École Normale Supérieure Paris-Saclay

AGRÉGATION – LEÇONS

Antoine BARRIER

antoine.barrier@ens-lyon.fr

https://perso.ens-lyon.fr/antoine.barrier/fr/

2018/2019 – Dernière mise à jour : 2 juin 2021

Ce document regroupe mes plans de leçons élaborés pendant mon année de préparation de l'Agrégation de Mathématiques (master M2 FESup de l'ÉNS Paris-Saclay).

Bien que de nombreux plans soient terminés, il reste beaucoup de travail et certains d'entre eux ne sont pas détaillés. Par ailleurs, il y a certainement bon nombre d'erreurs et d'imprécisions. À chaque fin de leçon j'ai essayé de rajouter différents commentaires sur la leçon ainsi que des questions types, qui ont souvent été prises à la volées et peuvent donc être imprécises. Certains commentaires concernent des plans de leçon présentés par d'autres étudiants en classe et sont donc dénués de sens vis-à-vis du plan associé dans ce document.

En utilisant ce document, veillez à garder à l'esprit que la liste et les intitulés des leçons ont évolué. N'hésitez pas à me signaler toute erreur.

Sommaire

I Leçons de Mathématiques Générales **1**

101 Groupe opérant sur un ensemble. Exemples et applications. **2**

102 Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications. **6**

103 Exemples de sous-groupes distingués et de groupes quotients. Applications. **10**

104 Groupes finis. Exemples et applications. **13**

105 Groupe des permutations d'un ensemble fini. Applications. **17**

106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications. **21**

107 Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel. Exemples. **23**

108 Exemples de parties génératrices d'un groupe. Applications. **26**

110 Structure et dualité des groupes abéliens finis. Applications. **29**

120 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications. **31**

121 Nombre premiers. Applications. **35**

122 Anneaux principaux. Applications. **39**

123 Corps finis. Applications. **43**

125 Extensions de corps. Exemples et applications. **46**

126 Exemples d'équations en arithmétique. **48**

141 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications. **51**

142 PGCD et PPCM, algorithmes de calcul. Applications. **53**

144 Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications. **56**

150 Exemples d'actions de groupes sur les espaces de matrices. **58**

151 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications. **62**

152 Déterminant. Exemples et applications. **66**

153 Polynômes d'endomorphisme en dimension finie. Réduction. Applications. **71**

154 Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications. **75**

155 Endomorphismes diagonalisables en dimension finie. **79**
156 Exponentielle de matrices. Applications. **83**
157 Endomorphismes trigonalisables. Endomorphismes nilpotents. **85**
158 Matrices symétriques réelles, matrices hermitiennes. **89**
159 Formes linéaires et dualité en dimension finie. Exemples et applications. **93**
160 Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie). **96**
161 Distances et isométries d'un espace affine euclidien. **100**
162 Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques. **102**
170 Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications. **106**
171 Formes quadratiques réelles. Coniques. Exemples et applications. **109**
181 Barycentres dans un espace affine réel de dimension finie, convexité. Applications. **112**
182 Applications des nombres complexes à la géométrie. **114**
183 Utilisation des groupes en géométrie. **116**
190 Méthodes combinatoires, problèmes de dénombrement. **118**

II Leçons d'Analyse et de Probabilités 121

201 Espaces de fonctions. Exemples et applications. **122**
202 Exemples de parties denses et applications. **124**
203 Utilisation de la notion de compacité. **127**
204 Connexité. Exemples et applications. **129**
205 Espaces complets. Exemples et applications. **131**
207 Prolongement de fonctions. Exemples et applications. **135**
208 Espaces vectoriels normés, applications linéaires continues. Exemples. **137**
209 Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications. **141**
213 Espaces de HILBERT. Bases hilbertiennes. Exemples et applications. **146**
214 Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie. **149**
215 Applications différentiables définies sur un ouvert de $\mathbb{R}^n$. Exemples et applications. **151**
219 Extremums : existence, caractérisation, recherche. Exemples et applications. **153**
220 Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2. **158**
221 Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications. **160**
222 Exemples d'équations aux dérivées partielles linéaires. **162**
223 Suites numériques. Convergences, valeurs d'adhérence. Exemples et applications. **163**

224 Exemples de développements asymptotiques de suites et de fonctions. **165**

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. **169**

228 Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications. **171**

229 Fonctions monotones. Fonctions convexes. Exemples et applications. **173**

230 Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples. **176**

233 Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples. **180**

234 Fonctions et espaces de fonctions LEBESGUE-intégrables. **182**

235 Problèmes d'interversion de limites et d'intégrales. **185**

236 Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables. **189**

239 Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications. **193**

241 Suites et séries de fonctions. Exemples et contre-exemples. **197**

243 Convergence des séries entières, propriétés de la somme. Exemples et applications. **201**

245 Fonctions holomorphes sur un ouvert de $\mathbb{C}$. Exemples et applications. **205**

246 Séries de FOURIER. Exemples et applications. **208**

250 Transformation de FOURIER. Applications. **211**

253 Utilisation de la notion de convexité en analyse. **214**

260 Espérance, variance et moments d'une variable aléatoire. **219**

261 Loi d'une variable aléatoire : caractérisations, exemples, applications. **223**

262 Convergences d'une suite de variables aléatoires. Théorèmes limite. Exemples et applications. **228**

264 Variables aléatoires discrètes. Exemples et applications. **231**

265 Exemples d'études et d'applications de fonctions usuelles et spéciales. **235**

Bibliographie **237**

Première partie

Leçons de Mathématiques Générales

101 GROUPE OPÉRANT SUR UN ENSEMBLE. EXEMPLES ET APPLICATIONS.

Soit $(G, .)$ un groupe et X un ensemble.

I. Action d'un groupe sur un ensemble [Rom17, §1.6-1.7, p19–25]

I. A. Action de groupe : double approche et vocabulaire

Définition 1. [Action d'un groupe sur un ensemble]
On dit que G opère à gauche sur X si on a une application $G \times X \longrightarrow X, (g, x) \longmapsto g.x$ telle que $\forall g, h \in G, \forall x \in X, g.(h.x) = (gh).x$ et $\forall x \in X, 1.x = x$.

Remarque 2.
- Il revient au même de se donner un morphisme de groupes $\phi : G \longrightarrow \mathfrak{S}(X)$ en posant $\phi(g)(x) = g.x$.
- Lorsque $\forall g, h \in G, \forall x \in X, g.(h.x) = (hg).x$, on parle d'action à droite.

Exemple 3.
- G opère sur lui-même par translation à gauche : $g.h = gh$.
- G opère sur lui-même par conjugaison : $g.h = ghg^{-1}$. On note $\mathrm{Int}(G) = \{\mathrm{Int}(g), g \in G\}$ où $\mathrm{Int}(g) : h \longmapsto ghg^{-1}$. On remarque alors que G agit sur tout sous-groupe distingué H de G par cette opération.
- $\mathfrak{S}(X)$ opère naturellement sur X : $\sigma.x = \sigma(x)$.

Théorème 4. [Théorème de Cayley] *G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$.*

Définition 5. [Orbites, transitivité, fidélité]
Soit G opérant sur X.
- Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = \{g.x \,|\, x \in X\}$. On note $\mathcal{O}$ l'ensemble des orbites de X. C'est une partition de X.
- On dit que l'action est transitive s'il n'y a qu'une seule orbite pour l'action de G sur X, c'est-à-dire si $\forall x \in X, O(x) = X$.
- On dit que l'action est fidèle si $\phi(g) = \mathrm{Id} \iff g = e$.

Exemple 6.
- L'action de G sur lui-même par translation à gauche est transitive et fidèle.
- Si $H < G$ agit sur G par translation à droite $h.g = gh^{-1}$, alors $O(g) = gH$ est la classe à gauche de g dans G/H. On note $[G : H]$ le cardinal des orbites lorsqu'il est fini.
- $\mathfrak{S}(X)$ opère transitivement sur X.
- Restreignons l'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ à $\langle\sigma\rangle$, où $\sigma \in \mathfrak{S}_n$. Chaque orbite correspond aux éléments d'un des cycles de la décomposition en cycles disjoints de σ.

Application 7. 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.

I. B. Les orbites comme outil de dénombrement

On considère . une action de G sur X.

Définition 8. [Stabilisateur, action libre, fixateur]
On appelle stabilisateur de $x \in X$ le groupe $\mathrm{Stab}(x) = \{g \in G \,|\, g.x = x\}$.
On dit que G opère librement sur X si $\mathrm{Stab}(x) = \{e\}$ pour tout $x \in X$.
Pour $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X \,|\, g.x = x\}$.

Proposition 9. *Soit $x \in X$. L'application $g \in G \longmapsto g.x \in O(x)$ a pour noyau $\mathrm{Stab}(x)$. L'application quotient est alors une bijection de $G/\mathrm{Stab}(x)$ dans $O(x)$.*
En particulier, si $|G| < +\infty$, on a $\forall x \in X, |O(x)| = [G : \mathrm{Stab}(x)] = \frac{|G|}{|\mathrm{Stab}(x)|}$.

Dans la suite de cette partie on suppose G et X finis.

Corollaire 10. [Équation aux classes]
Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Application 11. [Cardinal de $\mathcal{D}_n(\mathbb{F}_q)$] [Rom17, §5.6, p148–151]
Soit $n \in \mathbb{N}, q = p^r$ où p premier, $r \neq 0$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1 + \cdots + n_q = n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

Exemple 12. [Action par conjugaison] Si G agit par conjugaison sur lui-même, notons $Z_h(G) = \{g \in G \,|\, ghg^{-1} = h\}$. Alors $|G| = |Z(G)| + \sum_{O \in \mathcal{O} \,|\, |O| \geq 2} \frac{|G|}{|Z_{x_O}(G)|}$.

Corollaire 13. [Formule de Burnside] *[Rom17, §1.10, p37]*

$$|\mathcal{O}| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

Application 14. On peut colorier les 6 faces (toutes identiques) d'un cube avec 3 couleurs de 57 manières différentes.

II. Actions sur les groupes finis

On suppose toujours G de cardinal fini dans cette partie. On pose $|G| = n$.

II. A. Résultats généraux [Rom17, §1.1/1.7, p2/25]

Théorème 15. [Théorème de Lagrange]
L'ordre de tout sous-groupe de G divise n. En particulier, l'ordre d'un élément de G divise n.

Théorème 16. [Théorème de Cauchy]
Si p est un diviseur premier de n, alors il existe un élément d'ordre p dans G.

II. B. Cas particulier des p-groupes [Per96, §1.5, p18–20]

Soit p un nombre premier diviseur de n. On notera $n = p^a m$ où $p \nmid m$.

Définition 17. [p-groupe, p-sous-groupe de Sylow]
Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de Sylow (ou p-Sylow) un sous-groupe de G de cardinal p^a.

Application 18. [de l'exemple 12] Le centre d'un p-groupe non trivial est non trivial.

Théorème 19. [Théorème de Sylow 1] *Il existe au moins un p-Sylow dans G.*

Corollaire 20. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

Théorème 21. [Théorème de Sylow 2]
(i) Si $H < G$ est un p-groupe, alors il existe un p-Sylow S tel que $H < S$,
(ii) Les p-Sylow de G sont tous conjugués,
(iii) Notons Σ le nombre de p-Sylow de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.

Corollaire 22. *Soit S un p-Sylow de G. Alors $S \lhd G \iff S$ est l'unique p-Sylow de G.*

Application 23. Tout groupe d'ordre 63 ou 255 n'est pas simple.

II. C. Action sur le groupe $\mathfrak{S}_n$ [Rom17, Ch2, p39]

Lien entre orbites de l'action naturelle et support, décompositions en produits de cycles à support disjoints
Action par conjugaison : caractérisations des orbites par leur type.

III. Applications des actions de groupes en algèbre linéaire et en géométrie

III. A. Actions sur des ensembles matriciels [CG13, ChI/III, p2/83]

Soient $m, n \in \mathbb{N}^*$, $\mathbb{K}$ un corps.

Définition 24. [Action de Steinitz]
Posons $G = \mathcal{GL}_m(\mathbb{K}) \times \mathcal{GL}_n(\mathbb{K})$. On appelle action de Steinitz l'action :

$$\begin{array}{ccc} G \times \mathcal{M}_{m,n}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{m,n}(\mathbb{K}) \\ ((P,Q),A) & \longmapsto & PAQ^{-1} \end{array}$$

Les orbites pour cette action sont appelées classes d'équivalence.

Théorème 25. *Deux matrices sont équivalentes si et seulement si elles ont même rang.*
Ainsi $\mathcal{O} = \{O_r \mid 0 \leq r \leq \min(m,n)\}$ où $O_r = \{A \in \mathcal{M}_{m,n}(\mathbb{K}) \mid \mathrm{rg}(A) = r\}$.

Définition 26. [Action par conjugaison]
Les orbites de l'action de $\mathcal{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ sont appelées classes de similitude.

Proposition 27. *Dans $\mathbb{K} = \mathbb{C}$, $M \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si et seulement si sa classe de similitude est fermée dans $\mathcal{M}_n(\mathbb{K})$.*

III. B. Actions sur un espace vectoriel [Rom17, Ch6, p179]

Soit G un groupe et E un $\mathbb{C}$-espace vectoriel de dimension finie.

Définition 28. [Représentation]
Une représentation (linéaire) de G dans E est un morphisme de groupes $\rho : G \longmapsto \mathrm{GL}(E)$.

REMARQUE 29. Se donner une représentation de G dans E revient à se donner une action de groupes de G sur E en posant $\rho(g)(x) = g.x$.

EXEMPLE 30. [REPRÉSENTATION TRIVIALE] $\rho : g \longmapsto \mathrm{Id}_E$ est une représentation de G sur E.

EXEMPLE 31. Si E est de dimension 1 :
- les représentations de $\mathfrak{S}_n$ dans E sont $\rho : \sigma \longrightarrow \mathrm{Id}_E$ et $\rho : \sigma \longrightarrow \varepsilon(\sigma)\,\mathrm{Id}_E$.
- les représentations de $\mathbb{Z}/2\mathbb{Z}$ dans E sont $\rho : \overline{x} \longrightarrow \mathrm{Id}_E$ et ρ définie par $\rho(\overline{1}) = -\mathrm{Id}_E$.

Si E est de dimension 2, les représentations de $\mathbb{Z}/2\mathbb{Z}$ dans E sont $\rho : \overline{x} \longrightarrow \mathrm{Id}_E$ et ρ définie par $\rho(\overline{1}) = \mathrm{diag}(\pm 1, \pm 1)$ dans une certaine base.

EXEMPLE 32. [REPRÉSENTATIONS DE PERMUTATIONS]
$\mathfrak{S}_n \longrightarrow \mathcal{GL}_n(\mathbb{C}), \sigma \longmapsto P_\sigma$ est une représentation de $\mathfrak{S}_n$ sur $\mathbb{C}^n$.
Plus généralement, si G est fini de cardinal n et E est de dimension n, soit $(e_g)_{g\in G}$ une base de E. Alors l'application linéaire $\rho(g)$ définie par $\rho(g)(e_h) = e_{gh}$ pour $h \in G$ définit une représentation de G dans E.

III. C. Applications en géométrie

[Aud06, ChIII/V, p111/360] [Rom17, §3.4.3/6.1, p87/180]

EXEMPLE 33. Isométries du plan conservant un segment $[A, B]$ de centre O :
- Id l'identité,
- ρ la rotation d'angle π et de centre O,
- s la symétrie d'axe (AB),
- $s\rho$ la symétrie d'axe la droite orthogonale à (AB) passant par O.

On vérifie que ces isométries forment un groupe isomorphe au groupe de KLEIN $(\mathbb{Z}/2\mathbb{Z})^2$.

DÉFINITION 34. [DÉPLACEMENT, ANTIDÉPLACEMENT]
Un déplacement (resp. antidéplacement) est un isomorphisme dont la partie linéaire est de déterminant 1 (resp. -1).

Soit G groupe fini d'isométries. On note G^+ ses déplacements et G^- ses antidéplacements.

PROPOSITION 35.
- *Il existe un point fixe à toutes les isométries de G,*
- *G^+ est cyclique, engendré par une rotation ρ.*
- *Si G contient un antidéplacement σ, alors $[G : G^+] = 2$ et $G^- = \sigma G^+$. σ est une réflexion dont l'axe contient le centre de ρ. On a $G = \langle \sigma, \rho \rangle$.*

EXEMPLE 36. Le groupe des isométries du plan préservant un polygone régulier à n sommets de centre O contient les rotations d'ordre n autour du centre et les n réflexions par rapport aux droites joignant :
i) n rotations de centre O et d'angle $\frac{k2\pi}{n}$ pour $k \in [\![0, n-1]\!]$,
ii) n symétries d'axe 2 sommets opposés ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair.

C'est le groupe diédral D_{2n}.

APPLICATION 37. D_{2n} s'injecte naturellement dans $\mathcal{GL}_2(\mathbb{C})$, envoyant la rotation d'angle $2\pi/n$ et la symétrie sur

$$R = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On a donc une représentation naturelle de D_{2n} dans $\mathbb{C}^2$.

SPEECH

La théorie des actions de groupes permet d'étudier les interactions entre ensembles et ainsi d'obtenir des propriétés sur le groupe agissant ou l'ensemble sur lequel il agit.
Historiquement, les premières opérations apparaissent naturellement en géométrie dès l'antiquité (rotations, symétries, …).
Dans la première partie, on définit de deux manières différentes mais équivalentes les actions de groupes, ce qui offre deux visions différentes. On parle du théorème de CAYLEY, du vocabulaire associé aux actions de groupes. La notion de partitionnement en orbites amène l'équation aux classes qui possède de nombreuses applications notamment en dénombrement : on peut par exemple dénombrer le nombre de matrices inversibles diagonalisables à coefficients dans un corps fini, proposé en développement, ou encore utiliser la formule de BURNSIDE.
Ensuite,, on introduit des résultats généraux des actions sur des groupes finis, avec notamment le très utile théorème de LAGRANGE, et le théorème de CAUCHY qui constitue une forme de réciproque. Puis on parle de la théorie des p-SYLOW, dont le premier théorème constituera le second développement.
Enfin la dernière partie se consacre aux nombreux domaines d'applications des actions de groupes :

- notions de classes d'équivalences et de classes de similitudes dans le cas d'ensembles matriciels,
- représentations de groupes dans le cas d'espaces vectoriels (avec toujours 2 définitions comme au début),
- groupes isomorphes au groupe d'isométries préservant des figures (polygone à n côtés et tétraèdre) en géométrie.

COMMENTAIRES

Le produit semi-direct est hors programme, mais très rentable si on est à l'aise dessus (pour les groupes diédraux, la géométrie, …)
Dans la troisième partie, il n'y a pas vraiment de lien entre les applications, mais ce n'est pas grave car les actions de groupes sont des outils. On peut aller plus loin dans la théorie des représentations : application, transformée de FOURIER (le jury insiste dessus, voir [Pey04]).

QUESTIONS

Q Mise à part les matrices à coefficients réels ou complexes, y a-t-il des exemples naturels de groupes topologiques ?

Q Soit G fini tel que $\mathrm{Aut}(G)$ agit transitivement sur $G \setminus \{1\}$. Montrer que $Z(G) \neq \{1\}$.

R La transitivité de l'action implique que les ordres de tous les éléments distinct de 1 sont égaux, notons o cette ordre commun. Pour p diviseur premier de $n = |G|$, on a qu'il existe un élément d'ordre p (théorème de CAUCHY), donc $o = p$ puis $n = p$. Ainsi G est un groupe d'ordre p et on conclut avec l'exemple 12.

Q Calculer $|\mathcal{GL}_n(\mathbb{F}_q)|$, puis le nombre de sous-espaces vectoriels de dimension r de $(\mathbb{F}_q)^n$.

R Cela revient à dénombrer le nombre de bases[1] de $(\mathbb{F}_q)^n$. En effet si $\mathcal{B} = (e_1, \dots, e_n)$ est une base de $(\mathbb{F}_q)^n$, alors $\mathcal{GL}_n(\mathbb{F}_q) \longrightarrow B, M \longmapsto (Me_1, \dots, Me_n)$ où B est l'ensemble des bases de $(\mathbb{F}_q)^n$ est une bijection.
On a $q^n - 1$ choix pour le premier vecteur de la base, puis $q^n - q$ pour le deuxième, …, puis $q^n - q^{k-1}$ pour le k-ième. Finalement : $|\mathcal{GL}_n(\mathbb{F}_q)| = \prod_{k=1}^{n} q^n - q^{k-1}$.
Considérons ensuite l'action $\mathcal{GL}_n(\mathbb{F}_q) \times A_r \longrightarrow A_r, (M, V) \longmapsto M.V$ où A_r est l'ensemble des sous-espaces vectoriels de dimension r. L'action est transitive (penser aux matrices de passage, …). Calculons $\mathrm{Stab}(V)$. En se plaçant dans la bonne base, on voit que $M \in \mathrm{Stab}(V)$ si et seulement si $M = \begin{pmatrix} M_V & \star \\ 0 & M_U \end{pmatrix}$ où $M_V \in \mathcal{GL}_r, M_U \in \mathcal{GL}_{n-r}$.
Donc $|\mathrm{Stab}(V)| = |\mathcal{GL}_r(\mathbb{F}_q)|\,|\mathcal{GL}_{n-r}(\mathbb{F}_q)|\,q^{r(n-r)}$ et l'équation aux classes donne $|A_r| = |\mathcal{GL}_n(\mathbb{F}_q)| \,/\, |\mathrm{Stab}(V)|$.

BIBLIOGRAPHIE

[Aud06] M. AUDIN : *Géométrie*. EDP Sciences, 2006.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. PEYRÉ : *L'algèbre discrète de la transformée de* FOURIER. Ellipses, 2004.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

1. comptées avec l'ordre des éléments

102 GROUPE DES NOMBRES COMPLEXES DE MODULE 1. SOUS-GROUPES DES RACINES DE L'UNITÉ. APPLICATIONS.

I. De l'exponentielle complexe au groupe $\mathbb{U}$

I. A. Autour de l'exponentielle

[Rud98, Prologue, p1–4] [AF93, §VI.7, p226]

Définition 1. [Exponentielle, cosinus et sinus]
On définit les séries entières suivantes :

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

Proposition 2.
(i) $\exp, \sin, \cos$ *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,*
(ii) Pour tout $z \in \mathbb{C}$, *on a* $\exp(iz) = \cos(z) + i\sin(z)$,
(iii) Pour $\theta \in \mathbb{R}$, $\cos(\theta)$ *et* $\sin(\theta)$ *sont réels et* $\left|\mathrm{e}^{i\theta}\right| = 1$.
(iv) $\exp$ *est un morphisme surjectif de* $(\mathbb{C}, +)$ *dans* $(\mathbb{C}^*, \times)$ *de noyau* $ia\mathbb{Z}$ *pour un* $a \in \mathbb{R}_+$.
(v) Pour $z_1, z_2 \in \mathbb{C}$, $\exp(z_1 + z_2) = \exp(z_1)\exp(z_2)$,

Remarque 3. On note alors $\mathcal{E} : \mathbb{R} \longrightarrow \mathbb{C}^*, t \longmapsto \mathrm{e}^{it}$ et $\pi = a/2$ (ainsi $\mathrm{e}^{i\pi} + 1 = 0$).
Cette application associe à un angle t l'unique point u de module 1 dont l'angle entre $[Ox)$ et $[Ou)$ est t. On le précisera dans la partie II. A. .

Corollaire 4. [Formule de Moivre et d'Euler]
- *Pour* $n \in \mathbb{N}$ *et* $\theta \in \mathbb{R}$, *on a* $(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$.
- *Pour* $\theta \in \mathbb{R}$, *on a* $\cos(\theta) = \frac{\mathrm{e}^{i\theta} + \mathrm{e}^{-i\theta}}{2}$ *et* $\sin(\theta) = \frac{\mathrm{e}^{i\theta} - \mathrm{e}^{-i\theta}}{2i}$.

Application 5. Développement de $\cos(n\theta)$ et $\sin(n\theta)$ par la formule de Moivre. Linéarisation de $\cos^n(\theta)$ et $\sin^n(\theta)$ par les formules d'Euler. Exemples de $\cos^5(\theta)$ et $\sin(5\theta)$.

Application 6. Polynôme de Tchebychev.

Application 7. Calcul des noyaux de Dirichlet et Fejér :

$$D_N = \sum_{n=-N}^{N} \mathrm{e}^{in.} = \frac{\sin\left(\frac{2N+1}{2}.\right)}{\sin(./2)} \quad \text{et} \quad K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n = \sum_{n=-N}^{N} \left(1 - \frac{|n|}{N}\right) e_n = \frac{\sin^2(N./2)}{\sin^2(./2)}$$

I. B. Le groupe des nombres complexes de module 1

[AF93, §VI.7/8, p226]

On notera $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ le groupe des racines de l'unité, $\mathbb{U}_\mathbb{Q} = \left\{\mathrm{e}^{2ip\pi} \mid p \in \mathbb{Q}\right\}$. Pour $n \in \mathbb{N}^*$, on pose $\mathbb{U}_n = \left\{\mathrm{e}^{2i\frac{k\pi}{n}} \mid k \in \mathbb{N}^*\right\}$ le sous-groupe des racines n-ièmes de l'unité.

Exemple 8. $\mathbb{U}_1, \mathbb{U}_2, \mathbb{U}_3, \mathbb{U}_4$ et représentation sur le plan. **[voir annexe]**

Proposition 9.
- *Pour* $n \in \mathbb{N}^*$, $\mathbb{U}_n \subset \mathbb{U}_\mathbb{Q} \subset \mathbb{U}$ *sont des sous-groupes de* $(\mathbb{C}^*, \times)$ *et* $\mathbb{U}_n$ *est fini d'ordre* n.
- $\mathcal{E} : \mathbb{R} \longmapsto \mathbb{U}$ *est un morphisme surjectif et induit un isomorphisme* $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$.
- $\mathbb{R}_+^* \times \mathbb{U} : \mathbb{C}^* \longrightarrow, (r, u) \longmapsto r\mathcal{E}(u)$ *est un isomorphisme de groupes.*

Application 10. Pour $n \geq 2$, on a $\sum_{\omega\in\mathbb{U}_n} \omega = 0$.

