mathbb{R}$. En effet, soient $A > 0$ et $|x| \leqslant A$. Alors :

$$|n| \geqslant \frac{A}{\pi} \quad \Rightarrow \quad |x+2n\pi| \geqslant 2|n|\pi - |x| \geqslant 2|n|\pi - A \geqslant |n|\pi \quad \Rightarrow \quad |F(x+2n\pi)| \leqslant M\,(1+|n|\pi)^{-\alpha}$$

Or $M\,(1+|n|\pi)^{-\alpha}$ est le terme général d'une série convergente, donc $|F(x+2n\pi)|$ aussi. Comme F est continue par hypothèse, f l'est aussi par convergence normale. De plus, le changement d'indice $n+1 = p$ donne :

$$f(x+2\pi) = \sum_{n\in\mathbb{Z}} F(x+2n\pi+2\pi) = \sum_{n\in\mathbb{Z}} F(x+2(n+1)\pi) = \sum_{p\in\mathbb{Z}} F(x+2p\pi) = f(x)$$

Ainsi f est 2π-périodique.

Étape 2 : Calculons sa série de Fourier.

Pour tout $m \in \mathbb{Z}$:

$$c_m(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-imt}\,dt = \frac{1}{2\pi}\int_0^{2\pi} \sum_{n\in\mathbb{Z}} F(t+2n\pi)e^{-imt}\,dt = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \int_0^{2\pi} F(t+2n\pi)e^{-imt}\,dt$$

L'interversion de la somme et de l'intégrale est justifiée par la convergence normale de $\sum_{n\in\mathbb{Z}} F(t+2n\pi)$ sur $[0,2\pi]$ et que $|e^{-imt}| = 1$. On a ensuite :

$$c_m(f) = \sum_{n\in\mathbb{Z}} \frac{1}{2\pi}\int_0^{2\pi} F(t+2n\pi)e^{-im(t+2n\pi)}\,dt = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \int_n^{n+1} F(u)e^{-imu}\,dt = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(u)e^{-imu}\,dt = \frac{\widehat{F}(m)}{2\pi}$$

On a alors, par hypothèse :

$$\sum_{m\in\mathbb{Z}} |c_m(f)| = \frac{1}{2\pi}\sum_{m\in\mathbb{Z}} |\widehat{F}(m)| < +\infty$$

Ainsi, la série de Fourier de f converge normalement sur $\mathbb{R}$. On a alors :

$$2\pi \sum_{n\in\mathbb{Z}} F(x+2n\pi) = 2\pi f(x) = \sum_{n\in\mathbb{Z}} 2\pi c_n(f)e^{2i\pi nx} = \sum_{n\in\mathbb{Z}} \widehat{F}(n)e^{2i\pi nx}$$

En évaluant en $x = 0$, on obtient alors le résultat.

□

Application 2. *Pour tout $s > 0$, on a :*

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi n^2}{s}}$$

Démonstration.

Soit $a > 0$. On considère les fonctions suivantes :

$$\gamma_a : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & e^{-ax^2} \end{array} \right. \quad \text{et} \quad \theta : \left| \begin{array}{ccc} \mathbb{R}^{+\star} & \longrightarrow & \mathbb{R}^{+\star} \\ s & \longmapsto & \sum_{n\in\mathbb{Z}} e^{-\pi n^2 s} \end{array} \right.$$

Cela revient alors à montrer que $\theta(s) = \frac{1}{\sqrt{s}}\theta\left(\frac{1}{s}\right)$. On sait que $\widehat{\gamma_a} = \sqrt{\frac{\pi}{a}}\gamma_{\frac{1}{4a}}$. En appliquant la formule sommatoire de Poisson à γ_a, on obtient :

$$2\pi \sum_{n\in\mathbb{Z}} e^{-4a\pi^2 n^2} = 2\pi \sum_{n\in\mathbb{Z}} \gamma_a(2\pi n) = \sum_{n\in\mathbb{Z}} \widehat{\gamma_a}(n) = \sqrt{\frac{\pi}{a}} \sum_{n\in\mathbb{Z}} e^{-\frac{n^2}{4a}}$$

Pour tout $s > 0$, on pose $a = \frac{s}{4\pi}$. On a alors :

$$\theta(s) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 s} = \sum_{n\in\mathbb{Z}} e^{-4a\pi^2 n^2} = \frac{1}{2\pi}\sqrt{\frac{\pi}{a}} \sum_{n\in\mathbb{Z}} e^{-\frac{n^2}{4a}} = \frac{1}{2\pi}\sqrt{\frac{4\pi^2}{s}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi n^2}{s}} = \frac{1}{\sqrt{s}}\theta\left(\frac{1}{s}\right)$$

□

Références

[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation.* Dunod

Générateurs de $\mathcal{GL}(E)$ et de $\mathcal{SL}(E)$

Leçons concernées : 106 108 150 162

On considère un $\mathbb{K}$-espace vectoriel E de dimension finie $n \in \mathbb{N}^\star$.

Lemme 1. *On suppose E de dimension $n \geqslant 2$. Soient $x, y \in E \setminus \{0\}$. Il existe une transvection u ou un produit de deux transvections uv, tel que $u(x) = y$ ou $uv(x) = y$.*

Démonstration.

Supposons x et y non colinéaires. On cherche u sous la forme $u(x) = x + f(x)a$. On prend $a = y - x$ et H un hyperplan contenant a mais pas x. Soit $f \in \mathcal{L}(E)$ tel que $H = \mathrm{Ker}(f)$ et $f(x) = 1$. On peut alors prendre $u = Id_E + fa$. Si x et y sont colinéaires, on prend z non colinéaire, et on trouve, par ce qui précède, des transvections u, v telles que $u(x) = z$ et $v(z) = y$. □

Lemme 2. *Soit $z \in E \setminus \{0\}$. Soient H et H' deux hyperplans qui ne contiennent pas z. Alors il existe une transvection u telle que $u(z) = z$ et $u(H) = H'$.*

Démonstration.

Dans le cas où $H = H'$, on prend $u = Id_E$.

Si $H \neq H'$, alors $H \cap H'$ est de dimension $n-2$. Soit $h = \mathrm{Vect}(H \cap H', z)$. Comme $z \in h \setminus H$, on a $h \not\subset H$, donc $H \not\subset h$ car h et H sont des hyperplans. Soit alors $x \in H \setminus h$. De même, soit $y \in H' \setminus h$. Soit $f \in \mathcal{L}(E)$ tel que $h = \mathrm{Ker}(f)$. Comme $f(x) \neq 0$ et $f(y) \neq 0$, on peut choisir x et y tels que $f(x) = f(y) = 1$, et donc $x - y \in h$. On a alors $H = \mathrm{Vect}(H \cap H', x)$ et $H' = \mathrm{Vect}(H \cap H', y)$. Comme $H \neq H'$, x et y ne sont pas colinéaires. Ainsi, la transvection $Id_E + f \cdot (y - x)$ fixe h donc z, et envoie x sur y donc H sur H'. □

Théorème 3. *Les transvections engendrent $\mathcal{SL}(E)$.*

Démonstration.

On va montrer le résultat par récurrence sur n. Pour $n = 1$, le résultat est clair car $\mathcal{SL}(E) = \{Id_E\}$.

Supposons $n \geqslant 2$. Soient $u \in \mathcal{SL}(E)$ et $x \in E \setminus \{0\}$. Il existe τ un produit de transvections tel que $\tau \circ u(x) = x$. Soit H un hyperplan supplémentaire de $\mathrm{Vect}(x)$. Si $(\tau \circ u)|_H = Id_H$, on a $u = \tau^{-1}$ est un produit de transvections. Sinon, il existe une transvection t telle que $t(x) = x$ et $t(\tau \circ u(H)) = H$. Par hypothèse de récurrence, il existe des transvections τ_i de H telles que $t \circ \tau \circ u|_H = \tau_1 \circ \ldots \circ \tau_k$. En définissant les transvections $\tilde{\tau_i}$ sur E par $\tilde{\tau_i}|_H = \tau_i$ et $\tilde{\tau_i}(x) = x$, on a $t \circ \tau \circ u = \tilde{\tau_1} \circ \ldots \circ \tilde{\tau_k}$. Ainsi, u est un produit de transvections. □

Théorème 4. *Les transvections et les dilatations engendrent $\mathcal{GL}(E)$.*

Démonstration.

Soit $u \in \mathcal{GL}(E)$ avec $\det(u) = \lambda$, et soit v une dilatation de rapport λ^{-1}.
Alors vu est dans $\mathcal{SL}(E)$, et u est produit de la dilatation v^{-1} et de transvections. □

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses

Intégrale de Dirichlet

Leçons concernées : 228 235 236 239

Application 1. $\int_0^\infty \frac{\sin x}{x} dx = \frac{\pi}{2}$

Démonstration.

On considère la fonction suivante :

$$f : \left| \begin{array}{ccc} \mathbb{R}^+ \times \mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ (t,x) & \longmapsto & \begin{cases} \frac{\sin x}{x} e^{-tx} & \text{si} \quad x > 0 \\ 1 & \text{si} \quad x = 0 \end{cases} \end{array} \right.$$

On pose également $F(t) = \int_0^{+\infty} f(t,x)\,dx$ pour $t \in \mathbb{R}^{+\star}$. Cette application est bien définie sur $\mathbb{R}^{+\star}$ puisque $|f(t,x)| = \mathcal{O}\left(e^{-tx}\right)$ est intégrable et $x \mapsto f(t,x)$ est continue sur $\mathbb{R}^{+\star}$.

Étape 1 : Vérifions que l'intégrale de Dirichlet $F(0)$ est semi-convergente.

Pour tout $A \geqslant 0$, on a :

$$\int_0^A \frac{\sin x}{x}\,dx = \left[\frac{1-\cos x}{x}\right]_0^A + \int_0^A \frac{1-\cos x}{x^2}\,dx$$

Lorsque A tends vers $+\infty$, le crochet tend vers 0, et l'intégrale de droite converge puisque le terme sous l'intégrale est un $\mathcal{O}\left(\frac{1}{x^2}\right)$. Donc $F(0)$ est bien définie.

Étape 2 : Montrons que F est continue et dérivable sur $\mathbb{R}^{+\star}$.

On va appliquer le théorème de dérivabilité sous le signe intégral. En effet, on a :

- Pour tout $t > 0$, $x \mapsto f(t,x)$ est intégrable.
- Pour tout $x \geqslant 0$, $t \mapsto f(t,x)$ est dérivable, de dérivée $\frac{\partial f}{\partial t}(t,x) = -\sin(x)e^{-tx}$.
- Pour tous $t > \alpha > 0$, $\left|\frac{\partial f}{\partial t}(t,x)\right| = |\sin(x)|e^{-\alpha x} \leqslant e^{-\alpha x}$ est intégrable.

Ainsi F est dérivable sur $\mathbb{R}^{+\star}$, et pour tout $t > 0$, on a :

$$F'(t) = \int_0^{+\infty} \frac{\partial f}{\partial t}(t,x)\,dx = -\int_0^{+\infty} \sin(x)e^{-tx}\,dx = -\operatorname{Im}\left(\int_0^{+\infty} e^{(i-t)x}\,dx\right) = \operatorname{Im}\left(\frac{1}{i-t}\right) = -\frac{1}{1+t^2}$$

Étape 3 : Donnons une expression de F sur $\mathbb{R}^{+\star}$.

Puisque $F'(t) = -\frac{1}{1+t^2}$, on a $F(t) = C - \arctan(t)$ pour $t > 0$, où $C \in \mathbb{R}$ est une constante à déterminer. Comme $|f(t,x)| \leqslant e^{-\alpha x}$ pour $t \geqslant \alpha > 0$, le théorème de convergence dominée donne $\lim_{t\to+\infty} F(t) = 0$. On a alors $C = \frac{\pi}{2}$, donc $F(t) = \frac{\pi}{2} - \arctan(t)$ pour $t > 0$.

Étape 4 : Montrons que F est continue en 0.

Soient $t \geqslant 0$ et $A > 0$. Alors :

$$\begin{aligned} |F(t) - F(0)| &= \left|F(t) - \int_0^A f(t,x)dx + \int_0^A f(t,x)dx - \int_0^A f(0,x)dx + \int_0^A f(0,x)dx - F(0)\right| \\ &\leqslant \left|\int_A^{+\infty} \frac{\sin x}{x} e^{-tx}dx\right| + \left|\int_0^A (e^{-tx}-1)\frac{\sin x}{x}dx\right| + \left|\int_A^{+\infty} \frac{\sin x}{x}dx\right| \end{aligned}$$

Pour $B > A$, on a :

$$\begin{aligned}\int_A^B \frac{\sin x}{x} e^{-tx} dx &= \operatorname{Im}\left(\int_A^B \frac{e^{(i-t)x}}{x} dx\right) = \operatorname{Im}\left(\left[\frac{e^{(i-t)x}}{(i-t)x}\right]_A^B + \int_A^B \frac{e^{(i-t)x}}{(i-t)x^2}\, dx\right) \\ &= \operatorname{Im}\left(\frac{e^{(i-t)B}}{(i-t)B} - \frac{e^{(i-t)A}}{(i-t)A} + \int_A^B \frac{e^{(i-t)x}}{(i-t)x^2}\, dx\right)\end{aligned}$$

En faisant tendre B vers $+\infty$, on obtient :

$$\begin{aligned}\left|\int_A^B \frac{\sin x}{x} e^{-tx} dx\right| &= \left|\operatorname{Im}\left(-\frac{e^{(i-t)A}}{(i-t)A} + \int_A^{+\infty} \frac{e^{(i-t)x}}{(i-t)x^2}\, dx\right)\right| \\ &\leqslant \left|\frac{e^{(i-t)A}}{(i-t)A}\right| + \left|\int_A^{+\infty} \frac{e^{(i-t)x}}{(i-t)x^2}\, dx\right| = \frac{1}{|i-t|A} + \frac{1}{|i-t|}\int_A^{+\infty} \frac{1}{x^2}\, dx \leqslant \frac{2}{A}\end{aligned}$$

Fixons $\varepsilon > 0$, et choisissons A tel que $\frac{2}{A} \leqslant \frac{\varepsilon}{3}$ et $\left|\int_A^{+\infty} \frac{\sin x}{x} dx\right| \leqslant \frac{\varepsilon}{3}$. Alors, pour tout $t \geqslant 0$, on a :

$$|F(t) - F(0)| \leqslant \frac{2\varepsilon}{3} + \left|\int_0^A (e^{-tx} - 1)\frac{\sin x}{x} dx\right|$$

Par convergence dominée, cette dernière intégrale tend vers 0 lorsque t tend vers 0. Donc $|F(t) - F(0)| \leqslant \varepsilon$ pour t assez petit, et F est continue en 0.

Étape 5 : Conclusion.

On a finalement :

$$\int_0^{+\infty} \frac{\sin x}{x} dx = F(0) = -\arctan(0) + \frac{\pi}{2} = \frac{\pi}{2}$$

□

Références

[Can09] B. Candelpergher. *Calcul intégral.* Cassini

Inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$

Leçons concernées : 104

Lemme 1. *Soient $k \in \mathbb{N}^\star$ et p premier, alors $(1+p)^{p^k} = 1 + \lambda p^{k+1}$, avec $\lambda \in \mathbb{N}^\star$ premier avec p.*

Démonstration.

On va raisonner par récurrence sur n.

On suppose que $k = 1$. Alors :

$$(1+p)^p = \sum_{j=0}^{p} \binom{p}{j} p^j = 1 + \sum_{j=1}^{p-1} \binom{p}{j} p^j + p^p$$

Or, pour tout $j \in [\![1, p-1]\!]$, $j\binom{p}{j} = p\binom{p-1}{j-1}$, donc $p \mid j\binom{p}{j}$. Comme $j \wedge p = 1$, donc $p \mid \binom{p}{j}$ par le lemme de Gauss. Ainsi, pour tout $j \in [\![1, p-1]\!]$, il existe $a_j \in \mathbb{N}^\star$ tel que $\binom{p}{j} = pa_j$, donc :

$$(1+p)^p = 1 + \sum_{j=1}^{p-1} \binom{p}{j} p^j + p^p = 1 + p^2 \sum_{j=1}^{p-1} a_j p^{j-1} + p^p = 1 + p^2 \left(\sum_{j=1}^{p-1} a_j p^{j-1} + p^{p-2} \right)$$

On pose $\lambda = \sum_{j=1}^{p-1} a_j p^{j-1} + p^{p-2} = a_1 + \sum_{j=2}^{p-1} a_j p^{j-1} + p^{p-2}$. Comme $\binom{p}{1} = p = pa_1$, on a $a_1 = 1$, d'où $\lambda \wedge p = 1$.

On suppose le résultat vrai au rang $k \geqslant 1$. Alors :

$$(1+p)^{p^{k+1}} = ((1+p)^{p^k})^p = (1 + \lambda p^{k+1})^p = \sum_{j=0}^{p} \binom{p}{j} \lambda^j p^{j(k+1)} = 1 + \sum_{j=1}^{p} \binom{p}{j} \lambda^j p^{j(k+1)}$$

Le terme en $j = 1$ est λp^{k+2}, et p^{k+3} divise tous les termes en $j \geqslant 2$. Alors :

$$(1+p)^{p^{k+1}} = 1 + \lambda p^{k+2} + up^{k+3} = 1 + p^{k+2}(\lambda + up)$$

Or, $(\lambda + up) \wedge p = 1$ car $\lambda \wedge p = 1$, d'où le résultat.

□

Lemme 2. *Soient $a, b \in G$ d'ordre p et q. Si a et b commutent, et si $p \wedge q = 1$, alors ab est d'ordre pq.*

Démonstration.

On a $\mathrm{ord}(ab) \mid pq$. En effet, on a : $(ab)^{pq} = a^{pq}b^{pq} = (a^p)^q(b^q)^p = e$.
De plus, si $(ab)^n = a^n b^n = 1$, alors, en élevant à la puissance q, on obtient $a^{nq}b^{nq} = a^{pq}(b^q)^n = a^{nq} = 1$. Donc $p \mid nq$, puis $p \mid n$ par le lemme de Gauss. De même, on a $q \mid n$. Ainsi, $pq \mid n$.
En prenant $n = \mathrm{ord}(ab)$, on conclut que $pq = \mathrm{ord}(ab)$.

□

Proposition 3. *Soient $p \geqslant 3$ premier et $\alpha \in \mathbb{N} \setminus \{0,1\}$, alors :*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$$

Démonstration.

Par le Lemme 1, $(1+p)$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. En effet, $(1+p) \wedge p^\alpha = 1$, donc $1+p \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
De plus :

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1\ [p^\alpha] \quad \text{et} \quad (1+p)^{p^{\alpha-2}} = 1 + \lambda' p^{\alpha-1} \quad \text{avec} \quad \lambda \nmid p \quad \text{et} \quad \lambda' \nmid p$$

Ainsi, $(1+p)^{p^{\alpha-2}} \neq 1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.

On considère le morphisme de groupes :

$$\psi : \left| \begin{array}{ccc} (\mathbb{Z}/p^\alpha\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ \overline{k}^{p^\alpha} & \longmapsto & \overline{k}^p \end{array} \right.$$

ψ est bien définie, puisque si $\overline{k}^{p^\alpha} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, alors $k \wedge p^\alpha = 1$, et $k \wedge p = 1$, donc $\overline{k}^p \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Soit $\overline{k}^p \in (\mathbb{Z}/p\mathbb{Z})^\times$, donc $k \wedge p = 1$. Soit $d = k \wedge p^\alpha$, alors $d \mid p^\alpha$, donc $d = p^j$ avec $j \in [\![0, \alpha]\!]$.
Or, si $j \neq 0$, alors $p \mid p^j \mid k$, ce qui est contradictoire. Ainsi, $k \wedge p^\alpha = 1$, donc $\overline{k}^p = \psi\left(\overline{k}^{p^\alpha}\right)$.

Soit y un antécédent d'un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ qui est cyclique, et soit $m = \mathrm{ord}(y)$.
On a $1 = \psi(y^m) = \psi(y)^m$, donc $(p-1) \mid m$, et il existe $k \in \mathbb{N}^\star$ tel que $m = (p-1)k$.
En posant $x = y^k$, on a $x^{p-1} = y^{k(p-1)} = e$, et pour $\ell < p-1$ on a $x^\ell = y^{k\ell} \neq e$, car $k\ell < m$. Alors $\mathrm{ord}(x) = p-1$.
Posons $u = x(1+p)$. Par le Lemme 2, comme$(p-1) \wedge p^{\alpha-1} = 1$, u est d'ordre $p^{\alpha-1}(p-1)$.
Or, $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p^{\alpha-1}(p-1)$, donc $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p^{\alpha-1}(p-1)$, donc :

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$$

□

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses

Lemme de Morse

Leçons concernées : 158 170 171 214 215

Lemme 1. *Soit $A_0 \in \mathcal{GL}_n(\mathbb{R}) \cap \mathcal{S}_n(\mathbb{R})$. Alors il existe un voisinage V de A_0 dans $\mathcal{S}_n(\mathbb{R})$ et $\rho : V \to \mathcal{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ telle que, pour tout $A \in V$, on a ${}^t\rho(A)A_0\rho(A)$.*

Démonstration.

Étape 1 : Décomposons $\mathcal{M}_n(\mathbb{R})$ en somme directe.

On considère l'application :

$$\varphi : \left| \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{S}_n(\mathbb{R}) \\ M & \longmapsto & {}^tMA_0M \end{array} \right.$$

Alors φ est différentiable, et on a :

$$d\varphi(M) \cdot H = {}^tHA_0M + {}^tMA_0H \qquad \text{et en particulier} \qquad d\varphi(I_n) \cdot H = {}^tHA_0 + A_0H = {}^tA_0H + A_0H$$

On a donc $\mathrm{Ker}(d\varphi(I_n)) = A_0^{-1}\mathcal{A}_n(\mathbb{R})$. De plus $d\varphi(I_n)$ est surjective, car $d\varphi(I_n)(\frac{1}{2}A_0^{-1}A) = A$ pour $A \in \mathcal{S}_n(\mathbb{R})$. Posons $F = A_0^{-1}\mathcal{S}_n(\mathbb{R})$. Alors $\mathcal{M}_n(\mathbb{R}) = F \oplus \mathrm{Ker}(d\varphi(I_n))$, et $I_n \in F$.

Étape 2 : Appliquons le théorème d'inversion locale.

Posons $\psi = \varphi|_F$. On a $\mathrm{Ker}\, d\psi_{I_n} = \mathrm{Ker}\, d\chi_{I_n} \cap F = \{0\}$. Alors, ψ est de classe $\mathcal{C}^1$ et $d\psi_{I_n}$ est inversible, donc, par le théorème d'inversion locale, ψ est un $\mathcal{C}^1$-difféomorphisme local d'un voisinage U de I_n dans F vers un voisinage $V = \psi(U)$ de $A_0 = \psi(I_n)$ dans $\mathcal{S}_n(\mathbb{R})$. Quitte à remplacer U par $U' = U \cap \mathcal{GL}_n(\mathbb{R})$, qui est un ouvert car U et $\mathcal{GL}_n(\mathbb{R})$ le sont, on peut supposer que U est inclus dans $\mathcal{GL}_n(\mathbb{R})$. Pour $A \in V$, il existe donc une unique matrice $M \in U$ telle que $A = {}^tMA_0M$. On pose alors $\rho = \psi^{-1}$ qui convient. □

Théorème 2 (Lemme de Morse)**.** *Soit $f : U \to \mathbb{R}$ une fonction de classe $\mathcal{C}^3$ définie sur un ouvert U de $\mathbb{R}^n$ contenant 0. On suppose que $df(0) = 0$ et que $d^2f(0)$ est non dégénérée et de signature $(p, n-p)$. Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine dans $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = \sum_{i=1}^{p} \varphi_i(x)^2 - \sum_{i=p+1}^{n} \varphi_i(x)^2$ au voisinage de 0.*

Démonstration.

On commence par appliquer la formule de Taylor avec reste intégrale sur f :

$$f(x) - f(0) = df(0)(x) + \int_0^1 \frac{(1-t)^1}{1!} d^2f(tx)(x,x)dt = \int_0^1 (1-t)d^2f(tx)(x,x)dt = {}^txQ(x)x$$

Ainsi, Q est de classe $\mathcal{C}^1$ par dérivation sous l'intégrale, et $Q(0) = \frac{1}{2}d^2f(0)$ est symétrique inversible et de signature $(p, n-p)$. Par le lemme, il existe V un voisinage de $Q(0)$ dans $\mathcal{S}_n(\mathbb{R})$, et $\rho : V \to \mathcal{GL}_n(\mathbb{R})$ de classe $\mathcal{C}^1$ tel que ${}^t\rho(A)Q(0)\rho(A)$ pour tout $A \in V$. On pose $M(x) = \rho(Q(x))$ et $y = M(x)x$, on a alors $f(x) - f(0) = {}^tyQ(0)y$.

Comme $Q(0) = \frac{1}{2}d^2f(0)$ est de signature $(p, n-p)$, par la classification des formes quadratiques, il existe $A \in \mathcal{GL}_n(\mathbb{R})$ telle que :

$${}^tAQ(0)A = \begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix}$$

En posant $u = A^{-1}y$, on a :

$$f(x) - f(0) = {}^{t}yQ(0)y = {}^{t}u\,{}^{t}AQ(0)Au = \sum_{i=1}^{p} u_i^2 - \sum_{i=p+1}^{n} u_i^2$$

On pose alors $\varphi(x) = A^{-1}M(x)x$, on a bien $\varphi(0) = 0$, et φ est de classe $\mathcal{C}^1$ sur V. Puis, pour $h \in W$, on a :

$$\varphi(h) - \varphi(0) = A^{-1}M(h)h = A^{-1}M(0)h + o(\|h\|)$$

D'où $d\varphi_0 = A^{-1}M(0)$ qui est inversible. Par le théorème d'inversion locale, φ induit un $\mathcal{C}^1$-difféomorphisme entre deux voisinages de 0, ce qui donne le résultat.

□

Références

[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

Les biholomorphismes du disque unité

Leçons concernées : 245

Lemme 1 (Lemme de Schwarz)**.** *Soit $f \in \mathcal{H}(D(0,1))$ telle que $f(0) = 0$ et $\forall z \in D(0,1)$, $|f(z)| \leqslant 1$, alors $\forall z \in D(0,1)$, $|f(z)| \leqslant |z|$.*
S'il existe $z_0 \in D(0,1) \setminus \{0\}$ pour lequel $|f(z_0)| = |z_0|$, alors il existe une constante λ de Module 1 telle que $\forall z \in D(0,1)$, $f(z) = \lambda z$.

Démonstration.