Application 11. Résolution de $z^n = z_0$ pour un $z_0 \in \mathbb{C}$.

Proposition 12.
(i) Tout sous-groupe de $\mathbb{U}$ *est soit discret, soit dense dans* $\mathbb{U}$. *De plus les seuls sous-groupes discrets sont les* $(\mathbb{U}_n)_{n\in\mathbb{N}}$.
(ii) $\mathbb{U}_\mathbb{Q}$ *est dense et* $\mathcal{E}_{|\mathbb{Q}}$ *induit un isomorphisme* $\mathbb{Q}/\mathbb{Z} \simeq \mathbb{U}_\mathbb{Q}$.
(iii) Les sous-groupes compacts de $(\mathbb{C}^*, \times)$ *sont* $\mathbb{U}$ *et les* $(\mathbb{U}_n)_{n\in\mathbb{N}}$.
(iv) Chaque $\mathbb{U}_n$ *est cyclique et isomorphe à* $\mathbb{Z}/n\mathbb{Z}$. *Les générateurs de* $\mathbb{U}_n$ *sont les racines* n*-ièmes primitives de l'unité :* $\mathbb{U}_n^\times = \left\{\mathrm{e}^{2i\frac{k\pi}{n}} \mid k \in \mathbb{Z} \text{ et } k \wedge n = 1\right\}$.
(v) $\phi_n : \begin{array}{ccc} \mathbb{U} & \longrightarrow & \mathbb{U} \\ z & \longmapsto & z^n \end{array}$ *est un morphisme de groupe continu pour* $n \in \mathbb{Z}^*$, *de noyau* $\mathbb{U}_{|n|}$.

Exemple 13. Racines primitives $2, 3, 4, 8$-èmes de l'unité.

Proposition 14. *On note* $\varphi(n)$ *le cardinal de* $\mathbb{U}_n^\times$.
- $\mathbb{U}_d \subset \mathbb{U}_n$ *si et seulement si* $d \mid n$,
- $\mathbb{U}_n = \cup_{d|n} \mathbb{U}_d^\times$,
- $n = \sum_{d|n} \varphi(d)$.

Remarque 15. $u \in \mathbb{U}_n$ est d'ordre n si et seulement si $u^d \neq 1$ pour tout $d < n$ tel que $d \mid n$.

II. Angles orientés et argument

II. A. Angles orientés et rotations du plan [Aud06, §III.1, p73] [Rom17, §4.6, p112]

Notion d'angles orientés, lien avec l'argument d'un nombre complexe

Définition 16. [Rotation]
La rotation autour de 0 d'angle θ est l'application $r_\theta : \mathbb{C} \longrightarrow \mathbb{C}, z \longmapsto z\mathcal{E}(\theta)$.
La rotation autour de $a \in \mathbb{C}$ d'angle θ est l'application $r_{\theta,\,a} : \mathbb{C} \longrightarrow \mathbb{C}, z \longmapsto a + r_\theta(z-a)$.

Proposition 17. *Les rotations sont des isométries. En particulier $\mathbb{U}$ est stable par toute rotation autour de 0.*

Application 18. [Rotations préservant un polygone à n côtés]
Les rotations du plan préservant un polygone régulier à n côtés de centre O est un groupe constitué des n rotations de centre O et d'angle $\frac{k2\pi}{n}$ pour $k \in [\![0, n-1]\!]$. Autrement dit c'est $\{z \longmapsto z\omega \,|\, \omega \in \mathbb{U}_n\}$.

Remarque 19. Si l'on rajoute les n symétries d'axe 2 sommets ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair, on obtient le groupe des isométries du plan préservant le polygone régulier à n côtés : c'est le groupe diédral D_{2n}.

II. B. Argument continu et logarithme continu sur les ouverts de $\mathbb{C}^*$ [Tau06, §5.3, p62]

Définition 20. Soit Ω un ouvert de $\mathbb{C}^*$.
- Un argument continu sur Ω est une application continue $\Theta : \Omega \longrightarrow \mathbb{R}$ telle que pour tout $z \in \Omega$, $\frac{z}{|z|} = \mathcal{E} \circ \Theta(z)$.
- Un logarithme continu sur Ω est une application continue $\ell : \Omega \longrightarrow \mathbb{C}$ telle que pour tout $z \in \Omega, z = \exp \circ \ell(z)$.

Proposition 21. *Soit $\Omega = \mathbb{C} \setminus \mathbb{R}_-$.*
- *Il existe un argument continu Θ sur Ω. Si on suppose de plus Θ à valeurs dans $]-\pi, \pi[$, on a alors unicité et on appelle Θ la détermination principale de l'argument,*
- *Il existe un logarithme continu sur Ω.*

Proposition 22. *Soit Ω un ouvert connexe de $\mathbb{C}$ et $\ell : \Omega \longrightarrow \mathbb{C}$. Alors on a équivalence :*
- *Il existe $C \in \mathbb{C}$ tel que $C + \ell$ est un logarithme continu sur Ω,*
- *ℓ est une primitive de $z \longmapsto 1/z$ sur Ω.*

En particulier, tout logarithme continu sur Ω est holomorphe.

III. Polynômes cyclotomiques

III. A. Définitions et propriétés [Per96, §3.4, p80]

Soit $n \in \mathbb{N}^*$.

Définition 23. [Polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

Exemples, …

Proposition 24.
(i) Φ_n est unitaire de degré $\varphi(n) = \mathrm{card}(\{k \in [1, n] \,|\, k \wedge n = 1\})$.
(ii) $X^n - 1 = \prod_{d|n} \Phi_d$. En particulier, si n est premier : $\Phi_n = X^n - 1$.

Proposition 25. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 26. *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

Corollaire 27. *On a $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.*

III. B. Applications [Gou09, p89/93] [FGN07, p213]

Théorème 28. [Théorème de Wedderburn]
Toute algèbre à division finie est un corps.

Théorème 29. [Théorème de Kronecker]
Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes les racines de P sont de module inférieur ou égal à 1 et $P(0) \neq 0$, alors toutes les racines de P sont des racines primitives de l'unité.

Corollaire 30. [Théorème de Kronecker]
Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module inférieur ou égal à 1, alors $P = X$ ou $P = \Phi_k$ pour un $k \in \mathbb{N}^*$.

IV. Autres applications

IV. A. Représentations linéaires complexes / caractères d'un groupe abélien fini ? [Rom17, Ch6, p179] [Ser98, Ch2, p23]

Soit G un groupe et E un $\mathbb{C}$-espace vectoriel de dimension finie.

Définition 31. [Représentation]
Une représentation (linéaire) de G dans E est un morphisme de groupes $\rho : G \longmapsto \mathrm{GL}(E)$.

Remarque 32. Se donner une représentation de G dans E revient à se donner une action de groupes de G sur E en posant $\rho(g)(x) = g.x$.

Proposition 33. *Lorsque $\dim(E) = 1$ et G est fini, $E \simeq \mathbb{C}$ et on a $\rho(g)_{|\mathbb{U}} : \mathbb{U} \longrightarrow \mathbb{U}$ pour tout $g \in G$.*

Exemple 34. [Représentation triviale] $\rho : g \longmapsto \mathrm{Id}_E$ est une représentation de G sur E.

Exemple 35. Si E est de dimension 1 :
- les représentations de $\mathfrak{S}_n$ dans E sont $\rho : \sigma \longrightarrow \mathrm{Id}_E$ et $\rho : \sigma \longrightarrow \varepsilon(\sigma)\,\mathrm{Id}_E$.
- les représentations de $\mathbb{Z}/2\mathbb{Z}$ dans E sont $\rho : \overline{x} \longrightarrow \mathrm{Id}_E$ et ρ définie par $\rho(\overline{1}) = -\mathrm{Id}_E$.

Exemple 36. [Représentations de permutations]
$\mathfrak{S}_n \longrightarrow \mathrm{GL}_n(\mathbb{C}), \sigma \longmapsto P_\sigma$ est une représentation de $\mathfrak{S}_n$ sur $\mathbb{C}^n$.
Plus généralement, si G est fini de cardinal n et E est de dimension n, soit $(e_g)_{g\in G}$ une base de E. Alors l'application linéaire $\rho(g)$ définie par $\rho(g)(e_h) = e_{gh}$ pour $h \in G$ définit une représentation de G dans E.

Caractères : propriétés des caractères : somme de racines de l'unité, etc
Table des caractères irréductibles de $\mathbb{Z}/n\mathbb{Z}$: on retrouve des racines n-ièmes de l'unité ...

IV. B. Transformée de Fourier discrète et interpolation polynomiale [Pey04, §III.2, p65]

Soit $N \in \mathbb{N}^*$ et $\omega = \exp(2i\pi/N)$.

Définition 37. [Transformée de Fourier discrète]
Soit $f = (f_0, \dots, f_{N-1}) \in \mathbb{C}^{N+1}$. On définit la transformée de Fourier discrète de f par le vecteur $\hat{f}$ tel que :

$$\forall k \in [\![0, N-1]\!], \quad \hat{f}_k = \frac{1}{N}\sum_{j=0}^{N-1} f_j \omega^{-kj}$$

Proposition 38. *L'application $f \longmapsto \hat{f}$ est un isomorphisme d'espaces vectoriels de $\mathbb{C}^n$ dans lui-même.*

Remarque 39. Autrement dit, pour tout $(c_0, \dots, c_{N-1}) \in \mathbb{C}^n$, il existe un unique polynôme $P = \frac{1}{N}\sum_{i=0}^{N-1} a_i X^i \in \mathbb{C}_{N-1}[X]$ tel que pour tout $k \in [\![0, N-1]\!]$, on a $P(\omega^k) = c_k$.

Corollaire 40. *La transformée de Fourier inverse discrète de $\hat{f}$ est le vecteur de j-ième coordonnée $\sum_{k=0}^{N-1} \hat{f}_k \omega^{kj}$.*

Application 41. [Transformée de Fourier rapide]
On peut calculer la transformée de Fourier discrète d'un N-échantillon en $\mathcal{O}(N\log(N))$ (alors que la formule initiale donne un $\mathcal{O}(N^2)$).

ANNEXE

Dessin du cercle unité et racines primitives, polygones réguliers.
Table de caractères

SPEECH

Les nombres complexes sont un outil puissant, en géométrie comme en algèbre. Leur richesse est en grande partie déterminée par la sphère unité et les propriétés de ses éléments, notamment de ses sous-groupes, interviennent donc fréquemment.
Dans une première partie, on reconstruit $\mathbb{C}$ à partir de l'exponentielle complexe, cela mène aux propriétés de linéarisation et aux propriétés de $\mathbb{U}$.
Dans un second temps, on s'intéresse aux déterminations continues d'argument et de logarithme.
Ensuite, on regarde les applications en algèbre avec les polynômes cyclotomiques et leurs propriétés.
Enfin, il y a de nombreuses autres applications du groupe des racines de l'unité, nous regardons leur rôle dans les représentations linéaires complexes, puis dans les questions autour de la transformée de Fourier discrète, qui permet des multiplications rapides.

QUESTIONS

Q Pourquoi sait-on qu'il n'y a pas d'argument continu sur $\mathbb{C}^*$?

R Pour le logarithme, on sait que c'est une primitive de $z \longmapsto 1/z$, et en intégrant sur un chemin fermé on ne trouve pas 0.

Q Donner des applications des polynômes cyclotomiques ?

Q Soit $\alpha \in [0, \pi/2[$. Partant de $x_0 = 1$, on génère x_1 comme le point d'intersection distinct de x_0 du cercle trigonométrique avec la droite passant par x_0 et d'angle α avec la droite (Ox_1). Puis les points $x_2, x_3, \dots$ sont générés itérativement de manière similaire : x_{i+1} est obtenu comme le point d'intersection distinct de x_i du cercle trigonométrique avec la droite passant par x_i et telle que (Ox_i) est la bissectrice de $\widehat{x_{i-1}x_ix_{i+1}}$. Calculer $x_1, x_2, \dots$. Montrer que $\{x_i\}_{i\in\mathbb{N}}$ est fini ou dense dans $\mathbb{U}$.

R Distinguer selon que α/π soit commensurable ou non.

Q Peut-on trouver deux dés de lois indépendantes μ et ν telle que la somme des deux dés suive une loi uniforme sur $[\![2, 12]\!]$.

R Supposons que ce soit le cas. On calcule la fonction génératrice de la somme des deux dés et on obtient $g_{1+2}(s) = \frac{1}{11}s^2\frac{1-s^{11}}{1-s} = g_1(s)g_2(s)$. Ainsi g_{1+2} a 0 pour racine double et les 10 autres racines sont $\mathbb{U}_{11} \setminus \{1\}$, g_1 a 0 pour racine simple et des éléments de $\mathbb{U}_{11} \setminus \{1\}$ conjugués, tout comme g_2. C'est absurde puisqu'alors soit g_1 a 7 racines et g_2 en a 5, mais elles ne peuvent pas avoir chacune 6 racines.

BIBLIOGRAPHIE

[AF93] J.M. Arnaudiès et H. Fraysse : *Cours de mathématiques, Tome 1, Algèbre*. Dunod, 1993.

[Aud06] M. Audin : *Géométrie*. EDP Sciences, 2006.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. Peyré : *L'algèbre discrète de la transformée de* Fourier. Ellipses, 2004.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rud98] W. Rudin : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

[Ser98] J.-P. Serre : *Représentations linéaires des groupes finis*. Hermann, 1998.

[Tau06] P. Tauvel : *Analyse complexe pour la Licence 3*. Dunod, 2006.

103 EXEMPLES DE SOUS-GROUPES DISTINGUÉS ET DE GROUPES QUOTIENTS. APPLICATIONS.

Soit G un groupe et H un sous-groupe de G.

I. Définitions et premières propriétés [Per96, ChI, p9]

I. A. Classes à gauche

Définition d'une classe à gauche, ensemble quotient, indice, théorème de LAGRANGE.

I. B. Sous-groupes distingués [Rom17, §10.1, p277]

Définition groupe distingué, exemples (noyau d'un morphisme ...)
Cas des groupes abéliens (réciproque fausse, cf quaternions), sous-groupe distingué équivaut à réunion de classes de conjugaison
Exemple des sous-groupes d'indice 2 qui sont toujours distingués
Notion de groupe quotient, exemple de $\mathbb{Z}/n\mathbb{Z}$
Bijections entre sous-groupes de G contenant H et sous-groupes de G/H. Exemple des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

I. C. Liens avec d'autres sous-groupes

Groupe caractéristique, caractéristique implique distingué
centre d'un groupe : caractéristique
Commutateurs, groupe dérivé : c'est un groupe caractéristique et $G/D(G)$ est abélien. C'est le plus petit sous-groupe distingué pour lequel G/H est abélien.
Exemples de groupes dérivés pour le groupe symétrique
Normalisateur de H : plus grand sous-groupe de G dans lequel H est distingué.

I. D. Passage au quotient [Lan14, Ch1.3, p17]

Propriété universelle du groupe quotient, isomorphisme $G/\ker(f) \simeq \mathrm{Im}(f)$.
Application au groupe cycliques d'ordre n : isomorphes à $\mathbb{Z}/n\mathbb{Z}$, isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$ de l'exponentielle, déterminant
Théorèmes d'isomorphismes :

- si H est distingué dans G, H' est distingué dans G' et $f : G \longrightarrow G'$ tels que $f(H) \subset H'$, alors il existe $\overline{f} : G/H \longrightarrow G'/H'$ unique tel que $\pi' \circ f = \overline{f} \circ \pi$.
  Exemple de $u \in \mathcal{L}(E)$ possédant un sous-espace vectoriel F stable : endomorphisme quotient $u_{E/F}$ [MM16, §II.6, p18]. Exemple de l'opérateur par translation dans $\mathcal{L}^p$ laissant stable les fcts cstes pp : passage au quotient dans L^p,
- si $H \subset K$ sont distingués dans G : H est distingué dans K, K/H est distingué dans G/H et $G/K \simeq (G/H)/(H/K)$,
- si H est distingué dans G, $K < G$. Alors H est distingué dans KH, $H \cap K$ est distingué dans K et $HK/H \simeq K/(K \cap H)$.

II. Utilisation des sous-groupes distingués

II. A. Groupes simples [Per96, Ch1, p9]

Groupes simples. Exemple si G simple non abélien : $D(G) = G$.

PROPOSITION 1. *Pour $n \geq 5$, $\mathfrak{A}_n$ est simple.*

Application : sous-groupes distingués de $\mathfrak{S}_n$ pour $n \neq 4$: $\{\mathrm{id}\}, \mathfrak{A}_n, \mathfrak{S}_n$.
Un groupe infini possédant un sous-groupe strict d'indice fini n'est pas simple.

II. B. Théorèmes de SYLOW [Per96, §1.5, p18–20]

On suppose G fini d'ordre n.
Soit p un nombre premier diviseur de n. On notera $n = p^a m$ où $p \nmid m$.

DÉFINITION 2. [p-GROUPE, p-SOUS-GROUPE DE SYLOW]
Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de SYLOW (ou p-SYLOW) un sous-groupe de G de cardinal p^a.

THÉORÈME 3. [THÉORÈME DE SYLOW 1] *Il existe au moins un p-SYLOW dans G.*

COROLLAIRE 4. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

THÉORÈME 5. [THÉORÈME DE SYLOW 2]
(i) Si $H < G$ est un p-groupe, alors il existe un p-SYLOW S tel que $H < S$,
(ii) Les p-SYLOW de G sont tous conjugués,
(iii) Notons Σ le nombre de p-SYLOW de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.

COROLLAIRE 6. *Soit S un p-SYLOW de G. Alors $S \lhd G \iff S$ est l'unique p-SYLOW de G.*

APPLICATION 7. Tout groupe d'ordre 63 ou 255 n'est pas simple.

II. C. Produits direct et semi-direct

[Per96, §1.6, p20]

Définition 8. [produit direct]
- Soit G un groupe et $N, H < G$ tels que N, H commutent, $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit direct de N par H.
- Soit N et H des groupes. Le produit direct de N et H est le produit cartésien $G = N \times H$, muni de la loi $(n, h).(n', h') = (nn', hh')$.

Lemme 9. [lemme chinois]
$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si $m \wedge n = 1$.

Définition 10. [produit semi-direct]
- Soit G un groupe, $N \lhd G$ et $H < G$ tel que $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit semi-direct de N par H.
- Soit N et H des groupes et $\phi : H \longrightarrow \mathrm{Aut}(N)$. On définit le produit $(n, h).(n', h') = (n\phi(h)(n'), hh')$ sur $G = N \times H$. $(G, .)$ est alors une groupe appelé produit semi-direct de N par H. On note $G = N \rtimes_\phi H$.

Exemple 11. $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$ et le produit n'est pas direct.

Exemple 12. Groupe diédral

Exemple 13. Contre-exemple : $\mathbb{Z}/8\mathbb{Z}$ et le groupe des quaternions H_8 ne peuvent être écrits comme un produit semi-direct non trivial.

Proposition 14. *$N \rtimes_\phi H$ est bien un groupe dont $\overline{N} = N \times \{1_H\}$ est un sous-groupe distingué et $\overline{H} = \{1_N\} \times H$ est un sous-groupe, distingué si et seulement si $\phi = 1$.*

II. D. Théorie des représentations

[Rom17, Ch6, p182] [Ser98, Ch2, p23] [Pey04, §VIII.1.4/VIII.2.1, p228–232]

Caractères de degré 1. Isomorphisme $\widehat{G/D(G)} \simeq \hat{G}$ via la projection (par passage au quotient)
Représentation, caractère associé, produit scalaire sur les fonction centrales, caractères irréductibles : famille orthonormée *puis* base orthonormée, exemple des groupes abéliens
Cas de la représentation naturelle de G/N par permutation
$\overline{\rho}$ représentation de G/N implique $\rho = \overline{\rho} \circ \pi$ représentation de même degré, irréductible si et seulement si $\overline{\rho}$ l'est.
Table de caractères, exemple

Soit G un groupe fini. Soient $\chi_1, \dots, \chi_r$ ses caractères irréductibles.

Lemme 15. *Soit χ associé à une représentation (ρ, V) de G. Alors $\ker(\rho) = \ker(\chi) = \{g \in G \,|\, \chi(g) = \chi(1)\}$.*

Proposition 16. *Les sous-groupes distingués de G sont de la forme $\cap_{i \in I} \ker \chi_i$ où $I \subset [\![1, r]\!]$.*

Application 17. Table des caractères de $\mathfrak{S}_4$.

III. Le groupe linéaire

[Per96, ChIV, p95]

E est un $\mathbb{K}$-espace vectoriel de dimension finie n.
Les transvections engendrent $\mathrm{SL}(E)$, sont conjuguées deux à deux dans $\mathrm{SL}(E)$ pour $n \geq 3$
Centre de $\mathrm{GL}(E)$, de $\mathrm{SL}(E)$, groupe (spécial) projectif
$\mathrm{PSL}_n(\mathbb{K})$ est simple pour $n \geq 3$
Suite exacte de $\mathrm{PGL}_n(\mathbb{K})$
Quelques isomorphismes simples

ANNEXE

Treillis de quelques groupes en soulignant les groupes distingués

QUESTIONS

Q Décomposer $\mathcal{GL}_n(\mathbb{K})$ en un produit (semi-)direct.

R $\mathcal{GL}_n(\mathbb{K}) \simeq \mathcal{SL}_n(\mathbb{K}) \rtimes \mathbb{K}^*$ et on a la suite exacte $1 \to \mathrm{SL}_n(\mathbb{K}) \to \mathrm{GL}_n(\mathbb{K}) \overset{\det}{\to} \mathbb{K}^* \to 1$.

Q Et pour $\mathbb{Z}$?

R $1 \to \mathbb{Z} \overset{\iota}{\to} \mathbb{Z} \overset{\pi}{\to} \mathbb{Z}/n\mathbb{Z} \to 1$ où $\iota : m \longmapsto nm$

Q Soit $\mathcal{E}$ un espace affine contenant 0. Décomposer $\mathrm{GA}(\mathcal{E})$.

R On montre que $1 \to T(\mathcal{E}) \to \mathrm{GA}(\mathcal{E}) \to \mathrm{GL}(\mathcal{E}) \to 1$.

Q Pour les isométries du cube ?

R On vérifie que $\mathrm{Isom}^+(\mathcal{C}) \rtimes \langle s \rangle \simeq \mathrm{Isom}(\mathcal{C})$ où s est une symétrie.
Ici le produit est direct car le groupe est abélien.

Q Soit G un groupe d'ordre 300. G est-il simple ?

R Écrivons $300 = 2^2 \times 3 \times 5^2$ et regardons les 5-Sylow. Notons Σ_5 leur nombre. On sait que $\Sigma_5 \mid 12$ et $\Sigma_5 \equiv 1 \mod 5$, donc $\Sigma_5 \in \{1, 6\}$. Si G est simple, $\Sigma_5 = 6$ et G agit sur Σ_5. Regardons $f : G \longrightarrow \mathfrak{S}_{\Sigma_5} \simeq \mathfrak{S}_6$. Son noyau ne peut être G, c'est donc $\{1\}$ et les 5-sylow sont distingués : contradiction. Donc G n'est pas simple.

BIBLIOGRAPHIE

[Lan14] S. Lang : *Algèbre*. Dunod, 3ème édition, 2014.

[MM16] R. Mansuy et R. Mneimné : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. Peyré : *L'algèbre discrète de la transformée de* Fourier. Ellipses, 2004.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Ser98] J.-P. Serre : *Représentations linéaires des groupes finis*. Hermann, 1998.

104 GROUPES FINIS. EXEMPLES ET APPLICATIONS.

I. Généralités et outils des groupes finis

[Per96, Ch1, p9–18]

I. A. Vocabulaire des groupes finis

Définition 1. [Groupe, sous-groupe, morphisme, ordre]
- $(G, \times)$ est un groupe si G est un ensemble muni d'une loi de composition interne $\times$ associative, admettant un élément neutre 1 et telle que tout élément admet un élément inversible.
  G est dit commutatif ou abélien si $xy = yx$ pour $x, y \in G$.
  G est dit fini s'il est de cardinal fini.
- $H \subset G$ est un sous-groupe de G s'il est stable pour la loi de G et que c'est un groupe pour la loi induite.
- $\phi : G \longrightarrow G'$ est un morphisme de groupes si G, G' sont des groupes et si $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ pour tout $g_1, g_2 \in G$.
- Pour $g \in G$, on appelle ordre d'un élément $g \in G$ le plus petit entier n non nul tel que $g^n = 1$. On le note $o(g)$ et on a $|\langle g \rangle| = o(g)$.

Exemple 2. $\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$ sont des groupes finis. L'ordre de $\overline{1}$ est n, l'ordre de $(a_1\ a_1\ \dots\ a_\ell)$ est ℓ.

Soit $(G, .)$ un groupe fini d'ordre $n \in \mathbb{N}^*$.

Définition 3. [Classes à gauche]
Pour $H < G$, on définit $G/H = \{gH \mid g \in G\}$ l'ensemble des classes à gauche modulo H.
On note $[G : H] = |G/H|$.

Théorème 4. [Théorème de Lagrange]
L'ordre de tout sous-groupe de G divise n. En particulier, l'ordre d'un élément de G divise n.

Exemple 5. Pour $g \in G$, on a $o(g) \mid n$.

Définition 6. [Groupe distingué, groupe quotient, groupe simple]
$H < G$ est dit distingué si pour tout $g \in G$, $gH = Hg$. Dans ce cas, on note alors $H \lhd G$ et on remarque que G/H est muni naturellement d'une structure de groupe.

Exemple 7. Si $[G : H] = 2$, H est distingué dans G.

Définition 8. [Groupe cyclique]
G est dit cyclique si $G = \langle g \rangle$ pour un $g \in G$ (on rappelle que G est fini).

Remarque 9. Un groupe cyclique est abélien.

Exemple 10. Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est cyclique d'ordre n.

Définition 11. [Exposant d'un groupe]
On note $e(G)$ le PPCM des ordres des éléments de G.

Exemple 12. Si G est abélien, il existe $g \in G$ tel que $o(g) = e(G)$.

I. B. Actions de groupes

Définition 13. [Action d'un groupe sur un ensemble, vocabulaire des actions]
On dit que G opère à gauche sur X si on a une application $G \times X \longrightarrow X, (g, x) \longmapsto g.x$ telle que $\forall g, h \in G, \forall x \in X, g.(h.x) = (gh).x$ et $\forall x \in X, 1.x = x$.
Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = \{g.x \mid x \in X\}$. On note $\mathcal{O}$ l'ensemble des orbites de X. C'est une partition de X.
On appelle stabilisateur de $x \in X$ le groupe $\mathrm{Stab}(x) = \{g \in G \mid g.x = x\}$.
Pour $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X \mid g.x = x\}$.

Exemple 14. G opère sur lui-même par conjugaison : $g.h = ghg^{-1}$. On note $\mathrm{Int}(G) = \{\mathrm{Int}(g), g \in G\}$ l'ensemble des automorphismes intérieurs de G, où $\mathrm{Int}(g) : h \longmapsto ghg^{-1}$.
On remarque alors que G agit sur tout sous-groupe distingué H de G par cette opération.

Dans la suite de cette partie on suppose X fini.

Corollaire 15. [Équation aux classes]
Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Application 16. Notons $X^G = \{x \in X \mid \forall g \in G, g.x = x\} = \{x \in X \mid \mathrm{Fix}(x) = G\}$. Alors si G est un groupe d'ordre p^k où p est premier et $k > 1$, on a $\left|X^G\right| \equiv X \mod p$.

Exemple 17. [Action par conjugaison] Si G agit par conjugaison sur lui-même, notons $Z_h(G) = \left\{g \in G \mid ghg^{-1} = h\right\}$. Alors $|G| = |Z(G)| + \sum_{O \in \mathcal{O} \mid |O| \geq 2} \frac{|G|}{|Z_{x_O}(G)|}$.

Application 18. Le centre d'un groupe d'ordre p^k où p est premier et $k \geq 1$ est non trivial.

I. C. Sous-groupes de Sylow

Soit p un nombre premier diviseur de $n \in \mathbb{N}^*$. On notera $n = p^a m$ où $p \nmid m$.

Définition 19. [p-groupe, p-sous-groupe de Sylow]
Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de Sylow (ou p-Sylow) un sous-groupe de G de cardinal p^a.

Théorème 20. [Théorème de Sylow 1] *Il existe au moins un p-Sylow dans G.*

Corollaire 21. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

Théorème 22. [Théorème de Sylow 2]
(i) Si $H < G$ est un p-groupe, alors il existe un p-Sylow S tel que $H < S$,
(ii) Les p-Sylow de G sont tous conjugués,
(iii) Notons Σ le nombre de p-Sylow de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.

Application 23. Un groupe d'ordre 40 a 4 éléments d'ordre 5.

Corollaire 24. *Soit S un p-Sylow de G. Alors $S \lhd G \iff S$ est l'unique p-Sylow de G.*

Application 25. Tout groupe d'ordre 63 ou 255 n'est pas simple.

II. Exemples fondamentaux

Soit $n \in \mathbb{N}^*$ et p un entier premier.

II. A. Le groupe $\mathbb{Z}/n\mathbb{Z}$ [Rom17, §1.4, p14–15]

Définition 26. [Le groupe $\mathbb{Z}/n\mathbb{Z}$]
En remarquant que $n\mathbb{Z}$ est distingué dans $\mathbb{Z}$, on définit le groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Proposition 27. *$\mathbb{Z}/n\mathbb{Z}$ est cyclique, de générateurs les $\overline{d}$ tels que $d \wedge n = 1$.*

Proposition 28. *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 29. Un groupe de cardinal p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 30. *[Per96, §1.7, p24] On a $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. En particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est abélien de cardinal $\varphi(n)$.*
De plus, $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z})$.

II. B. Le groupe $\mathfrak{S}_n$ [Rom17, Ch2, p39]

Définition 31. [Groupe symétrique $\mathfrak{S}_n$]
On note $\mathfrak{S}_n$ le groupe des permutations de $[\![1, n]\!]$.

Théorème 32. [Théorème de Cayley]
Si G est d'ordre n, il est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Proposition 33. *Les familles suivantes engendrent $\mathfrak{S}_n$:*
- *les transpositions $((i\ j))_{1 \le i < j \le n}$,*
- *les transpositions $((1\ i))_{2 \le i \le n}$,*
- *les transpositions $((i\ i+1))_{1 \le i \le n-1}$,*
- *la transposition $(1\ 2)$ et le cycle $(1\ 2\ \dots\ n)$.*

Proposition 34. *Toute permutation σ de $\mathfrak{S}_n$ se décompose en un produit de cycles à supports disjoints. Ce produit est unique à l'ordre des cycles près. En particulier, la suite $(\ell_1, \ell_2, \dots, \ell_m)$ des longueurs des cycles est unique si on impose $\ell_1 \ge \ell_2 \ge \cdots \ge \ell_m$. On appelle cette suite le type de σ.*

Proposition 35. [Classes de conjugaisons de $\mathfrak{S}_n$]
Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type.

Proposition 36. *Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$: l'identité et le morphisme $\mathcal{E}$ qui envoie toute transposition sur -1.*

Définition 37. On appelle $\mathcal{E}$ l'application signature. On définit le groupe alterné $\mathfrak{A}_n$ comme étant le noyau de $\mathcal{E}$.

Proposition 38. *Pour $n \ge 5$, $\mathfrak{A}_n$ est simple.*

Corollaire 39. *Pour $n \ge 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

III. Applications

III. A. Constructions de groupes finis [Per96, §1.6, p20]

Idée : à partir des groupes que nous connaissons, créer des groupes finis « plus complexes ».

Définition 40. [Produit direct]
- Soit G un groupe et $N, H < G$ tels que N, H commutent, $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit direct de N par H.
- Soit N et H des groupes. Le produit direct de N et H est le produit cartésien $G = N \times H$, muni de la loi $(n, h).(n', h') = (nn', hh')$.

Lemme 41. [Lemme chinois]
$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si $m \wedge n = 1$.

Définition 42. [Produit semi-direct]
- Soit G un groupe, $N \lhd G$ et $H < G$ tel que $N \cap H = \{1\}$ et $G = NH$. Alors on dit que G est le produit semi-direct de N par H.
- Soit N et H des groupes et $\phi : H \longrightarrow \mathrm{Aut}(N)$. On définit le produit $(n, h).(n', h') = (n\phi(h)(n'), hh')$ sur $G = N \times H$. $(G, .)$ est alors une groupe appelé produit semi-direct de N par H. On note $G = N \rtimes_\phi H$.

Exemple 43. $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$ et le produit n'est pas direct.

Exemple 44. Contre-exemple : $\mathbb{Z}/8\mathbb{Z}$ et le groupe des quaternions $\mathbb{H}_8$ ne peuvent être écrits comme un produit semi-direct non trivial.

III. B. Le groupe diédral [Aud06, Ch3/5, p360] [Rom17, §3.4.3/6.1, p87/180]

Exemple 45. Isométries du plan conservant un segment $[A, B]$ de centre O :
Id l'identité,
ρ la rotation d'angle π et de centre O,
s la symétrie d'axe (AB),
$s\rho$ la symétrie d'axe la droite orthogonale à (AB) passant par O.
On vérifie que ces isométries forment un groupe isomorphe au groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$.

Définition 46. [Déplacement, antidéplacement]
Un déplacement (resp. antidéplacement) est un isomorphisme dont la partie linéaire est de déterminant 1 (resp. -1).

Soit G groupe fini d'isométries. On note G^+ ses déplacements et G^- ses antidéplacements.

Proposition 47.
- *Il existe un point fixe à toutes les isométries de G,*
- *G^+ est cyclique, engendré par une rotation ρ.*
- *Si G contient un antidéplacement σ, alors $[G : G^+] = 2$ et $G^- = \sigma G^+$. σ est une réflexion dont l'axe contient le centre de ρ. On a $G = \langle \sigma, \rho \rangle$.*

Exemple 48. Le groupe des isométries du plan préservant un polygône régulier à n côtés de centre O contient : contient les rotations d'ordre n autour du centre et les n réflexions par rapport aux droites joignant :
i) n rotations de centre O et d'angle $\frac{k2\pi}{n}$ pour $k \in [\![0, n-1]\!]$,
ii) n symétries d'axe 2 sommets ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair.
C'est le groupe diédral D_{2n}.

III. C. Classifications [Szp09, §6.VI/6.VII, p254/276-278]

Idée : on se donne un groupe fini. Peut-on le décomposer en produits de groupes « faciles » déjà construits ?

Exemple 49. Pour p premier, un groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

Proposition 50. *On a équivalence :*
- *tous les sous-groupes de Sylow de G sont distingués,*
- *G est le produit direct de ses sous-groupes de Sylow.*

Proposition 51. *Soit G de cardinal pq où $p < q$ sont premiers.* [Per96, §1.7, p27-28]
- *si $p \nmid q - 1$, $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$,*
- *si $p \mid q - 1$, $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}$, où ϕ est une action non triviale de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$.*

Théorème 52. [Structure des groupes abéliens] [Rom17, §1.9, p30]
Supposons G abélien fini d'ordre n. Alors il existe un unique entier ℓ et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que $d_{i+1} \mid d_i$ pour tout $i \leq \ell - 1$ et

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

Exemple 53. Structures possibles d'un groupe abélien de cardinal 120 ou 600.

Application 54. En utilisant les propriétés vues dans cette leçon, on obtient une classification des groupes de petits ordres. Voir le tableau en annexe.

ANNEXE

Classification des groupes de petits ordres :

n	Groupes de cardinal n (à isomorphisme près)
1	$\{1\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, D_6
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_8, $\mathbb{H}_8$
9	$\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^2$
10	$\mathbb{Z}/10\mathbb{Z}$, D_{12}
11	$\mathbb{Z}/11\mathbb{Z}$
$\vdots$	
15	$\mathbb{Z}/15\mathbb{Z}$
21	$\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$
25	$\mathbb{Z}/25\mathbb{Z}$, $(\mathbb{Z}/5\mathbb{Z})^2$
35	$\mathbb{Z}/35\mathbb{Z}$
36	$\mathbb{Z}/36\mathbb{Z}$, $(\mathbb{Z}/6\mathbb{Z})^2$
39	$\mathbb{Z}/39\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$
49	$\mathbb{Z}/49\mathbb{Z}$, $(\mathbb{Z}/7\mathbb{Z})^2$
51	$\mathbb{Z}/51\mathbb{Z}$
120	$\mathbb{Z}/120\mathbb{Z}$, $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$

Quelques treillis de groupes

SPEECH

La notion de groupe est historiquement fondamentale (géométrie, étude des racines des polynômes, …). Pédagogiquement, c'est la première structure algébrique qui apporte une richesse mathématique. Dans cette leçon, on essaye de construire des groupes de petits cardinaux.
Tout d'abord, quelques rappels de vocabulaire et le théorème de Lagrange qui est un résultat fondamental. Puis on introduit les actions de groupes qui sont des outils importants en théorie des groupes, et mènent notamment à l'équation aux classes. La théorie de Sylow, l'étude des p-groupes, a aussi un rôle majeur, car elle permet de donner des informations sur un groupe à partir de son cardinal. Le premier théorème de Sylow sera proposé en développement.
Ensuite, on s'intéresse à deux exemples fondamentaux : $\mathbb{Z}/n\mathbb{Z}$, avec notamment un isomorphisme classique avec les groupes cycliques, et $\mathfrak{S}_n$, dont l'intérêt de l'étude est appuyé par le théorème de Cayley. La simplicité de $\mathfrak{A}_n$ pour $n \geq 5$ sera proposée en développement.
Enfin, dans la dernière partie, on regarde comment créer de nouveaux groupes à partir de groupes simples connus, notamment via les produits (semi)-directs. Le produit semi-direct nous permet notamment de parler de groupe diédral. Puis inversement on s'intéresse à la classification des groupes de petits cardinaux.

COMMENTAIRES

Autres références possibles : [Ale99, Com98, Dem09]

QUESTIONS

Q Un groupe d'ordre 12 ou 30 est-il simple ?

R Pour $n = 12$, on a nécessairement 1 ou 4 3-Sylow. S'il y en a 1, le groupe n'est pas simple. Sinon, il y a 8 éléments d'ordre 3 car les 3-Sylow sont d'intersections $\{1\}$, donc il y a un seul 2-Sylowqui contient les 3 éléments restants et 1. Donc le groupe n'est pas simple non plus. Pour $n = 30$, c'est similaire.

Q Énumérer les groupes de cardinal 12. Y en a-t-il des non commutatifs ?

R Il y a 5 groupes de cardinal 12 (à isomorphisme près). 2 sont abéliens, les autres, comme le groupe diédral D_{12}, ne le sont pas.

Q Soit H non distingué. Peut-on munir G/H d'une structure de groupe ?

Q Tous les sous-groupes de $\mathbb{Z}$ sont distingués, est-ce normal ?

R Oui car $\mathbb{Z}$ est abélien.

Q Un groupe dont tous les sous-groupes sont distingués est-il abélien ?

R Par forcément : prendre l'exemple de $\mathbb{H}_8$!

Q Donner les groupes abéliens de cardinal 120, à isomorphisme près.

Q Soit $H \lhd G$, $S \lhd H$ un p-Sylow de H. Montrer que $S \lhd G$.

Q Pourquoi les groupes suivant sont-ils différents : $\mathbb{Z}/n\mathbb{Z}, \mathfrak{S}_n, D_n, \mathcal{GL}_n(\mathbb{K})$?

Q Soit A est un anneau intègre et G un sous-groupe fini de $A^\times$. Montrer que G est cyclique.

BIBLIOGRAPHIE

[Ale99] M. Alessandri : *Thèmes de géométrie*. Dunod, 1999.

[Aud06] M. Audin : *Géométrie*. EDP Sciences, 2006.

[Com98] F. Combes : *Algèbre et géométrie*. Bréal, 1998.

[Dem09] M. Demasure : *Cours d'algèbre*. Cassini, 2009.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Szp09] A. Szpriglas : *Algèbre L3*. Pearson Education, 2ème édition, 2009.

105 GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS.

Soit E un ensemble de cardinal fini $n \in \mathbb{N}^*$.

Définition 1. [$\mathfrak{S}(E)$, groupe symétrique $\mathfrak{S}_n$]
On note $\mathfrak{S}(E)$ le groupe des permutations de E (bijections de E dans lui-même). Il est de cardinal $n!$. On note $\mathfrak{S}_n = \mathfrak{S}(\llbracket 1, n \rrbracket)$ le groupe symétrique.
Pour $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$.

Proposition 2. *On a $\mathfrak{S}(E) \simeq \mathfrak{S}_n$.*

Remarque 3. Ainsi on étudiera dans cette leçon uniquement le groupe $\mathfrak{S}_n$.

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

I. Le groupe $\mathfrak{S}_n$: éléments et générateurs

I. A. Orbites et cycles

[Rom17, §2.3/2.1, p39]

On considère l'action naturelle de $\mathfrak{S}_n$ sur $\llbracket 1, n \rrbracket$: $(\sigma, k) \longmapsto \sigma(k)$.
Soit $\sigma \in \mathfrak{S}_n$ et $k \in \llbracket 1, n \rrbracket$ fixés.
On note $O_\sigma(k) = \{\sigma^q(k) \,|\, q \in \mathbb{Z}\}$ l'orbite de k par l'action restreinte à $\langle \sigma \rangle$.

Définition 5. [Support d'une permutation]
On appelle support de σ l'ensemble $\mathrm{Supp}(\sigma) = \{x \in \llbracket 1, n \rrbracket \,|\, \sigma(x) \neq x\}$.

Définition 6. [ℓ-cycle]
σ est un ℓ-cycle s'il n'y a qu'une unique orbite non ponctuelle et qu'elle est de cardinal ℓ. On note alors $\sigma = (x\ \sigma(x)\ \dots\ \sigma^{\ell-1}(x))$ où x est un élément de l'orbite non ponctuelle.
Lorsque $\ell = 2$, on parle de transposition.

Exemple 7. Considérons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 6 & 1 & 3 \end{pmatrix}$ et $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$.
On a $O_\sigma(1) = \{1, 5\}$, $O_\sigma(2) = \{2\}$ et $O_\sigma(3) = \{3, 4, 6\}$.
σ n'est pas un cycle mais un produit de 2 cycles : $\sigma = (1\,5)(3\,4\,6)$. $c = (1\,5\,3)$ est un 3-cycle.

Proposition 8.
- *Un ℓ-cycle est d'ordre ℓ,*
- *2 cycles à supports disjoints commutent,*
- *Pour $\sigma \in \mathfrak{S}_n$, on a $\sigma \circ (i_1\ i_2\ \dots\ i_\ell) \circ \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_\ell))$*

Exemple 9. $(1\,4)(2\,1\,5\,3\,4)(1\,4) = (2\,4\,5\,3\,1)$.

Théorème 10. [Théorème de Cauchy] [Rom17, §1.7, p24–25]
Si p est un diviseur premier de n, alors il existe un élément d'ordre p dans G.

I. B. Générateurs et classes de conjugaisons

[Rom17, §2.3–2.4, p42–47]

Proposition 11. *Toute permutation de $\mathfrak{S}_n$ se décompose en un produit de (au plus $n-1$) transpositions.*

Exemple 12. $(4\,3\,1) = (4\,3)(3\,1) = (3\,1)(1\,4)$.

Application 13. Les familles suivantes engendrent $\mathfrak{S}_n$:
- les transpositions $(1\,i)_{2 \leq i \leq n}$,
- les transpositions $(i\,i+1)_{1 \leq i \leq n-1}$,
- la transposition $(1\,2)$ et le cycle $(1\,2\ \dots\ n)$.

Proposition 14. *Toute permutation σ de $\mathfrak{S}_n$ se décompose en un produit de cycles à supports disjoints. Ce produit est unique à l'ordre des cycles près. En particulier, la suite $(\ell_1, \ell_2, \dots, \ell_m)$ des longueurs des cycles est unique si on impose $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_m$. On appelle cette suite le type de σ.*

Exemple 15. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 7 & 5 & 10 & 8 & 1 & 6 & 9 \end{pmatrix} = (1\,4\,7\,8)(2\,3)(6\,10\,9)$.

Proposition 16. [Classes de conjugaisons de $\mathfrak{S}_n$]
Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type.

Application 17. Le nombre de classes de conjugaison est le nombre de partitions de n.
Calcul du cardinal de la classe de conjugaison associée au type $(\ell_1, \dots, \ell_m)$. Deux calculs proposés, où l'on note $p_k = \mathrm{card}(\{i \,|\, \ell_i = k\})$:

$$\left(\prod_{i=1}^{m} \binom{n - \sum_{j<i} \ell_j}{\ell_i} (\ell_i - 1)!\right) \times \left(\prod_{k=1}^{n} \frac{1}{p_k!}\right) = \frac{n!}{\prod_{k=1}^{n} k^{p_k} p_k!}$$

Exemple 18. Liste des éléments de $\mathfrak{S}_5$ regroupés par classe.

Proposition 19. *L'ordre de σ est le PPCM de son type.*

Exemple 20. $(1\,4\,7\,8)(2\,3)(6\,10\,9)$ est de type $(4,2,3)$ et donc d'ordre 12.

II. Autour du groupe alterné

II. A. Signature et groupe alterné

[Rom17, §2.6–2.7, p48]

Proposition 21. *Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$: l'identité et le morphisme $\mathcal{E}$ qui envoie toute transposition sur -1.*

Définition 22. [Signature, groupe alterné]
On appelle $\mathcal{E}$ l'application signature. On définit le groupe alterné $\mathfrak{A}_n = \ker \mathcal{E}$.

Proposition 23.
- *$\mathcal{E}$ est à valeurs dans $\{-1,1\}$,*
- *La signature d'un ℓ-cycle vaut $(-1)^{\ell+1}$,*
- *Pour $\sigma \in \mathfrak{S}_n$, on a $\mathcal{E}(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^{i(\sigma)}$ où $i(\sigma)$ est le nombre d'inversions de σ.*

Proposition 24. *$\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$, de cardinal $n!/2$.*

Proposition 25. *Pour $n \geq 5$, $\mathfrak{A}_n$ est simple.*

II. B. Applications à l'étude des sous-groupes de $\mathfrak{S}_n$

[Rom17, Ch2, p39]

Corollaire 26. *Pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Application 27. Les sous-groupes d'indice n de $\mathfrak{S}_n$ sont isomorphes à $\mathfrak{S}_{n-1}$.

Remarque 28. $\mathfrak{S}_n \hookrightarrow \mathfrak{A}_{n+2}$.

Proposition 29. [Centre]
- *Pour $n \geq 3$, $Z(\mathfrak{S}_n) = \{\mathrm{Id}\}$,*
- *Pour $n \geq 4$, $Z(\mathfrak{A}_n) = \{\mathrm{Id}\}$.*

Proposition 30. [Groupe dérivé]
- $D(\mathfrak{S}_n) = \mathfrak{A}_n$
- $D(\mathfrak{A}_n) = \mathfrak{A}_n$ *pour $n \geq 5$.*

Application 31. Treillis de $\mathfrak{S}_3, \mathfrak{S}_4, \mathfrak{A}_3, \mathfrak{A}_4, \ldots$ **[voir annexe]**

III. Applications du groupe symétrique

III. A. Dérangements

[Rom17, Ch2, p53–55/73]

Définition 32. Pour $n \in \mathbb{N}^*$, on appelle dérangement de n une permutation de $[\![1,n]\!]$ sans point fixe. On note d_n le nombre de dérangements de n.

Proposition 33. *On a $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.*

Corollaire 34. *Le nombre de permutations de $\mathfrak{S}_n$ ayant exactement r points fixes est $\binom{r}{n} d_{n-r} = \frac{n!}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$.*

III. B. Déterminants

[Gou09, §3.5, p134–137]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n où $\mathbb{K}$ est un corps commutatif.

Théorème 35. [Propriétés de $\Lambda_n(E)$]
L'ensemble $\Lambda_n(E)$ des formes n-linéaires alternées de E est un espace vectoriel de dimension 1. Il existe une unique forme n-linéaire alternée égale à 1 sur une base donnée de $\mathcal{B}$.

Définition 36. [Déterminant dans une base]
Soit $\mathcal{B}$ une base de E. On appelle déterminant dans la base $\mathcal{B}$, et on note $\det_{\mathcal{B}}$, l'unique forme n-linéaire alternée égale à 1 sur $\mathcal{B}$.
On appelle déterminant de $A \in \mathcal{M}_n(\mathbb{K})$ le déterminant des vecteurs colonnes de A dans la base canonique de $\mathbb{K}^n$. On le note $\det(A)$.

Corollaire 37. [Expression de $\det_{\mathcal{B}}$]
Soient $x_1, \ldots, x_n$ des vecteurs de E. En notant $(x_{i,1}, \ldots, x_{i,n})$ les coordonnées de x_i dans une base $\mathcal{B}$ de E, on a :

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

Exemple 38. Règle de Sarrus : déterminant en dimension 3. **[voir annexe]**

Application 39. Il y a plus (resp. moins) de dérangements impairs que de dérangements pairs dans $\mathfrak{S}_n$ lorsque n est pair (resp $n > 1$ impair).

III. C. Matrices de permutation et représentation [Rom17, §2.8.3, p56–57]

Soit $\mathbb{K}$ un corps commutatif.

Définition 40. [Matrice de permutation]
Pour $\sigma \in \mathfrak{S}_n$, on appelle matrice de permutation associée à σ la matrice P_σ définie par $(P_\sigma)_{i\,j} = \mathbb{1}_{i=\sigma(j)}$.

Exemple 41. $P_{\mathrm{Id}} = I_n$ et $P_{(1\,2\,3\,\dots\,n)} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$.

Théorème 42. *$P : \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathcal{GL}_n(\mathbb{K}) \\ \sigma & \longmapsto & P_\sigma \end{array}$ est un morphisme de groupe injectif et on a $\det(P_\sigma) = \mathcal{E}(\sigma)$.*

Autrement dit on a une représentation naturelle de $\mathfrak{S}_n$ dans $\mathbb{K}^n$.

III. D. Polynômes symétriques [Rom17, §2.8.5, p57–58]

Soit $\mathbb{K}$ un corps commutatif de caractéristique différente de 2.

Définition 43. [Polynôme symétrique]
On dit que $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique si :

$$\forall \sigma \in \mathfrak{S}_n, P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$$

Exemple 44. Les polynômes $S_{k,n} = \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} X_{i_1} X_{i_2} \dots X_{i_n}$ (pour $0 \le k \le n$) sont des polynômes symétriques, appelés polynômes symétriques élémentaires.

Théorème 45. *Soit $P \in \mathbb{K}[X_1, \dots, X_n]$ un polynôme symétrique. Alors il existe un polynôme $Q \in \mathbb{K}[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(S_{1,n}, S_{2,n}, \dots, S_{n,n})$.*

Remarque 46. Le résultat est en fait vrai en remplaçant $\mathbb{K}$ par un anneau.

Exemple 47. [Gou09, §2.4, p79] Expressions de $P = X^3 + Y^3 + Z^3 \in \mathbb{R}[X, Y, Z]$ et $Q = \Sigma X_1^2 X_2^2 X_3 \in \mathbb{R}[X_1, \dots, X_n]$ pour $n \ge 5$.

III. E. Groupe symétrique et géométrie [Rom17, §3.4, p84] [CG13, §XII.3, p365]

Groupe des isométries préservant une partie de $\mathcal{E}$. Isométries positives/négatives ...
L'isobarycentre est conservé par une isométrie (en particulier un potentiel centre de symétrie).
Bijection isométries positives/négatives.
On se place maintenant dans un espace affine de dimension 3.
Définition d'un polyèdre.
Isométries préservant le tétraèdre régulier : isomorphe à $\mathfrak{S}_4$.