Comme f est holomorphe, elle est analytique, et on peut écrire :

$$f(z) = \sum_{n \geqslant 0} a_n z^n \quad \text{avec} \quad \forall n \in \mathbb{N}, a_n \in \mathbb{C}$$

Comme $f(0) = 0$, on a $a_0 = 0$, donc :

$$f(z) = \sum_{n \geqslant 1} a_n z^n = z \underbrace{\left(\sum_{n \geqslant 1} a_n z^{n-1} \right)}_{\varphi(z)} = z\varphi(z) \quad \text{avec} \quad \forall n \in \mathbb{N}, a_n \in \mathbb{C}$$

Soit $r < 1$, alors, par le principe du maximum appliqué à φ :

$$\max_{z \in D(0,r)} |\varphi(z)| \leqslant \max_{|z|=r} |\varphi(z)| = \max_{|z|=r} \left| \frac{f(z)}{z} \right| = \max_{|z|=r} \frac{|f(z)|}{r} \leqslant \frac{1}{r}$$

En faisant tendre r vers 1, on obtient :

$$\frac{|f(z)|}{|z|} = |\varphi(z)| \leqslant 1$$

Donc $|f(z)| \leqslant |z|$.

On suppose qu'il existe $z_0 \in D(0,1)$ tel que $|f(z_0)| = |z_0|$, alors $|\varphi(z_0)| = 1$.
Par le principe du maximum, φ est constante de Module 1.
Donc il existe λ de Module 1 tel que pour tout $z \in D(0,1)$, □

Corollaire 2. *Les automorphismes (bijections biholomorphes) de $D(0,1)$ tels que $f(0) = 0$ sont de la forme : $z \mapsto e^{i\theta} z$, où $\theta \in \mathbb{R}$.*

Démonstration.

Soit f un automorphisme de $D(0,1)$ tel que $f(0) = 0$.
On applique le lemme de Schwarz à f et f^{-1} : pour tout $z \in D(0,1)$, $|f(z)| \leqslant |z|$ et $|f^{-1}(z) \leqslant |z|$.
On en déduit que $|f(z)| \leqslant |z| \leqslant |f(z)|$, et donc $|f(z)| = |z|$.
Par le lemme de Schwarz, il existe $\theta \in \mathbb{R}$ tel que $f(z) = e^{i\theta} z$. □

Corollaire 3. $\mathrm{Aut}(D(0,1)) = \left\{ z \mapsto e^{i\theta}\left(\frac{z-z_0}{1-\overline{z_0}z}\right) \,\middle|\, \theta \in \mathbb{R}, |z_0| < 1 \right\}$

Démonstration.

Les transformations homographiques définies sur $D(0,1)$ de la forme :

$$f_{\theta,z_0} : z \mapsto e^{i\theta}\left(\frac{z-z_0}{1-\overline{z_0}z}\right) \quad \text{avec} \quad \theta \in \mathbb{R}, |z_0| < 1$$

sont holomorphes comme quotient de fonctions holomorphes, puisque $|\overline{z_0}z| < 1$ si $|z| < 1$, donc $1 - \overline{z_0}z \neq 0$. De plus, elles définissent une bijection de $D(0,1)$ dans lui-même. En effet, si $|z| = 1$, alors $z^{-1} = \overline{z}$, et :

$$|f_{\theta,z_0}(z)| = \left|\frac{z-z_0}{1-\overline{z_0}z}\right| = \left|\frac{1}{z}\frac{z-z_0}{\overline{z}-\overline{z_0}}\right| = \frac{1}{|z|}\frac{|z-z_0|}{|\overline{z}-\overline{z_0}|} = 1$$

Donc, par le principe du maximum, si $|z| < 1$, alors $f(z) \in D(0,1)$. De plus :

$$f_{\theta,z_0}(z) = y \Leftrightarrow e^{i\theta}(z-z_0) = y(1-z\overline{z_0}) \Leftrightarrow z(e^{i\theta}+y\overline{z_0}) = y + e^{i\theta}z_0 \Leftrightarrow z = \frac{y+e^{i\theta}z_0}{e^{i\theta}+y\overline{z_0}} = f_{-\theta,-e^{i\theta}z_0}(y)$$

Ainsi, $f^{-1}_{\theta,z_0} = f_{-\theta,-e^{i\theta}z_0}$, donc f^{-1}_{θ,z_0} est bijective de réciproque holomorphe.

Réciproquement, soit $z_0 = f^{-1}(0) \in D(0,1)$. On désigne par f_0 l'homographie $z \mapsto \frac{z-z_0}{1-\overline{z_0}z}$ définie sur l'ouvert $\mathbb{C} \setminus \{\frac{1}{\overline{z_0}}\}$, et on pose $g = f \circ f_0^{-1}$. Notons que g est un automorphisme de $D(0,1)$ comme composée. Dès lors, $g(0) = f \circ f_0^{-1}(0) = f(z_0) = 0$. Par le corollaire 2, on a $\theta \in \mathbb{R}$ tel que $g(z) = e^{i\theta}z$ pour tout $z \in D(0,1)$, donc :

$$f(z) = g \circ f_0(z) = e^{i\theta}\left(\frac{z-z_0}{1-\overline{z_0}z}\right)$$

□

Références

[Les14] A. Lesfari. *Variables complexes.* Ellipses

Loi de réciprocité quadratique

Leçons concernées : 120 121 123 126

Théorème 1 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs, alors :*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$$

Démonstration.

Soit Ω une clôture algébrique de $\mathbb{F}_p$, et soit $\omega \in \Omega$ une racine primitive q-ième de l'unité.
On peut donc définir :

$$y = \sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^x$$

Calculons y^2 :

$$y^2 = \left(\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^x\right)\left(\sum_{z\in\mathbb{F}_q}\left(\frac{z}{q}\right)\omega^z\right) = \sum_{(x,z)\in(\mathbb{F}_q)^2}\left(\frac{xz}{q}\right)\omega^{x+z} \overset{\substack{u=x+z\\ t\equiv z}}{=} \sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q}\left(\frac{t(u-t)}{q}\right)$$

$$y^2 = \sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\left(\frac{t(u-t)}{q}\right) = \sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\left(\frac{-t^2(1-ut^{-1})}{q}\right) = \sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\underbrace{\left(\frac{-1}{q}\right)}_{=(-1)^{\frac{q-1}{2}}}\underbrace{\left(\frac{t^2}{q}\right)}_{=1}\left(\frac{1-ut^{-1}}{q}\right)$$

Finalement : $y^2 = (-1)^{\frac{q-1}{2}}\sum_{u\in\mathbb{F}_q}\omega^u\sum_{t\in\mathbb{F}_q^\star}\left(\frac{1-ut^{-1}}{q}\right)$.
Ainsi, en posant $c_u = \sum\limits_{t\in\mathbb{F}_q^\star}\left(\frac{1-ut^{-1}}{q}\right)$, on a $y^2 = \sum\limits_{u\in\mathbb{F}_q}\omega^u c_u$.

Calculons maintenant c_u :

$$c_0 = \sum_{t\in\mathbb{F}_q^\star}\left(\frac{1}{q}\right) = |\mathbb{F}_q^\star| = q-1$$

De plus, pour $u \neq 0$, posons $s = 1-ut^{-1} \in \mathbb{F}_q \setminus \{1\}$, alors :

$$c_u = \sum_{s\in\mathbb{F}_q\setminus\{1\}}\left(\frac{s}{q}\right) = \sum_{s\in\mathbb{F}_q}\left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) = \sum_{s\in\mathbb{F}_q^\star}\left(\frac{s}{q}\right) - 1 = -1$$

En effet, il y a $\frac{p-1}{2}$ éléments de $\mathbb{F}_q^\star$ qui sont des carrés, et autant qui ne le sont pas.
La somme est donc nulle par définition du symbole de Legendre.

On obtient donc :

$$(-1)^{\frac{q-1}{2}}y^2 = \sum_{u\in\mathbb{F}_q}\omega^u c_u = q-1-\sum_{u\in\mathbb{F}_q^\star}\omega^u = q-\sum_{u\in\mathbb{F}_q}\omega^u = q-\frac{\omega^q-1}{\omega-1} = q$$

Ainsi, $y^2 = (-1)^{\frac{q-1}{2}}q$.

Calculons maintenant y^{p-1} :

$$y^{p-1} = y^{-1}y^p = y^{-1}\left(\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^x\right)^p = y^{-1}\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^{xp} \overset{z=xp}{=} y^{-1}\sum_{z\in\mathbb{F}_q}\left(\frac{zp^{-1}}{q}\right)\omega^z$$

$$y^{p-1} = y^{-1}\sum_{z\in\mathbb{F}_q}\left(\frac{z}{q}\right)\left(\frac{p^{-1}}{q}\right)\omega^z = y^{-1}\left(\frac{p}{q}\right)^{-1}\sum_{z\in\mathbb{F}_q}\left(\frac{z}{q}\right)\omega^z = y^{-1}\left(\frac{p}{q}\right)y = \left(\frac{p}{q}\right)$$

Ainsi :

$$\left(\frac{p}{q}\right) = y^{p-1} = (y^2)^{\frac{p-1}{2}} = ((-1)^{\frac{q-1}{2}}q)^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}q^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{q}{p}\right)$$

On obtient alors le résultat voulu :

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$$

□

Références

[Ser13] J.-P. Serre. *Cours d'Arithmétique*. PUF

Loi des évènements rares de Poisson

Leçons concernées : 261 262 264 266

Lemme 1. *Soient $y_1, \dots, y_n, z_1, \dots, z_n \in \mathbb{C}$ de modules inférieurs ou égaux à 1. On a alors :*

$$\left|\prod_{k=1}^{n} y_k - \prod_{i=1}^{n} z_k\right| \leqslant \sum_{k=1}^{n} |y_k - z_k|$$

Démonstration.

On raisonne par récurrence sur n.
Pour $n = 1$, le résultat est trivial. On suppose alors le résultat vrai au rang $n \geqslant 2$, montrons le au rang n :

$$\begin{aligned}\left|\prod_{k=1}^{n} y_k - \prod_{k=1}^{n} z_k\right| &= \left|\prod_{k=1}^{n-1} y_k \times y_n + \prod_{k=1}^{n-1} z_k \times y_n - \prod_{k=1}^{n-1} z_k \times y_n - \prod_{k=1}^{n-1} z_k \times z_n\right| \\ &= \left|\left(\prod_{k=1}^{n-1} y_k - \prod_{k=1}^{n-1} z_k\right) \times y_n + \prod_{i=1}^{n-1} z_k(y_n - z_n)\right| \leqslant \left|\prod_{k=1}^{n-1} y_k - \prod_{k=1}^{n-1} z_k\right| \times \underbrace{|y_n|}_{\leqslant 1} + \underbrace{\left|\prod_{k=1}^{n-1} z_k\right|}_{\leqslant 1} \times |y_n - z_n| \\ &\leqslant \left|\prod_{k=1}^{n-1} y_k - \prod_{k=1}^{n-1} z_k\right| + |y_n - z_n| \leqslant \sum_{k=1}^{n} |y_k - z_k|\end{aligned}$$

On a donc montré le résultat pour tout $n \in \mathbb{N}^\star$. □

Théorème 2. *Soit $(X_{n,j})_{n\in\mathbb{N}^\star, j\in[\![1,M_n]\!]}$ une suite de variables aléatoires indépendantes à valeurs dans $\{0,1\}$, avec $(M_n)_{n\in\mathbb{N}^\star}$ une suite croissante de $\mathbb{N}^\star$ qui tend vers $+\infty$. On pose $\mathbb{P}(X_{n,j} = 1) = p_{n,j}$ et $S_n = \sum_{j=1}^{M_n} X_{n,j}$. On suppose de plus que :*

$$\lim_{n\to+\infty} \max_{1\leqslant j\leqslant M_n} p_{n,j} = 0 \quad \text{et} \quad \lim_{n\to+\infty} \sum_{j=1}^{M_n} p_{n,j} = \lambda > 0$$

Alors la suite $(S_n)_{n\in\mathbb{N}^\star}$ converge en loi vers la loi de Poisson $\mathcal{P}(\lambda)$.

Démonstration.

On pose dans la suite $m_n = \max_{1\leqslant j\leqslant M_n} p_{n,j}$ et $s_n = \sum_{j=1}^{M_n} p_{n,j}$. Calculons la fonction caractéristique de S_n :

$$\varphi_{S_n}(t) = \prod_{j=1}^{M_n} \varphi_{X_{n,j}}(t) = \prod_{j=1}^{M_n} \mathbb{E}\left[e^{itX_{n,j}}\right] = \prod_{j=1}^{M_n} \left((1 - p_{n,j}) + e^{it} p_{n,j}\right) = \prod_{j=1}^{M_n} \left(1 + p_{n,j}(e^{it} - 1)\right)$$

Pour tout $n \in \mathbb{N}^\star$ et tout $j \in [\![1, M_n]\!]$, on considère des variables aléatoires indépendantes $P_{n,j}$ suivant les lois de Poisson $\mathcal{P}(p_{n,j})$. Posons $S'_n = \sum_{j=1}^{M_n} P_{n,j}$. On a alors :

$$\varphi_{S'_n}(t) = \prod_{j=1}^{M_n} \varphi_{P_{n,j}}(t) = \prod_{j=1}^{M_n} e^{p_{n,j}(e^{it}-1)} = e^{s_n(e^{it}-1)}$$

On obtient alors, grâce au Lemme 1 :

$$\left|\varphi_{S_n}(t) - \varphi_{S'_n}(t)\right| = \left|\prod_{j=1}^{M_n}\left(1 + p_{n,j}(e^{it}-1)\right) - \prod_{j=1}^{M_n} e^{p_{n,j}(e^{it}-1)}\right| \leqslant \sum_{j=1}^{M_n}\left|1 + p_{n,j}(e^{it}-1) - e^{p_{n,j}(e^{it}-1)}\right|$$

Soit alors $g : \mathbb{C} \to \mathbb{C}$ la fonction définie pour $z \in \mathbb{C}$ par $g(z) = |e^z - 1 - z|$. On a :

$$g(z) = \left|\sum_{j=2}^{\infty}\frac{z^k}{k!}\right| = \left|\sum_{j=0}^{\infty}\frac{z^{k+2}}{(k+2)!}\right| = |z|^2\left|\sum_{j=0}^{\infty}\frac{z^k}{k!}\frac{1}{(k+1)(k+2)}\right| \leqslant \frac{|z|^2}{2}\sum_{j=0}^{\infty}\frac{|z|^k}{k!} = \frac{|z|^2}{2}e^{|z|}$$

En utilisant les inégalités $|p_{n,j}(e^{it}-1)| \leqslant 2p_{n,j} \leqslant 2$, on obtient :

$$\left|\varphi_{S_n}(t) - \varphi_{S'_n}(t)\right| \leqslant \sum_{j=1}^{M_n} g(p_{n,j}(e^{it}-1)) \leqslant \sum_{j=1}^{M_n}\frac{(2p_{n,j})^2}{2}e^2 = 2e^2\sum_{j=1}^{M_n}p_{n,j}^2 \leqslant 2e^2 s_n m_n$$

Or, lorsque n tend vers $+\infty$, s_n tend vers λ et m_n tend vers 0, donc $\left|\varphi_{S_n}(t) - \varphi_{S'_n}(t)\right|$ tend vers 0. Alors :

$$\left|\varphi_{S_n}(t) - e^{\lambda(e^{it}-1)}\right| \leqslant \left|\varphi_{S_n}(t) - \varphi_{S'_n}(t)\right| + \left|\varphi_{S'_n}(t) - e^{\lambda(e^{it}-1)}\right| = \left|\varphi_{S_n}(t) - \varphi_{S'_n}(t)\right| + \left|e^{s_n(e^{it}-1)} - e^{\lambda(e^{it}-1)}\right|$$

Quand n tend vers $+\infty$, s_n tend vers λ, donc $\left|\varphi_{S_n}(t) - e^{\lambda(e^{it}-1)}\right|$ tend vers 0. La fonction caractéristique de S_n converge alors simplement vers la fonction caractéristique d'une loi de Poisson de paramètre λ, donc, par le théorème de Lévy, S_n converge en loi vers la loi de Poisson $\mathcal{P}(\lambda)$. □

Références

[Ouv09] J.-Y. Ouvrard. *Probabilités : Tome 2.* Cassini

Méthode de Newton

Leçons concernées : 219 223 226 228

Théorème 1. *Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f : [a,b] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ telle que $f(a) < 0 < f(b)$ et $f' > 0$ sur $[a,b]$. On considère la suite $(x_n)_{n\in\mathbb{N}}$ définie par :*

$$x_0 \in [a,b] \quad et \quad \forall n \in \mathbb{N},\ x_{n+1} = \phi(x_n) = x_n - \frac{f(x_n)}{f'(x_n)}$$

La fonction f admet un unique zéro $\alpha \in]a,b[$, et on a :

(i) Il existe $\varepsilon > 0$ tel que, pour $x_0 \in I =]\alpha - \varepsilon, \alpha + \varepsilon[$, la suite $(x_n)_{n\in\mathbb{N}}$ converge quadratiquement vers α, et il existe $C > 0$ tel que :

$$\forall n \in \mathbb{N},\ |x_{n+1} - \alpha| \leqslant C|x_n - \alpha|^2$$

(ii) Si de plus $f'' > 0$ sur $[\alpha, b]$, alors, pour $x_0 \in]\alpha, b]$, la suite $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante, et :

$$\forall n \in \mathbb{N},\ 0 \leqslant x_{n+1} - \alpha \leqslant C(x_n - \alpha)^2 \quad et \quad x_{n+1} - \alpha \sim \frac{f''(\alpha)}{2f'(\alpha)}(x_n - \alpha)^2$$

Puisque $f(a)$ et $f(b)$ sont de signes opposés, le théorème des valeurs intermédiaires nous donne l'existence d'un zéro α de f dans $]a,b[$. Ce zéro est unique car f est strictement croissante sur $]a,b[$.

La méthode de Newton consiste à approcher α en partant de x_0 une approximation plus grossière (obtenue depuis une méthode 'moins efficace', comme la dichotomie). C'est intéressant car nous allons voir que la convergence de la méthode de Newton est quadratique.

L'idée est de remplacer la courbe de f par sa tangente au point x_n, d'équation : $y = f'(x_n)(x - x_n) + f(x_n)$. Cette tangente coupe justement l'axe des abscisses au point d'abscisse x_{n+1}.

Démonstration.

(i) La formule de Taylor-Lagrange nous donne, pour $x \in [a,b]$, l'existence d'un $z_x \in]\alpha, x[$ tel que :

$$f(\alpha) = f(x) + (\alpha - x)f'(x) + \frac{(\alpha - x)^2}{2}f''(z_x)$$

En divisant par $f'(x) > 0$, et puisque $f(\alpha) = 0$, on obtient :

$$0 = \frac{f(x)}{f'(x)} + \alpha - x + \frac{(\alpha - x)^2}{2}\frac{f''(z_x)}{f'(x)} \quad \text{puis} \quad \phi(x) - \alpha = x - \frac{f(x)}{f'(x)} - \alpha = \frac{(\alpha - x)^2}{2}\frac{f''(z_x)}{f'(x)}$$

On peut alors passer à la valeur absolue et majorer violemment :

$$|\phi(x) - \alpha| = \left|\frac{(\alpha - x)^2}{2}\frac{f''(z_x)}{f'(x)}\right| = \frac{|\alpha - x|^2}{2}|f''(z_x)|\left|\frac{1}{f'(x)}\right| \leqslant \frac{|\alpha - x|^2}{2}\|f''\|_{\infty,[a,b]}\left\|\frac{1}{f'}\right\|_{\infty,[a,b]}$$

En posant $C = \frac{1}{2}\|f''\|_{\infty,[a,b]}\left\|\frac{1}{f'}\right\|_{\infty,[a,b]}$, on obtient alors :

$$|\phi(x) - \alpha| \leqslant C|\alpha - x|^2$$

Considérons $\varepsilon > 0$ suffisamment petit pour que $C\varepsilon < 1$ et que $I =]\alpha - \varepsilon, \alpha + \varepsilon[\subset [a, b]$. Alors, pour $x \in I$, on a $|\phi(x) - \alpha| \leqslant C\varepsilon^2 < \varepsilon$, d'où $\phi(I) \subset I$. En prenant $x_0 \in I$, la suite $(x_n)_{n\in\mathbb{N}}$ est alors une suite de I, qui vérifie, pour tout $n \in \mathbb{N}$:

$$|x_{n+1} - \alpha| = |\phi(x_n) - \alpha| \leqslant C|x_n - \alpha|^2 \quad \text{et} \quad C|x_n - \alpha| \leqslant (C|x_0 - \alpha|)^{2^n} \leqslant (C\varepsilon)^{2^n}$$

L'inégalité voulue est donc bien vérifiée, et on a une convergence quadratique car $C\varepsilon < 1$.

(ii) Pour $x \in [\alpha, b]$, on a $f'(x) > 0$ et $f(x) \geqslant 0$, donc :

$$\phi(x) = x - \frac{f(x)}{f'(x)} < x$$

De plus, par le premier point, on a :

$$\phi(x) - \alpha = \frac{1}{2}\frac{f''(z_x)}{f'(x)}(x - \alpha)^2 > 0$$

Ces deux inégalités donnent que l'intervalle $I = [\alpha, b]$ est stable par ϕ. Pour $x_0 \in I$, la suite $(x_n)_{n\in\mathbb{N}}$ est donc une suite de I strictement décroissante, elle converge donc vers une limite ℓ, qui doit être un point fixe de ϕ, donc $\ell = \alpha$, ceci donne le premier point. Pour le second, remarquons que, pour $n \in \mathbb{N}$, on a :

$$\frac{x_{n+1} - \alpha}{(x_n - \alpha)^2} = \frac{f''(z_{x_n})}{2f'(x_n)}$$

Par construction, on a $z_{x_n} \in]\alpha, x_n[$, donc la fraction converge vers $\frac{f''(\alpha)}{f'(\alpha)}$ par continuité. Donc :

$$x_{n+1} - \alpha \sim \frac{f''(\alpha)}{2f'(\alpha)}(x_n - \alpha)^2$$

□

Références

[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel.* Cassini

Méthode QR

Leçons concernées : 157 162 233

Théorème 1 (Méthode QR)**.** *Soit $A \in \mathcal{GL}_n(\mathbb{K})$ diagonalisable. On suppose que ses valeurs propres sont de modules distincts et on les classe par modules décroissants : $|\lambda_1| > |\lambda_2| > \ldots > |\lambda_n|$. On construit la suite :*

$$\begin{cases} A_0 = A \\ A_{k+1} = R_k Q_k \text{ où } A_k = Q_k R_k \text{ est la décomposition } QR \text{ de } A_k \end{cases}$$

On suppose qu'il existe $P \in \mathcal{GL}_n(\mathbb{K})$ tel que $A = P\,\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)P^{-1}$ et P^{-1} admet une décomposition LU. Alors la diagonale de A_k converge vers $\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$, et les coefficients sous la diagonale tendent vers 0.

Démonstration.

Pour tout $k \in \mathbb{N}$, puisque Q_k est unitaire, on a $R_k = Q_k^\star A$, donc $A_{k+1} = Q_k^\star A Q_k$. Par une récurrence immédiate, on a alors que $A_{k+1} = \mathcal{Q}_k^\star A \mathcal{Q}_k$, où $\mathcal{Q}_k = \prod_{i=1}^k Q_i$. De plus, on a également que $A^k = \mathcal{Q}_k \mathcal{R}_k$, où $\mathcal{R}_k = \prod_{i=1}^k R_{k-i}$:

$$\begin{aligned} A^k &= (Q_1R_1)\cdots(Q_1R_1) \\ &= Q_1(R_1Q_1)\cdots(R_1Q_1)R_1 = Q_1(Q_2R_2)\cdots(Q_2R_2)R_1 \\ &= Q_1Q_2(R_2Q_2)\cdots(R_2Q_2)R_2R_1 = \ldots = (Q_1Q_2\cdots Q_k)(R_k\cdots R_2R_1) \end{aligned}$$

Étape 1 : Calculons la décomposition QR de A^k d'une autre manière.

On note $P = QR$ et $P^{-1} = LU$ les factorisations QR et LU respectives et $\Lambda = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$. Alors :

$$\forall\, k \in \mathbb{N},\ A^k = P\Lambda^k P^{-1} = QR\Lambda^k LU = QR(\Lambda^k L \Lambda^{-k})\Lambda^k U$$

Or, pour tout $k \in \mathbb{N}$ et tous $i, j \in [\![1, n]\!]$, on a $\Lambda^k L \Lambda^{-k} = (\lambda_i^k L_{i,j} \lambda_j^{-k})_{1 \leqslant i,j \leqslant n}$ est triangulaire inférieure de termes diagonaux valant 1. De plus :

$$\forall\, k \in \mathbb{N},\ \forall\, 1 \leqslant j < i \leqslant n,\ (\Lambda^k L \Lambda^{-k})_{i,j} = \left(\frac{\lambda_i}{\lambda_j}\right)^k L_{i,j} \xrightarrow[k\to\infty]{} 0$$

Ainsi, $\lim_{k\to\infty}(\Lambda^k L \Lambda^{-k}) = I_n$. En particulier, $\lim_{k\to\infty} R(\Lambda^k L \Lambda^{-k})R^{-1} = I_n$. Notons O_kT_k la décomposition QR de $R(\Lambda^k L \Lambda^{-k})R^{-1}$. Par continuité de la décomposition QR, et puisque $O_kT_k = R(\Lambda^k L \Lambda^{-k})R^{-1}$ converge vers I_n, on en déduit que O_k et T_k convergent aussi vers I_n. On a ainsi obtenu :

$$A^k = QR(\Lambda^k L \Lambda^{-k})\Lambda^k U = (QO_k)(T_k R \Lambda^k U)$$

Or, la matrice QO_k est unitaire comme produit de matrices unitaires, et la matrice $T_k R \Lambda^k U$ est triangulaire supérieure comme produit de matrices triangulaires supérieures. Il existe alors une matrice $D_k \in \mathcal{M}_n(\mathbb{C})$ diagonale telle que :

$$D_kT_kR\Lambda^kU \in T_n^+(\mathbb{C}) \quad \text{et} \quad \forall\, i \in [\![1, n]\!],\ |(D_k)_{i,i}| = 1$$

Par unicité de la décomposition QR, on a alors :

$$\mathcal{Q}_k = QO_kD_k^\star \quad \text{et} \quad \mathcal{R}_k = D_kT_kR\Lambda^kU$$

Étape 2 : Montrons la convergence de A^k.

Grâce à ce que l'on vient de trouver, on peut écrire :

$$A_{k+1} = \mathcal{Q}_k^\star A \mathcal{Q}_k = (QO_kD_k^\star)^\star A(QO_kD_k^\star) = D_kO_k^\star Q^\star AQO_kD_k^\star$$

Or, puisque $A = P\Lambda P^{-1} = QR\Lambda^k R^{-1}Q^{-1}$ on obtient :

$$A_{k+1} = D_kO_k^\star Q^\star QR\Lambda R^{-1}Q^{-1}QO_kD_k^\star = D_kO_k^\star R\Lambda R^{-1}O_kD_k^\star$$

De plus, comme R est diagonale supérieure, et puisque O_k converge vers I_n, on a :

$$\lim_{k\to\infty} A_{k+1} = \lim_{k\to\infty} D_kO_k^\star(R\Lambda R^{-1})O_kD_k^\star = \lim_{k\to\infty} D_kO_k^\star \begin{pmatrix} \lambda_1 & & (*) \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} O_kD_k^\star = \begin{pmatrix} \lambda_1 & & (*') \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Ainsi A_k converge bien vers une matrice triangulaire supérieure dont la diagonale est $\mathrm{Diag}(\lambda_1, \dots, \lambda_n)$.