Théorème 48. *$\mathrm{Isom}(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Isom}^+(\mathcal{C}) \simeq \mathfrak{S}_4$.*

Lien entre isométries préservant le tétraèdre et le cube

Corollaire 49. [Formule de Burnside] *[Rom17, §1.10, p37]*

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Application 50. On peut colorier les 6 faces du cube avec 3 couleurs de 57 manières différentes.

ANNEXE

Règle de SARRUS, treillis de groupes

SPEECH

Étudier la structure du groupe $\mathfrak{S}_n$ est intéressant car ce groupe intervient naturellement dans de nombreuses situations, comme nous allons le voir. De plus, l'isomorphisme canonique $\mathfrak{S}_E \simeq \mathfrak{S}_n$ pour tout ensemble E tel que $|E| = n$ et le théorème de CAYLEY rajoutent de l'attrait pour ce groupe.
Dans une première partie, on regarde l'action de groupe naturelle de $\mathfrak{S}_n$ sur $[\![1, n]\!]$, on définit notamment les orbites et on a le théorème de CAUCHY. Cela mène à la décomposition des permutations en cycle disjoints et aux familles engendrant $\mathfrak{S}_n$.
La deuxième partie s'attaque à l'étude de l'unique morphisme de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}$ non trivial : la signature. Son noyau, $\mathfrak{A}_n$, possède de nombreuses propriétés, on montrera notamment en développement qu'il est simple pour $n \geq 5$.
Enfin on s'attardera sur les différentes applications du groupe $\mathfrak{S}_n$, aussi bien pour le dénombrement de dérangements, le calcul de déterminant que pour les polynômes symétriques. Notons aussi l'utilité de $\mathfrak{S}_n$ en théorie des représentations et en géométrie.

QUESTIONS

Q Dénombrer les classes de conjugaison de $\mathfrak{S}_6$.

Q Montrer qu'il existe un sous-groupe de $\mathfrak{S}_6$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Soit $i : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathfrak{S}_6$ un morphisme injectif. Quelle est la signature de $i((1,2))$?

R Par exemple, $\langle (1\,2), (3\,4\,5) \rangle$ est un sous-groupe de $\mathfrak{S}_6$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
Puis $(1,2)$ est d'ordre 6 donc $i((1,2))$ est aussi d'ordre 6 : c'est soit un 6-cycle, soit un produit d'un 3-cycle par un 2-cycle. Dans tous les cas, la signature est -1.
On pouvait aussi utiliser le théorème de CAYLEY pour trouver un sous-groupe isomorphe.

Q Soit G fini. Pour $g \in G$, on pose $\phi_g : x \longmapsto gx$. Montrer que si $|G| = 2n$ pour n impair, alors G n'est pas simple.

Q Quelles sont les isométries D préservant un tétraèdre régulier ?

R $D \simeq \mathfrak{S}_4$ puisque qu'en numérotant les sommets, on a directement l'injection. Comme de plus l'échange de deux sommets (par une symétrie) correspond à une transposition, $\mathfrak{S}_4 = \langle \{\text{transpositions}\} \rangle \subset D$.

Q Et pour les isométries du cube ?

R Les isométries positives sont isomorphes à $\mathfrak{S}_4$.

BIBLIOGRAPHIE

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

106 GROUPE LINÉAIRE D'UN ESPACE VECTORIEL DE DIMENSION FINIE E, SOUS-GROUPES DE $\mathrm{GL}(E)$. APPLICATIONS.

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, où $\mathbb{K}$ est un corps commutatif.

I. Introduction au groupe linéaire

[Rom17, §5.1, p125] [Per96, ChIV, p95]

Définition du groupe linéaire, c'est bien un groupe, exemples : homothéties, rotations
On se ramène à l'étude de $\mathcal{GL}_n(\mathbb{K})$ via un isomorphisme, et $\mathcal{GL}_n(\mathbb{K}) \simeq \mathcal{GL}_n(\mathbb{K})$
Proposition : morphisme du déterminant
Proposition $u \in \mathrm{GL}(E) \iff \ker u = \{0\} \iff \mathrm{Im}(u) = E \iff \det(u) \neq 0$
Définition de $\mathrm{SL}(E)$. Exemple
$\mathrm{SL}(E)$ distingué dans $\mathrm{GL}(E)$, le groupe quotient étant isomorphe à $\mathbb{K}^*$. $\mathrm{GL}(E)$ est alors un produit semi-direct, direct dans le cas $\mathbb{K} = \mathbb{R}$

II. Quelques éléments de $\mathrm{GL}(E)$

[Per96, §IV.2, p96]

II. A. Les homothéties

Homothéties, déterminant, u homothétie si et seulement si u stabilise toutes les droites $\to$ stabilisateur de l'action de $\mathrm{GL}(E)$ sur les droites

II. B. Les dilatations

Définition, propriétés des dilatations de rapport $\notin \{0, 1\}$
Deux dilatations de même rapport sont conjuguées

II. C. Les transvections

Définition, définitions équivalentes
Les transvections sont conjuguées (dans SL_n lorsque $n \geq 3$)
Formule de conjugaison

III. Étude du groupe linéaire

III. A. Générateurs

[Per96, §IV.2.d, p99]

$\mathcal{SL}_n(\mathbb{K})$ est engendré par les transvections, $\mathcal{GL}_n(\mathbb{K})$ est engendré par les transvections et les dilatations
Approche matricielle, pivot de Gauss
Applications : groupes dérivés, $\mathcal{SL}_n(\mathbb{K})$ est connexe par arcs

III. B. Centre et commutateurs

[Per96, §IV.2/3/5, p98]

$Z(\mathcal{GL}_n(\mathbb{K}))$ est l'ensemble des homothéties, $Z(\mathcal{SL}_n(\mathbb{K}))$ est l'ensemble des homothéties de déterminant 1
Définition de $\mathcal{PSL}_n(\mathbb{K}), \mathcal{PGL}_n(\mathbb{K})$
Isomorphismes pour de petites valeurs de n avec les groupes de permutation et/ou alterné

III. C. Quelques calculs de cardinalité

[Per96, §IV.5, p105] [Rom17, §5.6, p148–151]

Cardinaux de $\mathcal{GL}_n(\mathbb{F}_q), \mathcal{SL}_n(\mathbb{F}_q), \mathcal{PGL}_n(\mathbb{F}_q), \mathcal{PSL}_n(\mathbb{F}_q)$

Application 1. [Cardinal de $\mathcal{D}_n(\mathbb{F}_q)$]
Soit $n \in \mathbb{N}$, $q = p^r$ où p est premier et $r \in \mathbb{N}^*$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de taille n de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1+\cdots+n_q=n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

IV. Groupes orthogonal et unitaire

[Per96, §V.4, p123]

On se place en caractéristique différente de 2.

IV. A. Généralités

Forme quadratique q fixé. Définition de $O(q)$, de $O^+(q)$
$u \in O(q) \iff \det u = \pm 1 \iff \varphi(u(x), u(y)) = \varphi(x, y)$ où φ associée à q. Équivalence matricielle.
Exemple de $q(x, y) = x^2 - y^2$
Symétrie orthogonale, $E_+ \perp E_-$, conjugaison
Si q est définie positive, définition réflexion orthogonale, les réflexions orthogonales engendrent $O(q)$. Les renversements engendrent $O^+(q)$.
Centres de $O(q), O^+(q)$
Groupe unitaire, spécial unitaire pour une forme hermitienne définie positive. Même caractérisations et diagonalisabilité en base orthonormée

IV. B. Groupe orthogonal euclidien, groupe unitaire

Définition matricielle

Théorème 2. [Réduction des endomorphismes orthogonaux]
Sot $u \in O_n(\mathbb{R})$. Il existe une base orthonormée $\mathcal{B}$ de E telle que

$$M_{\mathcal{B}}(u) = \begin{pmatrix} I_s & & & & \\ & -I_t & & & \\ & & R_1 & & \\ & & & \ddots & \\ & & & & R_r \end{pmatrix}$$

où $s+t+2r=n$ et pour $1 \leq k \leq r$, $R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$ avec $\theta_k \not\equiv 0 \mod \pi$.

IV. C. Groupe orthogonal et géométrie de l'espace : les quaternions
[CG13, ChVII, p232]

Groupe des quaternions sous forme matricielle, conjugué, norme d'un quaternion, produit scalaire associé, base $(1, \mathrm{i}, \mathrm{j}, \mathrm{k})$ orthonormée, $\mathbb{H} = \mathbb{I} \oplus^{\perp} \mathbb{R}$, $\mathbb{R}$-espace vectoriel de dimension 4.
On définit $\mathrm{SU}_2(\mathbb{C}) = \{h \in \mathbb{H} \,|\, N(h) = 1\}$.

Théorème 3. *On a $\mathrm{SU}_2(\mathbb{C})/\{\pm I_2\} \simeq \mathrm{SO}_3(\mathbb{R})$.*

V. Topologie
[CG13, II.4/ChVI, p37/201] [Rom17, §5.7/Ch22.3, p151/697]

On se place sur le corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$
$\mathcal{GL}_n(\mathbb{K})$ est un ouvert dense dans $\mathcal{M}_n(\mathbb{K})$
Homéomorphismes
Compacité de $\mathcal{O}_n(\mathbb{R})$
Connexités par arcs selon le corps
Décomposition polaire

ANNEXE

Tableau d'actions de groupes de matrices, stabilisateurs, orbites [CG13, §II.E, p62]
$\mathcal{GL}_n(\mathbb{K})$ sur les bases vectorielles, $\mathcal{O}_n(\mathbb{K})$ sur les bases orthonormées euclidiennes, $\mathcal{SO}_n(\mathbb{K})$ sur les bases orthonormées euclidiennes directes, $\mathcal{U}_n(\mathbb{K})$ sur les bases orthonormées hermitiennes, $\mathcal{GL}_n(\mathbb{K})$
Transvections, dilatations

SPEECH

Les espaces vectoriels ont un caractère géométrique très naturel. On s'intéresse donc à cette vision géométrique en étudiant le groupe linéaire de ces espaces.
On peut également mettre une topologie sur $\mathrm{GL}(E)$ (voir la dernière partie).

COMMENTAIRES

Les trois premières parties sont des immanquables. Pour le reste on aurait aussi pu aller du côté des représentations.

QUESTIONS

Q Déterminer les idéaux bilatères stricts de $\mathcal{M}_n(\mathbb{K})$.
R Soit I un tel idéal. Soit $M \in I \backslash \{0\}$. Soit r le rang de M. Alors il existe P, Q tel que $PMQ^{-1} = I_r$ donc $I_r \in I$. Par suite toutes les matrices de rang r sont dans I.
Donc I est l'ensemble des matrices de rang $r_1, \dots r_k$ pour des entiers $r_1, \dots, r_k$ fixés.
Q Soit $G \subset \mathcal{GL}_n(\mathbb{C})$ fini. Montrer que $\sum_{M \in G} \mathrm{Tr}(M) \in \mathbb{Z}$.
R On a pour tout $H \in G$, $\sum_{M \in G} \mathrm{Tr}(HM) = \sum_{M \in G} \mathrm{Tr}(HM)$.
Soit $d = |G|$. Soit $M \in G$. $M^d = I_n$ et $X^d - 1$ est scindé à racines simples.

BIBLIOGRAPHIE

[CG13] P. Caldero et J. Germoni : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

107 REPRÉSENTATIONS ET CARACTÈRES D'UN GROUPE FINI SUR UN $\mathbb{C}$-ESPACE VECTORIEL. EXEMPLES.

On considère des groupes finis et des espaces vectoriels complexes de dimension finie.

I. Définitions et constructions de représentations
[Rom17, Ch6, p179] [Ser98, Ch1, p15]

Définition représentation, degré de la représentation
Remarque : on peut reformuler cela en terme d'action de groupes
Exemple : représentation triviale, représentation de degré 1 : morphisme de G dans $\mathbb{U}$
Injection naturelle si $G \subset \mathcal{GL}_n(\mathbb{C})$ Représentations de degré 1 et 2 sur $\mathfrak{S}_n$, sur $\mathbb{Z}/2\mathbb{Z}$
Représentation naturelle de D_{2n} dans $\mathcal{GL}_2(\mathbb{C})$
Application : pour tout g, $\rho(g)$ est diagonalisable
Représentation par permutation, représentation régulière
Représentation en somme directe
Morphisme de représentation, représentation homomorphique de degré $\dim(V)\dim(W)$

II. Sous-représentations, irréductibilité
[Rom17, §6.2, p182] [Ser98, §1.3/1.4, p17]

Sous-représentation, représentation quotient
Si on a un morphisme de représentation, le noyau est l'image sont des sous-représentations
Représentation irréductible. Exemple des représentations de degré 1. Contre-exemple : représentation régulière si $|G| > 1$
Si G est abélien, les représentations irréductibles sont les représentations de degré 1
Lemme de Schur, lemme de Maschke

III. Théorie des caractères
[Rom17, §6.3/6.4, p186] [Ser98, Ch2, p23]

III. A. Caractères et fonctions centrales

Caractère (irréductible) associé à une représentation (irréductible)
Exemple : en dimension 1 c'est un morphisme de groupes
Exemple : calcul du caractère de la représentation régulière
Les caractères sont constants sur les classes de conjugaison, $\chi(g)$ est somme de racines de l'unité, $\chi_{V\oplus W} = \chi_V + \chi_W$
Deux représentations isomorphes ont même caractère
Introduction de l'espace des fonctions centrales, du produit scalaire

III. B. Orthogonalité des caractères

Produit scalaire entre caractères irréductibles : 1 s'ils sont isomorphes, 0 sinon
Se donner une représentation irréductible revient à isomorphisme près à se donner un caractère irréductible
On a un nombre fini de caractère irréductibles, inférieur au nombre de classe de conjugaisons
Nombre d'apparitions d'un caractère irréductible dans une représentation
Deux représentations de même caractère sont isomorphes
Se donner une représentation revient à isomorphisme près à se donner un caractère ! L'ensembles des traces suffit à caractériser ρ : on réduit l'étude des représentations aux caractères !
$|G| = \sum_i n_i^2$ (via la représentation régulière), les caractères forment une base orthonormée des fonctions centrales. Il y a donc autant de caractères irréductibles que de classes de conjugaison
Définition d'une table de caractères, propriétés d'orthogonalité des lignes (pondérées par le cardinal de la classe !, signifie l'orthogonalité des caractères), des colonnes

IV. Exemples

IV. A. Groupes cycliques et abéliens **[Col11, §I.2.4, p250–252] [Rom17, §6.5, p197]**

Table des caractères d'un groupe cyclique

Soit G un groupe abélien fini.

Définition 1. L'exposant de G est le plus petit $d \in \mathbb{N}^*$ tel que $g^d = 1$ pour tout $g \in G$.

Théorème 2. [Structure des groupes abéliens finis]
Il existe un unique entier ℓ et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G, $d_{i+1} \mid d_i$ pour tout $i \leq \ell - 1$ et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$.

IV. B. Groupes de permutations **[Pey04, §VIII.1.4/VIII.2.1, p228–232]**

Il y a autant de classes de conjugaison que de représentations irréductibles : le nombre de partitions de n.
Représentations de degré 1 : signature et triviale
Exemple de $\mathfrak{S}_3$: caractère associé à l'action sur un triangle. Table des caractères.

Soit G un groupe fini. Soient $\chi_1, \ldots, \chi_r$ ses caractères irréductibles.

Lemme 3. *Soit χ associé à (ρ, V) représentation de G. Alors $\ker(\rho) = \ker(\chi) = \{g \in G \,|\, \chi(g) = \chi(1)\}$.*

Proposition 4. *Les sous-groupes distingués de G sont les $(\cap_{i\in I} \ker \chi_i)_{I\subset[\![1,r]\!]}$.*

Application 5. Table des caractères de $\mathfrak{S}_4$.

ANNEXE

Tables de caractères de quelques groupes.

SPEECH

Les représentations font un lien important entre groupes et géométrie.
Dans un premier temps on définit les représentations et comment construire/définir des représentations à partir d'autres : par exemple la représentation par permutation, ou la construction en augmentant le degré de la représentation ...
Est-il possible de faire l'inverse, de réduire une représentation ? C'est l'objet de la seconde partie où l'on introduit la notion de représentation irréductible, sorte de brique élémentaire des représentations.
Ensuite, on s'intéresse à la théorie des caractères, qui sont des fonctions centrales, ensemble qui peut être muni d'un produit scalaire pour lequel les caractères forment une base orthonormée, dont découlent de nombreux corollaires de décomposition … dont la caractérisation d'une représentation par son caractère !
Dans une dernière partie on s'intéresse aux exemples des groupes cycliques, abéliens, et au groupe des permutations.

COMMENTAIRES

Il faut maîtriser les interprétations géométriques des caractères (par exemple pour $\mathfrak{A}_4$).

QUESTIONS

Q Comment obtient-on la représentation régulière ? Pourquoi est-elle utile ?

R C'est une représentation naturellement induite par l'action par translation à gauche de G sur lui-même (ou idée des permutations).
Elle a l'avantage d'être fidèle, son caractère associé est très simple puisque $\chi(g) = |G|\,\mathbb{1}_{g=e}$ (attention ce n'est pas le cas de la représentation de permutation où $\mathfrak{S}_n$ agit sur $[\![1,n]\!]$ et non sur lui-même !). De plus, chaque représentation irréductible est une sous-représentation de la représentation régulière, ce qui lui confère un rôle important notamment pour montrer que les caractères forment une base des fonctions centrales, puis après obtenir des relations comme $|G| = \sum n_i^2$ et l'orthogonalité sur les colonnes/lignes.

Q À quoi sert de lemme de Schur ?

R Le lemme de Schur intervient notamment dans l'étude des calculs de produits scalaires, donc pour montrer que les caractères sont orthonormés, et l'orthogonalité des colonnes/-lignes.

Q Retrouver les caractères de $\mathfrak{S}_3$ et donner leur interprétations.

Q Soit G un groupe fini possédant 7 classes de conjugaison et pour lequel on connaît deux caractères :

	C_1	C_2	C_3	C_4	C_5	C_6	C_7
θ	1	1	1	ω	ω^2	ω	ω^2
χ	2	-2	0	-1	-1	1	1

où ω est une racine 3-ième de l'unité distincte de 1. Peut-on déterminer la table des caractères de G ? L'ordre de G ? Le cardinal de chaque classe de conjugaison ? Les groupes distingués ?

R On complète déjà la table par le caractère trivial. Ensuite, on remarque que le produit de deux caractères irréductibles est un caractère irréductible lorsque l'un d'entre eux est de degré 1 (en calculant le produit scalaire, on peut aussi donner la représentation associée), ce qui permet de compléter la table par θ^2, $\theta\chi$ et $\theta^2\chi$! (on pouvait aussi passer au caractère conjugué, caractère de la représentation duale associée ...)
Par ailleurs on sait qu'il y a 7 caractères irréductibles, il n'en manque qu'un :

	C_1	C_2	C_3	C_4	C_5	C_6	C_7
χ_{triv}	1	1	1	1	1	1	1
θ	1	1	1	ω	ω^2	ω	ω^2
χ	2	-2	0	-1	-1	1	1
θ^2	1	1	1	ω^2	ω	ω^2	ω
$\theta\chi$	2	-2	0	$-\omega$	$-\omega^2$	ω	ω^2
$\theta^2\chi$	2	-2	0	$-\omega^2$	$-\omega$	ω^2	ω
η	a	b	c				

Pour obtenir le dernier caractère, on veut utiliser l'orthogonalité des colonnes. Mais on ne connait aucune valeur. On sait juste que $a \in \mathbb{N}^*$! Cela permet alors d'assurer que les quatre dernières valeurs du caractère sont nulles ! Puis l'orthogonalité des trois premières colonnes donne $ab = 9, ac = -3, bc = -3$, d'où l'on déduit $a = b = 3$ puis $c = -1$. D'où finalement le dernier caractère :

	C_1	C_2	C_3	C_4	C_5	C_6	C_7
η	3	3	-1	0	0	0	0

En calculant la somme des carrés de la première colonne, on obtient que G est d'ordre 24.
Remarquons par ailleurs que pour toute classe C on a

$$\forall g \in G, \mathbb{1}_C(g) = \sum_\chi \langle \mathbb{1}_C \mid \chi\rangle \chi(g) = \sum_\chi \frac{1}{|G|} \sum_{h\in C} \overline{\chi(h)}\chi(g) = \sum_\chi \frac{|C|\,|\chi(g)|^2}{|G|}$$

Autrement dit $[G : C] = \sum_\chi |\chi(C)|^2$. Ce qui permet d'obtenir les ordres des éléments de chaque classe :

	C_1	C_2	C_3	C_4	C_5	C_6	C_7
cardinal	1	1	6	4	4	4	4

On déduit de la table le seul sous-groupe distingué strict : $G_8 = C_1 \cup C_2 \cup C_3$ (unique 8-Sylow).
On a $[G : G_8] = 3$ donc $G/G_8 \simeq \mathbb{Z}/3\mathbb{Z}$ et si $\alpha \notin G_8$, on a que α est d'ordre une puissance de 3, disons $3k$. Alors $\beta = \alpha^k$ est d'ordre 3.
On a $G_8 \cap \langle\beta\rangle = \{e\}$ puisque les éléments de G_8 sont d'ordre pairs et ceux de β d'ordre 3 (sauf e), et comme $|G_8|\,|\beta| = 24$ et G_8 est distingué, on en déduit que $G = G_8 \rtimes \langle\beta\rangle$.
Reste à étudier G_8. On sait que G_8 possède au moins 3 classes de conjugaison, donc n'est pas abélien. Il ne peut donc s'agir que de D_8 ou de $\mathbb{H}_8$.
Finalement $G = G_8 \rtimes \mathbb{Z}/3\mathbb{Z}$.

Q Une table de caractères permet-elle d'identifier le groupe en général ?

R Non ! Le groupe diédral D_8 et le groupe des quaternions $\mathbb{H}_8$ ont la même table de caractères, mais ne sont pas isomorphes !

BIBLIOGRAPHIE

[Col11] P. Colmez : *Éléments d'analyse et d'algèbre*. Les éditions de l'École Polytechnique, 2ème édition, 2011.

[Pey04] G. Peyré : *L'algèbre discrète de la transformée de* Fourier. Ellipses, 2004.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Ser98] J.-P. Serre : *Représentations linéaires des groupes finis*. Hermann, 1998.

108 EXEMPLES DE PARTIES GÉNÉRATRICES D'UN GROUPE. APPLICATIONS.

Sous-groupe engendré par une partie (c'est l'intersection des sous-groupes la contenant), partie génératrice
Exemple du groupe dérivé

I. Cas des groupes abéliens

I. A. Groupes monogènes et cycliques Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

[Rom17, §1.4-5/1.9/10.1, p13–19/27/277] [Per96, §1.1/1.7, p10/24]

Groupe monogène, cyclique, monogène/cyclique implique abélien

Exemple 1. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique à n éléments engendré par $\overline{1}$.

Application 2. Tout groupe cyclique à n éléments est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 3. $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$: considérer $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n, \overline{k} \longmapsto \mathrm{e}^{2ik\pi/n}$.

Si G est un groupe, $\langle a \rangle$ où $a \in G$ est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$ pour un $n \in \mathbb{N}^*$.

Proposition 4. *L'ordre de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{k \wedge n}$.*

Corollaire 5. *$(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par les $\overline{k}$ tels que $k \wedge n = 1$.*

Exemple 6. $\mathbb{Z}/8\mathbb{Z}$ est engendré par $\overline{1}, \overline{3}, \overline{5}$ et $\overline{7}$.

Application 7.
- Les sous-groupes d'un groupe cyclique sont cycliques.
- Si $|G| = p$, G est cyclique.

Définition 8. [Indicatrice d'Euler]
Pour $n \geq 2$, on définit $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 9. Pour $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$, on a $\varphi(p^\alpha) = p^\alpha(p-1)$.

Proposition 10. [Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$]
Pour $d \mid n$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, engendré par $\frac{n}{d}$ et formé des éléments dont l'ordre divise d.

Proposition 11. *Si $d \mid n$, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d.*

Application 12. $n = \sum_{d|n} \varphi(d)$

I. B. Groupes abéliens finis

[Ulm12, Ch12, p103]

Groupe abélien de type fini, exemple des groupes abéliens finis

Théorème 13. [Structure des groupes abéliens de type fini]
Soit G un groupe abélien de type fini. Alors il existe $\ell, r \in \mathbb{N}$ uniques et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que $d_{i+1} \mid d_i$ pour tout $i \leq \ell - 1$ et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z} \times \mathbb{Z}^r$.

Corollaire 14. [Structure des groupes abéliens finis]
Soit G un groupe abélien fini. Il existe un unique entier ℓ et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G, $d_{i+1} \mid d_i$ pour tout $i \leq \ell - 1$ et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$.

Exemple 15. Les groupes abéliens d'ordre 24 sont isomorphes à $\mathbb{Z}/24\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $(\mathbb{Z}/6\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Remarque 16. Dans le cas d'un groupe fini, on peut trouver des générateurs du groupe en trouvant un élément d'ordre l'exposant du groupe, puisque l'on montre que d_1 est l'exposant de G. Une fois ce premier élément trouvé, on peut se restreindre à un sous-groupe de G et réitérer l'opération, via la théorie des caractères.

II. Groupe symétrique

[Rom17, Ch2, p39]

On note $\mathfrak{S}_n$ le groupe des permutations de n éléments.

II. A. Générateurs

Les cycles engendre $\mathfrak{S}_n$. Application : décomposition en produit de cycles à support disjoints (unique à l'ordre près !)

Proposition 17. *Toute permutation de $\mathfrak{S}_n$ se décompose en un produit de (au plus $n-1$) transpositions.*

Exemple 18. $(4\,3\,1) = (4\,3)(3\,1) = (3\,1)(1\,4)$.

Application 19. La signature d'un élément σ de $\mathfrak{S}_n$ est déterminée par la parité du nombre de transpositions intervenant dans une décomposition de σ.