□

Références

[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation.* Masson

Nombres de Bell

Leçons concernées : 190 230 241 243

Proposition 1 (Nombres de Bell)**.** *Pour $n \in \mathbb{N}^\star$, on pose B_n le nombre de partitions de l'ensemble $[\![1, n]\!]$ avec la convention $B_0 = 1$, alors :*

$$\forall\, k \in \mathbb{N},\ B_k = \frac{1}{e}\sum_{n=0}^{\infty} \frac{n^k}{n}$$

Démonstration.

On considère la série entière $\sum \frac{B_n}{n!} z^n$, dont nous notons f la somme.

Étape 1 : Montrons que, pour tout $n \in \mathbb{N}$, $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

Soit $n \in \mathbb{N}$. Pour $k \leqslant n$, on note E_k l'ensemble des partitions de $[\![1, n+1]\!]$ telles que la partie contenant $n+1$ soit de cardinal $k+1$. Il existe $\binom{n}{k}$ parties de $[\![1, n+1]\!]$ de cardinal $k+1$ contenant $n+1$, et il existe B_{n-k} partitions des $n-k$ entiers restants. Il y a donc $\binom{n}{k} B_{n-k}$ telles partitions au total. Comme les ensembles E_k forment une partition de l'ensemble des partitions de $[\![1, n+1]\!]$, on a alors :

$$B_{n+1} = \sum_{k=0}^{n} |E_k| = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

Étape 2 : Montrons que, pour tout $n \in \mathbb{N}$, $B_n \leqslant n!$.

On raisonne par récurrence sur n. Le cas $n = 0$ est immédiat, ensuite on a :

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k \leqslant \sum_{k=0}^{n} \frac{n!}{(n-k)!} \leqslant n! \sum_{k=0}^{n} \frac{1}{(n-k)!} \leqslant n! \sum_{k=0}^{n} 1 \leqslant (n+1)!$$

Étape 3 : Établissons une équation différentielle dont f est solution, et calculons f.

Puisque $\frac{B_n}{n!} \leqslant 1$, f a pour rayon de convergence $R \geqslant 1$. Calculons sa dérivée :

$$f'(x) = \sum_{n=1}^{\infty} \frac{B_n}{(n-1)!} z^{n-1} = \sum_{n=0}^{\infty} \frac{B_{n+1}}{n!} z^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{n}{k} \frac{B_k}{n!} z^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \frac{B_k}{k!} z^k \frac{z^{n-k}}{(n-k)!}$$

On reconnaît alors un produit de Cauchy de deux séries entières :

$$f'(x) = \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n\right)\left(\sum_{n=0}^{\infty} \frac{z^n}{n!}\right) = f(z)e^z$$

Ainsi, f est solution du problème de Cauchy :

$$\begin{cases} y' &= e^z y \\ y(0) &= f(0) = 1 \end{cases}$$

On en déduit que $f(z) = \frac{1}{e} e^{e^z} = e^{e^z - 1}$.

Étape 4 : Concluons en calculant directement le développement en série entière de f.

Grâce au développement en série entière de l'exponentielle, on a :

$$e^{e^z} = \sum_{n=0}^{\infty} \frac{e^{nz}}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{\infty} \frac{(nz)^k}{k!} = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{(nz)^k}{n!k!}$$

On veut appliquer le théorème de Fubini. Montrons la sommabilité de $\left(\frac{(nz)^k}{n!k!}\right)_{n,k}$.

$$\sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \left| \frac{(nz)^k}{n!k!} \right| = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{|nz|^k}{n!k!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{\infty} \frac{|nz|^k}{k!} = \sum_{n=0}^{\infty} \frac{(e^{|z|})^n}{n!} = e^{e^{|z|}} < +\infty$$

D'où, par le théorème de Fubini :

$$f(z) = \frac{1}{e} \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \frac{(nz)^k}{n!k!} = \frac{1}{e} \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{(nz)^k}{n!k!} = \sum_{k=0}^{\infty} \frac{1}{k!} \left(\frac{1}{e} \sum_{n=0}^{\infty} \frac{n^k}{n!} \right) z^k$$

On obtient alors, par unicité du développement en série entière :

$$\forall\, k \in \mathbb{N},\ B_k = \frac{1}{e} \sum_{n=0}^{\infty} \frac{n^k}{n}$$

□

Références

[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Polynômes irréductibles unitaires sur $\mathbb{F}_q$

Leçons concernées : 123 125 141 144 190

Théorème 1. *Soient p un nombre premier, $\alpha, n \in \mathbb{N}^\star$ et $q = p^\alpha$. On note $\mathcal{P}_q(d)$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_q$. Alors :*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_q(d)} P(X)$$

Démonstration.

Notons $Q(X)$ le second membre de l'égalité précédente. Le polynôme X divise $X^{q^n} - X$.

Étape 1 : Montrons que $Q(X)$ divise $X^{q^n} - X$.

Soit d un diviseur de n, on pose $n = dk$. Soit $P \in \mathcal{P}_p(d)$. On pose $\mathbb{K} = \mathbb{F}_p[X]/(P)$. $\mathbb{K}$ est un corps de cardinal q^d, donc isomorphe à $\mathbb{F}_{q^d}$. Par une récurrence immédiate, on obtient, pour tout $x \in \mathbb{K}$:

$$x^{q^n} = x^{q^{dk}} = (((x^{q^d})^{q^d}) \cdots)^{q^d} = x$$

Autrement dit, $X^{q^n} - X = 0$ dans $\mathbb{K}[X]$, donc P divise $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme les éléments de $\mathcal{P}_q(d)$ sont irréductibles, le produit $Q(X)$ divise lui aussi $X^{q^n} - X$.

Étape 2 : Montrons que tout facteur irréductible de $X^{q^n} - X$ est une seule fois dans $Q(X)$.

Réciproquement, soit P un facteur irréductible de degré d de $X^{q^n} - X$ dans $\mathbb{F}_q[X]$. Comme $\mathbb{F}_{q^n}$ est un corps de décomposition de $X^{q^n} - X$, P est scindé sur $\mathbb{F}_{q^n}$. Si x est une racine de P, on a :

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)]\,[\mathbb{F}_q(x) : \mathbb{F}_q]$$

Or P est irréductible, donc $\mathbb{F}_q(x)$ est un corps de rupture de P de degré d sur $\mathbb{F}_q$, et d divise n. Il suffit alors de montrer que $X^{q^n} - X$ n'a pas de facteur double (ou plus). En effet, si tel était le cas, alors $X^{q^n} - X$ aurait une racine double. Cependant, comme le polynôme dérivé de $X^{q^n} - X$ est $q^n X^{q^n - 1} - 1 = -1$ en caractéristique p, donc $X^{q^n} - X$ n'a pas de racine double, ce qui termine la preuve.

□

Proposition 2 (Inversion de Möbius)**.** *On note μ la fonction de Möbius. Soit $g : \mathbb{N}^\star \to \mathbb{C}$. On pose $G(n) = \sum_{d|n} g(d)$. Alors :*

$$\forall n \in \mathbb{N}^\star,\ g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$$

Démonstration.

Pour $n \geqslant 2$, on a $\sum_{d|n} \mu(d) = 0$. En effet, si $n = \prod_{i=1}^r p_i^{\alpha_i}$, alors :

$$\sum_{d|n} \mu(d) = \sum_{\beta < \alpha} \mu\left(\prod_{i=1}^r p_i^{\beta_i}\right) = \sum_{\beta \in \{0,1\}^r} (-1)^\beta = \sum_{i=0}^r \binom{r}{i} (-1)^i = (1-1)^r = 0$$

Ensuite, si $n \in \mathbb{N}^\star$ et $d \mid n$, alors $d' \mid \frac{n}{d}$ si, et seulement si, $dd' \mid n$. On a donc :

$$\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{d' \mid \frac{n}{d}} g(d') = \sum_{d|n} \mu(d) \sum_{dd' \mid n} g(d') = \sum_{dd' \mid n} \mu(d) g(d') = \sum_{d' \mid n} g(d') \sum_{d \mid \frac{n}{d'}} \mu(d) = g(n)$$

□

Corollaire 3. *Si $I(q,d)$ désigne le cardinal de $\mathcal{P}_p(d)$, alors, pour tout $n \in \mathbb{N}^\star$, on a :*

$$I(q,n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \underset{+\infty}{\sim} \frac{q^n}{n}$$

Démonstration.

On pose $g(n) = nI(q,n)$ et $G(n) = \sum_{d|n} g(d)$. On a que :

$$q^n = \deg(X^{q^n} - X) = \sum_{d|n} \sum_{P \in \mathcal{P}_q(d)} \deg P = \sum_{d|n} dI(q,d) = \sum_{d|n} g(d) = G(n)$$

Par l'inversion de Möbius, on obtient :

$$I(q,n) = \frac{1}{n} g(n) = \frac{1}{n}\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right) = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}} = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

Ensuite, on pose $r_n = \sum_{\substack{d|n \\ d<n}} \mu\left(\frac{n}{d}\right) q^d$, et on a :

$$|r_n| \leqslant \sum_{\substack{d|n \\ d<n}} q^d \leqslant \sum_{d=0}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q-1}$$

Ainsi $r_n = \mathcal{O}(q^n)$. Or $I(q,d) = \frac{q^n + r_n}{n}$, d'où le résultat. □

Références

[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois.* Calvage et Mounet

Processus de Galton-Watson

Leçons concernées : 264 266

Théorème 1 (Galton-Watson). *Soient $(X_i^j)_{i,j\in\mathbb{N}^\star}$ des variables aléatoires indépendantes et identiquement distribuées à valeurs dans $\mathbb{N}$. On note μ leur loi et m leur espérance. On définit le processus $(Z_n)_{n\in\mathbb{N}}$ par $Z_0 = 1$ et $Z_{n+1} = \sum_{i=1}^{Z_n} X_i^{n+1}$ pour $n \in \mathbb{N}$. On note $\pi_\infty = \mathbb{P}(\exists\, n \in \mathbb{N},\ Z_n = 0)$. Alors si $\mu \neq \delta_1$, on a :*

(i) Si $m \leqslant 1$, alors $\pi_\infty = 1$: Il y a extinction presque sûre du processus.

(ii) Si $m > 1$, alors $\pi_\infty < 1$: Il y a une probabilité non nulle de survie.

Démonstration.

On note G la fonction génératrice de la loi μ

Étape 1 : Montrons que G est croissante convexe sur $[0,1]$, et strictement convexe si $\mu([2,+\infty[) > 0$.

En tant que fonction génératrice, G est une série entière convergente en 1, donc G est de classe $\mathcal{C}^\infty$ sur $[0,1[$. Pour tout $k \in \mathbb{N}$, notons $p_k = \mathbb{P}\left(X_i^j = k\right)$. Les p_k sont alors positifs, on a donc, pour $s \in [0,1]$:

$$G'(s) = \sum_{k=1}^{\infty} k\, p_k\, s^{k-1} \geqslant 0 \qquad \text{et} \qquad G''(s) = \sum_{k=2}^{\infty} k(k-1)\, p_k\, s^{k-2} \geqslant 0$$

Donc G est ainsi croissante et convexe sur $[0,1]$. Si $\mu([2,+\infty[) > 0$, il existe $k \geqslant 2$ tel que $p_k > 0$, donc la deuxième inégalité est en fait stricte pour $s \neq 0$, d'où la stricte convexité.

Étape 2 : Montrons par récurrence que $G_{Z_n} = G^n$ pour tout $n \in \mathbb{N}$.

Si $n = 0$, on a, pour $s \in [0,1]$, $G_{Z_0}(s) = G_1(s) = s$, donc $G_{Z_0} = Id$.

Pour $n \in \mathbb{N}$ et $s \in [0,1]$, on a :

$$G_{Z_{n+1}}(s) = \mathbb{E}\left[s^{\sum_{i=1}^{Z_n} X_i^{n+1}}\right] = \mathbb{E}\left[\prod_{i=1}^{Z_n} s^{X_i^{n+1}}\right] = \mathbb{E}\left[\sum_{N=0}^{\infty} \mathbb{1}_{Z_n=N} \prod_{i=1}^{N} s^{X_i^{n+1}}\right]$$

Par le théorème de Fubini, puis par indépendance de Z_n avec les X_i^{n+1} et des X_i^{n+1} entre eux, on obtient :

$$G_{Z_{n+1}}(s) = \sum_{N=0}^{\infty} \mathbb{E}\left[\mathbb{1}_{Z_n=N} \prod_{i=1}^{N} s^{X_i^{n+1}}\right] = \sum_{N=0}^{\infty} \mathbb{E}\left[\mathbb{1}_{Z_n=N}\right] \mathbb{E}\left[\prod_{i=1}^{N} s^{X_i^{n+1}}\right] = \sum_{N=0}^{\infty} \mathbb{P}(Z_n = N) \prod_{i=1}^{N} \mathbb{E}\left[s^{X_i^{n+1}}\right]$$

On a alors :

$$G_{Z_{n+1}}(s) = \sum_{N=0}^{\infty} \mathbb{P}(Z_n = N) \prod_{i=1}^{N} G(s) = \sum_{N=0}^{\infty} \mathbb{P}(Z_n = N)\, G(s)^N = (G_{Z_n} \circ G)(s)$$

Ainsi on a $G_{Z_{n+1}} = G_{Z_n} \circ G$, et par hypothèse de récurrence on a donc $G_{Z_{n+1}} = G^n$

Étape 3 : Montrons que π_∞ est le plus petit point fixe de G sur $[0,1]$.

Si $\pi_n = \mathbb{P}(Z_n = 0)$, on a $\pi_\infty = \lim_{n\to+\infty} \pi_n$ puisque $(Z_n = 0)$ est une suite croissante d'évènements. De plus :

$$\pi_{n+1} = \mathbb{P}(Z_{n+1} = 0) = G_{Z_{n+1}}(0) = G(G_{Z_n}(0)) = G(\mathbb{P}(Z_n = 0)) = G(\pi_n)$$

Comme G est continue sur $[0,1]$, on obtient que $G(\pi_\infty) = \pi_\infty$ par passage à la limite. De plus, si $u \in [0,1]$ est le plus petit point fixe de G, alors $[0,u]$ est stable par G, car G est croissante. Comme $\pi_0 = \mathbb{P}(Z_0 = 0) = 0 \in [0,u]$, on a $\pi_n \in [0,u]$ pour tout $n \in \mathbb{N}$, alors π_∞ est un point fixe de G dans $[0,u]$, donc $\pi_\infty = u$ est le plus petit point fixe de G.

Étape 4 : Conclusion.

Comme $G(1) = 1$ et $G'(1) = m$, la tangente à la courbe représentative de G en 1 a pour équation $y = m(x-1)+1$. On distingue alors plusieurs cas :

(i) Si $m > 1$, alors il existe $\eta < 1$ tel que $G(s) < s$ pour $s \in]\eta, 1[$. Comme $G(0) \geqslant 0$, le théorème des valeurs intermédiaires donne l'existence d'un point fixe de G sur $[0, \eta]$. Donc $\pi_\infty < 1$.

(ii) Si $m < 1$, alors, comme G est convexe, sa courbe représentative reste au-dessus de sa tangente, donc strictement au-dessus de la droite d'équation $y = x$, ce qui implique que 1 est le seul point fixe de G sur $[0, 1]$, donc $\pi_\infty = 1$.

(iii) Si $m = 1$, alors, comme $\mu \neq \delta_1$, il existe $k \geqslant 2$ tel que $p_k > 0$. Donc G est strictement croissante, donc reste strictement au-dessus de sa tangente d'équation $y = x$, ce qui implique que 1 est le seul point fixe de G sur $[0, 1]$, donc $\pi_\infty = 1$.

□

Références

[App13] W. Appel. *Probabilités pour les non probabilistes.* H&K

Projection sur un convexe fermé et théorème de Riesz

Leçons concernées : 205 208 213 219 253

Soit H un espace de Hilbert. Soit K un convexe fermé non vide de H.

Théorème 1. *Soit $f \in H$. Il existe un unique élément de K, noté $P_K(f)$, appelé projection de f, tel que :*

$$\|P_K(f) - f\| = \inf_{v \in K} \|v - f\|$$

De plus, $P_K(f)$ est caractérisée par :

$$\forall v \in K,\ \mathrm{Re}\left(\langle f - P_K(f), v - P_K(f)\rangle\right) \leqslant 0$$

Démonstration.

Étape 1 : Existence

Soit u_ε une suite minimisante pour le problème de minimisation associé :

$$m = \inf_{v \in K} \|v - f\| \leqslant \|u_\varepsilon - f\| < m + \varepsilon$$

On utilise l'identité du parallélogramme pour $f - u_\varepsilon$ et $f - u_{\varepsilon'}$:

$$2\|f - u_\varepsilon\|^2 + 2\|f - u_{\varepsilon'}\|^2 = 4\left\|f - \frac{u_\varepsilon + u_{\varepsilon'}}{2}\right\|^2 + \|u_\varepsilon - u_{\varepsilon'}\|^2$$

Comme K est convexe, l'isobarycentre de u_ε et $u_{\varepsilon'}$ est dans K. Alors :

$$\|u_\varepsilon - u_{\varepsilon'}\|^2 \leqslant 2(m+\varepsilon)^2 + 2(m+\varepsilon')^2 - 4m^2 = 4m(\varepsilon + \varepsilon') + 2(\varepsilon^2 + \varepsilon'^2)$$

La suite u_ε est donc de Cauchy dans H, donc converge dans H. De plus K est fermé, la limite est donc dans K.

Étape 2 : Unicité

Soient $u, v \in K$ vérifiant l'égalité voulue. On utilise l'identité du parallélogramme pour $f - u$ et $f - v$:

$$2\|f - u\|^2 + 2\|f - v\|^2 = 4\left\|f - \frac{u+v}{2}\right\|^2 + \|u - v\|^2$$

Il vient alors que $\|u - v\|^2 \leqslant 2m^2 + 2m^2 - 4m^2 = 0$, d'où l'unicité.

Étape 3 : Caractérisation

Soient $v \in K$ et $t \in]0, 1]$. Alors $P_K(f) + t(v - P_K(f)) \in K$ car K est convexe, et :

$$\begin{aligned}\|f - P_K(f)\|^2 &\leqslant \|f - P_K(f) - t(v - P_K(f))\|^2 \\ &\leqslant \|f - P_K(f)\|^2 + t^2\|v - P_K(f)\|^2 - 2t\,\mathrm{Re}\left(\langle f - P_K(f), v - P_K(f)\rangle\right)\end{aligned}$$

On obtient alors :

$$0 \leqslant -2t\,\mathrm{Re}\left(\langle f - u, v - P_K(f)\rangle\right) + t^2\|v - P_K(f)\|^2 \quad \text{puis} \quad \mathrm{Re}\left(\langle f - P_K(f), v - P_K(f)\rangle\right) \leqslant \frac{t}{2}\|v - P_K(f)\|^2$$

On obtient l'égalité voulue en faisant tendre t vers 0.

Réciproquement, soit u dans K vérifiant l'égalité, alors, pour tout $v \in K$, on a :

$$\|f - v\|^2 = \|f - u + u - v\|^2 = \|f - u\|^2 + \|u - v\|^2 + 2\,\mathrm{Re}\left(\langle f - u, u - v\rangle\right) \geqslant \|f - u\|^2$$

Par définition de la projection sur un convexe fermé, on a donc $u = P_K(f)$. □

Corollaire 2. *Soient M un sous-espace vectoriel fermé de H et $f \in H$. Alors $P_M(f)$ est caractérisé par :*

$$P_M(f) \in M \qquad et \qquad \forall\, v \in M,\ \langle f - P_M(f), v\rangle = 0$$

De plus, P_M est un opérateur linéaire.

Démonstration.

Par définition de la projection sur un convexe fermé, on a, pour tout $v \in M$ et tout $t \in \mathbb{R}$:

$$\langle f - P_M(f), tv - P_M(f)\rangle \leqslant 0$$

Or, faire tendre t vers $+\infty$ implique une contradiction si $\langle f - P_M(f), v\rangle \neq 0$. Donc $\langle f - P_M(f), v\rangle = 0$.

Inversement, si u vérifie la caractérisation voulue, l'appliquer avec $v - u \in M$, où $v \in M$, donne que $u = P_M(f)$ par la caractérisation de $P_M(f)$.

□

Théorème 3 (Riesz-Fréchet)**.** *Soit $\varphi \in H'$. Alors il existe un unique $f \in H$ tel que :*

$$\forall\, v \in H,\ \langle \varphi, v\rangle = \langle f, v\rangle$$

Démonstration.

Remarquons d'abord que si $\varphi = 0$, alors prendre $f = 0$ convient.

Supposons que $\varphi \neq 0$. Soit $M = \operatorname{Ker}\varphi$, un sous-espace vectoriel fermé de H. Comme $\varphi \neq 0$, alors $M \neq H$. Soit alors $g_0 \in H \setminus M$, et soit $g_1 = P_M(g_0)$. Posons maintenant $g = \frac{g_0 - g_1}{\|g_0 - g_1\|}$. Pour tout $v \in H$, on pose :

$$\lambda = \frac{\langle \varphi, v\rangle}{\langle \varphi, g\rangle} \in \mathbb{R} \qquad \text{et} \qquad w = v - \lambda g \in M$$

Il vient alors que $\langle g, w\rangle = \frac{\langle g_0 - g_1, w\rangle}{\|g_0 - g_1\|} = 0$ par le Corollaire 2, donc que :

$$\langle g, v\rangle = \langle g, w + \lambda g\rangle = \langle g, w\rangle + \lambda \langle g, g\rangle = \lambda$$

En posant $f = \langle \varphi, g\rangle\, g$, on a ainsi :

$$\langle \varphi, v\rangle = \frac{\langle \varphi, v\rangle}{\langle \varphi, g\rangle} \langle \varphi, g\rangle = \langle g, v\rangle \langle \varphi, g\rangle = \langle \langle \varphi, g\rangle\, g, v\rangle = \langle f, v\rangle$$

Pour l'unicité, soient f et f' deux candidats. Alors :

$$\forall\, v \in H,\ \langle f - f', v\rangle = \langle \varphi, v\rangle - \langle \varphi, v\rangle = 0$$

Ainsi $f = f'$, d'où l'unicité □

Références

[Bre87] H. Brezis. *Analyse fonctionelle.* Masson

Réduction de Jordan (par la dualité)

Leçons concernées : 151 153 154 157 159

On se place dans un $\mathbb{K}$-espace vectoriel E de dimension finie $n \in \mathbb{N}^\star$.

Lemme 1. *Soit $u \in \mathcal{L}(E)$ nilpotent d'indice q. Pour tout $x \in E$ tel que $u^{q-1}(x) \neq 0$, la famille $\mathcal{B}_{u,x} = (u^k(x))_{1 \leqslant k \leqslant q-1}$ est une famille libre de E, et $F = \mathrm{Vect}(\mathcal{B}_{u,x})$ est stable par u.*

Démonstration.

Comme $u^{q-1} \neq 0$ il existe $x \in E$ tel que $u^{q-1}(x) \neq 0$. Soient $\lambda_0, \dots, \lambda_{q-1} \in K$ tels que $\sum_{k=0}^{q-1} \lambda_k u^k(x) = 0$. Montrons par récurrence sur j que les λ_j sont tous nuls. Pour $j \in [\![0, q]\!]$, on a :

$$0 = u^{q-j-1}\left(\sum_{k=j+1}^{q-1} \lambda_k u^k(x)\right) = \sum_{k=0}^{q-1} \lambda_k u^{q-j-1+k}(x) = \sum_{k=0}^{j} \lambda_k u^{q-j-1+k}(x)$$

Ainsi, en prenant $j = 0$, on a $\lambda_0 u^{q-1}(x) = 0$, donc $\lambda_0 = 0$ car $u^{q-1}(x) \neq 0$. En réitérant le processus pour chaque $j \in [\![0, q]\!]$, on trouve que tous les λ_j sont nuls, et que la famille $\mathcal{B}_{u,x}$ est libre. La stabilité de F par u découle alors du fait que u est nilpotent. □

Théorème 2. *Soit $u \in \mathcal{L}(E)$ nilpotent d'indice q. Alors il existe une base $\mathcal{B} = B_1 \cup \ldots \cup B_r$ de E telle que chaque $E_i = \mathrm{Vect}\, \mathcal{B}_i$ soit stable par u et que la matrice de $u|_{E_i}$ soit :*

$$J_{q_i} = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_{q_i}(\mathbb{K}), \quad \text{avec } q_i = \dim_{\mathbb{K}} E_i$$

Démonstration.

Étape 1 : Décomposons E en une somme directe adaptée.

Comme u est nilpotent d'indice q, ${}^{\mathrm{t}}u$ est nilpotent d'indice q. Ainsi, il existe $\varphi \in E^\star$ tel que $({}^{\mathrm{t}}u)^{q-1}(\varphi) \neq 0$. On pose alors $H = \mathrm{Vect}(\varphi, {}^{\mathrm{t}}u(\varphi), \dots, ({}^{\mathrm{t}}u)^{q-1}(\varphi))$, qui est stable par ${}^{\mathrm{t}}u$ et de dimension q par le lemme. De plus, comme $({}^{\mathrm{t}}u)^{q-1}(\varphi) \neq 0$, il existe $x \in E$ tel que $\varphi \circ u^{q-1}(x) \neq 0$ et donc $u^{q-1}(x) \neq 0$. On pose maintenant $F = \mathrm{Vect}(x, \dots, u^{q-1}(x))$, qui est stable par ${}^{\mathrm{t}}u$ et de dimension q par le lemme. Soit maintenant $G = H^\circ$, on a :

$$\dim E = \dim E^\star = \dim G + \dim H = \dim G + \dim F$$

Montrons que $F \cap G = \{0\}$. Soit $y = \sum_{k=0}^{q-1} \lambda_k u^k(x) \in F \cap G$. Comme H est stable par ${}^{\mathrm{t}}u$, G est stable par u, et $u^{q-j-1}(y) \in G$ pour $j \in [\![0, q-1]\!]$. Alors :

$$0 = \varphi(u^{q-j-1}(y)) = \sum_{k=0}^{q-1} \lambda_k \varphi(u^{q-j-1+k}(x)) = \sum_{k=0}^{j} \lambda_k \varphi(u^{q-j-1+k}(x))$$

Ainsi, en prenant $j = 0$, on a $\lambda_0 \varphi(u^{q-1}(x)) = 0$, donc $\lambda_0 = 0$ car $\varphi(u^{q-1}(x)) \neq 0$. En réitérant le processus pour chaque $j \in [\![0, q-1]\!]$, on trouve que tous les λ_j sont nuls, donc que $y = 0$ et que $F \cap G = \{0\}$. Ainsi, $E = F \oplus G$.

Étape 2 : Concluons grâce à une récurrence sur n.

Le résultat est évident pour $n = 1$. Supposons alors le résultat vrai au rang pour tout sous-espace strict de E. On complète la base $\mathcal{B}_{u,x}$ de F par une base de G en une base $\mathcal{B}$ de E. On a alors :

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} J_q & 0 \\ 0 & A_{n-q} \end{pmatrix} \quad \text{où} \quad J_q = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_q(\mathbb{K})$$

A_{n-q} est la matrice de $u|_G$ dans la base considérée. Si $q = n$ c'est fini. Sinon, on applique l'hypothèse de récurrence à $u|_G$ qui est bien un endomorphisme nilpotent d'indice inférieur ou égal à q. □

Théorème 3. *Soit $u \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Notons $\lambda_1, \ldots, \lambda_r$ ses valeurs propres. Il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u soit de la forme :*

$$\begin{pmatrix} \tilde{J}_1 & & 0 \\ & \ddots & \\ 0 & & \tilde{J}_\rho \end{pmatrix} \quad \textit{avec} \quad \tilde{J}_k = \begin{pmatrix} \lambda_k & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & \lambda_k & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{k,\alpha_k-1} & \lambda_k & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & \lambda_k \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}), \quad \textit{où} \quad \varepsilon_{k,i} \in \{0,1\}$$

Démonstration.

Écrivons $\chi_u(X) = \prod_{k=1}^{r}(X - \lambda_k)^{\alpha_k}$. Par le lemme des noyaux, on a $E = \bigoplus_{k=1}^{p} \mathrm{Ker}(X - \lambda_k)^{\alpha_k}$. Notons $N_k = \mathrm{Ker}(X - \lambda_k)^{\alpha_k}$. Chaque N_k est de dimension α_k et stable par u. De plus, $v_k = (u - \lambda_k Id)|_{N_k}$ est nilpotente. Par le théorème précédent, il existe donc une base $\mathcal{B}_k$ de N_k telle que :

$$\mathrm{Mat}_{\mathcal{B}_k}(v_k) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ \varepsilon_{k,2} & 0 & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \varepsilon_{\alpha_k-1} & 0 & 0 \\ 0 & \cdots & 0 & \varepsilon_{k,\alpha_k} & 0 \end{pmatrix} \in \mathcal{M}_{\alpha_k}(\mathbb{K}), \quad \text{où} \quad \varepsilon_{k,i} \in \{0,1\}$$

Comme $u|_{N_k} = v_k + \lambda_k Id_{N_k}$, on obtient alors $\mathrm{Mat}_{\mathcal{B}_k}(u|_{N_k}) = \mathrm{Mat}_{\mathcal{B}_k}(v_k) + \lambda_k Id_{N_k} = \tilde{J}_k$. On a ainsi la décomposition voulue sur E en concaténant les bases $(\mathcal{B}_k)_{k\in[\![1,r]\!]}$. □

Références

[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck

Réduction des endomorphismes normaux

Leçons concernées : 151 153 154 155 158 160

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n. Soit $u \in \mathcal{L}(E)$ un endomorphisme normal.

Lemme 1. *Si F est un sous-espace vectoriel de E stable par u, alors F et $F^\perp$ sont stables par u et $u^\star$.*

Démonstration.

Soient $(e_1, \dots, e_p)$ une base orthonormée de F et $(e_{p+1}, \dots, e_n)$ une base orthonormée de $F^\perp$. Dans la base $(e_1, \dots, e_n)$, la matrice M de u s'écrit par blocs : $M = \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$. Comme u est normal, u commute avec son adjoint. Matriciellement, cette relation s'écrit :

$$ {}^tMM = M\,{}^tM \quad \Leftrightarrow \quad \begin{pmatrix} {}^tAA & {}^tAB \\ {}^tBA & {}^tBB + {}^tDD \end{pmatrix} = \begin{pmatrix} A\,{}^tA + B\,{}^tB & B\,{}^tD \\ D\,{}^tB & D\,{}^tD \end{pmatrix} $$

En particulier, on a ${}^tBB + {}^tDD = D\,{}^tD$. En prenant la trace, on trouve $\mathrm{tr}({}^tBB) = 0$, donc $B = 0$, et on a $M = \left(\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right)$. Ainsi, F et $F^\perp$ sont stables par u et $u^\star$. Enfin, on a de plus $A\,{}^tA = {}^tAA$ et $D\,{}^tD = {}^tDD$, $u|_F$ et $u|_{F^\perp}$ sont normaux. □

Lemme 2. *Supposons que $n = 2$. Alors :*

(i) Si u a une valeur propre réelle, u est diagonalisable dans une base orthonormée.

(ii) Si u n'a pas de valeur propre réelle, la matrice de u dans une base orthonormée est de la forme $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$.

Démonstration.

(i) Supposons que u admet une valeur propre réelle λ. Soit e_1 un vecteur propre de norme 1. Alors $(\mathbb{R}e_1)^\perp$ est une droite, engendrée par un vecteur e_2 de norme 1, et stable par u. Le vecteur e_2 est donc un vecteur propre de u, et la matrice de u est diagonale dans la base orthonormée (e_1, e_2).

(ii) Supposons que u n'admet pas de valeur propre réelle. Écrivons $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ sa matrice dans une base orthonormée de E. Comme u est normal, on a :

$$ {}^tMM = M\,{}^tM \quad \Leftrightarrow \quad \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix} $$

On a en particulier $b^2 = c^2$, donc $b = \pm c$. Si $b = c$, alors M est symétrique et admet des valeurs propres réelles, donc $b = -c$. On en déduit que $d - a = a - d$, donc que $a = d$, d'où le résultat.

□

Théorème 3. *Il existe une base orthonormée $\mathcal{B}$ de E telle que :*

$$ \mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & 0 & \\ & & \lambda_r & & & & \\ & & & \tau_1 & & & \\ & & & & \ddots & & \\ & 0 & & & & & \\ & & & & & & \tau_s \end{pmatrix} $$

où $n = r + 2s$, $\lambda_1, \dots, \lambda_r \in \mathbb{R}$ et $\tau_k = \left(\begin{smallmatrix} a_k & -b_k \\ b_k & a_k \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbb{R})$ pour $k \in [\![1, s]\!]$.

Démonstration.

On va raisonner par récurrence sur $n = \dim E$. Le résultat est évident pour $n = 1$, et on vient de traiter le cas $n = 2$. Supposons alors $n \geqslant 3$ et le résultat vrai en dimension inférieur strictement à n.

(i) Supposons que u admet une valeur propre réelle λ, dont on note E_λ l'espace propre associé, qui est stable par u. Alors $E_\lambda^\perp$ est stable par u, et on peut appliquer l'hypothèse de récurrence à $u|_{E_\lambda^\perp}$, puis obtenir le résultat en concaténant une base de orthonormée de E_λ avec la base obtenue, qui reste bien orthonormée.

(ii) Supposons que u n'admet pas de valeur propre réelle. Soit $Q(X) = X^2 - 2\alpha X + \beta$ un facteur irréductible de χ_u de degré 2 tel que $\alpha^2 < \beta$. Écrivons $Q(x) = (X - \lambda)(X - \overline{\lambda})$, avec $\lambda \in \mathbb{C}$ valeur propre de u. Alors :

$$\det Q(u) = \det(u - \lambda Id_E) \det(u - \overline{\lambda} Id_E) = 0$$

Ainsi, $Q(u)$ est non inversible, et $\operatorname{Ker} Q(u)$ non trivial. Soit $v = u|_{\operatorname{Ker} Q(u)}$. Alors $v^\star v$ est symétrique, donc admet une valeur propre réelle $\mu \in \mathbb{R}$. Soit x un vecteur propre associé, et $F = \operatorname{Vect}(x, u(x))$. On a aussi $u^2(x) = 2\alpha u(x) + \beta x$, ainsi $F = \operatorname{Vect}(u(x), u^2(x))$ est stable par u, et est de dimension 2. On peut donc appliquer l'hypothèse de récurrence à $u|_{F^\perp}$ et le cas $n = 2$ à $u|_F$, ce qui donne le résultat voulu dans la base concaténée.

□

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

Réduction des matrices orthogonales

Leçons concernées : 106 150 154 155 160

Lemme 1. *Soit $u \in \mathcal{O}(E)$, et soit F un sous-espace vectoriel stable par u. Alors $F^\perp$ est stable par u.*

Démonstration.

Soit $x \in F$, alors $u(x) \in F$.
Soit $(e_1, \dots, e_r)$ une base orthonormale de F, que l'on complète en une base $(e_1, \dots, e_n)$ de E.
Pour tout i, on note $f_i = u(e_i)$.
Alors $(f_1, \dots, f_r)$ est une base orthonormale de F, et $(f_{r+1}, \dots, f_n)$ est une base orthonormale de $F^\perp$.
Ainsi, si $x = \sum_{i=r+1}^{n} \lambda_i e_i \in F^\perp$, alors, $u(x) = \sum_{i=r+1}^{n} \lambda_i u(e_i) = \sum_{i=r+1}^{n} \lambda_i f_i \in F^\perp$.
$F^\perp$ est donc stable par u. □

Lemme 2. *Pour $M \in \mathcal{O}_n(\mathbb{R})$, il existe un sous-espace vectoriel W_n de $\mathbb{R}^n$ tel que $\dim W_n \leqslant 2$ stable par M.*

Démonstration.

Si M possède une valeur propre réelle λ de vecteur propre associé X, alors $W = Vect(X)$ convient.
En effet, $MX = \lambda X \in W$.

Sinon, soit $\lambda \in \mathbb{C} \setminus \mathbb{R}$ de vecteur propre X : $AX = \lambda X$. Alors $A\overline{X} = \overline{AX} = \overline{\lambda X} = \overline{\lambda X}$.
Comme $\lambda \notin \mathbb{R}$, $\lambda \neq \overline{\lambda}$, et X et $\overline{X}$ sont linéairement indépendants.
Soit $Y = X + \overline{X} \in \mathbb{R}^n \setminus \{0\}$. Comme $A^2 Y = \lambda AX + \overline{\lambda} A\overline{X} = (\lambda + \overline{\lambda})(AY) - \lambda\overline{\lambda}(Y) \in Vect(Y, AY)$.
Ainsi,$W = \mathrm{Vect}(Y, AY)$ convient. □

Lemme 3. *Pour $u \in \mathcal{O}(E)$, il existe des sous-espaces vectoriels $W_1, \dots, W_k$ de $\mathbb{R}^n$ stables par u tels que, pour tout i, $\dim W_i \leqslant 2$, et $E = \bigperp_{i=1}^{k} W_i$.*

Démonstration.

On raisonne par récurrence sur $n = \dim E$.
Si $n = 1$ ou $n = 2$, on peut prendre $k = 1$ et $W_1 = E$.
Supposons le résultat vrai jusqu'au rang $n-1$. Par le lemme 2, il existe W_1 stable par u tel que $\dim W_1 \leqslant 2$.
Alors $V = W_1^\perp$ vérifie $\dim V \leqslant n-1$, et on applique l'hypothèse de récurrence : il existe des sous-espaces vectoriels $W_2, \dots, W_k$ de $\mathbb{R}^n$ stables par u tels que, pour tout i, $\dim W_i \leqslant 2$, et $V = \bigperp_{i=2}^{k} W_i$.

Ainsi, $E = W_1 \perp V = \bigperp_{i=1}^{k} W_1$, avec $\dim W_i \leqslant 2$ et les W_i stables par u. □

Théorème 4. *Soit $M \in \mathcal{O}_n(\mathbb{R})$, alors M est semblable à :*

$$\begin{pmatrix} I_r & & & & 0 \\ & -I_m & & & \\ & & R_{\theta_1} & & \\ & & & \ddots & \\ 0 & & & & R_{\theta_s} \end{pmatrix} \quad \text{avec} \quad \begin{cases} \theta_i \in]0;2\pi[\setminus \{\pi\} \\ R_{\theta_i} = \begin{pmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{pmatrix} \end{cases}$$

Démonstration.

Grâce au lemme 3, on a des sous-espaces vectoriels $W_1, \dots, W_k$ de $\mathbb{R}^n$ stables par M tels que, pour tout i, $\dim W_i \leqslant 2$, et $E = \overset{k}{\underset{i=1}{\perp}} W_i$. On va écrire chaque $M|_{W_i}$ sous une forme adaptée.
Si $\dim W_i = 1$, comme $M|_{W_i}$ est orthogonale, on a $M|_{W_i} = \pm 1$.
Si $\dim W_i = 2$, on a $M|_{W_i} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
En prenant (e_1, e_2) une base orthonormale de W_i, on a $(Me_1, Me_1) = a^2 + b^2 = 1$ et $(Me_2, Me_2) = c^2 + d^2 = 1$.
On peut donc écrire $a = \cos\theta_i$, $b = \sin\theta_i$, $c = \sin\mu_i$ et $d = \cos\mu_i$, avec $\theta_i, \mu_i \in]0;2\pi[$.
Comme $M|_{W_i}$ est orthogonale, on a $\det M = ad - bc = \cos(\theta_i + \mu_i) = \pm 1$.
Si $\det M = 1$, $\mu_i = 2\pi - \theta_i$, donc $M|_{W_i} = \begin{pmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \cos\theta_i \end{pmatrix} = R_{-\theta_i}$. Si $\theta_i = \pi$, alors $M|_{W_i} = -I_2$.
Si $\det M = -1$, $\mu_i = \pi - \theta_i$, donc $M|_{W_i} = \begin{pmatrix} \cos\theta_i & \sin\theta_i \\ \sin\theta_i & -\cos\theta_i \end{pmatrix} = P \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} P^{-1}$.
On peut donc écrire une matrice semblable à M qui est sous la forme voulue. □

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet

Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$

Leçons concernées : 101 103 104 105 108

Proposition 1. *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Démonstration.

Notons G le sous-groupe de $\mathfrak{S}_n$ engendré par les 3-cycles. On a tout d'abord que $G \subseteq \mathfrak{A}_n$ car les 3-cycles ont pour signature 1 donc tous les éléments de G aussi.

Réciproquement, soit $\sigma \in \mathfrak{A}_n$. Considérons un décomposition $\prod_{i=1}^{p} \tau_i$ de σ en produit de transpositions. Comme σ est de signature 1, on a nécessairement que p est pair. Or, pour $i, j, k, l \in [\![1, n]\!]$ distincts, on a :

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l) \quad \text{et} \quad (i\ j)(k\ i) = (i\ k\ j)$$

Donc le produit de deux transpositions est un 3-cycle, et σ s'écrit comme un produit de $\frac{p}{2}$ 3-cycles. Ainsi, $\sigma \in G$. Finalement, on a bien que $G = \mathfrak{A}_n$. □

Proposition 2. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Démonstration.

Les 3-cycles forment une classe de conjugaison dans $\mathfrak{S}_n$. Donc, pour $a, b, c \in [\![1, n]\!]$ distincts et $d, e, f \in [\![1, n]\!]$ distincts, il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma(a\ b\ c)\sigma^{-1} = (d\ e\ f)$. Si $\sigma \in \mathfrak{A}_n$, c'est bon. Sinon, comme $n \geqslant 5$, on peut choisir $i, j \in [\![1, n]\!]$ distincts de a, b, c. Alors $\sigma' = \sigma(i\ j)$ est un élément de $\mathfrak{A}_n$ tel que $\sigma'(a\ b\ c)\sigma'^{-1} = (d\ e\ f)$. Les 3-cycles sont donc bien conjugués dans $\mathfrak{A}_n$. □

Théorème 3. *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

Démonstration.

Soit H un sous-groupe distingué non trivial de $\mathfrak{S}_n$. Par la Proposition 1, il suffit que H contienne les 3-cycles. Par la Proposition 2, il suffit que qu'il n'en continent qu'un. Montrons donc que H contient un 3-cycle.

Soit $\sigma \in H \setminus \{Id\}$. Prenons $a \in [\![1, n]\!]$ tel que $b = \sigma(a) \neq a$. Fixons $c \in [\![1, n]\!]$ distinct de $a, b, \sigma(b)$. C'est possible puisque $n \geqslant 5$. Considérons de plus le 3-cycle $\gamma = (a\ b\ c)$ puis $\sigma_2 = \sigma\gamma\sigma^{-1}\gamma^{-1}$.

On a $\sigma_2 \in H$ car $\sigma \in H$ et $\gamma\sigma^{-1}\gamma^{-1} \in H$. On a également que $\sigma_2 = (b\ \sigma(b)\ \sigma(c))(a\ c\ b)$. On va décomposer σ_2 en produit de cycles à supports disjoints, en remarquant que $\mathrm{supp}(\sigma_2) \subseteq \{a, b, c, \sigma(b), \sigma(c)\}$ a au plus 5 éléments. Puisque σ_2 a pour signature 1, en raisonnant sur le type de σ_2, on peut avoir :

- $[1, 1, 1, 1, 1]$ Si $\sigma_2 = Id$, cela entraîne que σ et γ commutent, ce qui est faux car $\sigma\gamma(a) = \sigma(b) \neq c = \gamma\sigma(a)$.
- $[2, 2, 1]$ Si $\sigma_2 = (i\ j)(k\ l)$, alors $\sigma_3 = (i\ j\ k\ l\ m)\sigma_2(i\ j\ k\ l\ m)^{-1}\sigma_2^{-1} \in H$ car H est distingué dans $\mathfrak{A}_n$, et on a $\sigma_3 = (i\ j\ k\ l\ m)(j\ i\ l\ k\ m)^{-1} = (i\ k\ m\ l\ j)$, et on se ramène au cas où le type est [5].
- $[3, 1, 1]$ Si σ_2 est un 3-cycle, c'est bon.
- $[5]$ Si $\sigma_2 = (i\ j\ k\ l\ m)$, alors de même $\sigma_3 = (i\ j\ k)\sigma_2(i\ j\ k)^{-1}\sigma_2^{-1} \in H$, et $\sigma_3 = (i\ j\ k)(j\ l\ k) = (i\ j\ l)$.

Dans tous les cas, on a donc bien trouvé un 3-cycle dans H. Ainsi $H = \mathfrak{A}_n$. □

Références

[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses

Sous-groupes distingués et caractères

Leçons concernées : 103 104 107
Soit G un groupe d'ordre n.

Lemme 1. *Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G de caractère χ. Alors :*

$$\mathrm{Ker}(\rho) = \mathrm{Ker}(\chi) = \{g \in G \,|\, \chi(g) = \chi(e)\}$$

Démonstration.

($\subseteq$) Pour $g \in G$, si $\rho(g) = \rho(1)$ alors $\chi(g) = \mathrm{tr}(Id_V) = \dim V = \chi(e)$. Donc $\mathrm{Ker}(\rho) \subseteq \mathrm{Ker}(\chi)$.

($\supseteq$) Réciproquement, soit $g \in G$ tel que $\chi(g) = \chi(e)$. De plus, ρ est diagonalisable de valeurs propres des racines de l'unité $\zeta_1, \dots, \zeta_d$, avec $d = \dim V$. $\chi(g)$ en est la somme, donc :

$$|\chi(g)| = \left|\sum_{i=1}^{d} \zeta_i\right| \leqslant \sum_{i=1}^{d} |\zeta_i| = d = \dim V = \chi(e)$$

Or, il y a égalité si, et seulement si, il y a égalité dans l'inégalité triangulaire, donc si les ζ_i sont tous égaux. Comme $\sum_{i=1}^{d} \zeta_i = \chi(g) = \dim V$, on a $\zeta_i = 1$ pour tout $i \in [\![1, d]\!]$. Donc $\rho(g)$ est diagonalisable avec pour seule valeur propre 1, c'est donc l'identité.

□

Proposition 2. *Soient $\chi_1, \dots, \chi_k$ les caractères irréductibles de G. Les sous-groupes distingués de G sont les $\bigcap_{i\in I} \mathrm{Ker}(\chi_i)$ où $I \subset [\![1, k]\!]$.*

Démonstration.

($\subseteq$) Une intersection de sous-groupes distingués est distinguée, donc tout sous-groupe du type $\bigcap_{i\in I} \mathrm{Ker}(\chi_i)$ où $I \subset [\![1, k]\!]$ est distingué.

($\supseteq$) Réciproquement, soit N distingué dans G. Soit $\tilde{\rho}$ la représentation régulière du groupe G/N. On l'étend en une représentation ρ de G via la projection $G \to G/N$. Alors :

$$\mathrm{Ker}(\rho) = \left\{g \in G \,\middle|\, \forall\, h \in G, \overline{gh} = \overline{h}\right\} = \left\{g \in G \,\middle|\, \forall\, h \in G, h^{-1}gh \in N\right\} = N$$

Décomposons ρ en somme directe de représentations irréductibles :

$$\rho = \bigoplus_{i=1}^{r} m_i\rho_i \quad \text{avec} \quad \rho_i : G \to GL(V_i) \text{ de caractère } \chi_i$$

avec m_i le nombre de fois où ρ_i apparaît dans ρ. Par le lemme précédent, on a donc :

$$g \in \mathrm{Ker}(\rho) \quad \Leftrightarrow \quad \chi(g) = \chi(e) \quad \Leftrightarrow \quad \sum_{i=1}^{r} m_i\chi_i(g) = \dim V$$

Pour $g \in \mathrm{Ker}(\rho)$, on obtient alors :

$$\dim V = \left|\sum_{i=1}^{r} m_i\chi_i(g)\right| \leqslant \sum_{i=1}^{r} m_i|\chi_i(g)| \leqslant \sum_{i=1}^{r} m_i\chi_i(e) = \sum_{i=1}^{r} m_i \dim V_i = \dim V$$

Ainsi $\sum_{i=1}^{r} m_i|\chi_i(g)| = \sum_{i=1}^{r} m_i\chi_i(e)$, ce qui équivaut à $m_i\chi_i(g) = m_i\chi_i(e)$ pour tout $i \in [\![1, r]\!]$, donc à $g \in \mathrm{Ker}(\chi_i)$ dès que $m_i \neq 0$. Posons $I = \{i \in [\![1, r]\!] \,|\, m_i \neq 0\}$. Alors :

$$N = \bigcap_{i\in I} \mathrm{Ker}(\chi_i)$$

□

Corollaire 3. *G est simple si, et seulement si, pour tout caractère irréductible non trivial de G et tout $g \in G \setminus \{e\}$ on a $\chi(g) \neq \chi(e)$.*

Démonstration.

— On suppose qu'il existe χ un caractère irréductible non trivial et $g \in G \setminus \{e\}$ vérifiant $\chi(g) = \chi(e)$. Alors $\mathrm{Ker}(\chi)$ est un sous-groupe distingué de G par la proposition précédente. $\mathrm{Ker}(\chi)$ n'est pas trivial car il contient $g \neq e$, et est distinct de G car χ n'est pas trivial. Donc G n'est pas simple.

— Réciproquement, si G n'est pas simple, soient H un sous-groupe distingué non trivial de G et $g \in H \setminus \{e\}$. Par la proposition précédente, on peut écrire $H = \bigcap_{i \in I} \mathrm{Ker}(\chi_i)$ avec χ_i des caractères irréductibles de G. Comme H est distinct de G, il existe $i_0 \in I$ tel que χ_{i_0} n'est pas le caractère trivial. Alors $g \in \mathrm{Ker}(\chi_{i_0})$, et $\chi_{i_0}(g) = \chi_{i_0}(e)$.

□

Références

[Pey08] G. Peyré. *L'algèbre discrète de la transformée de Fourier*. Ellipses

Structure des groupes abéliens finis

Leçons concernées : 102 104 107 120
Soit G un groupe abélien d'ordre n.

Proposition 1. *L'application suivante est un isomorphisme de groupe :*

$$\iota : \left| \begin{array}{ccc} G & \longrightarrow & \widehat{\widehat{G}} \\ g & \longmapsto & (\chi \mapsto \chi(g)) \end{array} \right.$$

Démonstration.
Pour $g \in G$, vérifions que $\iota(g) \in \widehat{\widehat{G}}$. En effet, pour $g \in G$, et $\chi_1, \chi_2 \in \widehat{G}$, on a :

$$\iota(g)(\chi_{triv}) = 1 \quad \text{et} \quad \iota(g)(\chi_1\chi_2) = (\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = \iota(g)(\chi_1)\iota(g)(\chi_1)$$

Puis ι est bien un morphisme de groupe, puisque pour $g, h \in G$ et $\chi \in \widehat{G}$ on a :

$$\iota(e)(\chi) = \chi(e) = 1 \quad \text{et} \quad \iota(gh)(\chi) = \chi(gh) = \chi(g)\chi(h) = \iota(g)(\chi)\iota(h)(\chi)$$

Puisque G est abélien, G, $\widehat{G}$ et $\widehat{\widehat{G}}$ ont même cardinal, donc il suffit de montrer l'injectivité de ι. Soit donc $g \in G$ tel que $\iota(g) = 1$. Comme les caractères de $\widehat{G}$ forment une base des fonctions centrales de G dans $\mathbb{C}^\star$, écrivons :

$$\mathbb{1}_g = \sum_{\chi \in \widehat{G}} \langle \mathbb{1}_g | \chi \rangle \, \chi \quad \text{avec} \quad \langle \mathbb{1}_g | \chi \rangle = \frac{1}{|G|} \sum_{h \in G} \mathbb{1}_g(h)\overline{\chi(h)} = \frac{\overline{\chi(g)}}{|G|} = \frac{1}{|G|}$$

Puis, en évaluant en e, il vient que $\mathbb{1}_g(e) = \sum_{\chi \in \widehat{G}} \frac{1}{|G|} \mathbb{1}_g \chi(e) = 1$, donc que $g = e$, d'où l'injectivité de ι. Ainsi, ι est un isomorphisme. □

Lemme 2. *Il existe un élément de G d'ordre l'exposant de G.*

Démonstration.
Vérifions que l'ensemble des ordres des éléments de G est stable par ppcm, puisqu'alors on trouvera un élément d'ordre l'exposant de G en un nombre fini d'itérations. Soient donc $x, y \in G$ d'ordres a et b. Montrons que l'on peut trouver un élément d'ordre $\text{ppcm}(a, b)$. Écrivons :

$$k = \prod_{\substack{p \in \mathcal{P} \\ v_p(a) > v_p(b)}} p^{v_p(a)} \qquad \text{et} \qquad \ell = \prod_{\substack{p \in \mathcal{P} \\ v_p(a) \leqslant v_p(b)}} p^{v_p(b)}$$

Alors $\text{ppcm}(a, b) = k\ell$, et k et ℓ sont premiers entre eux. Posons alors $x' = x^{\frac{a}{k}}$ et $y' = y^{\frac{b}{\ell}}$ qui sont d'ordre k et ℓ respectivement. Alors $x'y'$ est d'ordre $k\ell = \text{ppcm}(a, b)$. □

Proposition 3. *G et $\widehat{G}$ ont même exposant.*

Démonstration.
Soit H un groupe commutatif fini d'exposant d. Si $\chi \in \widehat{H}$, on a alors, pour tout $h \in H$:

$$\chi^d(h) = \chi(h)^d = \chi(h^d) = \chi(e) = 1 \quad \text{donc} \quad \chi^d = 1$$

Ainsi l'exposant de $\widehat{H}$ est plus petit que celui de H. En appliquant à $H = G$ puis à $H = \widehat{G}$, on a $d(\widehat{\widehat{G}}) \leqslant d(\widehat{G}) \leqslant d(G)$. Mais on a en fait égalité puisque $G \cong \widehat{\widehat{G}}$. □

Théorème 4. *Il existe un unique entier ℓ et une unique suite $d_\ell | \cdots | d_2 | d_1$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G et :*

$$G \cong \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Démonstration.
On va raisonner par récurrence sur $|G|$.
Avec la convention $\prod_{i=1}^{0} = \{e\}$, le résultat est évident si $|G| = 1$ en prenant $\ell = 0$.
Supposons donc $|G| > 1$ et le résultat vrai pour tout groupe H tel que $|H| < |G|$. Soit d l'exposant de G. Pour $\chi \in \widehat{G}$ et $g \in G$, $\chi(g)$ est une racine d-ième de l'unité. De plus, on sait que d est l'exposant de $\widehat{G}$, on peut donc trouver $\chi_1 \in \widehat{G}$ tel que χ_1 est d'ordre d. $\chi_1(G)$ est alors un sous-groupe de μ_d, le groupe des racines d-ièmes de l'unité. Par ailleurs, si $|\chi_1(G)| = d' < d$, alors $\chi_1^{d'}(g) = 1$ pour tout $g \in G$, donc χ_1 serait d'ordre $d' < d$, ce qui est faux. Ainsi $\chi_1(G) = \mu_d$.
Soit alors $g_1 \in G$ tel que $\chi_1(g_1) = e^{\frac{2i\pi}{d}}$. On sait alors que g_1 est d'ordre d, et ainsi $H_1 = \langle g_1 \rangle$ est cyclique d'ordre d, donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$.
Vérifions que $G \cong H_1 \times G_1$, où $G_1 = \mathrm{Ker}(\chi_1)$:

- D'une part, on a $\chi(H_1) = \mu_d$, ce qui assure que $\mathrm{Ker}(\chi_1) \cap H_1 = \{e\}$.
- D'autre part, si $g \in G$, il existe $h \in H_1$ tel que $\chi_1(h) = \chi_1(g)$, et alors $gh^{-1} \in \mathrm{Ker}(\chi_1)$, d'où $g = (gh^{-1})h \in G_1H_1$. Ainsi, $G = G_1H_1$.