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

- les transpositions $(1\,i)_{2\leq i\leq n}$,
- les transpositions $(i\,i+1)_{1\leq i\leq n-1}$,
- la transposition $(1\,2)$ et le cycle $(1\,2\ \ \dots\ n)$.

Utilité : petites familles de générateurs : deux éléments suffisent à engendrer le groupe

II. B. Groupe alterné

Proposition 21. *Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$: l'identité et le morphisme $\mathcal{E}$ qui envoie toute transposition sur -1.*

Définition 22. On définit le groupe alterné $\mathfrak{A}_n$ comme étant le noyau de la signature.

Proposition 23.
- *$\mathcal{E}$ est à valeurs dans $\{-1,1\}$,*
- *La signature d'un ℓ-cycle vaut $(-1)^{\ell+1}$,*
- *Pour $\sigma\in\mathfrak{S}_n$, on a $\mathcal{E}(\sigma)=\prod_{1\leq i<j\leq n}\frac{\sigma(i)-\sigma(j)}{i-j}=(-1)^{i(\sigma)}$ où $i(\sigma)$ est le nombre d'inversions de σ.*

Proposition 24. *$\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$. Il est de cardinal $n!/2$.*

Lemme 25. *$\mathfrak{A}_n$ est le sous-groupe engendré par les trois cycles.*

Proposition 26. *Pour $n\geq 5$, $\mathfrak{A}_n$ est simple.*

Corollaire 27. *Pour $n\geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Application 28. [Groupe dérivé]
- $D(\mathfrak{S}_n)=\mathfrak{A}_n$
- $D(\mathfrak{A}_n)=\mathfrak{A}_n$ pour $n\geq 5$.

III. Groupes linéaires/spéciaux

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, où $\mathbb{K}$ est un corps commutatif
Définition du groupe linéaire, de $\mathrm{SL}(E)$. Exemple des homothéties
On se ramène à l'étude de $\mathcal{GL}_n(\mathbb{K})$ via un isomorphisme, et $\mathcal{GL}_n(\mathbb{K})\simeq\mathcal{GL}_n(\mathbb{K})$
Proposition : $u\in\mathrm{GL}(E)\iff\ker u=\{0\}\iff\mathrm{Im}(u)=E\iff\det(u)\neq 0$

III. A. Générateurs de $\mathcal{GL}_n(\mathbb{K})$ [Per96, ChIV, p95]

Homothéties, déterminant, u homothétie si et seulement si u stabilise toutes les droites $\to$ stabilisateur de l'action de $\mathrm{GL}(E)$ sur les droites
Dilatations, propriétés des dilatations de rapport $\notin\{0,1\}$
Deux dilatations de même rapport sont conjuguées
Transvections, définitions équivalentes
Les transvections sont conjuguées (dans $\mathcal{SL}_n(\mathbb{K})$ lorsque $n\geq 3$)
Formule de conjugaison
$\mathcal{SL}_n(\mathbb{K})$ est engendré par les transvections, $\mathcal{GL}_n(\mathbb{K})$ est engendré par les transvections et les dilatations
Approche matricielle, pivot de Gauss
$\mathcal{SL}_n(\mathbb{K})$ est connexe par arcs
$Z(\mathcal{GL}_n(\mathbb{K}))$ est l'ensemble des homothéties, $Z(\mathcal{SL}_n(\mathbb{K}))$ est l'ensemble des homothéties de déterminant 1.
Groupes dérivés

III. B. Groupe orthogonal/unitaire [Per96, ChVI, p142] [CG13, §VII.3, p232]

Groupe orthogonal, engendré par les réflexions orthogonales. Groupe spécial orthogonal engendré par les renversements
Déplacement engendré par un nombre pair de réflexions
Groupes dérivés
Application : groupe des quaternions sous forme matricielle, conjugué, norme d'un quaternion, produit scalaire associé, base $(1,\mathrm{i},\mathrm{j},\mathrm{k})$ orthonormée, $\mathbb{H}=\mathbb{I}\oplus^{\perp}\mathbb{R}$, $\mathbb{R}$-espace vectoriel de dimension 4. On définit $\mathrm{SU}_2(\mathbb{C})=\{h\in\mathbb{H}\,|\,N(h)=1\}$.

Théorème 29. *On a $\mathrm{SU}_2(\mathbb{C})/\{\pm I_2\}\simeq\mathrm{SO}_3(\mathbb{R})$.*

III. C. Groupe diédral [Aud06, ChIII/V, p360] [Rom17, §3.4.3/6.1, p87/180]

Sous-groupe D_{2n} de $\mathcal{O}_2(\mathbb{R})$ des isométries préservant un polygone régulier à n sommets.
D_{2n} est engendré par la symétrie et la rotation d'angle $\frac{2\pi}{n}$, d'ordres 2 et 4, ce qui donne la liste des éléments de D_{2n}.

Application 30. D_{2n} s'injecte naturellement dans $\mathcal{GL}_2(\mathbb{C})$, envoyant la rotation d'angle $2\pi/n$ et la symétrie sur

$$R=\begin{pmatrix}\cos(2\pi/n) & -\sin(2\pi/n)\\ \sin(2\pi/n) & \cos(2\pi/n)\end{pmatrix}\quad\text{et}\quad S=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

Énumérations des isométries positives, des isométries négatives

ANNEXE

Transvections, dilatations
Groupe diédral

SPEECH

L'intérêt des parties génératrices est de réduire l'étude d'un groupe à ses générateurs, ce qui permet d'obtenir des propriétés de celui-ci, comme par exemple montrer la surjectivité d'un morphisme ou la simplicité d'un groupe.

QUESTIONS

Q Que peut-on dire du groupe $G = \langle (i\,j), (1\,2\,\dots\,n) \rangle$?

R Regardons l'action de G sur $[\![1, n]\!]$. Posons $\ell = (j - i) \wedge n$.
Pour $\sigma \in \mathfrak{S}_n$, on note $P(\sigma)$ la propriété $\forall u, v \in [\![1, n]\!], u \equiv v \mod \ell \implies \sigma(u) \equiv \sigma(v) \mod \ell$.
Les éléments de G vont vérifier cette propriété. En effet $P((1\,2))$ et $P((1\,2\,\dots\,n))$ sont vraies, et si $P(\sigma)$ et $P(\sigma')$ sont vraies, alors $P(\sigma^{-1})$ et $P(\sigma\sigma')$ le sont aussi.
Ainsi $P(\sigma)$ est vraie pour $\sigma \in G$. Or pour $n \geq 3$, $P((1\,2))$ n'est vraie que si $\ell = 1$. Ainsi si $\ell > 1$, $G \neq \mathfrak{S}_n$.
Réciproquement si $\ell = 1$, on vérifie que $G = \mathfrak{S}_n$.

BIBLIOGRAPHIE

[Aud06] M. Audin : *Géométrie*. EDP Sciences, 2006.

[CG13] P. Caldero et J. Germoni : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Ulm12] F. Ulmer : *Théorie des groupes*. Ellipses, 2012.

110 STRUCTURE ET DUALITÉ DES GROUPES ABÉLIENS FINIS. APPLICATIONS.

Soit G un groupe abélien fini d'ordre n.

I. Caractères des groupes abéliens finis

I. A. Caractères et liens avec $\mathbb{C}^G$ [Pey04, Ch1, p2]

Définition des caractères, structure de groupe, $\widehat{G \times H} \simeq \hat{G} \times \hat{H}$
Exemples des caractères de $\mathbb{Z}/n\mathbb{Z}$, de $\mathfrak{S}_n$
χ est à valeurs dans $\mathbb{U}_n$, $\chi(g^{-1}) = \chi(g)^{-1}$, constant sur chaque classe de conjugaison
Prolongement d'un caractère de $H < G$ en un caractère de G
$|\hat{G}| = |G|$

Définition 1. Pour $f, g : G \longrightarrow \mathbb{C}$, on définit le produit scalaire :

$$\langle f \mid g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$$

Orthogonalité des caractères $\rightarrow$ base orthonormée, expression de f sur la base orthonormée

I. B. Théorème de structure des groupes abéliens finis
[Col11, §I.2.4, p250–252] [Pey04, §I.2.2, p8]

Bidual
L'application $\iota : G \longrightarrow \hat{\hat{G}}, g \longmapsto (\chi \longmapsto \chi(g))$ est un isomorphisme de groupes.
En particulier $|\hat{\hat{G}}| = |G|$

Définition 2. On appelle exposant de G le plus petit $d \in \mathbb{N}^*$ tel que $g^d = 1$ pour tout $g \in G$.

Théorème 3. [Structure des groupes abéliens finis]
Il existe un unique entier ℓ et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G, $d_{i+1} \mid d_i$ pour tout $i \leq \ell - 1$ et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$.

Corollaire : $\hat{G} \simeq G$ (non canoniquement)
Exemple : il y a 6 groupes abéliens d'ordre 600 à isomorphisme près.

II. Transformée de Fourier discrète

II. A. Définitions et premiers résultats [Pey04, §II.3, p44]

Définition 4. [Transformée de Fourier discrète]
Soit $f : G \longrightarrow \mathbb{C}$. On définit le coefficient de Fourier associé à $\chi \in \widehat{G}$ par $c_f(\chi) = \langle f \mid \chi \rangle$ et la transformée de Fourier de f par $\widehat{f} : \chi \in \widehat{G} \longmapsto |G|\, c_f(\overline{\chi}) = \sum_{g \in G} f(g)\chi(g)$.

Proposition 5. [Propriétés de la transformée de Fourier]
- *La transformée de Fourier discrète $f \longmapsto \hat{f}$ est un isomorphisme de $\mathbb{C}^G$ dans $\mathbb{C}^{\hat{G}}$,*
- *Pour $f : G \longrightarrow \mathbb{C}$, on a $f = \sum_{\chi \in \widehat{G}} c_f(\chi)\chi = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi^{-1}$,*
- *formule de Fourier-Plancherel,*
- *$\widehat{f * g} = \hat{f}\hat{g}$.*

Définition 6. On définit $H^\# = \{\chi \in \widehat{G} \mid \forall h \in H, \chi(h) = 1\}$ l'orthogonal de H.

Lemme 7. *$H^\# \simeq \widehat{G/H}$ est de cardinal $|G| / |H|$.*

Proposition 8. [Formule de Poisson discrète]
Pour toute fonction $f : G \longrightarrow \mathbb{C}$, et pour tout $g \in G$, on a :

$$\sum_{h \in H} f(gh) = \frac{|H|}{|G|} \sum_{\chi \in H^\#} \widehat{f}(\overline{\chi})\chi(g)$$

En particulier ($g = 1$), on a $\sum_{h \in H} f(h) = \frac{|H|}{|G|} \sum_{\chi \in H^\#} \widehat{f}(\overline{\chi})$.

II. B. Transformée de Fourier rapide [Per96, §III.2, p65]

Notons $G_a = \mathbb{Z}/N\mathbb{Z}$ où $N = 2^p$ pour $p \in \mathbb{N}^*$. Soit $f \in \mathbb{C}^G$. On veut calculer efficacement $\hat{f}$.
Note : ne considérer que les groupes de la forme G_p reste intéressant, par rapport à la transformée de Fourier discrète en analyse de signaux.
On adopte justement des notations de transformée de Fourier en traitement du signal … c'est équivalent avec la formulation de la TFD sur un groupe. On verra donc f comme une fonction de $\mathbb{C}^N$. On note $\omega_N = \mathrm{e}^{2i\pi/N}$.
Remarque : l'algorithme naïf calcule $\hat{f}$ en $\mathcal{O}(N^2)$.
Idée : on sépare le vecteur f en 2 vecteurs et la TFD de f se sépare en deux sommes sur ses

vecteurs de taille $n/2$.
Définition : si $f \in \mathbb{C}^N$, on définit $f_{\text{paire}}, f_{\text{impaire}} \in \mathbb{C}^{N/2}$ par $f_{\text{paire}}(a) = f(2a)$ et $f_{\text{impaire}}(a) = ...$
On a $\hat{f}(k) = \widehat{f_{\text{paire}}}(k) + \omega_N^{-k} \widehat{f_{\text{impaire}}}(k)$
On obtient une complexité en $\mathcal{O}(N \ln(N))$.
Application : calcul du produit de convolution en passant en FOURIER, multiplication rapide de polynômes

III. Caractères des corps finis

[Per96, ChII, p27]

Soit p un nombre premier, $q = p^r$ une puissance de p (avec $r \in \mathbb{N}^*$).
Caractères additifs et multiplicatifs
Exemple : $x \longmapsto \zeta^x$ est un caractère additif de $\mathbb{F}_q$, pour tout ζ. Le symbole de LEGENDRE est un caractère multiplicatif sur $\mathbb{F}_p$
ζ générateur de $\mathbb{F}_q^*$. Permet d'obtenir un isomorphisme $\mathbb{F}_q^* \simeq \widehat{\mathbb{F}_q^*}$
Application trace : forme linéaire sur $\mathbb{F}_q$ (en tant que $\mathbb{F}_p$-espace vectoriel)
Caractère additif canonique, générateur de $\widehat{\mathbb{F}_q}$
Sommes de GAUSS. TDF additive, multiplicative associée ...
On retrouve la loi de réciprocité quadratique en travaillant notamment avec $G\left(\left(\frac{\cdot}{p}\right), \Psi_1\right)$

SPEECH

L'intérêt de la dernière partie est de voir $\mathbb{F}_q$ da manière additive (comme $\mathbb{F}_p$-espace vectoriel) mais aussi de manière multiplicative ($\mathbb{F}_q^*$). Cela permet de combiner deux types de caractères.

QUESTIONS

Q Appliquer le théorème de structure à $(\mathbb{Z}/56\mathbb{Z})^\times$ et $(\mathbb{Z}/35\mathbb{Z})^\times$.

R C'est bien un groupe abélien (groupe fini d'inversibles). On a $\varphi(56) = \varphi(2^3 \times 7) = \varphi(8)\varphi(7) = 4 \times 6 = 24$ donc le groupe est d'ordre 24.
On a $24 = 3 \times 2^3$ et le théorème chinois donne :

$$(\mathbb{Z}/56\mathbb{Z})^\times \simeq (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/8\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Puis de même :

$$(\mathbb{Z}/35\mathbb{Z})^\times \simeq (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Si $p \neq 2$:

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* = \mathbb{Z}/(p^\alpha - p^{\alpha-1})\mathbb{Z}$$

Et

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \begin{cases} \{1\} & \text{si } \alpha = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{si } \alpha = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z} & \text{si } \alpha \geq 3 \end{cases}$$

BIBLIOGRAPHIE

[Col11] P. COLMEZ : *Éléments d'analyse et d'algèbre*. Les éditions de l'École Polytechnique, 2ème édition, 2011.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. PEYRÉ : *L'algèbre discrète de la transformée de* FOURIER. Ellipses, 2004.

120 ANNEAUX $\mathbb{Z}/n\mathbb{Z}$. APPLICATIONS.

Soit $n \in \mathbb{N}^*$. On désigne par $\mathcal{P}$ l'ensemble des nombres premiers.

I. Structure de $\mathbb{Z}/n\mathbb{Z}$

I. A. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

[Rom17, §1.4-5/1.9/10.1, p13–19/27/277] [Per96, §1.1/1.7, p10/24]

Définition 1. Deux entiers x, y sont dis congrus modulo n si $x - y \in n\mathbb{Z}$. C'est une relation d'équivalence sur $\mathbb{Z}$. On note $\overline{x}$ la classe de x et $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$.

Proposition 2. *$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique à n éléments engendré par $\overline{1}$.*

Application 3. Tout groupe cyclique à n éléments est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 4. $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$: considérer $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n, \overline{k} \longmapsto \mathrm{e}^{2ik\pi/n}$.

Proposition 5. *L'ordre de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{k \wedge n}$.*

Corollaire 6. *$(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par les $\overline{k}$ tels que $k \wedge n = 1$.*

Exemple 7. $\mathbb{Z}/8\mathbb{Z}$ est engendré par $\overline{1}, \overline{3}, \overline{5}$ et $\overline{7}$.

Définition 8. [Indicatrice d'Euler]
Pour $n \geq 2$, on définit $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 9. Pour $p \in \mathcal{P}$, on a $\varphi(p^\alpha) = p^\alpha(p-1)$ pour $\alpha \in \mathbb{N}^*$.

Proposition 10. [Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$]
Pour $d \mid n$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, engendré par $\frac{\overline{n}}{d}$ et formé des éléments dont l'ordre divise d.

Proposition 11. *Si $d \mid n$, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d.*

Application 12. $n = \sum_{d|n} \varphi(d)$

Théorème 13. [Structure des groupes abéliens finis]
Soit G un groupe abélien fini. Alors il existe $r \geq 1$ et $2 \leq d_1 \mid \cdots \mid d_r$ uniques tels que $G \simeq \prod_{i=1}^r \mathbb{Z}/d_i\mathbb{Z}$.

Exemple 14. Les groupes abéliens d'ordre 24 sont isomorphes à $\mathbb{Z}/24\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

I. B. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

[Rom17, §10.1-3, p277–288] [Per96, §1.7, p24–28]

Proposition 15. *Les idéaux de $\mathbb{Z}$ sont les $(k\mathbb{Z})_{k\in\mathbb{N}}$.*

Définition 16. L'ensemble des classes modulo n est muni d'une structure d'anneau : on définit l'anneau commutatif $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Remarque 17. Les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les sous-groupes du groupe $\mathbb{Z}/n\mathbb{Z}$.

Application 18. Soit A un anneau commutatif unitaire. Il existe un unique entier positif, appelé caractéristique de A, noté $\mathrm{car}(A)$, tel que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/\mathrm{car}(A)\mathbb{Z}$.

Proposition 19. *Les inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les $\overline{k}$ tels que $k \wedge n = 1$. Ils forment un groupe à $\varphi(n)$ éléments.*

Application 20. On a l'isomorphisme $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \simeq ((\mathbb{Z}/n\mathbb{Z})^\times, \times)$.

Proposition 21. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si c'est un corps si et seulement si $n \in \mathcal{P}$.*
[Rom17, §11.5, p324–327]

Théorème 22. [Théorème chinois]
Si $n, m \geq 1$, alors on a l'isomorphisme d'anneaux $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si $n \wedge m = 1$.

Corollaire 23. *Si $n = \prod_{i=1}^r p_i^{\alpha_i}$, alors $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ et on en déduit $\varphi(n) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1)$.*

Théorème 24. *Si $p \in \mathcal{P}$, $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ est cyclique.*

II. Application à l'arithmétique dans $\mathbb{Z}$

II. A. Tests de primalité [Rom17, §10.2/11.5-6, p280–282/324–329] [Gou09, §1.4, p34–37]

Théorème 25. [Théorème d'Euler] *Soit $a \in \mathbb{Z}$ premier avec n. Alors $a^{\varphi(n)} \equiv 1 \mod n$.*

Théorème 26. [Petit théorème de Fermat]
Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tels que $p \nmid a$. Alors $a^{p-1} \equiv 1 \mod p$.

Remarque 27. La réciproque est fausse! Par exemple avec 561. En revanche, pour tout $a \in \mathbb{Z}$, on a $a^p \equiv 1 \mod p$.

Définition 28. [Nombre de Carmichaël]
Un entier $n > 1$ non premier est de Carmichaël si $\forall a \in \mathbb{Z}, a \wedge n = 1 \implies a^{n-1} \equiv 1 \mod n$.

Proposition 29. *Un nombre de Carmichaël est impair et sans facteur carré.*

Application 30. [Algorithme RSA]
Alice veut envoyer un message privé à Bob.

- Bob choisit deux entiers premiers distincts $p, q \in \mathcal{P}$ et pose $n = pq$, puis il choisit ensuite $d, e \in \mathbb{Z}$ tels que $de \equiv 1 \mod \varphi(n)$ (on a $\varphi(n) = (p-1)(q-1)$ et il suffit de trouver d premier à $\varphi(n)$ et son inverse).
- Bob diffuse la clé publique (n, d) à tout le monde et converse la clé secrète (n, e).
- Pour envoyer son message $m \mod n$, Alice envoie le message chiffré $M \equiv m^d \mod n$.
- Bob déchiffre le message $m = M^e \mod n$ d'après le théorème d'Euler.

Le succès de cet algorithme réside dans la difficulté de factorisation d'un entier.

Théorème 31. [Théorème de Wilson] *Si $n \geq 2$, on a $n \in \mathcal{P} \iff (n-1)! \equiv -1 \mod n$.*

II. B. Équations arithmétiques [Rom17, §10.3-4, p283–290]

Soient $n, m \geq 2$.

Théorème 32. *Soit $a \in \mathbb{N}^*, b \in \mathbb{Z}$. On note $\delta = a \wedge n$ et on écrit $a = \delta a'$ et $n = \delta n'$. L'équation $ax \equiv b \mod n$ a des solutions entières si et seulement si $\delta \mid b$ et dans ce cas, si $b = \delta b'$, les solutions sont les $b'x_0' + kn'$ avec $k \in \mathbb{Z}$ et x_0' est une solution particulière de $a'x \equiv 1 \mod n'$.*

Théorème 33. *Dans le Théorème 22, l'isomorphisme est donné par $\psi : a \mod nm \longmapsto (a \mod n, a \mod m)$ de réciproque $\psi^{-1} : (a \mod n, b \mod m) \longmapsto unb + vma \mod nm$ où l'on a choisit $u, v \in \mathbb{Z}$ tels que $un + vm = 1$.*

Application 34. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations $\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$ d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors

- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k \in \mathbb{Z}}$.

Exemple 35. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k \in \mathbb{Z}}$.

II. C. Résidus quadratiques modulo p [Rom17, §13.6-7, p429–436] [Per96, §3.2, p72–76]

Soit $p \in \mathcal{P}$. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \left\{x^2 \mid x \in \mathbb{F}_p\right\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 36. *Si $p = 2$, alors $\mathbb{F}_p^2 = \mathbb{F}_p$. Sinon, on a $\left|\mathbb{F}_p^2\right| = \frac{p+1}{2}$.*

Application 37. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

On suppose dans la suite p impair.

Lemme 38. *On a $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.*

Exemple 39. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 40. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 41. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Exemple 42. -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$.

Proposition 43. *$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ pour tout $a, k \in \mathbb{Z}$. On peut donc définir $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. C'est l'unique morphisme de groupes non trivial de $(\mathbb{F}_p^*, \times)$ vers $(\{\pm 1\}, \times)$.*

Remarque 44. Pour $a \in \mathbb{Z}$, le nombre de solutions de $x^2 = \overline{a}$ dans $\mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Théorème 45. [Loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 46. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n.

Exemple 47. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

III. Applications aux polynômes et à la théorie des corps

III. A. Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p

[Rom17, §12.11.4, p381–383] [Per96, §3.3-3.4, p76–85] [FGN07, §5.16, p188–190]

Proposition 48. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et irréductible dans $\mathbb{Q}[X]$.*

Proposition 49. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. Si $p \nmid a_r$, $\forall i < r, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 50. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 51. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 52. $X^3+462X^2+2433X-67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme X^p-X-1 pour tout $p \in \mathcal{P}$.

Définition 53. [Polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times}(X - \zeta)$.

Proposition 54. *$\Phi_n \in \mathbb{Z}[X]$.*

Théorème 55. *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

Corollaire 56. *On a $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.*

III. B. Corps finis

[Per96, §3.2, p72–76] [Rom17, Ch13, p415]

Proposition 57. *Si $\mathbb{K}$ est un corps fini, sa caractéristique est un nombre premier $p \in \mathcal{P}$ et son sous-corps premier est isomorphe à $\mathbb{F}_p$.*

Corollaire 58. *Si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectorieloù $p = \mathrm{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(\mathbb{K})$. De plus, tout sous-corps de $\mathbb{K}$ est de cardinal p^d pour un $d \mid n$ et réciproquement pour tout $d \mid n$ il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d.*

Théorème 59. *Il existe un corps fini à $q = p^n$ éléments pour tout $p \in \mathcal{P}, n \in \mathbb{N}^*$. Il s'agit du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ ou de tout autre polynôme irréductible de $\mathbb{F}_p$. Ce corps est unique à isomorphisme près.*

Exemple 60. $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 éléments de caractéristique 2.

Corollaire 61. *Tout corps de rupture d'un polynôme P irréductible sur $\mathbb{F}_p[X]$ est un corps de décomposition de P sur $\mathbb{F}_p$.*

SPEECH

Lorsque l'on fait de l'arithmétique dans $\mathbb{Z}$, on s'intéresse rapidement à l'arithmétique modulaire, c'est-à-dire le reste d'un nombre modulo n. La puissance de l'arithmétique modulaire provient surtout des différentes structures de $\mathbb{Z}/n\mathbb{Z}$, naturellement héritées de la structure de $\mathbb{Z}$.
Dans la première partie, on quotiente $\mathbb{Z}$ par $n\mathbb{Z}$. Tout groupe cyclique est de ce type, et on connaît précisément ses générateurs. En ajoutant la multiplication, on obtient une structure d'anneau. On peut alors déterminer les inversibles de $\mathbb{Z}/n\mathbb{Z}$, ce qui set par exemple pour les équations arithmétiques. Le cas particulier des corps (n premier) et le théorème chinois sont des résultats très utiles.
Ensuite, on s'intéresse à l'arithmétique dans $\mathbb{Z}$, avec le théorème de FERMAT, dont la réciproque est fausse et les contre-exemples sont les nombres de CARMICHAËL. Les applications en cryptographie sont importantes comme par exemple l'algorithme RSA, mais. De nombreux résultats sur les équations diophantiennes découlent également de notre étude. Enfin le cas particulier des corps mène à la loi de réciprocité quadratique afin de savoir rapidement si un nombre est un carré ou non dans $\mathbb{Z}/p\mathbb{Z}$.
Enfin, l'étude de $\mathbb{Z}/n\mathbb{Z}$ amène des avancées dans d'autres domaines de l'algèbre, notamment des résultats d'irréductibilité de polynômes et la construction de tous les corps finis à partir d'un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.