On applique alors l'hypothèse de récurrence à $\mathrm{Ker}(\chi_1)$ de cardinal strictement inférieur à celui de G. On obtient que $G_1 \cong \prod_{i=2}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$ pour un entier ℓ et une suite $d_\ell | \cdots | d_2 | d_1$ d'entiers supérieurs à 2. Il suffit que vérifier que $d_2 | d_1 = d$. Or d_2 est l'exposant de G_1 et divise d l'exposant de G. □

Références

[Col09] P. Colmez. *Éléments d'analyse et d'algèbre.* Les éditions de l'École Polytechnique

Surjectivité de l'exponentielle de matrice

Leçons concernées : 156 204 214

Lemme 1. *Pour $A \in \mathcal{M}_n(\mathbb{C})$, $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.*

Démonstration.

Soit $A \in \mathcal{GL}_n(\mathbb{C})$.

Étape 1 : Montrons que $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \mathcal{GL}_n(\mathbb{C})$.

($\subseteq$) On a $\mathbb{C}[A]^\times \subseteq \mathbb{C}[A]$, et pour tout $M \in \mathbb{C}[A]^\times$, il existe $N \in \mathbb{C}[A]$ telle que $MN = I_n$, donc $M \in \mathcal{GL}_n(\mathbb{C})$. Finalement, $\mathbb{C}[A]^\times \subseteq \mathbb{C}[A] \cap \mathcal{GL}_n(\mathbb{C})$.

($\supseteq$) Soit $M \in \mathbb{C}[A] \cap \mathcal{GL}_n(\mathbb{C})$. On considère son polynôme caractéristique $\chi_M = \sum_{i=0}^{n} a_i X^i$.
Comme $M \in \mathcal{GL}_n(\mathbb{C})$, on a $a_0 = \det M \neq 0$, et, par le théorème de Cayley-Hamilton, on a $\chi_M(M) = 0$.

$$\chi_M(M) = \sum_{i=0}^{n} a_i M^i = 0 \Leftrightarrow M\left(\sum_{i=1}^{n} a_i M^{i-1}\right) = -a_0 I_n \Leftrightarrow M\left(-\frac{1}{a_0}\sum_{i=1}^{n} a_i M^{i-1}\right) = I_n$$

Ainsi, comme $M \in \mathbb{C}[A]$, on a $-\frac{1}{a_0}\sum_{i=1}^{n} a_i M^{i-1} \in \mathbb{C}[A]$, donc $M \in \mathbb{C}[A]^\times$.

Étape 2 : Montrons que $\exp(\mathbb{C}[A]) \subseteq \mathbb{C}[A]^\times$.

Soit $M \in \exp(\mathbb{C}[A])$, on a donc $M \in \mathcal{GL}_n(\mathbb{C})$, et il existe $N \in C[A]$ tel que $M = \exp(N)$.
Il reste donc à prouver que $\exp(N)$ est un polynôme en A.
L'ensemble $\mathbb{C}[A]$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ qui est de dimension finie, donc $\mathbb{C}[A]$ est fermé.
De plus, pour tout entier n, $\sum_{i=0}^{n} \frac{N^i}{i!} \in \mathbb{C}[A]$.
On en conclut par passage à la limite que $\exp(N) \in \mathbb{C}[A]$.

Étape 3 : Montrons que $\mathbb{C}[A]^\times$ est connexe.

Soient M_1 et M_2 dans $\mathbb{C}[A]^\times$. Pour $z \in \mathbb{C}$, on pose $M(z) = zM_1 + (1-z)M_2 \in \mathbb{C}[A]$, et $P(z) = \det(M(z)) \in \mathbb{C}$.
On cherche un chemin $\gamma : [0,1] \to \mathbb{C}$ continu, avec $\gamma(0) = 0$ et $\gamma(1) = 1$, et tel que $P \circ \gamma$ reste dans $\mathbb{C}^\times$.
Or le polynôme P n'est pas nul ($P(0) \neq 0$), donc P ne s'annule qu'un nombre fini de fois. Notons Z l'ensemble de ses racines. Comme $\mathbb{C} \setminus Z$ est connexe par arcs, puisqu'on a enlevé un nombre fini de points, il existe un chemin γ qui évite les points de Z. Ainsi, il existe un chemin continu qui relie M_1 et M_2 dans $\mathcal{GL}_n(\mathbb{C})$.
Donc $\mathbb{C}[A]^\times$ est connexe par arcs, donc connexe.

Étape 4 : Montrons que $\exp(\mathbb{C}[A])$ est ouvert dans $\mathbb{C}[A]^\times$.

On applique le théorème d'inversion locale à $\exp : \mathbb{C}[A] \to \mathbb{C}[A]^\times$: comme $d_0 \exp = Id$ est inversible, il existe un voisinage ouvert $\mathcal{U}$ de 0 dans $\mathbb{C}[A]$ et un voisinage ouvert $\mathcal{V}$ de I_n dans $\mathbb{C}[A]^\times$, tels que exp soit un $\mathscr{C}^1$-difféomorphisme entre $\mathcal{U}$ et $\mathcal{V}$. En particulier, $\exp(\mathbb{C}[A])$ contient un voisinage de I_n.
Soit maintenant $M \in \mathbb{C}[A]$. On pose $\mathcal{V}_M = \{V \exp(M) \mid V \in \mathcal{V}\}$.
On a $\exp(M) \in \mathcal{V}_M$, et $\mathcal{V}_M$ est ouvert car $\mathcal{V}$ l'est et $\exp(M)$ est inversible.
De plus, pour tout $V \in \mathcal{V}$, il existe $U \in \mathcal{U}$ tel que $V = \exp(U)$, d'où :

$$V \exp(M) = \exp(U)\exp(M) = \exp(U+M) \in \exp(\mathbb{C}[A])$$

Ainsi, $\mathcal{V}_M$ est un voisinage ouvert de $\exp(M)$, donc $\exp(\mathbb{C}[A])$ est un ouvert de $\mathbb{C}[A]^\times$.

Étape 5 : Montrons que $\exp(\mathbb{C}[A])$ est fermé dans $\mathbb{C}[A]^\times$.

On va montrer que $E = \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])$ est un ouvert de $\mathbb{C}[A]^\times$.
Pour cela, montrons que :

$$E = \bigcup_{M \in E} M \exp(\mathbb{C}[A])$$

($\subseteq$) Soit $M \in E$, on a $M = M\exp(0) \in \bigcup_{M \in E} M\exp(\mathbb{C}[A])$.

($\supseteq$) Soient $M \in E$ et $P \in \mathbb{C}[X]$. Si $N = M\exp(P(A))$, alors $M = N\exp(-P(A))$.
Ainsi, si $N \in \exp(\mathbb{C}[A])$, on aura aussi $M \in \exp(\mathbb{C}[A])$, ce qui est exclu, car $M \in E$.
On a donc que $N \notin \exp(\mathbb{C}[A])$, donc $N \in E$.

Or, pour tout $M \in E$, on a $M\exp(\mathbb{C}[A])$ qui est un ouvert de $\mathbb{C}[A]^\times$, car M est inversible est que $\exp(\mathbb{C}[A])$ est ouvert par l'étape précédente. Ainsi E est ouvert dans $\mathbb{C}[A]^\times$ comme réunion d'ouvert, donc $\exp(\mathbb{C}[A])$ est fermé dans $\mathbb{C}[A]^\times$.

Étape 6 : Conclusion.

L'ensemble $\exp(\mathbb{C}[A])$ est ouvert et fermé dans $\mathbb{C}[A]^\times$ qui est connexe.
Or, $I_n = \exp(0)$ est dans $\exp(\mathbb{C}[A])$, qui est donc non vide. On en conclut que $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.

□

Théorème 2. $\exp(\mathcal{M}_n(\mathbb{C})) = \mathcal{GL}_n(\mathbb{C})$

Démonstration.

Soit $A \in \mathcal{GL}_n(\mathbb{C})$, on a donc $A \in \mathbb{C}[A]^\times$, donc par le lemme il existe $P \in \mathbb{C}[X]$ tel que $A = \exp(P(A))$.
On a donc bien un antécédent dans $\mathcal{M}_n(\mathbb{C})$. □

Théorème 3. $\exp(\mathcal{M}_n(\mathbb{R})) = \left\{A^2 \,\middle|\, A \in \mathcal{GL}_n(\mathbb{R})\right\}$

Démonstration.

($\subseteq$) Si $A \in \exp(\mathcal{M}_n(\mathbb{R}))$, on a $B \in \mathcal{M}_n(\mathbb{R})$ telle que $A = \exp(B)$.
Alors $A = \exp\left(\frac{B}{2}\right)^2$, avec $\exp\left(\frac{B}{2}\right) \in \mathcal{GL}_n(\mathbb{R})$.

($\supseteq$) Soit $A \in \mathcal{GL}_n(\mathbb{R})$, on a donc $A \in \mathbb{C}[A]^\times$, et par le lemme il existe $P \in \mathbb{C}[X]$ tel que $A = \exp(P(A))$.
P est complexe, mais A est réelle, donc, en passant au conjugué, on a $A = \exp\left(\overline{P(A)}\right)$. On a alors :

$$A^2 = \exp(P(A))\exp\left(\overline{P(A)}\right) = \exp\left(P(A) + \overline{P(A)}\right) = \exp\left(\left(P + \overline{P}\right)(A)\right)$$

Or $P + \overline{P}$ est à coefficients réels, donc $\left(P + \overline{P}\right)(A)$ est dans $\mathcal{M}_n(\mathbb{R})$.
Donc $\left(P + \overline{P}\right)(A)$ est un antécédent de A pour l'exponentielle.

□

Références

[Zav13] M. Zavidovique. *Un Max de Math.* Calvage et Mounet

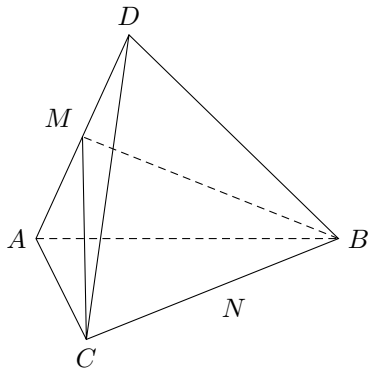
Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre

Leçons concernées : 101 103 104 105 107 161 191

Théorème 1. *Soit $\mathcal{T}$ un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$.*

Démonstration.

On commence par remarquer que $\mathrm{Isom}(\mathcal{T})$ induit une permutation des sommets $\{A, B, C, D\}$ de $\mathcal{T}$.
Ceci donne un morphisme de groupes $\varphi : \mathrm{Isom}(\mathcal{T}) \to \mathfrak{S}_4$.



Soit $g \in \mathrm{Isom}(\mathcal{T})$. Si $\varphi(g) = Id$, alors g préserve les 4 sommets, donc g est l'identité. Ainsi, φ est injectif.
Soit maintenant s la symétrie orthogonale par rapport au plan (BCM). On a alors $\varphi(s) = (AD)$. On peut de la même manière obtenir toutes les transpositions de $\mathfrak{S}_4$. Puisque les transpositions engendrent $\mathfrak{S}_4$, on obtient la surjectivité de φ.
Finalement, φ est bijectif, et $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$. □

Application 2. *La table de caractères de $\mathfrak{S}_4$ est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

Démonstration.

Les deux premières lignes sont remplies facilement. En effet, le caractère trivial et la signature sont des caractères irréductibles.

On note $\rho : \mathfrak{S}_4 \to \mathcal{GL}_3(\mathbb{R})$ la représentation linéaire naturelle de $\mathfrak{S}_4$, qui à $\sigma \in \mathfrak{S}_4$ associe la matrice de la partie linéaire de l'isométrie correspondante dans la base canonique de $\mathbb{R}^3$. On note χ le caractère de ρ.

Pour chaque classe de conjugaison, on choisira une base dans laquelle il sera simple de calculer la matrice de σ, donc son caractère. Il y a cinq classes de conjugaison : l'identité, les 6 transpositions, les 3 doubles transpositions, les 8 3-cycles, et les 6 4-cycles.

— Si $\sigma = Id$, alors $\chi(\sigma) = 3$.

— Si σ est une transposition, prenons par exemple $\sigma = (AD)$. C'est la symétrie par rapport au plan (BCM). Dans la base $(\overrightarrow{MB}, \overrightarrow{MC}, \overrightarrow{MD})$, la matrice de σ est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. On a donc $\chi(\sigma) = 1$.

— Si σ est une double transposition, prenons par exemple $\sigma = (AD)(BC)$. C'est la symétrie par rapport à la droite (MN). Dans la base $(\overrightarrow{MN}, \overrightarrow{MD}, \overrightarrow{NB})$, la matrice de σ est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. On a donc $\chi(\sigma) = -1$.

— Si σ est un 3-cycle, prenons par exemple $\sigma = (BCD)$. C'est la rotation d'axe (AG), où G est le centre de gravité du triangle équilatéral BCD. La matrice de σ est donc semblable à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}$, où $\alpha = \frac{2\pi}{3}$. On a donc $\chi(\sigma) = 1 + 2\cos\alpha = 0$.

— Si σ est un 4-cycle, prenons par exemple $\sigma = (ABCD)$. Si on note O le centre du tétraèdre $\mathcal{T}$, on a $\overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC} + \overrightarrow{OD} = 0$. Dans la base $(\overrightarrow{OA}, \overrightarrow{OB}, \overrightarrow{OC})$, la matrice de σ est $\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$. On a donc $\chi(\sigma) = -1$.

Enfin, χ est irréductible, puisque :

$$\langle \chi, \chi \rangle = (\chi|\chi) = \frac{1}{|\mathfrak{S}_4|}\left(1 \times 3^2 + 6 \times 1^2 + 3 \times (-1)^2 + 8 \times 0^2 + 6 \times (-1)^2\right) = \frac{24}{24} = 1$$

Ainsi χ est irréductible, et on peut l'ajouter à la table de caractère.

Par le même argument, on vérifie que $\varepsilon\chi$ est un caractère irréductible que l'on peut ajouter à la table de caractères. En notant θ le dernier caractère irréductible, on a $24 = 1 + 1 + 3^2 + 3^2 + \theta(Id)^2$, donc $\theta(Id) = 2$. On complète alors la dernière ligne par orthogonalité des colonnes. On trouve ainsi la table de caractères de $\mathfrak{S}_4$. □

Références

[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann

Théorème central limite et intervalle de confiance

Leçons concernées : 261 262 265 266

Lemme 1. *Pour tout $z \in \mathbb{C}$, on a $\left|e^z - \left(1+\frac{z}{n}\right)^n\right| \leqslant e^{|z|} - \left(1+\frac{|z|}{n}\right)^n$.*

Démonstration.

En posant $\alpha_n^k = 1 - \frac{n!}{(n-k)!n^k}\mathbb{1}_{k\leqslant n} \in [0,1]$, on a :

$$\left|e^z - \left(1+\frac{z}{n}\right)^n\right| = \left|\sum_{k\geqslant 0}\frac{z^k}{k!} - \sum_{k=0}^{n}\binom{n}{k}\frac{z^k}{n^k}\right| = \left|\sum_{k=0}^{n}\frac{z^k}{k!}\alpha_n^k\right| \leqslant \sum_{k=0}^{n}\frac{|z|^k}{k!}\alpha_n^k = e^{|z|} - \left(1+\frac{|z|}{n}\right)^n$$

□

Théorème 2 (Théorème central limite)**.** *Soit $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires indépendantes, identiquement distribuées et de carré intégrable. Alors :*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(X_i - \mathbb{E}[X_i]) \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0, \mathrm{Var}(X_i))$$

Démonstration.

Si les $(X_n)_{n\in\mathbb{N}^\star}$ sont constantes presque sûrement, le résultat est clair. On va donc les supposer non constantes presque sûrement. De plus, quitte à remplacer X_i par $\frac{X_i - \mathbb{E}[X_i]}{\mathrm{Var}(X_i)}$, on peut supposer que $\mathbb{E}[X_i] = 0$ et $\mathrm{Var}(X_i) = 1$ pour tout $i \in \mathbb{N}^\star$. Posons alors $S_n = \sum_{i=1}^n X_i$.

Fixons $t \in \mathbb{R}$. Par indépendance et équidistribution, on a alors :

$$\varphi_{\frac{S_n}{\sqrt{n}}}(t) = \mathbb{E}\left[e^{it\frac{S_n}{\sqrt{n}}}\right] = \mathbb{E}\left[e^{i\frac{t}{\sqrt{n}}\sum_{i=1}^n X_i}\right] = \prod_{i=1}^{n}\mathbb{E}\left[e^{i\frac{t}{\sqrt{n}}X_i}\right] = \prod_{i=1}^{n}\varphi_{X_i}\left(\frac{t}{\sqrt{n}}\right)^n = \varphi_{X_1}\left(\frac{t}{\sqrt{n}}\right)^n$$

Comme X_1 est de carré intégrable, φ_{X_1} est deux fois dérivable sur $\mathbb{R}$, avec :

$$\varphi'_{X_1}(0) = i\mathbb{E}[X_1] = 0 \quad \text{et} \quad \varphi''_{X_1}(0) = -\mathbb{E}\left[X_1^2\right] = -\mathrm{Var}(X_1) = -1$$

On obtient alors le développement de Taylor-Young à l'ordre 2 en 0 de φ_{X_1} :

$$\varphi_{X_1}(u) = 1 - \frac{u^2}{2} + \mathrm{o}\left(u^2\right)$$

On a donc :

$$\varphi_{\frac{S_n}{\sqrt{n}}}(t) = \left(1 - \frac{t^2}{2n} + \mathrm{o}\left(\frac{1}{n}\right)\right)^n = \left(1+\frac{z_n}{n}\right)^n \quad \text{où} \quad z_n = -\frac{t^2}{2}\left(1+\mathrm{o}(1)\right) \in \mathbb{C}$$

De plus, par continuité de l'exponentielle, on a :

$$e^{|z_n|} - \left(1+\frac{|z_n|}{n}\right)^n = e^{\frac{t^2}{2}|1+\mathrm{o}(1)|} - e^{n\ln\left(1+\frac{|z_n|}{n}\right)} = e^{\frac{t^2}{2}|1+\mathrm{o}(1)|} - e^{|z_n|(1+\mathrm{o}(1))} \xrightarrow[n\to+\infty]{} e^{\frac{t^2}{2}} - e^{\frac{t^2}{2}} = 0$$

Ainsi, par le Lemme 1, on a :

$$\varphi_{\frac{S_n}{\sqrt{n}}}(t) \underset{n\to+\infty}{\sim} e^{z_n} \xrightarrow[n\to+\infty]{} e^{-\frac{t^2}{2}}$$

Le théorème de Lévy permet alors de conclure que $\frac{S_n}{\sqrt{n}} \xrightarrow[n\to+\infty]{\mathcal{L}} \mathcal{N}(0,1)$. □

Application 3. *Soit $(X_n)_{n\in\mathbb{N}^\star}$ une suite de variables aléatoires indépendantes, identiquement distribuées et de loi $\mathcal{B}(p)$ pour $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\widehat{p_n} = \frac{1}{n}\sum_{k=1}^{n} X_i$. Il s'agit de :*

$$IC_\alpha = \left[\widehat{p_n} \pm \frac{q_{1-\frac{\alpha}{2}}}{2\sqrt{n}}\right]$$

où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Démonstration.

Les $(X_n)_{n\in\mathbb{N}^\star}$ satisfont les hypothèses du théorème central limite, avec $\mathbb{E}[X_1] = p$ et $\mathrm{Var}(X_1) = p(1-p)$. Ainsi :

$$\frac{\sqrt{n}}{\sqrt{p(1-p)}}(\widehat{p_n} - p) = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}\frac{X_i - p}{\sqrt{p(1-p)}} \quad \xrightarrow[n\to+\infty]{\mathcal{L}} \quad \mathcal{N}(0,1)$$

La fonction de répartition de $\mathcal{N}(0,1)$ étant continue, on a, pour tous $a, b \in \mathbb{R}$:

$$\mathbb{P}\left(a \leqslant \frac{\sqrt{n}}{\sqrt{p(1-p)}}(\widehat{p_n} - p) \leqslant b\right) \quad \xrightarrow[n\to+\infty]{} \quad \mathbb{P}(a \leqslant \mathcal{N}(0,1) \leqslant b)$$

En prenant $a = q_{\frac{\alpha}{2}}$ et $b = q_{1-\frac{\alpha}{2}}$, on a $a = -b$, et donc :

$$\mathbb{P}\left(\left|\frac{\sqrt{n}}{\sqrt{p(1-p)}}(\widehat{p_n} - p)\right| \leqslant q_{1-\frac{\alpha}{2}}\right) \quad \xrightarrow[n\to+\infty]{} \quad \mathbb{P}\left(q_{\frac{\alpha}{2}} \leqslant \mathcal{N}(0,1) \leqslant q_{1-\frac{\alpha}{2}}\right) = 1-\alpha$$

Ce que l'on réécrit comme :

$$\mathbb{P}\left(p \in \left[\widehat{p_n} \pm q_{1-\frac{\alpha}{2}}\frac{\sqrt{p(1-p)}}{\sqrt{n}}\right]\right) \quad \xrightarrow[n\to+\infty]{} \quad 1-\alpha$$

On en déduit le résultat annoncé en remarquant que $p(1-p) \leqslant \frac{1}{4}$. □

Références

[BL07] P. Barbe et M. Ledoux. *Probabilité*. EDP Sciences

Théorème de Brouwer en dimension 1 et 2

Leçons concernées : 181 190 203 204 253

Théorème 1. *Toute application continue de la boule unité fermée de $\mathbb{R}^n$ dans elle-même admet (au moins) un point fixe.*

Démonstration.

On note B la boule unité fermée et S la sphère unité de $\mathbb{R}^n$ (pour la norme euclidienne).

Étape 1 : Montrons le résultat en dimension 1.

On va montrer le résultat pour tout intervalle $[a,b]$ de $\mathbb{R}$. Soit $F : [a,b] \to [a,b]$ une fonction continue. On considère la fonction $\varphi : x \mapsto F(x) - x$. φ est alors continue et vérifie $\varphi(a) = F(a) - a \geqslant 0$ et $\varphi(b) = F(b) - b \leqslant 0$. Ainsi, par le théorème des valeurs intermédiaires, φ s'annule au moins une fois sur $[a,b]$, donc F admet au moins un point fixe.

Étape 2 : Si l'énoncé était faux, montrons qu'il existerait une rétraction de la boule sur la sphère.

Soit $F : B \to B$ une application sans point fixe. On note G l'application qui à $x \in B$ associe l'intersection de S avec la demi-droite issue de $F(x)$ passant par x. Pour tout $x \in B$, $G(x)$ vérifie alors :

$$\|G(x)\|^2 = 1 \quad \text{et} \quad G(x) - F(x) = \lambda(x - F(x)) \quad \text{avec} \quad \lambda > 0$$

On obtient alors :

$$P_x(\lambda) = \|G(x)\| - 1 = \lambda^2 \|x - F(x)\|^2 + 2\lambda \langle x - F(x), F(x)\rangle + \|F(x)\|^2 - 1 = 0$$

$P_x(\lambda)$ est alors un polynôme de degré 2 en λ. On a de plus $P_x(0) = \|F(x)\| - 1 \leqslant 0$ et :

$$\begin{aligned} P_x(1) &= \|x - F(x)\|^2 + 2\langle x - F(x), F(x)\rangle + \|F(x)\|^2 - 1 \\ &= \|x\|^2 - 2\langle x, F(x)\rangle + \|F(x)\|^2 + 2\langle x, F(x)\rangle - 2\|F(x)\|^2 + \|F(x)\|^2 - 1 \\ &= \|x\|^2 - 1 \\ &\leqslant 0 \end{aligned}$$

Enfin, comme $\|x - F(x)\|^2 > 0$, on a $\lim_{|\lambda|\to\infty} P_x(\lambda) = +\infty$. Ainsi, P_x admet deux racines réelles distinctes, une sur $]-\infty, 0]$ et une sur $[1, +\infty[$. On a alors un discriminant strictement positif pour tout $x \in B$:

$$\Delta(x) = 4\langle x - F(x), F(x)\rangle^2 - 4\|x - F(x)\|^2 (\|F(x)\|^2 - 1)$$

La racine positive $\lambda(x)$ de P_x est donc :

$$\lambda(x) = \frac{-\langle x - F(x), F(x)\rangle + \sqrt{\langle x - F(x), F(x)\rangle^2 - \|x - F(x)\|^2 (\|F(x)\|^2 - 1)}}{\|x - F(x)\|^2}$$

On en déduit alors que $x \mapsto \lambda(x)$ est continue, donc que G est continue sur B. De plus, $P_x(1) = 0$ si $x \in S$, d'où $\lambda(x) = 1$ dans ce cas et $G(x) = x$ sur S.
Ainsi, G est continue sur B et sa restriction à S est l'identité, c'est donc une rétraction.