COMMENTAIRES

Pour les tests de primalité et les algorithmes de chiffrement, voir aussi [Zé17].
Il faut connaître :

- les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ s'identifient au groupe $\mathbb{Z}/(n \wedge m)\mathbb{Z}$. Si $m \mid n$ le seul morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est $\overline{k}_n \longmapsto \overline{k}_m$. Sinon, il n'y a aucun morphisme,
- les diviseurs de 0 de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les $\overline{k}$ avec $k \wedge n = 1$. Les éléments nilpotents forment l'idéal de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{p_1 \dots p_r}$ où $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$,
- savoir ce que devient le théorème chinois si n et m ne sont plus premiers entre eux,
- savoir que la réciproque du théorème de réduction modulo p pour les polynômes de $\mathbb{Z}[X]$ est vraie : voir pour $X^4 + 1$ dans [Per96].

QUESTIONS

Q Démontrer la proposition 7.

Q Quel est l'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$?

R $\mathrm{PPCM}(m, n)$.

Q Quelle est la caractéristique de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ pour $a, b \in \mathbb{N}$? Et de $\prod_{k \in \mathbb{N}^*} \mathbb{Z}/k\mathbb{Z}$?

R $\mathrm{PPCM}(a, b)$ puis 0, bien que $\prod_{k \in \mathbb{N}^*} \mathbb{Z}/k\mathbb{Z}$ « contienne » tous les $\mathbb{Z}/n\mathbb{Z}$.

Q Expliciter l'isomorphisme du théorème chinois.

Q Résoudre $x \iff 1 \mod 3, x \equiv 4 \mod 5$ et $x \equiv 0 \mod 7$.

R On trouve une relation de BÉZOUT ($3 + 5 - 7 = 1$) ou on résout deux systèmes puis on ajoute le troisième.

Q Quels sont les nilpotents de $\mathbb{Z}/n\mathbb{Z}$?

R Écrivons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Si $m \in \prod_{i=1}^{r} p_i\mathbb{Z}$, alors m est nilpotent d'ordre au plus $\max_{1 \leq i \leq r} \alpha_i$. Réciproquement si m est nilpotent alors pour tout $1 \leq i \leq r$, on a $p_i \mid m$.
Attention : être nilpotent ne signifie pas être non inversible ! Par exemple 2 dans $\mathbb{Z}/6\mathbb{Z}$ n'est ni nilpotent, ni inversible.

Q Condition nécessaire pour que $P \in \mathbb{Z}/n\mathbb{Z}[X]$ soit inversible ?

Q Soit $n \geq 2$ et e premier avec $\varphi(n)$. Montrer que $\mathbb{Z}/n\mathbb{Z}^* \longrightarrow \mathbb{Z}/n\mathbb{Z}^*, x \longmapsto x^e$ est une bijection, et exhiber la réciproque (voir l'algorithme RSA).

Q Soient p, q premiers impairs, $\psi : (\mathbb{Z}/pq\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ et $E = \left\{x \in (\mathbb{Z}/pq\mathbb{Z})^* \mid 1 \leq x < \frac{pq}{2}\right\}$. Déterminer $\mathrm{Im}(E)$.

BIBLIOGRAPHIE

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Zé17] G. ZÉMOR : *Cours de cryptographie*. Cassini, 2017.

121 NOMBRE PREMIERS. APPLICATIONS.

On désigne par $\mathcal{P}$ l'ensemble des nombres premiers.

I. Généralités et arithmétique dans $\mathbb{Z}$ [Rom17, Ch11, p301]

I. A. Nombres premiers et premiers entre eux

Définition 1. [entier premier]
$p \in \mathbb{N}$ est dit premier (et on note $p \in \mathcal{P}$) si p a exactement deux diviseurs positifs 1 et $|p|$.

Remarque 2. $(\mathbb{Z}, +, \times)$ est euclidien donc principal, ses idéaux sont les $(n\mathbb{Z})_{n\in\mathbb{N}}$. Dire que $p \in \mathcal{P}$ c'est dire que $p\mathbb{Z}$ est un idéal maximal.

Exemple 3. Les premiers nombres premiers sont $2, 3, 5, 7, 9, 11, 13, 17, \ldots$. Mais $6 = 2 \times 3$ n'est pas premier.

Définition 4. [entiers premiers entre eux, dans leur ensemble]
Deux entiers a et b sont dits premiers entre eux si le plus grand diviseur entier de a et b est 1.
Des entiers $(a_i)_{i\in I}$ sont dits premiers dans leur ensemble si le plus grand diviseur entier de chacun des $(a_i)_{i\in I}$ est 1.

Exemple 5. Si $p \in \mathcal{P}$ et $a \in \mathbb{N}$, p et a sont premiers entre eux si et seulement si $p \nmid a$.
$\{6, 10, 15\}$ sont premiers dans leur ensemble bien que $\{6, 10\}$, $\{6, 15\}$ et $\{10, 15\}$ ne soient pas premiers entre eux.

Application 6. Deux groupes de cardinaux premiers entre eux sont d'intersection triviale.

Lemme 7. [lemme d'Euclide] *Tout entier $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ admet un diviseur premier.*

Théorème 8. [décomposition en produit de facteurs premiers]
Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ où $r \in \mathbb{N}^*$, $p_1 < p_2 < \cdots < p_r \in \mathcal{P}$ et $(\alpha_i)_{1\leq i\leq r} \in (\mathbb{N}^*)^r$.

Exemple 9. $1663200 = 2^5 \times 3^3 \times 5^2 \times 7 \times 11$.

I. B. Arithmétique [Rom17, Ch8, p231]

Définition 10. [PGCD, PPCM] On définit le PGCD (resp. PPCM) d'une famille d'éléments comme le plus grand diviseur (resp. le plus petit multiple) commun à chacun de ses éléments.

Application 11. $\mathrm{PGCD}(10, 30) = 10, \mathrm{PGCD}(2, 15) = 1, \mathrm{PPCM}(2, 3, 5, 7) = 210$.

Application 12. Calcul des PGCD et PPCM d'une famille d'éléments en fonction de leur décomposition en produit de facteurs premiers. On pourra introduire les valuations p-adique.

Théorème 13. [identité de Bézout]
Soit $r \geq 2$ et $(a_1, \ldots, a_r)$ des entiers relatifs. Si $\delta = \mathrm{PGCD}((a_i)_{1\leq i\leq r})$, alors il existe des entiers relatifs $u_1, \ldots, u_r$ tels que $\sum_{i=1}^r u_i a_i = \delta$.
Les $(a_i)_{1\leq i\leq r}$ sont premiers entre eux si et seulement si il existe des entiers relatifs $u_1, \ldots, u_r$ tels que $\sum_{i=1}^r u_i a_i = 1$.

Lemme 14. [lemme de Gauss] *Soient $a, b, c \in \mathbb{Z}$.*
(i) Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.
(ii) Si $a \mid bc$ et $b \wedge c = 1$, alors $a \mid b$ et $a \mid c$.

Application 15. Pour $p \in \mathcal{P}$ et $k \in [\![1, p-1]\!]$, on a $p \mid \binom{p}{k}$.

I. C. Répartition des nombres premiers

Théorème 16. *$\mathcal{P}$ est de cardinal infini.*

Application 17. Le crible d'Ératosthène permet de trouver tous les nombres premiers compris entre 2 et un entier $n > 2$ fixé.

Proposition 18. *Il existe des segments de longueur arbitraire sans nombre premier.*

Théorème 19. *(admis) Notons $\Pi(n) = \mathrm{card}(\mathcal{P} \cap [\![1, n]\!])$. Alors $\Pi(n)/n \sim \frac{1}{\ln(n)}$.*

II. Tests de primalité [Rom17, §10.2/11.5-6, p280–282/324–329] [Gou09, §1.4, p34–37]

Théorème 20. [théorème d'Euler] *Soit $a \in \mathbb{Z}$ premier avec n. Alors $a^{\varphi(n)} \equiv 1 \mod n$.*

Théorème 21. [petit théorème de Fermat]
Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tels que $p \nmid a$. Alors $a^{p-1} \equiv 1 \mod p$.

Remarque 22. La réciproque est fausse! Par exemple avec 561. En revanche, pour tout $a \in \mathbb{Z}$, on a $a^p \equiv 1 \mod p$.

Définition 23. [Nombre de Carmichaël]
Un entier $n > 1$ non premier est de Carmichaël si $\forall a \in \mathbb{Z}, a \wedge n = 1 \implies a^{n-1} \equiv 1 \mod n$.

Proposition 24. *Un nombre de* Carmichaël *est impair et sans facteur carré.*

Application 25. [Algorithme RSA]
Alice veut envoyer un message privé à Bob.
- Bob choisit deux entiers premiers distincts $p, q \in \mathcal{P}$ et pose $n = pq$, puis il choisit ensuite $d, e \in \mathbb{Z}$ tels que $de \equiv 1 \mod \varphi(n)$ (on a $\varphi(n) = (p-1)(q-1)$ et il suffit de trouver d premier à $\varphi(n)$ et son inverse).
- Bob diffuse la clé publique (n, d) à tout le monde et converse la clé secrète (n, e).
- Pour envoyer son message $m \mod n$, Alice envoie le message chiffré $M \equiv m^d \mod n$.
- Bob déchiffre le message $m = M^e \mod n$ d'après le théorème d'Euler.

Le succès de cet algorithme réside dans la difficulté de factorisation d'un entier.

Théorème 26. [Théorème de Wilson] *Si $n \geq 2$, on a $n \in \mathcal{P} \iff (n-1)! \equiv -1 \mod n$.*

III. Applications en algèbre

III. A. Théorie de Sylow

[Per96, §1.5, p18–20]

Soit G un groupe fini d'ordre n, et $p \in \mathcal{P}$ diviseur de n. On notera $n = p^a m$ où $p \nmid m$.

Définition 27. [p-groupe, p-sous-groupe de Sylow]
Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de Sylow (ou p-Sylow) un sous-groupe de G de cardinal p^a.

Corollaire 28. [Équation aux classes]
Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Application 29. Le centre d'un p-groupe non trivial est non trivial.

Théorème 30. [Théorème de Sylow 1] *Il existe au moins un p-*Sylow *dans G.*

Corollaire 31. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

Théorème 32. [Théorème de Sylow 2]
*(i) si $H < G$ est un p-groupe, alors il existe un p-*Sylow *S tel que $H < S$,*
*(ii) les p-*Sylow *sont tous conjugués,*
*(iii) notons Σ le nombre de p-*Sylow *de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.*

Corollaire 33. *Soit S un p-*Sylow *de G. Alors $S \lhd G \iff S$ est l'unique p-*Sylow *de G.*

Application 34. Tout groupe d'ordre 63 ou 255 n'est pas simple.

III. B. Propriétés des corps finis

[Per96, §3.2, p72–76] [Rom17, Ch13, p415]

Pour $p \in \mathcal{P}$, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition 35. Soit A un anneau commutatif unitaire. Il existe un unique entier positif, appelé caractéristique de A, noté $\mathrm{car}(A)$, tel que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/\mathrm{car}(A)\mathbb{Z}$.

Proposition 36. *Si $\mathbb{K}$ est un corps fini, sa caractéristique est un nombre premier $p \in \mathcal{P}$ et son sous-corps premier est isomorphe à $\mathbb{F}_p$.*

Corollaire 37. *Si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectorieloù $p = \mathrm{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(\mathbb{K})$. De plus, tout sous-corps de $\mathbb{K}$ est de cardinal p^d pour un $d \mid n$ et réciproquement pour tout $d \mid n$ il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d.*

Théorème 38. *Il existe un corps fini à $q = p^n$ éléments pour tout $p \in \mathcal{P}, n \in \mathbb{N}^*$. Il s'agit du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ ou de tout autre polynôme irréductible de $\mathbb{F}_p$. Ce corps est unique à isomorphisme près. On le note $\mathbb{F}_q$*

Exemple 39. $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 éléments de caractéristique 2.

Corollaire 40. *Tout corps de rupture d'un polynôme P irréductible sur $\mathbb{F}_p[X]$ est un corps de décomposition de P sur $\mathbb{F}_p$.*

Définition 41. [Morphisme de Frobenius]
$\mathrm{Frob} : \mathbb{F}_q \longrightarrow \mathbb{F}_q, x \longmapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius.

Proposition 42. *Frob est un automorphisme et les sous-corps de $\mathbb{F}_q$ sont exactement les ensembles des points fixes de Frob^d pour $d \mid n$.*

Théorème 43. *Frob est cyclique d'ordre n et on a $\mathrm{Aut}(\mathbb{F}_q) = \langle \mathrm{Frob} \rangle$.*

III. C. Résidus quadratiques modulo p

[Rom17, §13.6-7, p429–435] [Per96, §3.2, p72–76]

Soit $p \in \mathcal{P}$. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 44. *Si $p = 2$, alors $\mathbb{F}_p^2 = \mathbb{F}_p$. Sinon, on a $\left|\mathbb{F}_p^2\right| = \frac{p+1}{2}$.*

Application 45. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

On suppose dans la suite p impair.

Lemme 46. *On a $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.*

Exemple 47. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 48. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 49. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Exemple 50. -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$.

Proposition 51. *$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ pour tout $a, k \in \mathbb{Z}$. On peut donc définir $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. C'est l'unique morphisme de groupes non trivial de $(\mathbb{F}_p^*, \times)$ vers $(\{\pm 1\}, \times)$.*

Remarque 52. Le nombre de solutions de $x^2 = a$ pour $a \in \mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Théorème 53. [Loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 54. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n :

Exemple 55. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

III. D. Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p

[Per96, §3.3-3.4, p76–85]

Proposition 56. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et irréductible dans $\mathbb{Q}[X]$.*

Proposition 57. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. Si $p \nmid a_r$, $\forall i < r, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 58. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 59. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 60. $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme $X^p - X - 1$ pour tout $p \in \mathcal{P}$.

Définition 61. [Polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

Proposition 62. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 63. [Irréductibilité de Φ_n] *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

SPEECH

Les nombres premiers apparaissent naturellement dans de nombreux domaines mathématiques. C'est pourquoi ils ont été étudié très tôt dans l'histoire des mathématiques.
La première partie contient les définitions de bases et la formulation équivalente en terme d'idéaux. Le premier résultat important est la décomposition en facteurs premiers. Notons aussi le lemme de GAUSS qui est fondamental en arithmétique. La répartition des nombres premiers est un problème très étudié, de nombreux résultats sont connus, nous en rappelons quelques uns.
Dans une deuxième partie, on s'intéresse aux applications des nombres premiers en arithmétique avec notamment les théorèmes de FERMAT et de WILSON. Cela mène aujourd'hui aux algorithmes de cryptographie qui s'appuient sur les nombres premiers.
Ensuite, on regarde les applications en algèbre, que ce soit en théorie des groupes avec les p-SYLOW, mais aussi en théorie des corps avec la notion de caractéristique, la cardinal d'un corps de caractéristique p … Le morphisme de FROBENIUS caractérise les sous-corps de $\mathbb{F}_q$. On regarde ensuite les carrés dans un corps fini via la loi de réciprocité quadratique (en développement). Citons enfin des critères d'irréductibilité de polynômes sur des anneaux comme $\mathbb{Z}[X]$ (critère d'EISENSTEIN) mais aussi l'irréductibilité des polynômes cyclotomiques (en développement) dont la preuve s'appuie sur les nombres premiers.

BIBLIOGRAPHIE

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

122 ANNEAUX PRINCIPAUX. APPLICATIONS.

Soit A un anneau unitaire commutatif intègre et $\mathbb{K}$ un corps commutatif.

I. Arithmétique dans les anneaux

I. A. Vocabulaire

[Per96, §II.3, p45] [Rom17, Ch7, p205]

Définition 1. [idéal]
$I \subset A$ est un idéal si $(I,+)$ est un sous-groupe de $(A,+)$ et si $\forall (a,i) \in A \times I, ai \in I$.

Exemple 2. Pour $a \in A$, $(a) = aA$ le plus petit idéal contenant a est dit principal.

Définition 3. [divisibilité]
Pour $a, b \in A$, on dit que a divise b et on note $a \mid b$ si $\exists c \in A \mid b = ac$, ou encore $(b) \subset (a)$.

Définition 4. [éléments associés]
$a, b \in A$ sont dits associés si $a \mid b$ et $b \mid a$ (ou s'il existe $u \in A^\times$ tel que $a = ub$).

Remarque 5. C'est une relation d'équivalence (notée $\sim$). Deux éléments associés sont indiscernables du point de vue de la divisibilité.

Définition 6. [premier, irréductible] $a \in A$ non inversible et non nul est dit :
- premier si pour tout $b, c \in A$ tels que $a \mid bc$, alors $a \mid b$ ou $a \mid c$,
- irréductible si pour tout $b, c \in A$ tels que $a = bc$, alors $b \in A^\times$ ou $c \in A^\times$.

Proposition 7. *Si $a \in A$ est premier alors a est irréductible.*

Exemple 8. Dans $\mathbb{Z}$, les éléments premiers sont les nombres premiers et leurs opposés, tout comme les irréductibles (on a équivalence dans ce cas, comme on le verra plus loin).

Définition 9. [PGCD, PPCM] Soient $a, b \in A$. On dit que
- $d \in A$ est un PGCD de a et b et on note $d = a \wedge b$ si $\forall c \in A, c \mid a$ et $c \mid b \Longrightarrow c \mid d$,
- $m \in A$ est un PPCM de a et b et on note $m = a \vee b$ si $\forall c \in A, a \mid c$ et $b \mid c \Longrightarrow m \mid c$.

a et b sont dits premiers entre eux si $a \wedge b = 1$.

Remarque 10. 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 11. *Deux* PGCD *(resp.* PPCM*) de $a, b \in A$ sont associés.*

I. B. Anneaux principaux

[Per96, §2.3-4, p49–51] [Rom17, Ch8, p231] [Com98, Ch11, p237]

Définition 12. [anneau principal]
A est dit principal si tous ses idéaux sont principaux (engendrés par un élément).

Exemple 13. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.

Proposition 14. *$A[X]$ est principal si et seulement si A est un corps.*

Soit désormais A principal.

Théorème 15. [théorème de Bachet-Bézout]
Soient $a, b \in A^*$. Alors il existe $d \in A \mid (a,b) = (a) + (b) = (d)$. d est alors un PGCD *de a et b et il existe $u, v \in A$ tels que $au + bv = d$.*

Proposition 16. *Soient $a, b \in A^*$. Alors il existe $m \in A \mid (a) \cap (b) = (m)$. On a $m = a \vee b$.*

Remarque 17. On peut là encore généraliser à toute famille finie d'éléments.

Théorème 18. [théorèmes de Gauss]
Soient $a, b, c \in A^*$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$. Si $ab \mid c$ et $b \wedge c = 1$, alors $a \mid c$.

Théorème 19. [théorème des restes chinois]
Soient $a_1, \ldots, a_r \in A$ deux à deux premiers. Alors l'application $\phi : x \mod a_1 \ldots a_r \longmapsto (x \mod a_i)_{1 \leq i \leq r}$ est un isomorphisme d'anneaux de $A/(a_1 \ldots a_r)$ sur $\prod_{i=1}^r A/(a_i)$.

Remarque 20. Si les $(a_i)_{1 \leq i \leq r}$ ne sont pas deux à deux premiers, le résultat est faux : par exemple $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Proposition 21. *Soit $p \in A^*$. Alors p est irréductible si et seulement si $A/(p)$ est intègre si et seulement si $A/(p)$ est un corps.*

Corollaire 22. *Dans un anneau principal, premier équivaut à irréductible.*

Proposition 23.
- *Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
- *Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racines.*
- *$\mathbb{Q}[X]$ possède des irréductibles de degré arbitrairement grand.*

I. C. Anneau factoriel

[Per96, §2.3, p47] [Rom17, §7.6/8.2, p217/237]

Définition 24. [Anneau factoriel]
Un anneau A est factoriel si pour tout $a \in A^*$:
(E) il existe $n \in \mathbb{N}, p_1, \dots, p_n \in A$ irréductibles et $u \in A^\times$ tels que $a = up_1 \dots p_n$.
(U) si de plus on peut aussi écrire $a = vq_1 \dots q_r$ pour un $r \in \mathbb{N}, q_1, \dots, q_r \in A$ irréductibles et $v \in A^\times$, alors $r = n$ et il existe $\sigma \in \mathfrak{S}_n$ tel que $p_i \sim q_{\sigma(i)}$ pour tout $1 \leq i \leq n$.

Proposition 25. *Soit $\mathcal{P}$ un système de représentants d'éléments irréductibles à association près. Alors tout élément $a \in A^*$ s'écrit de manière unique sous la forme (le produit ne comporte qu'un nombre fini de termes distincts de 1) :*

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{où } u \in A^\times \text{ et } v_p(a) = \max\{n \in \mathbb{N} \mid p^n \mid a\}$$

Corollaire 26. *Soit $(a_i)_{i\in I}$ une famille d'éléments de A. Alors $(a_i)_{i\in I}$ possède un PGCD et si I est fini, $(a_i)_{i\in I}$ possède un PPCM. On a :*

$$\mathrm{PGCD}((a_i)_{i\in I}) = \prod_{p\in\mathcal{P}} p^{\min_{i\in I} v_p(a_i)} \quad \text{et} \quad \mathrm{PPCM}((a_i)_{i\in I}) = \prod_{p\in\mathcal{P}} p^{\max_{i\in I} v_p(a_i)}$$

Corollaire 27. *Soient $a, b \in A^*$. Alors $a \mid b \iff \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$.*

Proposition 28. *Un anneau principal est factoriel.*

Exemple 29. $\mathbb{Z}$ est factoriel. Ainsi tout entier $n \in \mathbb{Z}^*$ s'écrit de manière unique $n = \varepsilon \prod_{p\in\mathcal{P}} p^{v_p(n)}$ où $\varepsilon = \pm 1$ et $\mathcal{P}$ est l'ensemble des nombres premiers.

Exemple 30. $\mathbb{K}[X]$ est factoriel. En particulier :
- pour $P \in \mathbb{C}[X]$, il existe $a \in \mathbb{C}$, $(\lambda_i)_{1\leq i\leq \ell} \in \mathbb{C}^\ell$ distincts et $(\alpha_i)_{1\leq i\leq \ell} \in (\mathbb{N}^*)^\ell$ tels que
$$P = a \prod_{i=1}^{\ell} (X - \lambda_i)^{\alpha_i}$$
- pour $P \in \mathbb{R}[X]$, il existe $a \in \mathbb{R}$,$(\lambda_i)_{1\leq i\leq \ell} \in \mathbb{R}^\ell$ distincts et $(\alpha_i)_{1\leq i\leq \ell} \in (\mathbb{N}^*)^\ell$, puis $(\mu_j, \nu_j)_{1\leq j\leq m} \in (\mathbb{R}^2)^m$ distincts et $(\beta_j)_{1\leq j\leq m} \in \mathbb{N}^*$ tels que $\mu_j^2 - 4\nu_j < 0$ pour tout j et
$$P = a \prod_{i=1}^{\ell} (X - \lambda_i)^{\alpha_i} \prod_{j=1}^{m} (X^2 + \mu_j X + \nu_j)^{\beta_j}$$

Théorème 31. [Théorème de Gauss] *Si A est factoriel, alors $A[X]$ factoriel.*

Corollaire 32. *Si A est factoriel alors pour tout $n \in \mathbb{N}$, $A[X_1, \dots X_n]$ est factoriel.*

Exemple 33. Un anneau factoriel n'est pas nécessairement principal ! Considérer par exemple $\mathbb{Z}[X]$ et $(2, X)$ qui n'est pas principal.

II. Applications aux anneaux euclidiens

II. A. Généralités

[Per96, §2.3-5, p50] [Rom17, Ch9, p257] [Com98, §11.2, p238]

Définition 34. [Stathme, anneau euclidien]
Un stathme sur A est une application $\varphi : A^* \longrightarrow \mathbb{N}$ telle que pour $a, b \in A \times A^*$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Exemple 35. $\mathbb{Z}$ muni de la valeur absolue et $\mathbb{K}[X]$ muni du degré sont euclidiens.

Proposition 36. *Un anneau euclidien est principal.*

Proposition 37. *$\mathbb{K}[X]$ est euclidien.*

Application 38. [Algorithme d'Euclide] Dans un anneau euclidien, il existe un algorithme permettant de trouver le PGCD de deux éléments.

Proposition 39. *$\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais non euclidien.*

II. B. L'anneau des entiers de Gauss

[Per96, §2.3, p50] [Rom17, §9.4.3, p263] [Com98, §11.6, p246]

Définition 40. On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.

Proposition 41. *Muni du stathme $N(a + ib) = a^2 + b^2$, $\mathbb{Z}[i]$ est euclidien.*

Proposition 42. $\mathbb{Z}[i]^\times = N^{-1}(\{1\}) = \{\pm 1, \pm i\}$.

On définit $\Sigma = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N} \mid n = a^2 + b^2\}$. On cherche à quelle(s) condition(s) $n \in \Sigma$.

Exemple 43. $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$ mais pas $3, 6, 7, 11$.

Lemme 44. *Σ est stable par produit.*

Lemme 45. *Si $p \in \mathcal{P}$, alors $p \in \Sigma \iff p \equiv 1, 2 \mod 4$.*

Théorème 46. [Théorème des deux carrés de Fermat]
$n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ tel que $p \mid n$ et $p \mid 3 \mod 4$, alors $2 \mid v_p(n)$.

Proposition 47. *Les irréductibles de $\mathbb{Z}[i]$ sont :*
- *les $p \in \mathcal{P}$ tels que $p \equiv 3 \mod 4$,*
- *les $a + ib$ tels que $a^2 + b^2 \in \mathcal{P}$.*

III. Autres applications

III. A. Équations diophantiennes

[Rom17, §8.3/10.4, p243/288]

Théorème 48. *Dans le Théorème 19, l'isomorphisme réciproque est $\psi^{-1} : (x_i \mod a_i)_{1\le i\le r} \longmapsto \sum_{i=1}^r x_i u_i b_i \mod a_1 \dots a_r$ où $b_i = a/a_i$ et $\sum_{i=1}^r u_i b_i = 1$.*

Application 49. Soit $a, b, c \in A$ principal. On note $d = a \wedge b = au + bv$ et on écrit $a = da'$ et $b = db'$. L'équation $ax + bv = c$ admet une solution si et seulement si $d \mid c$, disons $c = dc'$ et dans ce cas les solutions sont de la forme $(c'u + kb', c'v - ka')_{k\in A}$.