Étape 3 : Montrons le résultat en dimension 2.

On considère l'application :

$$\gamma : \left| \begin{array}{ccc} [0,1]\times[0,1] & \longrightarrow & S \\ (s,t) & \longmapsto & \gamma_s(t) = G(s\cos(2\pi t), s\sin(2\pi t)) \end{array} \right.$$

Cette application est continue sur $[0,1]\times[0,1]$ à valeurs dans la sphère unité, et déforme continument γ_0 et γ_1 sans rencontrer l'origine. Leurs indices par rapport à l'origine sont alors égaux. Or, en identifiant $\mathbb{R}^2$ à $\mathbb{C}$, on a :

$$\mathrm{Ind}_{\gamma_0}((0,0)) = \frac{1}{2i\pi}\int_{\gamma_0}\frac{dz}{z} = 0 \quad \text{et} \quad \mathrm{Ind}_{\gamma_1}((0,0)) = \frac{1}{2i\pi}\int_{\gamma_1}\frac{dz}{z} = 1$$

□

Références

[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel*. Cassini

Théorème de Carathéodory

Leçons concernées : 181

Théorème 1 (Carathéodory)**.** *Soient X un espace affine de dimension finie n, et $S \subset X$. Alors* $\mathrm{Conv}(S)$ *est l'ensemble des barycentres à poids positifs d'au plus $n+1$ points pondérés de S.*

Démonstration.

On note $\tilde{S}$ l'ensemble des barycentres à poids positifs de familles finies de points de S.

Étape 1 : Montrons que $\mathrm{Conv}(S) = \tilde{S}$**.**

On sait que $S \subset \mathrm{Conv}(S)$, et que $\mathrm{Conv}(S)$ est convexe. Il vient alors que $\mathrm{Conv}(S)$ contient tous les barycentres à poids positifs de familles finies de points de $\mathrm{Conv}(S)$, et donc tous les barycentres à poids positifs de familles finies de points de S. Ainsi, $\tilde{S} \subset \mathrm{Conv}(S)$.

Réciproquement, montrons maintenant que $\mathrm{Conv}(S) \subset \tilde{S}$. Pour cela, il suffit de montrer que $\tilde{S}$ est convexe. Par définition de $\mathrm{Conv}(S)$, on aura alors le résultat, puisque $S \subset \tilde{S}$. Soient alors $A, B \in \tilde{S}$. Écrivons de plus $A = \mathrm{Bar}(A_i, a_i)_{i\in[\![1,p]\!]}$ et $B = \mathrm{Bar}(B_i, b_i)_{i\in[\![1,q]\!]}$, avec $a_i, b_i > 0$. Soit maintenant $P \in [AB]$. Il existe alors $t \in [0,1]$ tel que $P = \mathrm{Bar}((A,t),(B,1-t))$. Par associativité du barycentre, on obtient :

$$P = \mathrm{Bar}((A,t),(B,1-t)) = \mathrm{Bar}((A_i, ta_i),(B_j,(1-t)b_j))_{i\in[\![1,p]\!],j\in[\![1,q]\!]}$$

Ainsi, $P \in \tilde{S}$ qui est donc convexe, d'où $\mathrm{Conv}(S) \subset \tilde{S}$, puis $\mathrm{Conv}(S) = \tilde{S}$.

Étape 2 : Montrons qu'on peut se restreindre à des familles d'au plus $n-1$ points.

Soit $A \in \mathrm{Conv}(S)$. Écrivons $A = \mathrm{Bar}(A_i, \lambda_i)_{i\in[\![1,p]\!]}$ avec $\lambda_1, \dots, \lambda_p > 0$ et $\sum_{i=1}^p \lambda_i = 1$. Sans perte de généralité, on peut supposer que p est le nombre minimal de termes intervenant dans une écriture comme combinaison convexe de x. Raisonnons par l'absurde, et supposons que $p \geqslant n+2$. La famille $(\overrightarrow{A_1A_i})_{i\in[\![2,p]\!]}$ est liée, car $p-1 \geqslant n+1 > n$. Donc il existe $\alpha_2, \dots, \alpha_p \in \mathbb{R}$ non tous nuls tels que $\sum_{i=2}^p \alpha_i \overrightarrow{A_1A_i} = 0$. En posant $\alpha_1 = -\sum_{i=2}^p \alpha_i$, on a $\sum_{i=1}^p \alpha_i \overrightarrow{OA_i} = 0$ pour tout $O \in X$ et $\sum_{i=1}^p \alpha_i = 0$. Ainsi, pour tout $t \in \mathbb{R}$, on a $A = \mathrm{Bar}(A_i, \lambda_i + t\alpha_i)_{i\in[\![1,p]\!]}$ et $\sum_{i=1}^p \lambda_i + t\alpha_i = 1$. On considère maintenant l'ensemble :

$$F = \{t \in \mathbb{R} \mid \forall\, i \in [\![1,p]\!],\ \lambda_i + t\alpha_i \geqslant 0\} = \left(\bigcap_{\alpha_i>0} \left[-\frac{\lambda_i}{\alpha_i}, +\infty\right[\right) \bigcap \left(\bigcap_{\alpha_i<0} \left]-\infty, -\frac{\lambda_i}{\alpha_i}\right]\right)$$

Ainsi F contient 0 donc est non vide. De plus, il existe au moins un α_i non nul, donc F n'est pas $\mathbb{R}$. Il existe également un autre α_i de signe opposé, car $\sum_{i=1}^p \alpha_i = 0$. Alors F admet une borne inférieure et une borne supérieure, de la forme $-\frac{\lambda_{i_0}}{\alpha_{i_0}}$ pour un certain i_0 et noté t_0. On a alors :

$$A = \mathrm{Bar}(A_i, \lambda_i + t_0\alpha_i)_{i\in[\![1,p]\!]} = \mathrm{Bar}(A_i, \lambda_i + t_0\alpha_i)_{i\in[\![1,p]\!]\setminus\{i_0\}} \qquad \text{avec} \qquad \forall\, i \in [\![1,p]\!],\ \lambda_i + t_0\alpha_i \geqslant 0$$

Cela contredit la minimalité de p. On en déduit que $p \leqslant n+1$, ce qui conclut.

□

Corollaire 2. *Soit S un compact d'un espace euclidien E. Alors* $\mathrm{Conv}(S)$ *est compact.*

Démonstration.

Considérons $K = \left\{(\lambda_1, \dots, \lambda_{n+1}) \in (\mathbb{R}^+)^{n+1} \,\middle|\, \sum_{i=1}^{n+1} \lambda_i = 1\right\}$. C'est un ensemble fermé du compact $[0,1]^{n+1}$, donc c'est un compact. On considère l'application :

$$\varphi : \left| \begin{array}{ccc} K \times S^{n+1} & \longrightarrow & E \\ ((\lambda_1, \dots, \lambda_{n+1}), A_1, \dots, A_{n+1}) & \longmapsto & \sum_{i=1}^{n+1} \lambda_i A_i \end{array} \right.$$

Par le théorème de Carathéodory, $\mathrm{Conv}(S) = \varphi(K \times S^{n+1})$. Or $K \times S^{n+1}$ est compact, comme produit de compacts, et φ est continue, donc $\mathrm{Conv}(S)$ est compact. □

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses

Théorème de Fourier-Plancherel

Leçons concernées : 201 207 208 234 235 250

Théorème 1 (Fourier-Plancherel)**.**

(i) Soit $f \in L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$, alors $\widehat{f} \in L^2(\mathbb{R}^d)$ et $\left\|\widehat{f}\right\|_2 = \|f\|_2$.

(ii) La transformée de Fourier définie sur $L^1 \cap L^2$ se prolonge en une unique application $\mathcal{F}$ sur L^2, proportionnelle à une isométrie, appelé transformée de Fourier-Plancherel.

Démonstration.

(i) Soit $f \in L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$. On note $\tilde{f} : x \mapsto \overline{f(-x)}$ et $g = f * \tilde{f}$.

$$g(x) = \int_{\mathbb{R}} f(x-y)\tilde{f}(y)dy = \int_{\mathbb{R}} f(x-y)\overline{f(-y)}dy = \int_{\mathbb{R}} f(x+y)\overline{f(y)}dy = \langle f_{-x}, f\rangle_{L^2}$$

où, f_{-x} est la translatée de f. Ainsi, g est uniformément continue et $g(0) = \|f\|_2^2$. De plus :

$$\widehat{\tilde{f}}(x) = \int_{\mathbb{R}} \overline{f(-t)}e^{-ixt}dt = \overline{\int_{\mathbb{R}} f(u)e^{-ixu}du} = \overline{\widehat{f}(x)} \qquad \text{puis} \qquad \widehat{g} = \widehat{f * \tilde{f}} = \widehat{f}\widehat{\tilde{f}} = \left|\widehat{f}\right|^2$$

Comme f et $\tilde{f}$ sont dans L^1, alors $\|g\|_1 = \left\|f * \tilde{f}\right\|_1 \leqslant \|f\|_1 \left\|\tilde{f}\right\|_1 = \|f\|_1^2$.
On a également $\|g\|_\infty = \left\|f * \tilde{f}\right\|_\infty \leqslant \|f\|_2 \left\|\tilde{f}\right\|_2 = \|f\|_2^2$ par l'inégalité de Cauchy-Schwarz.

Pour $n \in \mathbb{N}^\star$ et $t \in \mathbb{R}$, on pose $\phi_n(t) = e^{-\frac{|t|}{n}}$. On a alors, pour $x \in \mathbb{R}$:

$$\begin{aligned}\varphi_n(x) = \frac{1}{2\pi}\widehat{\phi_n}(t) &= \frac{1}{2\pi}\int_{\mathbb{R}} e^{-\frac{|t|}{n}-ixt}dt = \frac{1}{2\pi}\left(\int_{\mathbb{R}^-} e^{\frac{t}{n}-ixt}dt + \int_{\mathbb{R}^+} e^{-\frac{t}{n}-ixt}dt\right)\\ &= \frac{1}{2\pi}\left(\frac{1}{\frac{1}{n}-ix} - \frac{1}{-\frac{1}{n}-ix}\right) = \frac{1}{2\pi}\left(\frac{n}{1-inx} + \frac{n}{1+inx}\right) = \frac{1}{\pi}\frac{n}{1+n^2x^2}\end{aligned}$$

On obtient alors :

$$(\varphi_n * g)(0) = \int_{\mathbb{R}} \varphi_n(y)g(-y)\,dy = \frac{1}{2\pi}\int_{\mathbb{R}}\int_{\mathbb{R}} \phi_n(t)e^{-iyt}g(-y)\,dt\,dy$$

Or, on a :

$$\int_{\mathbb{R}}\int_{\mathbb{R}} |\phi_n(t)|\left|e^{-iyt}\right||g(-y)|\,dt\,dy = \|\phi_n\|_1\|g\|_1 < +\infty$$

Donc, par Fubini, on a :

$$(\varphi_n * g)(0) = \frac{1}{2\pi}\int_{\mathbb{R}} \phi_n(t)\int_{\mathbb{R}} e^{-iyt}g(-y)\,dy\,dt = \frac{1}{2\pi}\int_{\mathbb{R}} \phi_n(t)\overline{\widehat{g}(t)}dt = \frac{1}{2\pi}\int_{\mathbb{R}} \phi_n(t)\left|\widehat{f}\right|^2 dt$$

Soit $\varepsilon > 0$. Par uniforme continuité de g, il existe $\eta > 0$ tel que pour tout $x \in \mathbb{R}$, $|x| < \eta$ implique $|g(x) - g(0)| < \varepsilon$, alors :

$$\begin{aligned}|(\varphi_n * g)(0) - g(0)| &= \left|\int_{\mathbb{R}} \varphi_n(y)g(-y)\,dy - \int_{\mathbb{R}} \varphi_n(y)g(0)\,dy\right|\\ &\leqslant \underbrace{\int_{-\eta}^{\eta} \varphi_n(y)\,|g(-y)-g(0)|\,dy}_{\leqslant \varepsilon} + \underbrace{\int_{|y|>\eta} \varphi_n(y)\,|g(-y)-g(0)|\,dy}_{\leqslant 2\|g\|_\infty \int_{|y|>\eta}\varphi_n(y)\,dy \xrightarrow[n\to\infty]{} 0}\end{aligned}$$

Il existe donc un rang à partir duquel $|(\varphi_n * g)(0) - g(0)| \leqslant 2\varepsilon$. Ainsi $\lim\limits_{n\to\infty}(\varphi_n * g)(0) = g(0)$.

Par convergence monotone, comme $0 \leqslant \phi_n(t)\left|\widehat{f}\right|^2 \leqslant \phi_{n+1}(t)\left|\widehat{f}\right|^2$, on a :

$$\lim_{n\to\infty}(\varphi_n * g)(0) = \lim_{n\to\infty}\frac{1}{2\pi}\int_{\mathbb{R}}\phi_n(t)\left|\widehat{f}\right|^2 dt = \frac{1}{2\pi}\int_{\mathbb{R}}\lim_{n\to\infty}\phi_n(t)\left|\widehat{f}\right|^2 dt = \frac{1}{2\pi}\int_{\mathbb{R}}\left|\widehat{f}\right|^2 dt = \frac{1}{2\pi}\left\|\widehat{f}\right\|_2^2$$

Finalement, on a $\widehat{f} \in L^2(\mathbb{R}^d)$, et :

$$\|f\|_2^2 = g(0) = \lim_{n\to\infty}(\varphi_n * g)(0) = \frac{1}{2\pi}\left\|\widehat{f}\right\|_2^2$$

(ii) On désigne par Y l'espace de toutes les transformées de Fourier des fonctions de $L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$.
On vient de démontrer que $Y \subset L^2(\mathbb{R}^d)$. Montrons que Y est dense dans L^2, autrement dit que $Y^\perp = \{0\}$.
Pour tout réel α, et tout $n \in \mathbb{N}^\star$, les fonctions $x \mapsto 2\pi e^{i\alpha x}\phi_n(x)$ sont dans $L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$, et leurs transformée de Fourier sont les fonctions $t \mapsto \varphi_n(\alpha - t)$ qui sont dans Y.
Soit $w \in L^2(\mathbb{R}^d)$. On suppose $w \in Y^\perp$, alors, pour tout réel α, on a :

$$(\varphi_n * w)(\alpha) = \int_{\mathbb{R}}\varphi_n(\alpha - t)w(t)\,dt = 0$$

On en déduit alors que $w = 0$ et ainsi Y est dense dans $L^2(\mathbb{R}^d)$.

On note $\Phi : f \mapsto \widehat{f}$. On a démontré jusqu'ici que Φ est une application d'un sous-espace dense de $L^2(\mathbb{R}^d)$, en fait $L^1(\mathbb{R}^d) \cap L^2(\mathbb{R}^d)$ sur un autre, en fait Y. On en déduit que Φ peut se prolonger en une application $\tilde{\Phi}$ de $L^2(\mathbb{R}^d)$ dans lui-même.

□

Références

[Rud09] W. Rudin. *Analyse réelle et complexe.* Dunod

Théorème de l'élément primitif en caractéristique nulle

Leçons concernées : 125

Théorème 1. *Soit $\mathbb{K}$ un corps de caractéristique nulle, et soit $P \in \mathbb{K}[X]$ irréductible. Si $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$, alors P est à racines simples dans $\mathbb{L}$.*

Démonstration.

Le polynôme P est irréductible, donc $P \wedge P'$ vaut 1 ou P. Par l'absurde, si $P \wedge P' = P$, alors P divise P'. Comme P' est de plus petit degré que P, il vient que $P' = 0$. Donc P est constant puisque la caractéristique de $\mathbb{K}$ est nulle, ce qui est absurde. Ainsi P et P' sont premiers entre eux dans $\mathbb{K}[X]$, donc dans $\mathbb{L}[X]$. □

Théorème 2 (Élément primitif en caractéristique nulle)**.** *Toute extension finie d'un corps de caractéristique nulle est monogène.*

Démonstration.

Soit $\mathbb{L}$ une extension finie d'un corps $\mathbb{K}$. Il existe alors $x_1, \dots, x_n \in \mathbb{L}$ tels que $\mathbb{L} = \mathbb{K}(x_1, \dots, x_n)$. Par une récurrence immédiate, il suffit de montrer le théorème pour $n = 2$.

Soient $x, y \in \mathbb{L}$ tels que $\mathbb{L} = \mathbb{K}(x, y)$. Soient π_x et π_y les polynômes minimaux de x et y. Soit $\mathbb{M}$ le corps de décomposition de $\pi_x \pi_y$. On pose :

$$\pi_x = \prod_{i=1}^{p}(X - x_i) \quad \text{et} \quad \pi_y = \prod_{i=1}^{q}(X - y_i) \quad \text{avec} \quad x = x_1 \quad \text{et} \quad y = y_1$$

Comme π_x et π_y sont irréductibles sur $\mathbb{K}$ qui est de caractéristique nulle, ils sont à racines simples dans $\mathbb{M}$. Ainsi, les x_i sont distincts deux à deux, tout comme les y_i. On pose alors :

$$\Gamma = \left\{ \frac{x_i - x_{i'}}{y_j - y_{j'}} \,\middle|\, 1 \leqslant i, i' \leqslant p, 1 \leqslant j \neq j' \leqslant q \right\}$$

L'ensemble Γ est fini et $\mathbb{K}$ est infini, donc il existe $t \in \mathbb{K}^\star \setminus \Gamma$. Ainsi, tous les $x_i + t y_i$ sont distincts deux à deux.

On pose $z = x + ty$, et on travaille dans $\mathbb{K}(z)[X]$. Alors y est racine de $P(X) = \pi_y(X)$ et de $Q(X) = \pi_x(z - tX)$. Soit $S = \operatorname{pgcd}(P, Q)$. Si S est de degré 1, alors $y \in \mathbb{K}(z)$. Sinon, comme S divise π_y, il existe $j > 2$ tel que y_j soit racine de S, donc racine de Q. Ainsi, il existe $i \in [\![1, p]\!]$ tel que $z - t b_j = a_i$, ce qui est exclu par hypothèse sur t. Ainsi, on a que $y \in \mathbb{K}(z)$ et $x = z - ty \in \mathbb{K}(z)$, donc $\mathbb{K}(x, y) \subseteq \mathbb{K}(z)$. Réciproquement, $\mathbb{K}(z) \subseteq \mathbb{K}(x, y)$ car $z = x + ty$. Finalement, $\mathbb{K}(x, y) = \mathbb{K}(z)$, d'où le résultat.

□

Application 3. *Soient p, q premiers. Alors $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.*

Démonstration.

Soit $a = \sqrt{p} + \sqrt{q}$. On a $\mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$. De plus, $(a - \sqrt{p})^2 = q = a^2 - 2a\sqrt{p} + p$, donc $\sqrt{p} \in \mathbb{Q}(a)$. De même, on a $\sqrt{q} \in \mathbb{Q}(a)$. Ainsi, $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{Q}(a)$, d'où $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. □

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

Théorème de Lax-Milgram et application

Leçons concernées : 205 208 213 222

Théorème 1 (Lax-Milgram)**.** *Soient H un espace de Hilbert, a une forme bilinéaire continue et coercive sur H, et $\ell \in H'$. Alors il existe un unique $u \in H$ tel que, pour tout $v \in H$, $a(u,v) = \ell(v)$.*

Démonstration.

Par le théorème de représentation de Riesz, il existe un unique $w \in H$ tel que, pour tout $v \in H$, on a $\ell(v) = \langle w, v\rangle$. De plus, comme a est linéaire par rapport à sa deuxième variable, on a également l'existence, pour tout $u \in H$, d'un élément $A_u \in H$ tel que, pour tout $v \in H$, on a $a(u,v) = \langle A_u, v\rangle$. Considérons l'application suivante :

$$A : \left| \begin{array}{ccc} H & \longrightarrow & H \\ u & \longmapsto & A_u \end{array} \right.$$

Étape 1 : Montrons que cette application est linéaire et continue.

D'une part, pour tous $u, u' \in H$, tout $\lambda \in \mathbb{R}$ et tout $v \in H$, on a :

$$\langle A_{u+\lambda u'} - A_u - \lambda A_{u'}, v\rangle = \langle A_{u+\lambda u'}, v\rangle - \langle A_u, v\rangle - \lambda \langle A_{u'}, v\rangle = a(u+\lambda u', v) - a(u,v) - \lambda a(u', v) = 0$$

Ainsi A est linéaire. D'autre part, par continuité de a, il existe $M > 0$ tel que, pour tout $u, v \in H$, on a $|a(u,v)| \leqslant M \|u\| \|v\|$. On a alors :

$$\|Au\|^2 = \langle A_u, A_u\rangle = A(u, A_u) \leqslant M \|u\| \|Au\|$$

Donc $\|Au\| \leqslant M \|u\|$, et A est continue.

Étape 2 : Montrons qu'il existe un unique $u \in H$ tel que $A_u = w$.

Par coercivité de a, il existe $\nu > 0$ tel que, pour tout $u \in H$, on a $a(u,u) \geqslant \nu \|u\|$. En posant $\eta = \frac{\nu}{M^2} > 0$, on considère l'application :

$$T : \left| \begin{array}{ccc} H & \longrightarrow & H \\ u & \longmapsto & u - \eta(Au - w) \end{array} \right.$$

On a ainsi $A_u = w$ si, et seulement si, u est un point fixe de T. Or, pour tous $u, v \in H$, on a :

$$\begin{aligned} \|Tu - Tv\|^2 &= \|u - v - \eta(Au - Av)\|^2 \\ &= \|u - v\|^2 - 2\eta \langle u - v, A(u-v)\rangle + \eta^2 \|A(u-v)\|^2 \\ &= \|u - v\|^2 - 2\eta a(u - v, u - v) + \eta^2 \|A(u-v)\|^2 \\ &\leqslant \|u - v\|^2 \left(1 - 2\eta\nu + \eta^2 M^2\right) \\ &\leqslant \|u - v\|^2 \left(1 - \frac{\nu^2}{M^2}\right) \end{aligned}$$

Comme $1 - \frac{\nu^2}{M^2} < 1$, T est contractante. De plus, comme H est un espace de Hilbert, c'est en particulier un espace complet. Par le théorème de point fixe de Picard, T admet un unique point fixe $u \in H$. Ainsi, il existe un unique $u \in H$ tel que, pour tous $u, v \in H$, on a $a(u,v) = \langle A_u, v\rangle = \langle w, v\rangle = \ell(v)$.

□

Application 2. *Pour $f \in L^2(\Omega)$, l'équation de Poisson $-\Delta u = f$ avec $u = 0$ sur $\partial\Omega$ admet une unique solution faible.*

Démonstration.

La formulation variationnelle de ce problème est, pour tout $v \in H_0^1(\Omega)$:

$$\int_\Omega -\Delta u \cdot v = \int_\Omega fv \quad \Leftrightarrow \quad \int_\Omega \nabla u \cdot \nabla v = \int_\Omega fv \quad \Leftrightarrow \quad \langle \nabla u, \nabla v \rangle_{L^2} = \langle f, v \rangle_{L^2}$$

En posant $a(u,v) = \langle \nabla u, \nabla v \rangle_{L^2}$ et $\ell(v) = \langle f, v \rangle_{L^2}$, on a facilement que a est une forme bilinéaire continue, et que ℓ est une forme linéaire continue grâce à l'inégalité de Cauchy-Schwarz et au fait que $\|.\|_{L^2} \leqslant \|.\|_{H^1}$. De plus, grâce à l'inégalité de Poincaré, il existe $C > 0$ tel que, pour tout $u \in H$, on a :

$$a(u,u) = \|\nabla u\|_{L^2}^2 = \frac{1}{2}\|\nabla u\|_{L^2}^2 + \frac{1}{2}\|\nabla u\|_{L^2}^2 \geqslant \frac{1}{2}\|\nabla u\|_{L^2}^2 + \frac{C^2}{2}\|u\|_{L^2}^2 = \frac{\min(1, C^2)}{2}\|u\|_{H^1}^2$$

Ainsi, a est coercive. Par le théorème de Lax-Milgram, il existe une unique solution faible à l'équation de Poisson. □

Références

[Bre87] H. Brezis. *Analyse fonctionelle.* Masson

Théorème de Riesz-Fischer

Leçons concernées : 201 205 208 234 241

Théorème 1 (Riesz-Fischer). *Pour tout $1 \leqslant p \leqslant +\infty$, L^p est un espace de Banach.*

Démonstration.

Étape 1 : Supposons que $p = \infty$.

Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans L^∞, montrons que cette suite converge dans L^∞. Par définition, on a :

$$\forall\, k \in \mathbb{N}^\star,\ \exists\, N_k \in \mathbb{N},\ \forall\, m,n \geqslant N_k,\ \|f_n - f_m\|_\infty \leqslant \frac{1}{k}$$

Pour tout $k \in \mathbb{N}^\star$, il existe donc un ensemble E_k négligeable tel que :

$$\forall\, x \in \Omega \setminus E_k,\ \forall\, m,n \geqslant N_k,\ |f_m(x) - f_n(x)| \leqslant \frac{1}{k}$$

Enfin, en posant $E = \bigcup_{k\in\mathbb{N}^\star} E_k$, on voit que, pour tout $x \in \Omega \setminus E$, la suite $(f_n(x))_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{R}$. On note donc $f(x) = \lim_{n\to\infty} f_n(x)$. En faisant tendre m vers $+\infty$, on obtient :

$$\forall\, x \in \Omega \setminus E_k,\ \forall\, n \geqslant N_k,\ |f(x) - f_n(x)| \leqslant \frac{1}{k}$$

Ainsi, $f \in L^\infty$ et, pour tout $n \geqslant N_k$, $\|f - f_n\|_{L^\infty} \leqslant \frac{1}{k}$. Par conséquent, $\lim_{n\to\infty} \|f - f_n\|_{L^\infty} = 0$.

Étape 2 : Supposons que $1 \leqslant p < \infty$.

Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans L^p. On extrait une sous-suite (f_{n_k}) telle que :

$$\forall\, k \in \mathbb{N},\ \left\|f_{n_{k+1}} - f_{n_k}\right\|_{L^p} \leqslant \frac{1}{2^k}$$

Posons $\tilde{f}_k = f_{n_k}$. On va montrer que $(\tilde{f}_k)_{k\in\mathbb{N}}$ converge dans L^p. Pour tout $n \in \mathbb{N}$, on considère :

$$g_n(x) = \sum_{k=1}^{n} |\tilde{f}_{k+1}(x) - \tilde{f}_k(x)|$$

On obtient alors :

$$\|g_n\|_{L^p} \leqslant \sum_{k=1}^{n} \left\|\tilde{f}_{k+1} - \tilde{f}_k\right\|_{L^p} \leqslant \sum_{k=1}^{n} \frac{1}{2^k} \leqslant 1$$

On déduit du théorème de convergence monotone que $g_n(x)$ converge presque partout sur Ω vers une limite finie, notée $g(x)$, avec $g \in L^p$. D'autre part, on a, pour tous $m \geqslant n \geqslant 2$:

$$|\tilde{f}_m(x) - \tilde{f}_n(x)| \leqslant \sum_{k=n+1}^{m} |\tilde{f}_k(x) - \tilde{f}_{k-1}(x)| \leqslant g_m(x) - g_n(x) \leqslant g(x) - g_n(x) \quad \xrightarrow[n\to+\infty]{} \quad 0$$

Il en résulte que, pour presque tout $x \in \Omega$, $(\tilde{f}_n(x))_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{R}$, donc converge vers une limite finie, notée $f(x)$. Or, on a, pour tout $n \geqslant 2$, $|f(x) - \tilde{f}_n(x)| \leqslant g(x)$. En particulier, $|f| \leqslant g + |\tilde{f}_k|$, donc $f \in L^p$. Par convergence dominée, on obtient $\lim_{k\to\infty} \left\|f - \tilde{f}_k\right\|_{L^p} = 0$. Ainsi $(f_n)_{n\in\mathbb{N}}$ est une suite de Cauchy dans L^p admettant une valeur d'adhérence $f \in L^p$, donc converge vers $f \in L^p$.

□

Références

[Bre87] H. Brezis. *Analyse fonctionelle.* Masson

Théorème de Sophie Germain

Leçons concernées : 120 121 126 142

Théorème 1. *Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p+1$ soit premier. Il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0[p]$ et $x^p + y^p + z^p = 0$.*

Démonstration.

Raisonnons par l'absurde. On suppose qu'il existe un triplet $(x,y,z) \in \mathbb{Z}^3$ solution.

Étape 1 : Montrons qu'on peut supposer x, y et z premiers entre eux deux à deux.

Quitte à diviser par $\text{pgcd}(x,y,z)$, on suppose que $\text{pgcd}(x,y,z) = 1$. Si alors $\text{pgcd}(x,y) > 1$, soit p_0 un diviseur premier de x et y. Alors $z^p = -(x^p + y^p)$ est divisible par p_0, et donc $\text{pgcd}(x,y,z) \geqslant p_0$, ce qui est contradictoire. Ainsi, on a $\text{pgcd}(x,y) = \text{pgcd}(x,z) = \text{pgcd}(y,z) = 1$.

Étape 2 : Soit $m \in \mathbb{Z}$ non divisible par $q = 2p+1$. Montrons que $m^p \equiv \pm 1 \mod q$.

Par le petit théorème de Fermat, on a :

$$(m^p)^2 \equiv m^{2p} \equiv m^{q-1} \equiv 1 \mod q$$

Comme q est premier, $\mathbb{Z}/q\mathbb{Z}$ est un corps, donc il est intègre, et $m^p \equiv \pm 1 \mod q$.

Étape 3 : Montrons qu'un seul des trois entiers x, y, z est divisible par q

Si $q \nmid xyz$, alors $x^p, y^p, z^p \equiv \pm 1 \mod q$ par le point précédent, et $0 = x^p + y^p + z^p \equiv \pm 1$ ou $\pm 3 \mod q$, ce qui est absurde car q est impair et supérieur à 5. Ainsi $q \mid xyz$, et supposons par exemple que $q \mid x$. Comme on a vu que $\text{pgcd}(x,y) = \text{pgcd}(x,z) = 1$, on a donc que $q \nmid yz$.

Étape 4 : Écrivons $y+z$, $x+z$, $x+y$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ comme des puissances de p.

En notant $u = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$, on a :

$$-x^p = y^p + z^p = y^p - (-z)^p = (y+z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = (y+z)u$$

Montrons par l'absurde que $\text{pgcd}(y+z,u) = 1$. Soit alors p_0 un diviseur premier de $\text{pgcd}(y+z,u)$. Comme $p_0^2 \mid x^p$, on a donc $p_0 \mid x$. Or, comme $y \equiv -z \mod p_0$, on a :

$$0 \equiv u \equiv \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \mod p_0$$

Donc $p_0 \mid py^{p-1}$, et ainsi :

(i) soit $p_0 \mid p$, mais alors $p_0 = p$, ce qui n'est pas possible puisque $p \nmid x$.

(ii) soit $p_0 \mid y$, mais alors $1 = \text{pgcd}(x,y) \geqslant p_0$, ce qui est absurde.

Ainsi $\text{pgcd}(y+z,u) = 1$. Comme le produit de u et $y+z$ est une puissance de p, et que ces deux termes sont premiers entre eux, chacun des deux est une puissance de p. On a ainsi l'existence de $a, \alpha \in \mathbb{Z}$ tels que $y+z = a^p$ et $u = \alpha^p$. Le même raisonnement donne l'existence de $b, c \in \mathbb{Z}$ tels que $x+z = b^p$ et $x+y = c^p$.

Étape 5 : Conclusion.

On obtient ainsi le système suivant grâce aux étapes précédentes :

$$\begin{cases} b^p + c^p - a^p = 2x \equiv 0 & \mod q \\ c^p \equiv y \equiv \pm 1 & \mod q \\ b^p \equiv z \equiv \pm 1 & \mod q \end{cases}$$

Si $q \nmid a$, alors $a^p \equiv \pm 1 \mod q$, donc $b^p + c^p - a^p \equiv \pm 1$ ou $\pm 3 \mod q$, ce qui est encore contradictoire. Ainsi $q \mid a$, et alors $y \equiv -z \mod q$. Comme par ailleurs $y \equiv \pm 1 \mod q$, il vient que :

$$\alpha^p = u \equiv py^{p-1} \equiv p \mod q$$

Or, $a^p \equiv 0$ ou $\pm 1 \mod q$, ce qui est contradictoire. Finalement, il n'existe pas de triplet satisfaisant.

□

Références

[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini

Théorème de Wedderburn

Leçons concernées : 101 123

Théorème 1 (Wedderburn)**.** *Tout corps fini est commutatif.*

Démonstration.

Soit $\mathbb{K}$ un corps fini. Notons $Z = \{a \in \mathbb{K} \mid \forall\, x \in \mathbb{K}, ax = xa\}$ le centre de $\mathbb{K}$. C'est un sous-corps commutatif de $\mathbb{K}$ de cardinal $q \geqslant 2$, et comme $\mathbb{K}$ est un Z-espace vectoriel, on a $|\mathbb{K}| = q^n$ avec $n \in \mathbb{N}^\star$.

Supposons par l'absurde que $\mathbb{K}$ n'est pas commutatif, donc que $n > 1$. Alors $\mathbb{K}^\times$ agit sur lui-même par conjugaison. Pour tout $x \in \mathbb{K}^\times$, on note $\omega(x)$ l'orbite de x. On pose par ailleurs $\mathbb{K}_x = \{y \in \mathbb{K} \mid yx = xy\}$, sous-corps de Z et de $\mathbb{K}$, qui est alors de cardinal q^{d_x} avec $d_x \mid n$.

Le stabilisateur de $x \in \mathbb{K}^\times$ est $\{y \in \mathbb{K}^\times \mid yx = xy\} = \mathbb{K}_x^\times$. Le cardinal de son orbite $\omega(x)$ est alors :

$$|\omega(x)| = \frac{|\mathbb{K}^\times|}{|\mathbb{K}_x^\times|} = \frac{q^n - 1}{q^{d_x} - 1}$$

En notant θ un système de représentants des orbites, l'équation aux classes donne alors :

$$q^n - 1 = |\mathbb{K}^\times| = |Z^\times| + \sum_{x \in \theta \setminus Z^\times} |\omega(x)| = |Z^\times| + \sum_{x \in \theta \setminus Z^\times} \frac{|\mathbb{K}^\times|}{|\mathbb{K}_x^\times|} = q - 1 + \sum_{x \in \theta \setminus Z^\times} \frac{q^n - 1}{q^{d_x} - 1}$$

Or, pour $x \in \theta \setminus Z^\times$, on a $d_x \neq n$, car sinon on a $x \in Z^\times$. On peut donc écrire :

$$q^n - 1 = q - 1 + \sum_{\substack{d \mid n \\ d \neq n}} \lambda_d \frac{q^n - 1}{q^d - 1}$$

où λ_d désigne le nombre de $x \in \theta \setminus Z^\times$ tels que $|\omega(x)| = q^d - 1$.

Si $d \mid n$ et $d \neq n$, on a :

$$X^n - 1 = \Phi_n \prod_{\substack{e \mid n \\ e \neq n}} \Phi_e = \Phi_n \left(\prod_{e \mid d} \Phi_e \right) \left(\prod_{\substack{e \mid n \\ e \neq n, e \nmid d}} \Phi_e \right) = \Phi_n (X^d - 1) \left(\prod_{\substack{e \mid n \\ e \neq n, e \nmid d}} \Phi_e \right)$$

Ainsi, Φ_n divise $\frac{X^n - 1}{X^d - 1}$ dans $\mathbb{Z}[X]$, puis $\Phi_n(q)$ divise $q - 1$. En particulier, $|\Phi_n(q)| \leqslant q - 1$. Or $n \neq 1$, donc :

$$|\Phi_n(q)| = \prod_{\xi \in \mu_n(\mathbb{C})} |q - \xi| > \prod_{i=1}^{\varphi(n)} |q - 1| \geqslant |q - 1|$$

Cela est absurde. Le corps fini $\mathbb{K}$ est donc commutatif.

□

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

Théorème de Weierstrass

Leçons concernées : 201 203 209 228 241

Théorème 1 (Weierstrass). *L'ensemble des polynômes sur $[a,b]$ est dense dans $(\mathcal{C}^0([a,b],\mathbb{R}),\|.\|_\infty)$.*

Démonstration.

Fixons $\varepsilon > 0$, $f : [a,b] \to \mathbb{R}$ continue à support compact, et $(\chi_n)_{n\in\mathbb{N}}$ une approximation de l'unité.

Étape 1 : Montrons que la suite $(f * \chi_n)$ converge uniformément vers f.

Comme f est à support compact, elle est uniformément continue par le théorème de Heine. Il existe donc $\delta > 0$ tel que, pour tous $x, y \in \mathbb{R}$, $|x-y| < \delta$ entraîne $|f(x) - f(y)| < \varepsilon$. Par ailleurs, on peut choisir $N \in \mathbb{N}$ tel que, pour tout $n \geqslant N$, $\int_{|t|>\delta} \chi_n(t)\,dt < \varepsilon$. Alors, pour $n \geqslant N$, on a :

$$\begin{aligned}
|(\chi_n * f)(x) - f(x)| &= \left| \int_{\mathbb{R}} \chi_n(t) f(x-t)\,dt - f(x) \right| \\
&= \left| \int_{\mathbb{R}} \chi_n(t)(f(x-t) - f(x))\,dt \right| \\
&\leqslant \int_{\mathbb{R}} \chi_n(t)\,|f(x-t) - f(x)|\,dt \\
&\leqslant \int_{-\delta}^{\delta} \chi_n(t)\,|f(x-t) - f(x)|\,dt \; + \int_{|t|>\delta} \chi_n(t)\,|f(x-t) - f(x)|\,dt \\
&\leqslant \varepsilon \int_{-\delta}^{\delta} \chi_n(t)\,dt \; + 2\,\|f\|_\infty \int_{|t|>\delta} \chi_n(t)\,dt \\
&\leqslant \varepsilon \int_{\mathbb{R}} \chi_n(t)\,dt \; + 2\varepsilon\,\|f\|_\infty \int_{\mathbb{R}} \chi_n(t)\,dt \\
&\leqslant (1 + 2\,\|f\|_\infty)\varepsilon
\end{aligned}$$

Ainsi, $\|(\chi_n * f) - f\|_\infty < (1 + 2\,\|f\|_\infty)\varepsilon$, d'où la convergence uniforme.

Étape 2 : On suppose f à support dans $\left[-\frac{1}{2}, \frac{1}{2}\right]$.

On considère, pour tout $n \in \mathbb{N}$, $a_n = \int_{-1}^{1} (1-t^2)^n\,dt$, et P_n la fonction définie par :

$$P_n : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & \begin{cases} \frac{(1-t^2)^n}{a_n} & \text{si } |t| \leqslant 1 \\ 0 & \text{sinon} \end{cases} \end{array} \right.$$

On a que P_n est une approximation de l'unité. Montrons que $P_n * f$ est un polynôme sur $\left[-\frac{1}{2}, \frac{1}{2}\right]$. On a :

$$(P_n * f)(x) = \int_{-\frac{1}{2}}^{\frac{1}{2}} P_n(x-t) f(t)\,dt$$

Pour $x \in \left[-\frac{1}{2}, \frac{1}{2}\right]$, on a ainsi $|x-t| \leqslant 1$, et :

$$P_n(x-t) = \frac{(1-(x-t)^2)^n}{a_n} = \sum_{k=0}^{2n} q_k(t) x^k$$

avec q_k un polynôme. Ainsi :

$$(P_n * f)(x) = \sum_{k=0}^{2n} x^k \int_{-\frac{1}{2}}^{\frac{1}{2}} q_k(t) f(t)\, dt$$

Donc $P_n * f$ est bien un polynôme sur $\left[-\frac{1}{2}, \frac{1}{2}\right]$.

Étape 3 : Cas général.

Soit $f : [a, b] \to \mathbb{R}$ continue. On considère $c < d$ dans $\mathbb{R}$ tels que $[a, b] \subset]c, d[$. On prolonge f par :

— Une fonction affine sur $[c, a]$, valant 0 en c et $f(a)$ en a.

— Une fonction affine sur $[b, d]$, valant $f(b)$ en b et 0 en d.

On obtient ainsi une fonction continue à support dans $[c, d]$. On considère la fonction :

$$\varphi : \left| \begin{array}{ccc} \left[-\frac{1}{2}, \frac{1}{2}\right] & \longrightarrow & [c, d] \\ x & \longmapsto & (d-c)x + \frac{c+d}{2} \end{array} \right.$$

On obtient que $f \circ \varphi^{-1}$ est limite uniforme d'une suite de polynômes ψ_n par les étapes précédentes, donc f est limite uniforme de la suite de polynômes $\psi_n \circ \varphi$.

□

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses

Théorème des deux carrés

Leçons concernées : 121 122 126

On note $\Sigma = \left\{a^2 + b^2 \in \mathbb{N} \,\middle|\, a, b \in \mathbb{N}\right\}$ l'ensemble des entiers s'écrivant comme somme de deux carrés. On note également $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss. Soit $N : \mathbb{Z}[i] \to \mathbb{N}$ l'application définie par $N(z) = a^2 + b^2$ pour $z = a + ib \in \mathbb{Z}[i]$. On remarque que $\mathbb{Z}[i]$ est un anneau intègre car inclus dans $\mathbb{C}$.

Proposition 1. $(\mathbb{Z}[i])^\star = \{\pm 1, \pm i\}$

Démonstration.

Soit $z = a + ib \in (\mathbb{Z}[i])^\times$. On a $N(z)N(z^{-1}) = N(zz^{-1}) = 1$. Comme $N(z), N(z^{-1}) \in \mathbb{N}$, on a $N(z) = 1$. On en déduit que $a^2 + b^2 = 1$, et donc que si $a = 0$ alors $b = \pm 1$, et inversement. Donc $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$. □

Théorème 2. *$\mathbb{Z}[i]$ est euclidien relativement à N, donc principal.*

Démonstration du théorème.

Pour $z, t \in \mathbb{Z}[i] \setminus \{0\}$, on écrit $\frac{z}{t} = x + iy$. Soit $q = a + ib$ où a et b sont les entiers les plus proches de x et y.

$$\left|\frac{z}{t} - q\right| = |(x - a) + i(y - b)| = \sqrt{(x - a)^2 + (y - b)^2} \leqslant \sqrt{\frac{1}{4} + \frac{1}{4}} = \frac{\sqrt{2}}{2} < 1$$

Posons $r = z - qt \in \mathbb{Z}[i]$. On a $|r| = |t| \left|\frac{z}{t} - q\right| < |t|$, donc $N(r) < N(t)$. Alors $z = qt + r$ avec $N(r) < N(t)$. Ainsi $\mathbb{Z}[i]$ est un anneau euclidien relativement à N, donc c'est un anneau principal. □

Lemme 3. *Σ est stable par produit.*

Démonstration.

On a $n \in \Sigma$ si, et seulement si, il existe $z \in \mathbb{Z}[i]$ tel que $n = N(z)$. Soient $n, n' \in \Sigma$ et $z = a + ib, z' = a' + ib' \in \mathbb{Z}[i]$ tels que $n = N(z)$ et $n' = N(z')$. Alors $nn' = N(z)N(z') = N(zz') \in \Sigma$. □

Lemme 4. *Soit p un nombre premier impair. Alors $p \in \Sigma$ si, et seulement si, p est réductible dans $\mathbb{Z}[i]$.*

Démonstration.

Soit $p \in \Sigma$ premier. On écrit $p = a^2 + b^2 = (a + ib)(a - ib)$. Or $N(a + ib) = N(a - ib) = p > 1$, donc $a + ib$ et $a - ib$ ne sont pas inversibles, et p est réductible.

Réciproquement, soit $p = zz'$ avec z et z' non inversibles. Alors $p^2 = N(p) = N(zz') = N(z)N(z')$. Ainsi, $N(z) = N(z') = p$, car $N(z) \neq 1 \neq N(z')$. Comme $z = a + ib$ avec $a, b \in \mathbb{Z}$, on a $p = N(z) = a^2 + b^2 \in \Sigma$. □

Théorème 5. *Soit p un nombre premier. Alors $p \in \Sigma$ si, et seulement si, $p = 2$ ou $p \equiv 1$ [4].*

Démonstration.

On sait déjà que $2 \in \Sigma$. Supposons donc que p est un nombre premier impair.

Si $p = a^2 + b^2$, a ou b est impair, et alors $p \equiv (2k + 1)^2 \equiv 1$ [4].

Réciproquement, soit $p \in \Sigma$. Alors p est non irréductible dans $\mathbb{Z}[i]$ principal, donc (p) n'est pas un idéal premier, et $\mathbb{Z}[i]/(p)$ n'est pas intègre. Or, on a :

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[X]/(X^2+1) \cong \mathbb{Z}[X]/(p, X^2+1) \cong (\mathbb{Z}[X]/(p))/(X^2+1) \cong \mathbb{F}_p[X]/(X^2+1)$$

Ainsi, X^2+1 n'est pas irréductible sur $\mathbb{F}_p$, donc admet une racine dans $\mathbb{F}_p$. Alors -1 est un carré dans $\mathbb{F}_p$, donc $(-1)^{\frac{p-1}{2}} = 1$, ce qui équivaut à $p \equiv 1$ [4]. □

Corollaire 6. *Soit $n \in \mathbb{N}^\star$. Soit $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$ sa décomposition en produit de facteurs premiers. Alors $n \in \Sigma$ si, et seulement si, pour tout $p \in \mathcal{P}$ tel que $p \mid n$ et $p \equiv 3$ [4] on a $2 \mid v_p(n)$.*

Démonstration.

Si $v_p(n)$ est pair pour tout $p \in \mathcal{P}$ tel que $p \mid n$ et $p \equiv 3$ [4], alors $n \in \Sigma$ car Σ est stable par produit.

Réciproquement, soit $p \equiv 3$ [4]. Alors p est irréductible dans $\mathbb{Z}[i]$. Si p divise $n = a^2+b^2 = (a+ib)(a-ib)$, alors p divise par exemple $a+ib$, donc $p \mid a$ et $p \mid b$, et $p^2 \mid n$. On itère le processus avec $n' = \frac{n}{p^2}$ tant que $p \mid n'$, et on obtient que $v_p(n)$ est pair. □

Références

[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses

Théorèmes d'Abel angulaire et taubérien faible

Leçons concernées : 207 230 235 241 243

Théorème 1 (Abel angulaire)**.** *Soit $\sum a_n z^n$ une série entière de rayon de convergence 1 telle que $\sum a_n$ converge. On note f sa somme et :*

$$\Delta_\theta = \left\{ z \in \mathbb{C} \;\middle|\; 1 - z = \rho e^{i\varphi},\ \rho > 0,\ |\varphi| < \theta \right\} \quad \textit{pour} \quad 0 \leqslant \theta < \frac{\pi}{2}$$

Alors :

$$\lim_{\substack{z \to 1 \\ z \in \Delta_\theta}} f(z) = \sum_{n=0}^{\infty} a_n$$

Démonstration.

Soit $N \in \mathbb{N}$. On note $R_n = \sum_{k=n+1}^{\infty} a_k$, et on effectue une transformation d'Abel :

$$\begin{aligned}
\sum_{n=0}^{N} a_n z^n - \sum_{n=0}^{N} a_n &= \sum_{n=0}^{N} a_n (z^n - 1) = \sum_{n=1}^{N} (R_{n-1} - R_n)(z^n - 1) \\
&= \sum_{n=1}^{N} R_{n-1}(z^n - 1) - \sum_{n=1}^{N} R_n (z^n - 1) = \sum_{n=0}^{N-1} R_n (z^{n+1} - 1) - \sum_{n=0}^{N} R_n (z^n - 1) \\
&= \sum_{n=0}^{N-1} R_n (z^{n+1} - z^n) - R_N (z^N - 1) = (z-1) \sum_{n=0}^{N-1} R_n z^n - R_N (z^N - 1)
\end{aligned}$$

En faisant tendre N vers $+\infty$, et en notant $\ell = \sum_{n=0}^{\infty} a_n$, on obtient :

$$f(z) - \ell = (z-1) \sum_{n=0}^{\infty} R_n z^n$$

Soit maintenant $\varepsilon > 0$, et soit $N \in \mathbb{N}$ tel que $|R_n| < \varepsilon$ pour tout $n > N$. Pour $|z| < 1$, on a :

$$\begin{aligned}
|f(z) - \ell| = |z-1| \left| \sum_{n=0}^{N} R_n z^n + \sum_{n=N+1}^{\infty} R_n z^n \right| &\leqslant |z-1| \left| \sum_{n=0}^{N} R_n z^n \right| + |z-1| \left| \sum_{n=N+1}^{\infty} R_n z^n \right| \\
&\leqslant |z-1| \sum_{n=0}^{N} |R_n| |z|^n + |z-1| \sum_{n=N+1}^{\infty} |R_n| |z|^n \leqslant |z-1| \sum_{n=0}^{N} |R_n| + \varepsilon \frac{|z-1|}{1-|z|}
\end{aligned}$$

Soit $z = 1 - \rho e^{i\varphi} \in \Delta_\theta$, avec $\rho > 0$ et $|\varphi| < \theta$. Alors $|z|^2 = 1 - 2\rho\cos\varphi + \rho^2$, et si $\rho \leqslant \cos\theta$, on a :

$$\frac{|z-1|}{1-|z|} = \frac{|z-1|}{1-|z|^2}(1+|z|) = \frac{\rho}{2\rho\cos\varphi - \rho^2}(1+|z|) \leqslant \frac{2}{2\cos\varphi - \rho} \leqslant \frac{2}{2\cos\theta - \cos\theta} \leqslant \frac{2}{\cos\theta}$$

À présent, si $\alpha > 0$ est tel que $\alpha \sum_{n=0}^{N} |R_n| < \varepsilon$, on voit que si $z \in \Delta_\theta$ et $|z-1| \leqslant \inf\{\alpha, \cos\theta\}$, alors :

$$|f(z) - \ell| \leqslant \varepsilon + \varepsilon \frac{2}{\cos\theta}$$

D'où le résultat. □

Théorème 2 (Taubérien faible)**.** *Soit f la somme d'une série entière $\sum a_n z^n$ de rayon de convergence 1. On suppose que $\lim_{x\to 1^-} f(z) = \ell$ existe et que $a_n = o\left(\frac{1}{n}\right)$. Alors $\sum a_n$ converge et $\ell = \sum_{n=0}^{\infty} a_n$.*

Démonstration.

Pour tout $n \in \mathbb{N}$, on pose $S_n = \sum_{k=0}^{n} a_k$. On a :

$$\forall\, n \in \mathbb{N}^\star,\ \forall\, x \in]0,1[,\ S_n - f(x) = \sum_{k=0}^{n} a_k - \sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{n} a_k(1-x^k) - \sum_{k=n+1}^{\infty} a_k x^k$$

et comme $1 - x^k = (1-x)\sum_{i=0}^{k-1} x^i \leqslant k(1-x)$ pour $0 < x < 1$, on a :

$$|S_n - f(z)| \leqslant (1-x)\sum_{k=1}^{n} k|a_k| + \sum_{k=n+1}^{\infty} \frac{k|a_k|}{n} x^k \leqslant (1-x)nM + \frac{\sup_{k>n} k|a_k|}{n(1-x)}$$

où M désigne un majorant de $(k|a_k|)_k$. Fixons à présent $0 < \varepsilon < 1$, alors :

$$\forall\, n \in \mathbb{N}^\star,\ \left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leqslant M\varepsilon + \frac{\sup_{k>n} k|a_k|}{\varepsilon}$$

Comme $(ka_k)_k$ converge vers 0, on peut choisir N_0 tel que $\sup_{k>N_0} ka_k < \varepsilon^2$, alors :

$$\forall\, n \geqslant N_0,\ \left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| \leqslant (M+1)\varepsilon$$

Par hypothèse, $f(x)$ tends vers ℓ quand x tend vers 1^-, donc il existe $N_1 \geqslant N_0$ tel que $\left|f\left(1-\frac{\varepsilon}{n}\right) - \ell\right| < \varepsilon$ pour tout $n \geqslant N_1$, ainsi :

$$\forall\, n \geqslant N_1,\ |S_n - \ell| \leqslant \left|S_n - f\left(1 - \frac{\varepsilon}{n}\right)\right| + \left|f\left(1 - \frac{\varepsilon}{n}\right) - \ell\right| \leqslant (M+2)\varepsilon$$

Donc (S_n) converge vers ℓ, d'où le résultat. □

Références

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse.* Ellipses

Théorèmes de Sylow

Leçons concernées : 101 103 104

Lemme 1. *Soit G un groupe fini d'ordre $p^\alpha m$, où $p \nmid m$. Soit H un groupe, et soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Démonstration.

On considère l'action de G sur G/S définie par :

$$\varphi : \left| \begin{array}{ccc} G \times G/S & \longrightarrow & G/S \\ (g, aS) & \longmapsto & g \cdot (aS) = (ga)S \end{array} \right.$$

En effet, φ est une action de groupe, puisque, pour tous $g, g' \in G$ et tout $a \in G$, on a :

$$\varphi(e, aS) = e \cdot (aS) = (ea)S = aS$$

$$\varphi(g, \varphi(g', aS)) = \varphi(g, g' \cdot (aS)) = \varphi(g, (g'a)S) = g \cdot (g'a)S = (gg'a)S = (gg') \cdot (aS) = \varphi(gg', aS)$$

On note S_{aS} le stabilisateur de aS sous l'action de G sur G/S. Alors :

($\subseteq$) Soit $g \in S_{aS}$, alors $gaS = aS$, c'est-à-dire qu'il existe $s_1, s_2 \in S$ tels que $gas_1 = as_2$.
Ainsi $g = as_2s_1^{-1}a^{-1} \in aSa^{-1}$, donc $S_{aS} \subseteq aSa^{-1}$.