Remarque 50. Dans le cas où l'anneau est euclidien, on peut déterminer u et v par l'algorithme d'Euclide.

Application 51. [Le cas de $\mathbb{Z}$] Soient $n, m \ge 2$. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors
- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k\in\mathbb{Z}}$.

Exemple 52. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k\in\mathbb{Z}}$.

III. B. Algèbre linéaire

[MM16] [BMP05, §4.2.1, p158–161] [Gou09, §5.4, p224–226]

Soit $M \in \mathcal{M}_n(\mathbb{K})$.

Définition 53. [Polynôme minimal]
L'application $\varphi_M : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[M] \\ P & \longmapsto & P(M) \end{array}$ est un morphisme d'algèbres. Son noyau est un idéal de $\mathbb{K}[X]$ principal donc est engendré par un unique polynôme unitaire π_M appelé polynôme minimal de M.

Proposition 54. *On a $\dim(\mathbb{K}[M]) = \deg(\pi_M)$.*

Proposition 55. *$\mathbb{K}[M]$ est un corps si et seulement si π_M est irréductible dans $\mathbb{K}[X]$.*

Lemme 56. [Lemme des noyaux]
Soit $(P_i)_{1\le i\le r}$ une famille de polynômes deux à deux premiers entre eux et $f \in \mathcal{L}(E)$. Alors en posant $P = \prod_{i=1}^r P_k$, on a $\ker(P(f)) = \bigoplus_{i=1}^r \ker(P_i(f))$.
De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Exemple 57. En pratique, on utilise souvent ce lemme avec P annulateur de E. On obtient alors une décomposition de E en sous-espaces stables, car $\ker(Q(f))$ est stable par f pour tout polynôme Q.

Proposition 58. *M est trigonalisable (resp. diagonalisable) si et seulement si π_M est scindé (resp. scindé racines simples).*

Théorème 59. [Décomposition de Dunford]
Supposons M de polynôme caractéristique scindé. Alors il existe un unique couple $(D, N) \in \mathcal{M}_n(\mathbb{K})^2$ tel que D est diagonalisable, N est nilpotente, $M = D + N$ et M commute avec N.
De plus, D et N sont des polynômes en M.

Définition 60. [Endomorphisme semi-simple]
M est dite semi-simple si tout sous-espace vectoriel de $\mathbb{K}^n$ M-stable admet un supplémentaire M-stable.

Théorème 61. *M est semi-simple si et seulement si π_m est sans facteur carré.*

Exemple 62. Si M est nilpotente, alors M est semi-simple si et seulement si $M = 0$.

ANNEXE

Algorithme d'EUCLIDE

Soit A un anneau euclidien. L'algorithme d'EUCLIDE détermine le PGCD de deux éléments :

Entrée : $a, b \in A, b \neq 0$

Sortie : d, u, v tels que $au + bv = d$ et $d = a \wedge b$

Algorithme : $u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1, r_0 = a, r_1 = b, i = 1$

Tant que $r_i \neq 0$:

$r_{i+1} \leftarrow r_{i-1} - q_i r_i$ (division euclidienne de r_{i-1} par r_i)

$u_{i+1} \leftarrow u_{i-1} - q_i u_i$

$v_{i+1} \leftarrow v_{i-1} - q_i v_i$

$i \leftarrow i + 1$

Renvoyer $r_{i-1}, u_{i-1}, v_{i-1}$

SPEECH

On souhaite généraliser les propriétés des anneaux classiques, et notamment de $\mathbb{Z}$ ($\mathbb{Z}$ notamment). *Avant de parler du plan écrire au tableau les implications entre anneaux : euclidien implique principal implique factoriel, puis expliquer que la notion de* PGCD *(et* PPCM*) définie sur un anneau factoriel va profiter des propriétés des autres types d'anneaux.*

Dans la première partie, on s'intéresse à l'arithmétique dans les anneaux, avec les définitions d'idéal, d'idéal principal, d'élément premier, irréductible, de PGCD et de PPCM. On regarde le cas des anneaux principaux avec le théorème de BACHET-BÉZOUT, l'existence d'un PPCM, mais aussi théorème chinois qui permet par exemple de simplifier la résolution de systèmes de congruences (cf troisième partie), mais aussi l'équivalence entre élément premier et irréductible. Enfin les anneaux factoriels permettent des manipulations algébriques plus simples, on a une décomposition en produits irréductibles et théorème de GAUSS.

Ensuite, on s'intéresse aux anneaux euclidiens qui sont des exemples d'anneaux principaux dans lesquels on a un algorithme permettant de trouver facilement le PGCD de deux éléments. Le cas particulier de l'anneau des entiers de GAUSS sera étudié.

La dernière partie s'intéresse aux applications des anneaux principaux, que ce soit pour la résolution d'équations diophantiennes via le théorème chinois dont on connaît la réciproque et qui devient effectif dans un anneau eucliden, mais aussi en algèbre linéaire avec le lemme des noyaux (principalité de $\mathbb{K}[X]$) qui mène par exemple à la décomposition de DUNFORD.

QUESTIONS

Q Résoudre $x^2 + y^2 = z^2$ d'inconnues $x, y, z \in \mathbb{N}$.

R On va regarder cette équation dans $\mathbb{Z}[i]$.
Comme $x, y, z \in \mathbb{N}$, on a $d = \mathrm{PGCD}_{\mathbb{Z}}(x, y, z) = \mathrm{PGCD}_{\mathbb{Z}[i]}(x, y, z)$ et on peut supposer que $d = 1$ quitte à diviser les trois inconnues par d.
Soit $z \in \mathbb{N}$ et $w = x + iy \in \mathbb{Z}[i]$ tels que $N(w) = z^2$. Soit a un diviseur de w et $\overline{w}$. Alors $a \mid 2x = w - \overline{w}$ et $a \mid 2y = (w + \overline{w})/i$.
On peut choisir a irréductible puisque x, y, z sont premiers entre eux, et alors $a \mid 2$ ou $a \mid x$. Si $a \mid 2$, on a $N(a) \in \{1, 2, 4\}$. [...] On finit par montrer que $w \wedge w' = 1$ et on conclut en considérant la décomposition de z en irréductibles de $\mathbb{Z}[i]$ [...].

Q Décomposer $3 + j$ en irréductibles de $\mathbb{Z}[j]$.

R Les irréductibles de $\mathbb{Z}[j]$ sont (aux inversibles $\{\pm 1, \pm j, \pm j^2\}$ près) :
- les $p \in \mathcal{P}$ tels que $p \equiv 2 \mod 3$,
- les $a + bj \in \mathbb{Z}[j]$ tels que $N(a + bj) \in \mathcal{P}$.

On calcule $N(3 + j) = 7 \in \mathcal{P}$ donc $3 + j$ est irréductible.

Q Soit A principal. Montrer qu'il existe $v : A \longrightarrow \mathbb{N}$ telle que
- $v(a) = 0 \iff a = 0$,
- $v(ab) \geq v(a)$ pour $a, b \in A, b \neq 0$,
- si $v(a) \geq v(b)$ pour $a, b \in A, b \neq 0$, alors $b \mid a$ ou $\exists q, d \in A \,|\, 0 < v(ad - bq) < v(b)$.

R On prend pour $v(a)$ le nombre de facteurs irréductibles comptés avec leur multiplicité. On démontre le dernier point par l'absurde en utilisant l'identité de BÉZOUT.

Q L'ensemble des fonctions holomorphes sur un ouvert U est un anneau satisfaisant une relation de BÉZOUT entre ses éléments. Montrer cependant qu'il n'est pas principal.

R On montre en fait qu'il n'est pas factoriel. On vérifie que si f holomorphe est irréductible, alors nécessairement f n'a qu'un seul 0. On en déduit que toute fonction possédant une infinité de 0 n'admet pas d'écriture finie en produit d'irréductibles (par exemple $\sin$).

Q Trouver les nombres premiers s'écrivant sous la forme $p = a^2 + 2b^2$.

R $a^2 + 2b^2 = (a + i\sqrt{2}b)(a - i\sqrt{2}b)$. On se place dans $A = \mathbb{Z}[i\sqrt{2}]$. Le stathme $N = |.|^2$ montre que A est principal. Puis on procède similairement au théorème des deux carrés.

Q $\mathbb{C}[X, Y]/(Y^2 - X^3)$ et $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ sont-ils principaux ?

R Seul le second l'est !

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Com98] F. COMBES : *Algèbre et géométrie*. Bréal, 1998.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[MM16] R. MANSUY et R. MNEIMNÉ : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

123 CORPS FINIS. APPLICATIONS.

Soit $\mathcal{P}$ l'ensemble des nombres premiers. Les corps considérés seront supposés commutatifs.

I. Notion de corps fini

[Per96, §3.2, p72–76] [Rom17, Ch13, p415]

I. A. Vocabulaire général sur les corps

Cloture algébrique unique à isomorphisme près (admis).
Corps de rupture / de décomposition.
Théorème de WEDDERBURN

I. B. Premiers résultats

DÉFINITION 1. Un corps fini est un corps de cardinal fini.

PROPOSITION 2. *Pour $p \in \mathcal{P}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps fini à p éléments.*

PROPOSITION 3. *Soit $\mathbb{K}$ un corps. L'application $\mathbb{Z} \longrightarrow \mathbb{K}, m \longmapsto m1_K$ est un morphisme d'anneaux de noyau $n\mathbb{Z}$ pour un $n \in \mathbb{N}$.*

DÉFINITION 4. L'image de cette application est un sous-corps de $\mathbb{K}$ appelé sous-corps premier. n est appelé caractéristique de $\mathbb{K}$, noté $\mathrm{car}(\mathbb{K})$.

PROPOSITION 5. *Si $\mathbb{K}$ est fini, on a $\mathrm{car}(\mathbb{K}) \in \mathcal{P}$.*

APPLICATION 6. Le sous-corps premier de $\mathbb{K}$ est alors isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Pour $p \in \mathcal{P}$, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

COROLLAIRE 7. *Si $\mathbb{K}$ est un corps fini de caractéristique p, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel où $p = \mathrm{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(\mathbb{K})$.*

APPLICATION 8. Il n'existe par de corps à 6 éléments.

I. C. Existence et unicité

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. Soit $q = p^n$.

DÉFINITION 9. [MORPHISME DE FROBENIUS]
Soit $\mathbb{K}$ un corps de caractéristique p. $\mathrm{Frob} : \mathbb{K} \longrightarrow \mathbb{K}, x \longmapsto x^p$ est un morphisme de corps appelé morphisme de FROBENIUS.

PROPOSITION 10. *Frob est injectif et si $\mathbb{K}$ est fini, c'est un automorphisme.*

PROPOSITION 11. *Pour $\mathbb{K} = \mathbb{F}_p$, on a $\mathrm{Frob} = \mathrm{Id}$.*

PROPOSITION 12. *Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Alors l'ensemble des racines de $X^{p^n} - X$ dans $\overline{\mathbb{F}_p}$ est un sous-corps de $\overline{\mathbb{F}_p}$ à $q = p^n$ éléments, contenant $\mathbb{F}_p$.*

COROLLAIRE 13. *Il existe un corps fini à q éléments, unique à isomorphisme près : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.*

II. Eléments de structure

[Per96, §III.2, p73]

II. A. Structure d'un corps fini

$\mathbb{F}_q$ est un $\mathbb{F}_p$-espace vectoriel de dimension n, donc isomorphe à $\mathbb{F}_p^n$
$\mathbb{F}_q^\times = \mathbb{F}_q^*$ est cyclique, donc isomorphe à $(\mathbb{Z}/(q-1)\mathbb{Z}, +)$
Racine primitive, nombre de racines primitives
Élement primitif : une racine primitive est un élément primitif

II. B. Inclusion entre corps finis

PROPOSITION 14. *Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ pour $d \mid n$.*

THÉORÈME 15. [THÉORÈME DE LA BASE TÉLESCOPIQUE]
Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.
En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

APPLICATION 16. On a alors $[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] = \frac{n}{d}$.

EXEMPLE 17. Schéma des inclusions des sous-corps de $\mathbb{F}_{2^{20}}$.

II. C. Structure du groupe des isomorphismes

[Rom17, §13.4, p426]

$\mathrm{Aut}(\mathbb{F}_q)$ est un groupe de neutre id
Si $f \in \mathrm{Aut}(\mathbb{F}_q)$, alors $\mathbb{F}_p \subset \{x \in \mathbb{F}_q \mid f(x) = x\}$
$\mathrm{Aut}(\mathbb{F}_q)$ est cyclique d'ordre n, engendré par Frob

III. Applications

III. A. Résolution d'équations de degré 2

[Rom17, §13.6-7, p429-435] [Per96, §III.2, p72-76]

Soit $p \in \mathcal{P}$ et $q = p^n$ où $n \in \mathbb{N}^*$. On note $\mathbb{F}_q^2 = \left\{x^2 \mid x \in \mathbb{F}_q\right\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 18. *Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon, on a $\left|\mathbb{F}_q^2\right| = \frac{q+1}{2}$.*

Application 19. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p^2$.

On suppose dans la suite p impair.

Lemme 20. *On a $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.*

Exemple 21. -1 est un carré modulo q si et seulement si $q \mid 1 \mod 4$.

Exemple 22. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 23. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 24. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Proposition 25. *$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ pour tout $a, k \in \mathbb{Z}$. On peut donc définir $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. C'est l'unique morphisme de groupes non trivial de $(\mathbb{F}_p^*, \times)$ vers $(\{\pm 1\}, \times)$.*

Remarque 26. Le nombre de solutions de $x^2 = a$ pour $a \in \mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Théorème 27. [Loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 28. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n :

Exemple 29. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

III. B. Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p

[Per96, §3.3-3.4, p76-85]

Proposition 30. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et irréductible dans $\mathbb{Q}[X]$.*

Proposition 31. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^r a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. Si $p \nmid a_r$, $\forall i < r, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 32. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 33. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^r a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 34. $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme $X^p - X - 1$ pour tout $p \in \mathcal{P}$.

Définition 35. [Polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times}(X - \zeta)$.

Proposition 36. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 37. [Irréductibilité de Φ_n] *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

Liens entre irréductibilité et degré des extensions [Per96, p78-79]

SPEECH

Dans la première partie, on essaie de comprendre ce qu'est un corps fini. Les outils principaux étant les notions de caractéristique et de sous-corps premier, le morphisme de FROBENIUS. Cela va mener à l' unicité du corps de cardinal p^d à isomorphisme près.
Ensuite, on regarde la structure de ces corps finis, avec notamment les racines primitives et les éléments primitifs. Le problème est qu'il n'y a pas de méthode générale pour exhiber une racine primitive. On s'intéresse aux sous-corps d'un corps fini et aux degrés des différentes extensions et on étudie également le lien entre les automorphismes du corps et le morphisme de FROBENIUS.
La dernière partie s'intéresse aux applications des corps finis, avec la résolution d'équations de degré 2 dans ces corps (loi de réciprocité quadratique), et les critères d'irréductibilité de polynômes.

COMMENTAIRES

Voir aussi le [Dem09].

BIBLIOGRAPHIE

[Dem09] M. DEMASURE : *Cours d'algèbre*. Cassini, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

125 EXTENSIONS DE CORPS. EXEMPLES ET APPLICATIONS.

I. Généralités sur les extensions de corps

[Per96, §III, p65] [Cog00, §2.1, p60–62]

On ne considère que des corps commutatifs.

Définition 1. [Extension de corps, degré]
Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$. $\mathbb{L}$ est alors un $\mathbb{K}$-e.v.. Lorsque $\dim(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est finie.

Exemple 2. $\mathbb{R} \subset \mathbb{C}, \mathbb{Q} \subset \mathbb{Q}(i)$.

Une extension de corps est un espace vectoriel sur le corps de base. On note $[\mathbb{L} : \mathbb{K}]$ le degré de cet espace vectoriel (éventuellement infini). Exemples

Théorème 3. [Théorème de la base télescopique]
Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$. En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Sous-corps contenant une partie. Exemple

Définition 4. [Élément algébrique, transcendant]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\phi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\phi_{|\mathbb{K}} = \mathrm{id}$ et $\phi(T) = \alpha$.
Si ϕ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\phi) = (P)$. P est appelé polynôme minimal de α.

Exemple 5. $\sqrt{2}, i$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants sur $\mathbb{Q}$.

Théorème 6. [Caractérisation d'un algébrique]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty$$

Théorème 7. *Pour tout entier $n \in \mathbb{N}$ et toute famille $p_1, \dots, p_n$ d'entiers supérieurs ou égaux à 2, tous sans facteur carré, et premiers deux à deux, on a :*

$$[\mathbb{Q}[\{\sqrt{p_i}\}_{1\leq i\leq n}] : \mathbb{Q}] = 2^n$$

Dans le cas transcendant, isomorphisme $\mathbb{K}[\alpha] \simeq \mathbb{K}[X]$ et $\mathbb{K}(\alpha) \simeq \mathbb{K}(X)$
Extension algébrique
Lorsque $[\mathbb{L} : \mathbb{K}] < +\infty$, l'extension est algébrique

II. Extensions de corps et polynômes

[Per96, §III.1.c, p70]

II. A. Corps de rupture

Corps de rupture d'un polynôme irréductible
Il existe un unique corps de rupture à isomorphisme près.
Exemple de $\mathbb{C}$, de $\mathbb{Q}[\sqrt{2}]$
Degré du corps de rupture

II. B. Corps de décomposition

Corps de décomposition
Existence et unicité à isomorphisme près
Exemple de $\mathbb{Q}(i, \sqrt{2})$
Théorème de l'élément primitif

II. C. Clôture algébrique

Corps algébriquement clos. Formulations équivalentes
Théorème de D'Alembert-Gauss [Rom17, p378]
Application : toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable
Polynôme ne s'annulant pas sur un corps fini $\to$ tout corps fini n'est pas algébriquement clos
Clôture algébrique
Tout corps admet une clôture algébrique unique à isomorphisme près

III. Applications

III. A. Irréductibilité de polynômes et réduction

[Per96, §3.3-3.4, p76–85] [Rom17, §12.11.4, p381–383]

Soit A un anneau factoriel. On note $K = \mathrm{Frac}(A)$

Proposition 8. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $A[X]$ si et seulement si il est de contenu 1 et irréductible dans $K[X]$.*

Proposition 9. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 10. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 11. *Soit I un idéal premier de A et $B = A/I$. Soit $P = \sum_{i=0}^{r} a_i X^i \in A[X]$ et $\overline{P}$ la réduction de P modulo I. Si $\overline{a_n}$ dans B, et si $\overline{P}$ est irréductible sur B ou $\mathrm{Frac}(B)$, alors P est irréductible sur K.*

Que l'on reformule dans le cas $A = \mathbb{Z}$, $I = (p)$, $B = \mathbb{F}_p$:

Proposition 12. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 13. $X^3+462X^2+2433X-67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme X^p-X-1 pour tout $p \in \mathcal{P}$.

Liens entre irréductibilité et degré des extensions [Per96, p78–79]

III. B. Cyclotomie

[Per96, §3.4, p80] [Rom17, §12.11.5, p383]

Soit $n \in \mathbb{N}^*$.

Définition 14. [polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

Proposition 15.
(i) Φ_n *est unitaire de degré* $\varphi(n) = \mathrm{card}(\{k \in [1,n] \mid k \wedge n = 1\})$.
(ii) $X^n - 1 = \prod_{d|n} \Phi_d$. *En particulier, si n est premier :* $\Phi_n = X^n - 1$.

Corollaire 16.
- *On en déduit la fameuse formule* $\phi(n) = \sum_{d \mid n} \phi(d)$.
- *Pour* $n \geq 2$, $\sum_{\omega \in \mathbb{U}_n} \omega = 0$.

Proposition 17. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 18. Φ_n *est irréductible sur* $\mathbb{Z}$ *et donc sur* $\mathbb{Q}$.

Corollaire 19. *On a* $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.

ANNEXE

Schémas d'extensions de corps avec leur degré.

BIBLIOGRAPHIE

[Cog00] M. Cognet : *Algèbre linéaire*. Bréal, 2000.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

126 EXEMPLES D'ÉQUATIONS EN ARITHMÉTIQUE.

Définition d'une équation diophantienne [Com98, §12.7, p273]

I. Équations diophantiennes linéaires [Rom17, §10.4, p288]

Cas de l'équation $ax = b$
PGCD d'une famille d'éléments, algorithme d'Euclide, théorème de Bachet-Bézout
Lemmes d'Euclide, de Gauss sur la divisibilité d'un produit
Équation $ax + ny = c$, réécrite $ax \equiv c \mod n$: ensemble des solutions, existence ssi $a \wedge n \mid b$, dans ce cas une solution particulière est donnée par l'identité de Bézout, exemples
Soient $n, m \geq 2$.

Théorème 1. *Soit $a \in \mathbb{N}^*, b \in \mathbb{Z}$. On note $\delta = a \wedge n$ et on écrit $a = \delta a'$ et $n = \delta n'$. L'équation $ax \equiv b \mod n$ a des solutions entières si et seulement si $\delta \mid b$ et dans ce cas, si $b = \delta b'$, les solutions sont les $b'x'_0 + kn'$ avec $k \in \mathbb{Z}$ et x'_0 est une solution particulière de $a'x \equiv 1 \mod n'$.*

Généralisation à $\sum a_i x_i = b$: calcul par récurrence d'une solution
Équivalent du nombre de solutions S_n de $\sum \alpha_i n_i = n$ [Gou08, §4.4, p249]

II. Systèmes de congruence [Rom17, §10.3-4, p283–290]

Théorème 2. [Théorème des restes chinois]
Soient $n_1, \dots, n_r \in \mathbb{N}$ des entiers distincts. Ces entiers sont premiers entre eux si et seulement si $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^r \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes, où $n = \prod_{j=1}^r n_j$. Plus précisément, l'application $\phi : \overline{k}_n \longmapsto (\overline{k}^{n_i})_{1 \leq i \leq r}$ est un isomorphisme d'anneaux.

Exemple 3. $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Théorème 4. *L'isomorphisme inverse est donné par $(\overline{k_i}^{n_i})_{1 \leq i \leq r} \longmapsto \overline{\sum_{j=1}^r k_j u_j \frac{n}{n_j}}^n$ où l'on a choisit $(u_j)_{1 \leq j \leq r}$ tels que $\sum_{j=1}^r u_j \frac{n}{n_j} = 1$.*

Soient $n, m \geq 2$.

Application 5. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations $\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$ d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors

- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k \in \mathbb{Z}}$.

Exemple 6. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k \in \mathbb{Z}}$.

III. Nombres premiers et équations diophantiennes

Théorème de Dirichlet (faible) : existence d'un nombre infini de nombres premiers d'une certaine forme

III. A. Réduction [Rom17, §13.6-7, p429–436] [Per96, §3.2, p72–76]

Soit $p \in \mathcal{P}$. On peut regarder l'équation modulo p.
S'il n'y a pas de solution dans $\mathbb{Z}/p\mathbb{Z}$, il n'y en a pas non plus sur $\mathbb{Z}$.
Soit $p \in \mathcal{P}$. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 7. *Si $p = 2$, alors $\mathbb{F}_p^2 = \mathbb{F}_p$. Sinon, on a $\left|\mathbb{F}_p^2\right| = \frac{p+1}{2}$.*

On suppose dans la suite p impair.

Lemme 8. *On a $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.*

Exemple 9. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 10. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 11. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Exemple 12. -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$. Donc $x^2 + 1 = p$ n'a pas de solution pour $p \equiv 3 \mod 4$.

Proposition 13. *$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ pour tout $a, k \in \mathbb{Z}$. On peut donc définir $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. C'est l'unique morphisme de groupes non trivial de $(\mathbb{F}_p^*, \times)$ vers $(\{\pm 1\}, \times)$.*

Application 14. Pour $a \in \mathbb{Z}$, le nombre de solutions de $x^2 = \overline{a}$ dans $\mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Application 15. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

Exemple : $x^2 + y^2 = pz^2$ selon $p \mod 4$ [Com98, §12.7, p275]

Théorème 16. [Loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 17. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n.

Exemple 18. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

$x^2 + py = r$ avec p premier impair er $p \nmid r$, alors on a une solution si et seulement si $\left(\frac{q}{p}\right) = 1$ et dans ce cas on a une paramétrisation de l'ensemble des solutions

IV. Équations diophantiennes non linéaires

IV. A. Exemples de résolutions

[Com98, §12.7, p273] [FGN07, §4.39, p167]

Solutions de $x^2 + y^2 = z^2$
Méthode de descente infinie, exemple de $x^4 + y^4 = z^2$ ou z^4
Autre exemple [FGN07, §4.38, p165]

Théorème 19. [Théorème de Sophie Germain]
Soit p un nombre premier impair tel que $q = 2p + 1$ est premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $p \nmid xyz$ et $x^p + y^p + q^p = 0$.

Théorème de Fermat

IV. B. L'anneau des entiers de Gauss

[Per96, §2.3, p50] [Rom17, §9.4.3, p263]

Définition 20. On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.

Proposition 21. *Muni du stathme $N(a + ib) = a^2 + b^2$, $\mathbb{Z}[i]$ est euclidien.*

Proposition 22. $\mathbb{Z}[i]^\times = N^{-1}(\{1\}) = \{\pm 1, \pm i\}$.

On définit $\Sigma = \left\{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N} \mid n = a^2 + b^2\right\}$. On cherche à quelle(s) condition(s) $n \in \Sigma$.

Exemple 23. $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$ mais pas $3, 6, 7, 11$.