($\supseteq$) Soit $h \in aSa^{-1}$. Il existe $s \in S$ tel que $h = asa^{-1}$. Ainsi $h \cdot aS = (asa^{-1}a)S = aS$, et $S_{aS} \supseteq aSa^{-1}$.

On a donc finalement que $S_{aS} = aSa^{-1}$.

En restreignant φ à H, on a que H agit sur G/S.
En notant S'_{aS} le stabilisateur de aS sous l'action de H, on obtient que $S'_{aS} = aSa^{-1} \cap H$.
En choisissant $a_1, \dots, a_m$ un système de représentants des orbites, l'équation aux classes donne :

$$m = |G/S| = \sum_{i=1}^{m} \frac{|H|}{|a_i S a_i^{-1} \cap H|}$$

Or, si pour tout $i \in [\![1, m]\!]$, on a $p \mid [H : S'_{aS}]$, alors $p \mid |G/S| = m$, ce qui contredit le fait que S soit un p-Sylow.
Il existe donc $i \in [\![1, m]\!]$ tel que $p \wedge [H : S'_{aS}] = 1$.

De plus, $a_i S a_i^{-1} \cap H$ est un sous-groupe de $a_i S a_i^{-1}$, donc $a_i S a_i^{-1} \cap H$ est un p-groupe, donc $|a_i S a_i^{-1} \cap H| = p^k$ et $|H| = p^j n$, où $k \leqslant j \leqslant \alpha$ et $n \mid m$. Cependant, $[H : S'_{aS}] = p^{j-k} n \wedge p = 1$, donc $j = k$.
Finalement, $a_i S a_i^{-1} \cap H$ est un p-Sylow de H.

□

Lemme 2. *Soit G un p-groupe agissant sur X. On note X^G l'ensemble des points fixes de X par G. Alors $|X| \equiv |X^G| \mod p$.*

Démonstration.

On écrit X comme réunion disjointe de ses orbites sous G. Si $x \notin X^G$, alors son orbite $\omega(x)$ est de cardinal strictement supérieur à 1, mais comme ce cardinal divise $|G| = p^n$, on a que $p \mid |\omega(x)|$. Si θ est un système de représentants, alors l'équation aux classe donne :

$$|X| \equiv |X^G| + \sum_{x \in \theta \setminus X^G} |\omega(x)| \equiv |X^G| \mod p$$

□

Théorème 3 (Sylow). *On suppose G fini d'ordre $n = p^\alpha m$, où $p \nmid m$.*
(i) L'ensemble $Syl_p(G)$ des p-Sylow de G est non vide.
(ii) Tous les p-Sylow sont conjugués.
(iii) $|Syl_p(G)| \equiv 1 \mod p$ et $|Syl_p(G)| \mid m$.

Démonstration.

(i) Par le théorème de Cayley, on sait qu'il existe un isomorphisme $g : G \to A$, où $A \subseteq \mathfrak{S}_n$.
Soit $(e_1, \dots, e_n)$ une base de $\mathbb{F}_q^n$. On considère l'application :

$$\psi : \left| \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & GL_n(\mathbb{F}_p) \\ \sigma & \longmapsto & u_\sigma : \left| \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ e_i & \longmapsto & e_{\sigma(i)} \end{array} \right. \end{array} \right.$$

De plus, ψ est un morphisme de groupes. En effet, pour tous $\sigma, \sigma' \in \mathfrak{S}_n$, et tout $i \in [\![1, n]\!]$, on a :

$$\psi(\sigma \circ \sigma')(e_i) = e_{\sigma(\sigma(i))} = \psi(\sigma)(\psi(\sigma')(e_i)) = (\psi(\sigma) \circ \psi(\sigma'))(e_i)$$

Donc $\psi(\sigma \circ \sigma') = (\psi(\sigma) \circ \psi(\sigma'))$, et ψ est un morphisme de groupes.
On a également l'injectivité de ψ, puisque :

$$\mathrm{Ker}(\psi) = \{\sigma \in \mathfrak{S}_n \,|\, u_\sigma = Id\} = \left\{\sigma \in \mathfrak{S}_n \,\middle|\, \forall\, i \in [\![1, n]\!],\ e_{\sigma(i)} = e_i\right\} = \{Id\}$$

En posant $\theta = \psi|_A \circ g$, θ est un morphisme de groupe de G dans $GL_n(\mathbb{F}_p)$.
De plus, θ est injectif, donc, par le premier théorème d'isomorphie, on a $G \cong \mathrm{Im}(\theta)$.
Or, $\mathrm{Im}(\theta)$ est un sous-groupe de $GL_n(\mathbb{F}_p)$, qui possède un p-Sylow.
Par le Lemme 1, $\mathrm{Im}(\theta)$ contient également un p-Sylow, et donc G aussi par isomorphie.

(ii) Soit H un p-sous-groupe de G, et soit S un p-Sylow de G.
Par le Lemme 1, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.
On a donc $|H| = p^k$ et $aSa^{-1} \cap H \subseteq H$, et $|aSa^{-1} \cap H| = p^k$, donc $aSa^{-1} \cap H = H$, et $H \subseteq aSa^{-1}$.
Si de plus H est un p-Sylow, alors $H = aSa^{-1}$.

(iii) Soit S un p-Sylow de G. On considère l'action par conjugaison de S sur $Syl_p(G)$.
Pour tout $s \in S$, on a $sSs^{-1} = S$, donc $S \in (Syl_p(G))^S$. Montrons que c'est le seul point fixe.
Soit $T \in (Syl_p(G))^S$, donc tel que, pour tout $s \in S$, on a $sTs^{-1} = T$.
On pose $N = \langle S, T\rangle$ le sous-groupe de G engendré par S et T. On a $T \leqslant N \leqslant G$.
Comme T est un p-Sylow de G, c'est aussi un p-Sylow de N. De même pour S.
T et S sont donc deux p-Sylow de N, donc il existe $a \in N$ tel que $S = aTa^{-1}$.
Or, comme S normalise T, on a que $T \trianglelefteq N$, d'où $aTa^{-1} = T$.
Le Lemme 2 donne que $|Syl_p(G)| \equiv 1 \mod p$.

Enfin, on considère l'action par conjugaison de G sur l'ensemble de ses sous-groupes.
$Syl_p(G)$ forme une orbite sous cette action par le point précédent.
On a alors $|Syl_p(G)| \mid |G| = p^\alpha m$ et $|Syl_p(G)| \wedge p = 1$, donc, par le lemme de Gauss, on a $|Syl_p(G)| \mid m$.

□

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses

Transformée de Fourier d'une gaussienne

Leçons concernées : 236 245 250 265 267

Proposition 1. *Si $\gamma_a(x) = e^{-ax^2}$ pour $a > 0$ et $x \in \mathbb{R}$, alors $\widehat{\gamma_a} = \sqrt{\frac{\pi}{a}}\gamma_{\frac{1}{4a}}$.*

Démonstration.

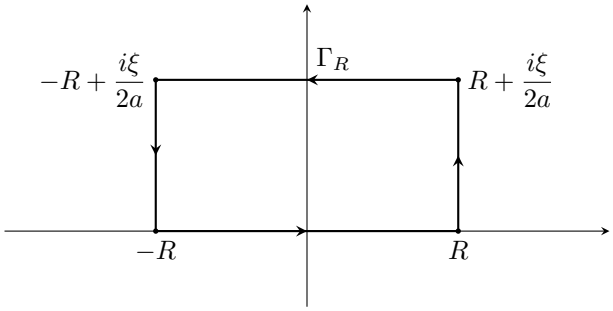
Soit $a > 0$. Pour tous $x, \xi \in \mathbb{R}$, on a :

$$ax^2 + ix\xi = a\left(x^2 + i\frac{x\xi}{a}\right) = a\left(\left(x + \frac{i\xi}{2a}\right)^2 + \frac{\xi^2}{4a^2}\right) = a\left(x + \frac{i\xi}{2a}\right)^2 + \frac{\xi^2}{4a}$$

On en déduit alors que, pour tout $\xi \in \mathbb{R}$, on a :

$$\widehat{\gamma_a}(\xi) = \int_{-\infty}^{+\infty} e^{-ax^2 - ix\xi}\,dx = \int_{-\infty}^{+\infty} e^{-a\left(x+\frac{i\xi}{2a}\right)^2 - \frac{\xi^2}{4a}}\,dx = e^{-\frac{\xi^2}{4a}}\int_{-\infty}^{+\infty} e^{-a\left(x+\frac{i\xi}{2a}\right)^2}\,dx$$

Considérons la fonction complexe $z \mapsto e^{-az^2}$. Pour $R > 0$ et $\xi \in \mathbb{R}$ fixés, notons Γ_R le contour suivant :



On a ainsi :

$$\int_{\Gamma_R} e^{-az^2}\,dz = \underbrace{\int_{-R}^{R} e^{-ax^2}\,dx}_{I_1(R)} + \underbrace{\int_0^{\frac{\xi}{2a}} e^{-a(R+it)^2}\,dt}_{I_2(R)} - \underbrace{\int_{-R}^{R} e^{-a\left(x+\frac{i\xi}{2a}\right)^2}\,dx}_{I_3(R)} - \underbrace{\int_0^{\frac{\xi}{2a}} e^{-a(-R+it)^2}\,dt}_{I_4(R)}$$

Or, on a, par changement de variable :

$$\lim_{R\to+\infty} I_1(R) = \sqrt{\frac{\pi}{a}} \quad \text{car} \quad \int_{-\infty}^{+\infty} e^{-x^2}\,dx = \sqrt{\pi}$$

De plus, on a :

$$|I_2(R)| \leqslant \int_0^{\frac{\xi}{2a}} e^{-a(R^2-t^2)}\,dt = e^{-aR^2}\int_0^{\frac{\xi}{2a}} e^{at^2}\,dt \xrightarrow[R\to+\infty]{} 0$$

De la même manière, on obtient $\lim_{R\to+\infty} I_4(R) = 0$.
Il reste à étudier $I_3(R)$. Puisque l'intégrale généralisée $\int_{-\infty}^{+\infty} e^{-a\left(x+\frac{i\xi}{2a}\right)^2}\,dx$ converge absolument, on a :

$$\lim_{R\to+\infty} I_3(R) = \int_{-\infty}^{+\infty} e^{-a\left(x+\frac{i\xi}{2a}\right)^2}\,dx = e^{\frac{\xi^2}{4a}}\widehat{\gamma_a}(\xi)$$

Puisque $z \mapsto e^{-az^2}$ est holomorphe sur $\mathbb{C}$ et que le contour $\Gamma(R)$ est fermé, le théorème de Cauchy donne :

$$0 = \int_{\Gamma_R} e^{-az^2}\,dz = I_1(R) + I_2(R) - I_3(R) - I_4(R) \xrightarrow[R\to+\infty]{} \sqrt{\frac{\pi}{a}} + 0 - e^{\frac{\xi^2}{4a}}\widehat{\gamma_a}(\xi) - 0 = \sqrt{\frac{\pi}{a}} - e^{\frac{\xi^2}{4a}}\widehat{\gamma_a}(\xi)$$

On obtient finalement que :

$$\widehat{\gamma_a}(\xi) = \sqrt{\frac{\pi}{a}}e^{-\frac{\xi^2}{4a}} = \sqrt{\frac{\pi}{a}}\gamma_{\frac{1}{4a}}(\xi)$$

□

Références

[El 08] M. El Amrani. *Analyse de Fourier dans les espaces fonctionnels.* Ellipses

Un critère de diagonalisabilité

Leçons concernées : 153

Proposition 1. *Soient $f \in \mathcal{L}(E)$ et F un sous-espace vectoriel strict de E stable par f. En notant $g = f|_F$ la restriction de f à F, on a que g est dans $\mathcal{L}(E)$ et que χ_g divise χ_f.*

Démonstration.

Soit $\mathcal{B}' = (e_1, \dots, e_r)$ une base de F, que l'on complète en une base $\mathcal{B} = (e_1, \dots, e_n)$ de E.
Alors $\mathrm{Mat}_{\mathcal{B}}(f)$ est de la forme :

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \text{ avec } A = \mathrm{Mat}_{\mathcal{B}'}(g)$$

On obtient alors :

$$\chi_f(X) = \begin{vmatrix} A - XI_r & C \\ 0 & B - XI_{n-r} \end{vmatrix} = \chi_g(X) \cdot \det(B - XI_{n-r})$$

□

Proposition 2. *Soit $f \in \mathcal{L}(E)$, et soit $\lambda \in \mathbb{K}$ une racine de χ_f de multiplicité h, alors $\dim E_\lambda \leqslant h$.*

Démonstration.

On applique la proposition précédente pour $F = E_\lambda$.
On a que $g = f|_{E_\lambda} = \lambda Id_{E_\lambda}$, donc $\chi_g(X) = (X - \lambda)^{\dim E_\lambda}$.
Comme χ_g divise χ_f, on a que $\dim E_\lambda \leqslant h$. □

Théorème 3. *Soit $f \in \mathcal{L}(E)$, les assertions suivantes sont équivalentes :*

(i) f est diagonalisable

(ii) χ_f est scindé sur $\mathbb{K}$, et toute racine λ est de multiplicité $\dim E_\lambda$.

(iii) Il existe des valeurs propres $\lambda_1, \dots, \lambda_p$ de f vérifiant $E = \bigoplus_{i=1}^{p} E_{\lambda_i}$.

Démonstration.

Étape 1 : Montrons que $(i) \Rightarrow (ii)$.

Soient $\lambda_1, \dots, \lambda_r$ les valeurs propres de f, et soit $\mathcal{B}$ une base de vecteurs propres.
Comme f est diagonalisable, on a :

$$\mathrm{Mat}_{\mathcal{B}}(f) = P \begin{pmatrix} \lambda_1 I_{h_1} & & 0 \\ & \ddots & \\ 0 & & \lambda_r I_{h_r} \end{pmatrix} P^{-1} \text{ où } P \in \mathcal{GL}_n(\mathbb{K})$$

Ainsi, $h_i = \dim E_{\lambda_i}$ et $\chi_f(X) = \prod_{i=1}^{r} (X - \lambda_i)^{h_i}$.

Étape 2 : Montrons que $(ii) \Rightarrow (iii)$**.**

On écrit $\chi_f(X) = \prod_{i=1}^{r} (X - \lambda_i)^{h_i}$.
On a $F = \bigoplus_{i=1}^{r} E_{\lambda_i} \subseteq E$. De plus :

$$\dim F = \sum_{i=1}^{r} \dim E_{\lambda_i} = \sum_{i=1}^{r} h_i = \deg \chi_f = n = \dim E$$

On a donc $E = \bigoplus_{i=1}^{p} E_{\lambda_i}$.

Étape 3 : Montrons que $(iii) \Rightarrow (i)$**.**

Soit $\mathcal{B}_i$ une base de E_{λ_i}, et $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r$ une base de vecteurs propres.
Comme $f|_{E_{\lambda_i}} = \lambda_i Id_{E_{\lambda_i}}$, on a :

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} \lambda_1 I_{h_1} & & 0 \\ & \ddots & \\ 0 & & \lambda_r I_{h_r} \end{pmatrix}$$

donc f est diagonalisable.

□

Application 4. *Un endomorphisme est diagonalisable si, et seulement si, il admet un polynôme annulateur scindé à racines simples sur* $\mathbb{K}$*.*

Démonstration.

($\Rightarrow$) Soit $f \in \mathcal{L}(E)$ diagonalisable.
Soient $\lambda_1, \ldots, \lambda_r$ ses valeurs propres, et $E_{\lambda_1}, \ldots, E_{\lambda_r}$ les sous-espaces propres associés.
Soit alors $P(X) = \prod_{i=1}^{r} (X - \lambda_i)$, qui est scindé à racines simples. De plus, par le lemme des noyaux :

$$\mathrm{Ker}\, P(f) = \bigoplus_{i=1}^{r} \mathrm{Ker}(f - \lambda_i Id_E) = \bigoplus_{i=1}^{r} E_{\lambda_i} = E$$

Ainsi $P(f) = 0$.

($\Leftarrow$) Soit $f \in \mathcal{L}(E)$, et soit $P \in \mathbb{K}[X]$ annulateur de f, scindé à racines simples.
On note $\lambda_1, \ldots, \lambda_r$ les racines de P, alors par le lemme des noyaux, on a :

$$E = \mathrm{Ker}\, P(f) = \bigoplus_{i=1}^{r} \mathrm{Ker}(f - \lambda_i Id_E)$$

f est donc diagonalisable.

□

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

Un homéomorphisme induit par l'exponentielle

Leçons concernées : 155 156 158 160

Lemme 1. *Pour tout $M \in \mathcal{S}_n^{++}(\mathbb{R})$, on a $||M||_2 = \rho(M)$.*

Démonstration.

Soit $M \in \mathcal{S}_n^{++}(\mathbb{R})$. Alors M est diagonalisable dans une base orthonormée, donc $|||M|||_2 = |||\mathrm{Diag}(\lambda_1, \dots, \lambda_n)|||_2$, où $\lambda_1, \dots, \lambda_n > 0$ sont les valeurs propres de M. On a alors pour $x \in \mathbb{R}^n$:

$$\|Mx\|_2 \leqslant |||M|||_2 \, \|x\|_2 = |||\mathrm{Diag}(\lambda_1, \dots, \lambda_n)|||_2 \, \|x\|_2 \leqslant \rho(M) \, \|x\|_2$$

De plus, si $x = e_{i_0}$, où i_0 est tel que $\lambda_{i_0} = \rho(M)$, on a $|||Mx|||_2^2 = \rho(M)^2$. Ceci donne $|||M|||_2 = \rho(M)$. □

Théorème 2. $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ *est un homéomorphisme.*

Démonstration.

Étape 1 : Montrons que l'application est bien définie, et continue.

Soit $S \in \mathcal{S}_n(\mathbb{R})$. Alors S est diagonalisable dans une base orthonormée. On écrit $S = P \, \mathrm{Diag}(\lambda_1, \dots, \lambda_n) \, {}^tP$, où $P \in \mathcal{O}_n(\mathbb{R})$ et $\lambda_1, \dots, \lambda_n > 0$ sont les valeurs propres de S. On a $\exp(S) = P \, \mathrm{Diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) \, {}^tP \in \mathcal{S}_n^{++}(\mathbb{R})$. L'application considérée est donc bien définie, et continue comme restriction d'une application continue.

Étape 2 : Montrons que l'application est surjective.

Soit $B \in \mathcal{S}_n(\mathbb{R})$. Alors B est diagonalisable dans une base orthonormée. On écrit $B = P \, \mathrm{Diag}(\mu_1, \dots, \mu_n) \, {}^tP$, où $P \in \mathcal{O}_n(\mathbb{R})$ et $\mu_1, \dots, \mu_n > 0$ sont les valeurs propres de B. Posons alors $A = P \, \mathrm{Diag}(\ln(\mu_1), \dots, \ln(\mu_n)) \, {}^tP$. On a $A \in \mathcal{S}_n(\mathbb{R})$ et $\exp(A) = B$, d'où la surjectivité.

Étape 3 : Montrons que l'application est injective.

Soient $A, A' \in \mathcal{S}_n(\mathbb{R})$ telles que $\exp(A) = \exp(A')$. On note $\lambda_1, \dots, \lambda_n$ les valeurs propres de A, et $\mu_1, \dots, \mu_n$ les valeurs propres de A'. On fixe $P \in \mathcal{O}_n(\mathbb{R})$ telle que $A = P \, \mathrm{Diag}(\lambda_1, \dots, \lambda_n) \, {}^tP$. Soit Q un polynôme interpolateur de Lagrange tel que $Q(e^{\lambda_i}) = \lambda_i$ pour tout $i \in [\![1, n]\!]$. Alors A' commute avec $Q(\exp(A')) = Q(\exp(A))$, or :

$$Q(\exp(A)) = Q(P \, \mathrm{Diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) \, {}^tP) = PQ(\mathrm{Diag}(e^{\lambda_1}, \dots, e^{\lambda_n})) \, {}^tP = P \, \mathrm{Diag}(\lambda_1, \dots, \lambda_n) \, {}^tP = A$$

Ainsi, A et A' commutent, et par diagonalisation simultanée, on a :

$$\mathrm{Diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) = {}^tP \exp(A) P = {}^tP \exp(A') P = \mathrm{Diag}(e^{\mu_1}, \dots, e^{\mu_n})$$

Donc, pour tout $i \in [\![1, n]\!]$, on a $e^{\lambda_i} = e^{\mu_i}$, puis $\lambda_i = \mu_i$ et $A = A'$, d'où l'injectivité.

Étape 4 : Montrons que l'application est bicontinue.

Soit $(B_p)_{p \in \mathbb{N}}$ une suite de $\mathcal{S}_n^{++}(\mathbb{R})$ qui converge vers $B \in \mathcal{S}_n^{++}(\mathbb{R})$. Par surjectivité, écrivons $B_p = \exp(A_p)$ et $B = exp(A)$. Montrons que $(A_p)_{p \in \mathbb{N}}$ converge vers A.

La suite $(B_p)_{p \in \mathbb{N}}$ étant convergente, elle est bornée pour $\|.\|_2$. Par le lemme, on a $\|B_p\|_2 = \rho(B_p)$, donc tous les spectres des B_p sont majorés par une constante C. Par le même raisonnement appliqué à $(B_p^{-1})_{p \in \mathbb{N}}$, qui converge vers B^{-1} par continuité de l'inverse, les spectres des B_p sont minorés par une constante C'. Toutes les valeurs propres des B_p sont donc dans le compact $[C, C']$ de $\mathbb{R}^{+\star}$, donc toutes les valeurs propres des A_p sont dans le compact $[\ln C', \ln C]$ de $\mathbb{R}$.

La suite $(A_p)_{p\in\mathbb{N}}$ est donc bornée pour $\|.\|_2$, et sa seule valeur d'adhérence est A. En effet, soit $(A_{p_k})_{k\in\mathbb{N}}$ est une sous-suite de $(A_p)_{p\in\mathbb{N}}$ qui converge vers $\overline{A}$. On a alors $\exp(\overline{A}) = \lim_{k\to\infty} \exp(A_{p_k}) = B = \exp(A)$, donc $\overline{A} = A$ par injectivité. La suite $(A_p)_{p\in\mathbb{N}}$ étant bornée et ayant une unique valeur d'adhérence A, elle converge vers A. On a donc montré la bicontinuité de $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$.

□

Références

[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet

Bibliographie

[All12] G. Allaire. *Analyse numérique et optimisation*. Éditions de l'École Polytechnique.

[App13] W. Appel. *Probabilités pour les non probabilistes*. H&K.

[Aud06] M. Audin. *Géométrie*. EDP Sciences.

[Ave83] A. Avez. *Calcul différentiel*. Masson.

[BL07] P. Barbe et M. Ledoux. *Probabilité*. EDP Sciences.

[BMP05] V. Beck, J. Malick, et G. Peyré. *Objectif Agrégation*. H&K.

[BP12] M. Briane et G. Pagès. *Théorie de l'intégration*. Vuilbert.

[Bre87] H. Brezis. *Analyse fonctionelle*. Masson.

[BSF05] B. Beck, I. Selon, et C. Feuillet. *HPrépa Maths 2e année MP-MP**. Hachette.

[Can09] B. Candelpergher. *Calcul intégral*. Cassini.

[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1*. Calvage et Mounet.

[CG15] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 2*. Calvage et Mounet.

[Cho20] M. Choulli. *Analyse complexe*. DeBoeck.

[Cia88] P. Ciarlet. *Introduction à l'analyse numérique et à l'optimisation*. Masson.

[Col09] P. Colmez. *Éléments d'analyse et d'algèbre*. Les éditions de l'École Polytechnique.

[Com98] F. Combes. *Algèbre et géométrie*. Bréal.

[dB04] J. de Biasi. *Mathématiques pour le CAPES et l'agrégation interne*. Ellipses.

[Dem06] J.-P. Demailly. *Analyse numérique et équations différentielles*. EDP Sciences.

[DG12] C. David et P. Gosselet. *Équations aux dérivées partielles*. Dunod.

[El 08] M. El Amrani. *Analyse de Fourier dans les espaces fonctionnels*. Ellipses.

[El 11] M. El Amrani. *Suites et séries numériques, Suites et séries de fonctions*. Ellipses.

[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1*. Cassini.

[FGN13b] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 2*. Cassini.

[FGN13c] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 3*. Cassini.

[FGN13d] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 1*. Cassini.

[FGN13e] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Analyse 4*. Cassini.

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre*. Ellipses, 2e édition.

[Gou08] X. Gourdon. *Les Maths en Tête : Analyse*. Ellipses.

[Gri11] J. Grifone. *Algèbre Linéaire*. Cépaduès, 4e édition.

[Hau07] B. Hauchecorne. *Les Contre-exemples en Mathématiques*. Ellipses.

[HL99] F. Hirsch et G. Lacombe. *Éléments d'analyse fonctionnelle*. Dunod.

[Les14] A. Lesfari. *Variables complexes*. Ellipses.

[Mai13] F. Maisonneuve. *Fonction d'une variable complexe*. Bréal.

[Ouv08] J.-Y. Ouvrard. *Probabilités : Tome 1*. Cassini.

[Ouv09] J.-Y. Ouvrard. *Probabilités : Tome 2*. Cassini.

[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses.

[Pey08] G. Peyré. *L'algèbre discrète de la transformée de Fourier*. Ellipses.

[Pom97] A. Pommelet. *Cours d'Analyse*. Ellipses.

[RDO91] E. Ramis, C. Deschamps, et J. Odoux. *Cours de Mathématiques, Topologie et éléments d'analyse*. Masson.

[Rom19] J.-E. Rombaldi. *Éléments d'analyse réelle*. EDP Sciences.

[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie*. DeBoeck.

[Rou15] F. Rouvière. *Petit Guide de Calcul Différentiel*. Cassini.

[Rud09] W. Rudin. *Analyse réelle et complexe*. Dunod.

[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis*. Hermann.

[Ser13] J.-P. Serre. *Cours d'Arithmétique*. PUF.

[Tau05] P. Tauvel. *Cours de Géométrie*. Dunod.

[Tau06] P. Tauvel. *Analyse complexe pour la licence 3*. Dunod.

[Tau08] P. Tauvel. *Corps commutatifs et théorie de Galois*. Calvage et Mounet.

[Ulm12] F. Ulmer. *Théorie des groupes*. Ellipses.

[Zav13] M. Zavidovique. *Un Max de Math*. Calvage et Mounet.

[ZQ13] C. Zuily et H. Queffélec. *Analyse pour l'agrégation*. Dunod.