Lemme 24. *Σ est stable par produit.*

Lemme 25. *Si $p \in \mathcal{P}$, alors $p \in \Sigma \iff p \equiv 1, 2 \mod 4$.*

Théorème 26. [Théorème des deux carrés de Fermat]
$n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ tel que $p \mid n$ et $p \mid 3 \mod 4$, alors $2 \mid v_p(n)$.

Proposition 27. *Les irréductibles de $\mathbb{Z}[i]$ sont :*
- *les $p \in \mathcal{P}$ tels que $p \equiv 3 \mod 4$,*
- *les $a + ib$ tels que $a^2 + b^2 \in \mathcal{P}$.*

Généralisation : anneaux quadratiques [Duv07, Ch5, p47]
Ou encore théorème des quatre carrés de Lagrange : tout nombre entier est somme de 4 carrés.
[Duv07, §6.6, p73] [FGN07, §4.36, p162]

QUESTIONS

Q On s'intéresse à $y^2 = x^3 - x$ et au nombre de points de cette courbe sur $\mathbb{F}_p$. On note N_p le nombre de solutions. Montrer que $N_p = p + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3-x}{p}\right)$. Calculer N_7. Montrer en fait que pour $p \equiv 3 \mod 4$, on a $N_p = p$.

R On utilise le fait que $\mathrm{card}(\{y^2 = a \,|\, y \in \mathbb{F}_p\}) = 1 + \left(\frac{a}{p}\right)$. On a :

$$N_p = \sum_x \mathrm{card}(\{y^2 = x^3 - x\} \mid y \in \mathbb{F}_p) = \sum_x 1 + \left(\frac{x^3-x}{p}\right) = p + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3-x}{p}\right)$$

Pour calculer N_7, on calcule les $\left(\frac{x^3-x}{7}\right)$ pour $x \in \mathbb{F}_7$, on obtient dans l'ordre pour $x = 0, \dots, 6$: $0, 1, -1, -1, 1, 1, -1$, d'où $N_7 = 7$.
Si $p \equiv 3 \mod 4$, on a pour f impaire : $\left(\frac{f(-x)}{p}\right) = \left(\frac{-f(x)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f}{p}\right) = -\left(\frac{f(x)}{p}\right)$ ce qui assure que la somme est nulle dans la formule de N_p, et ainsi $N_p = p$.

Q Que dire de $f : x \longrightarrow \frac{1+x}{1-x}$ pour $x \in \mathbb{F}_p \setminus \{1\}$.

R L'application est-elle injective ? si $f(x) = f(y)$, on a $(1+x)(1-y) = (1-x)(1+y)$ donc $2x = 2y$ puis $x = y$ si $p \geq 3$. Supposons $p \geq 3$. L'application est injective et son image est $\mathbb{F}_p$ privée d'un point : -1 puisque $1 + x = x - 1$ n'a pas de solution.

Q En déduire le nombre de solutions de $x^2 + y^2 = 1$?

R Écrivons $x^2 = 1 - y^2 = \frac{1+y}{1-y}(1-y)^2$. Donc :

$$N_p = p + \sum_y \left(\frac{1-y^2}{p}\right) = p + 0 + \sum_{y\neq 1} \left(\frac{\frac{1+y}{1-y}}{p}\right) = p + \sum_{z\neq -1} \left(\frac{z}{p}\right) = p - \left(\frac{-1}{p}\right)$$

BIBLIOGRAPHIE

[Com98] F. COMBES : *Algèbre et géométrie*. Bréal, 1998.

[Duv07] D. DUVERNEY : *Théorie des nombres*. Dunod, 2007.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

141 POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS.

Soit $\mathbb{K}$ un corps et A un anneau intègre, tous deux commutatifs.

I. Polynômes irréductibles [Per96, §II.3/III.3, p45–53/76] [Rom17, §12.8, p368]

I. A. Irréductibilité

Définition de l'irréductibilité de polynômes
Dans le cas d'un corps : simplification de l'irréductibilité, cas des polynômes de degré 1, exemples, lien entre réductibilité et existence de racines pour $\deg(P) \leq 3$
Lemme d'Euclide pour $A[X]$ principal/factoriel, exemple de $(X^2+1)^2$ réductible sur $\mathbb{R}[X]$ bien qu'il n'admette pas de racine
Décomposition en produit d'irréductibles
Il y a une infinité de polynômes irréductibles

I. B. Propriétés de $A[X]$ [Per96, §II.4, p50]

$A[X]$ principal correspond à A est un corps
A factoriel implique $A[X]$ factoriel
Notion de contenu, polynôme primitif, lemme de Gauss
Dans un corps : P irréductible si et seulement si (P) maximal

I. C. Critères d'irréductibilité [FGN07, §5.16, p188–190]

On suppose que A est un anneau factoriel
Lien entre les irréductibles de A et les irréductibles de $\mathrm{Frac}(A)$

Proposition 1. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 2. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 3. *Soit I un idéal premier de A et $B = A/I$. Soit $P = \sum_{i=0}^{r} a_i X^i \in A[X]$ et $\overline{P}$ la réduction de P modulo I. Si $\overline{a_n}$ dans B, et si $\overline{P}$ est irréductible sur B ou $\mathrm{Frac}(B)$, alors P est irréductible sur K.*

Que l'on reformule dans le cas $A = \mathbb{Z}$, $I = (p)$, $B = \mathbb{F}_p$:

Proposition 4. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 5. $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme $X^p - X - 1$ pour tout $p \in \mathcal{P}$.

Cependant la réciproque est fausse, mais dans certains cas particuliers on peut s'en tirer en jonglant entre les corps utilisés

II. Extensions de corps et polynômes

II. A. Extensions de corps [Per96, §III.1, p65–66]

On ne considère que des corps commutatifs.

Définition 6. [Extension de corps, degré]
Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$. $\mathbb{L}$ est alors un $\mathbb{K}$-e.v.. Lorsque $\dim(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est finie.

Exemple 7. $\mathbb{R} \subset \mathbb{C}, \mathbb{Q} \subset \mathbb{Q}(i)$.

Degré d'une extension, exemples

Théorème 8. [Théorème de la base télescopique]
Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$. En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 9. [Élément algébrique, transcendant]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\phi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\phi_{|\mathbb{K}} = \mathrm{id}$ et $\phi(T) = \alpha$.
Si ϕ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\phi) = (P)$. P est appelé polynôme minimal de α.

Exemple 10. $\sqrt{2}, i$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants sur $\mathbb{Q}$.

Théorème 11. [Caractérisation d'un algébrique]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty$$

Liens entre irréductibilité et degré des extensions [Per96, §III.3, p77–79]

II. B. Corps de rupture et de décomposition [Per96, §III.1.c, p70]

Corps de rupture d'un polynôme irréductible, existence et unicité à isomorphisme près.
Exemple de $\mathbb{C}$, de $\mathbb{Q}[\sqrt{2}]$
Degré du corps de rupture
Corps de décomposition, existence et unicité à isomorphisme près
Exemple de $\mathbb{Q}(i, \sqrt{2})$
Théorème de l'élément primitif

II. C. Cloture algébrique [Per96, §III.1.c, p70]

Extension algébrique, corps algébriquement clos, formulations équivalentes
Théorème de D'ALEMBERT-GAUSS [Rom17, p378]
Application : toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable
Polynôme ne s'annulant pas sur un corps fini $\to$ tout corps fini n'est pas algébriquement clos
Clôture algébrique, tout corps admet une clôture algébrique unique à isomorphisme près

III. Polynômes cyclotomiques [Per96, §3.4, p80] [Rom17, §12.11.5, p383]

Soit $n \in \mathbb{N}^*$.

DÉFINITION 12. [POLYNÔMES CYCLOTOMIQUES]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

PROPOSITION 13.
(i) Φ_n *est unitaire de degré* $\varphi(n) = \mathrm{card}(\{k \in [1, n] \mid k \wedge n = 1\})$.
(ii) $X^n - 1 = \prod_{d|n} \Phi_d$. *En particulier, si* n *est premier :* $\Phi_n = X^n - 1$.

COROLLAIRE 14.
- *On en déduit la fameuse formule* $\phi(n) = \sum_{d \mid n} \phi(d)$.
- *Pour* $n \geq 2$, $\sum_{\omega \in \mathbb{U}_n} \omega = 0$.

PROPOSITION 15. $\Phi_n \in \mathbb{Z}[X]$.

THÉORÈME 16. Φ_n *est irréductible sur* $\mathbb{Z}$ *et donc sur* $\mathbb{Q}$.

COROLLAIRE 17. *On a* $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.

APPLICATION 18. Théorème de DIRICHLET faible

COMMENTAIRES

Autres références : [BMP05, Gou09].

QUESTIONS

Q $X^4 + 1$ est-il irréductible ?
R Oui, il n'a pas de racine et on peut appliquer le critère d'EISENSTEIN à $(X + 1)^4 + 1$ avec $p = 2$.
Q $X^4 + 1$ est-il irréductible sur $\mathbb{F}_p$?
R Sur $\mathbb{F}_{p^2}$ cyclique, $X^8 - 1 = (X^4 + 1)(X^4 - 1)$ et $8 \mid (p^2 - 1) = (p - 1)(p + 1)$.
Q Peut-on construire une famille de polynômes $(X^n + a)_n$ irréductibles sur $\mathbb{Q}$ pour tout n ?

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

142 PGCD ET PPCM, ALGORITHMES DE CALCUL. APPLICATIONS.

Soit A un anneau unitaire commutatif intègre et $\mathbb{K}$ un corps.

I. Notion de PGCD et de PPCM sur un anneau factoriel

I. A. Généralités

[Per96, §II.3, p45] [Rom17, Ch7, p205]

Définition 1. [DIVISIBILITÉ]
Pour $a, b \in A$, on dit que a divise b et on note $a \mid b$ si $\exists c \in A \mid b = ac$, ou encore $(b) \subset (a)$.

Définition 2. [ÉLÉMENTS ASSOCIÉS]
$a, b \in A$ sont dits associés si $a \mid b$ et $b \mid a$ (ou s'il existe $u \in A^\times$ tel que $a = ub$).

Remarque 3. C'est une relation d'équivalence (notée $\sim$). Deux éléments associés sont indiscernables du point de vue de la divisibilité.

Définition 4. [IRRÉDUCTIBLE] $a \in A$ non inversible et non nul est dit irréductible si pour tout $b, c \in A$ tels que $a = bc$, alors $b \in A^\times$ ou $c \in A^\times$.

Exemple 5. Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.

Définition 6. [PGCD, PPCM] Soient $a, b \in A$. On dit que
- $d \in A$ est un PGCD de a et b et on note $d = a \wedge b$ si $\forall c \in A, c \mid a$ et $c \mid b \implies c \mid d$,
- $m \in A$ est un PPCM de a et b et on note $m = a \vee b$ si $\forall c \in A, a \mid c$ et $b \mid c \implies m \mid c$.

a et b sont dits premiers entre eux si $a \wedge b = 1$.

Remarque 7. 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 8. *Deux PGCD (resp. PPCM) de $a, b \in A$ sont associés.*

Anneau factoriel, propriété d'existence et d'unicité. Dans la suite A est factoriel.
Écriture en produit d'irréductibles, valuation p-adique

Exemple 9. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont factoriels.

Existence de PGCD, PPCM, expression en fonction des décompositions en produit d'irréductibles, expression en terme d'idéaux $\rightarrow$ ok pour le PPCM mais pas pour le PGCD (l'anneau n'est pas nécessairement principal !)
Application pour le PPCM : dans un groupe, il existe un élément d'ordre l'exposant du groupe
Lemmes de GAUSS

Exemples dans $\mathbb{Z}$, dans les anneaux de polynômes.
On a $(a \wedge b)(a \vee b) = ab$ et $a \wedge (b \vee a) = a = a \vee (b \wedge a)$

I. B. Contenu d'un polynôme

[FGN07, §5.16, p188–190] [Per96, p51]

Contenu, lemme de GAUSS

Proposition 10. [CRITÈRE D'EISENSTEIN]
Soit A un anneau factoriel. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Théorème de GAUSS : $A[X]$ factoriel si A l'est

II. Vers le théorème de BÉZOUT : PGCD sur un anneau principal

[Rom17, §8.2, p237] [Per96, §II.3.e, p49]

Anneau principal, exemple de $\mathbb{Z}$, de $\mathbb{K}[X]$
$\mathbb{K}[X, Y]$ est factoriel non principal
Si A est principal, on a bien $(a \wedge b) = (a) + (b)$ (théorème de BÉZOUT). En particulier condition pour que a et b soient premiers entre eux ! Exemples
Généralisation à une famille d'éléments
Application : lemme des noyaux

III. Algorithmes de calcul dans les anneaux euclidiens

III. A. Obtention du PGCD

[Rom17, §9.2, p260]

Anneau euclidien, stathme, exemple de $\mathbb{K}[X]$ avec le degré
Euclidien implique principal implique factoriel
Exemple d'anneau principal non euclidien
Algorithme d'EUCLIDE : on utilise la division euclidienne en s'appuyant sur le fait que si $a = bq + r$ avec $r \neq 0$ alors $a \wedge b = b \wedge r$
Exemple d'application de l'algorithme

III. B. Recherche d'une relation de BÉZOUT

Algorithme d'EUCLIDE étendu : en remontant dans l'algorithme, on obtient une relation de BÉZOUT.
Exemple avec le PGCD de polynômes

IV. Applications aux équations en arithmétique

IV. A. Équations diophantiennes

[Rom17, §10.4, p288] [FGN07, §4.39, p167]

Définition d'une équation diophantienne [Com98, §12.7, p273]
Cas de l'équation $ax = b$
Équation $ax + ny = c$, réécrite $ax \equiv c \mod n$: ensemble des solutions, existence si et seulement si $a \wedge n \mid b$, dans ce cas une solution particulière est donnée par l'identité de Bézout, exemples
Soient $n, m \geq 2$.

Théorème 11. *Soit $a \in \mathbb{N}^*, b \in \mathbb{Z}$. On note $\delta = a \wedge n$ et on écrit $a = \delta a'$ et $n = \delta n'$. L'équation $ax \equiv b \mod n$ a des solutions entières si et seulement si $\delta \mid b$ et dans ce cas, si $b = \delta b'$, les solutions sont les $b'x'_0 + kn'$ avec $k \in \mathbb{Z}$ et x'_0 est une solution particulière de $a'x \equiv 1 \mod n'$.*

Généralisation à $\sum a_i x_i = b$: calcul par récurrence d'une solution

Théorème 12. [Théorème de Sophie Germain]
Soit p un nombre premier impair tel que $q = 2p + 1$ est premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $p \nmid xyz$ et $x^p + y^p + q^p = 0$.

IV. B. Systèmes de congruence

[Rom17, §10.3-4, p283–290]

Théorème 13. [Théorème des restes chinois]
Soient $n_1, \dots, n_r \in \mathbb{N}$ des entiers distincts. Ces entiers sont premiers entre eux si et seulement si $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^r \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes, où $n = \prod_{j=1}^r n_j$. Plus précisément, l'application $\phi : \overline{k}_n \longmapsto (\overline{k}^{n_i})_{1 \leq i \leq r}$ est un isomorphisme d'anneaux.

Exemple 14. $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Théorème 15. *L'isomorphisme inverse est donné par $(\overline{k_i}^{n_i})_{1 \leq i \leq r} \longmapsto \overline{\sum_{j=1}^r k_j u_j \frac{n}{n_j}}^n$ où l'on a choisit $(u_j)_{1 \leq j \leq r}$ tels que $\sum_{j=1}^r u_j \frac{n}{n_j} = 1$.*

Soient $n, m \geq 2$.

Application 16. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations $\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$ d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors

- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k \in \mathbb{Z}}$.

Exemple 17. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k \in \mathbb{Z}}$.

ANNEXE

Algorithme d'EUCLIDE

Soit A un anneau euclidien. L'algorithme d'EUCLIDE détermine le PGCD de deux éléments :

Entrée : $a, b \in A, b \neq 0$

Sortie : d, u, v tels que $au + bv = d$ et $d = a \wedge b$

Algorithme : $u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1, r_0 = a, r_1 = b, i = 1$

Tant que $r_i \neq 0$:

$r_{i+1} \leftarrow r_{i-1} - q_i r_i$ (division euclidienne de r_{i-1} par r_i)

$u_{i+1} \leftarrow u_{i-1} - q_i u_i$

$v_{i+1} \leftarrow v_{i-1} - q_i v_i$

$i \leftarrow i + 1$

Renvoyer $r_{i-1}, u_{i-1}, v_{i-1}$

Algorithme d'EUCLIDE étendu

SPEECH

L'objectif est de généraliser les notions de PGCD et de PPCM connue sur $\mathbb{N}$ à des anneaux.

QUESTIONS

Q En quoi le lemme des noyaux est une application du théorème de BÉZOUT ?

Q Dans le cas des anneaux euclidiens, retrouve-t-on exactement les mêmes résultats que dans $\mathbb{Z}$?

R Dans $\mathbb{Z}$ on a unicité de la division euclidienne. Dans A euclidien, il faudrait imposer une condition supplémentaire pour l'avoir.

Q Quelle est la complexité de l'algorithme d'EUCLIDE ?

R $\mathcal{O}(\ln(a)/\ln(b))$.

Q Connaissez-vous un algorithme plus simple que l'algorithme d'EUCLIDE ?

R On a $a \wedge b = (a - b) \wedge b$ pour $a, b \in \mathbb{N}$.
Tant que a sont b sont non nuls, on remplace le $\max(a, b)$ par $\max(a, b) - \min(a, b)$.
Une autre possibilité récursive :
- si a et b sont pairs, $\mathrm{PGCD}(a, b) = 2\,\mathrm{PGCD}(a/2, b/2)$,
- si a est pair et b impair, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a/2, b)$,
- si les deux sont impairs, on regarde s'ils sont divisibles par 3 …

Q Montrer que $\mathbb{Z}[\sqrt{5}] \simeq \mathbb{Z}[X]/(X^2 - 5)$. Calculer $d = 9 \wedge 3(2 + i\sqrt{5})$.

R $z = a + \sqrt{5}b$, $N(z) = a^2 + 5b^2$. z inversible correspond à $N(z) = 1$ ou encore $z \in \{\pm 1\}$.
3 est un diviseur commun donc $3 \mid d$. On a $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$
Si $zz' = 2 + i\sqrt{5}$, on a $N(z)N(z') = 9$

Q Que dire des orbites de l'action de $\mathrm{GL}_2(\mathbb{Z})$ sur $\mathbb{Z}^2$?

R $(a\,b) \sim (c\,d)$ si $a \wedge b = c \wedge d = e$ (si $e = au + bv$: $\begin{pmatrix} u & v \\ -b/e & a/e \end{pmatrix}\begin{pmatrix} a \\ -b/e \end{pmatrix} = \begin{pmatrix} e \\ b \end{pmatrix}$).
Réciproquement, deux vecteurs dans la même orbite ont même PGCD par transitivité.

Q Et pour l'action de $\mathrm{GL}_n(\mathbb{Z})$ sur $\mathbb{Z}^n$?

R On espère le même résultat. Par le théorème BÉZOUT, on a $\sum_i a_i u_i = d$ mais on ne va pas pouvoir trouver explicitement la matrice correspondante.
En revanche, si $V = \mathbb{Z}(u_1, \ldots, u_n)^\top$ et $W = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid \sum a_i x_i = 0\}$, alors $W \cap V = 0$ et donc $W \simeq \mathbb{Z}^{n-1}$ est un sous-groupe d'un groupe abélien libre donc est un groupe abélien libre. On a donc la matrice qu'il nous faut via cet isomorphisme.

BIBLIOGRAPHIE

[Com98] F. COMBES : *Algèbre et géométrie*. Bréal, 1998.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

144 RACINES D'UN POLYNÔME. FONCTIONS SYMÉTRIQUES ÉLÉMENTAIRES. EXEMPLES ET APPLICATIONS.

Soit $\mathbb{K}$ un corps commutatif. [Rom17, p365]

I. Racines d'un polynôme

[Gou09, §2.2, p59] [Rom17, §12.5, p358]

Fonction polynomiale associée, racine d'un polynôme, a racine $\iff X-a \mid P$,
Exemple : un polynôme de $\mathbb{R}[X]$ de degré impair à une racine réelle. Polynômes cyclotomiques
Application aux polynômes d'endomorphismes : si $P(f)=0$, $P(\mathrm{Sp}(f))=0$. Cas de $P=\chi_f$ et $P=\mu_f$.
Majoration du nombre de racines par le degré du polynôme s'il est non nul
Application : polynôme d'interpolation de LAGRANGE
Identification d'un polynôme et de sa fonction polynomiale sur un corps infini
Multiplicité, formule de TAYLOR
Lien entre multiplicité et zéros des polynômes dérivés
Polynôme scindé, corps algébriquement clos
Théorème de D'ALEMBERT-GAUSS [Rom17, p378]
Application : toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable
Les racines (complexes) de $P \in \mathbb{Q}[X]$, ou $P \in \mathbb{R}[X]$ sont simples si P est scindé

II. Fonctions symétriques élémentaires et polynômes symétriques

II. A. Fonctions symétriques et relations coefficients/racines

[Gou09, §2.2, p59] [Rom17, §12.5, p358]

Fonctions symétriques élémentaires, exemples de $\sigma_1, \sigma_2, \sigma_n$
Toute expression symétrique en $x_1, \dots, x_n$ est un polynôme en $\sigma_1, \dots, \sigma_n$
Relations coefficients/racines
Formules de NEWTON, application à la caractérisation des matrices nilpotentes

II. B. Structure des polynômes symétriques

[Rom17, §2.8.5, p57] [CG13, §V.D, p197] [Tau07, §XIII, p140]

Théorème de structure des polynômes symétriques
Algorithme de factorisation, exemple

PROPOSITION 1. [FORME DE HANKEL]
Soit $P \in \mathbb{R}[X]$ de degré n et $x_1, \dots, x_t$ ses racines distinctes, de multiplicité $m_1, \dots, m_t$. On définit $s_k = \sum_{\ell=1}^{t} m_\ell x_\ell^k$ pour $k \in \mathbb{N}$ puis on pose

$$\forall (X_0, \dots, X_{n-1}) \in \mathbb{C}^n, \quad s(X_1, \dots, X_n) = \sum_{0 \le i,j \le n-1} s_{i+j} X_i X_j$$

Alors $s_{\mathbb{R}}$ (la restriction de s à $\mathbb{R}^n$) est une forme quadratique sur $\mathbb{R}^n$, de signature (p,q) où $p+q=t$ et $p-q$ est le nombre de racines réelles de P.

III. Localisation des racines

III. A. Premiers résultats

[FGN07a, §5.33, p213] [Gou09, §2.2/2.5, p66/83/89]

Les racines de P sont dans un disque déterminé par les coefficients de P
Théorème de GAUSS-LUCAS

THÉORÈME 2. [THÉORÈME DE KRONECKER]
Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes les racines de P sont de module inférieur ou égal à 1 et $P(0) \neq 0$, alors toutes les racines de P sont des racines de l'unité.

COROLLAIRE 3. [THÉORÈME DE KRONECKER]
Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module inférieur ou égal à 1, alors $P=X$ ou $P=\Phi_k$ pour un $k \in \mathbb{N}^*$.

III. B. Disques de GERSHGÖRIN

[FGN07b, §2.8, p80] [Ser01, §4.5, p49]

On cherche les racines de $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$.
Introduction de la matrice compagnon
Matrice à diagonale dominante, disque de GERSHGÖRIN
$\mathrm{Sp}(A) \subset \cup_{i=1}^{n} D_i$
p racines dans une composante connexe regroupant p disques (via l'analyse complexe)

III. C. Approximation d'une racine

[Rou99, Ch4, p140] [AK02, §11.1, p215]

Si P a des racines réelles $\alpha_1 < \cdots < \alpha_r$, la méthode de NEWTON partant de $x_0 \ge \alpha_r$ converge vers α_r. Vitesse de convergence selon la multiplicité
Méthode de la puissance

IV. Racines de polynômes et extensions de corps [Per96, §III.1.c, p70]

IV. A. Rappels sur les extensions de corps

Extension de corps, degré, théorème de la base télescopique, exemples, algébricité

IV. B. Corps de rupture et corps de décomposition

Corps de rupture d'un polynôme irréductible, existence et unicité à isomorphisme près
Exemple de $\mathbb{C}$, de $\mathbb{Q}[\sqrt{2}]$
Degré du corps de rupture
Corps de décomposition, existence et unicité à isomorphisme près
Exemple de $\mathbb{Q}(i, \sqrt{2})$
Théorème de l'élément primitif

IV. C. Clôture algébrique

Corps algébriquement clos
Formulations équivalentes
Polynôme ne s'annulant pas sur un corps fini $\to$ tout corps fini n'est pas algébriquement clos
Clôture algébrique
Tout corps admet une clôture algébrique unique à isomorphisme près

SPEECH

Tout au long de cette leçons on s'intéresse à 3 problèmes fondamentaux liés aux racines d'un polynôme :

- l'existence de racines d'un polynôme $P \in \mathbb{K}[X]$ ainsi que leur calcul exact. On peut identifier polynôme et fonction polynomiale dans le cas d'un corps infini. Trouver les racines d'un polynôme reste un problème que l'on ne peut pas résoudre en général,
- localisation approchée des racines (Gauss-Lucas, Gershgörin, autres méthodes),
- et le problème inverse du premier : soit k une extension de K et $x \in k$. Existe-t-il $P \in K[X]$ tel que $P(x) = 0$? On va ensuite regarder la structure de l'ensemble des racines de P_x le polynôme minimal de x. Théorème de l'élément primitif.
  On peut aussi présenter cette partie avec une version théorie des corps, question d'existence de racines résolue par corps de rupture/décomposition.

QUESTIONS

Q Soit $P_n = \sum_{k=0}^{n} \frac{X^k}{k!}$. Montrer que P_n n'a que des racines simples dans $\mathbb{C}$.

R On vérifie que $P_n' = P_{n-1} = P_n - \frac{X^n}{n!}$. Une racine de P_n et de P_{n-1} ne peut donc être que 0, ce qui n'est pas le cas.

Q Soit $\varphi : \mathcal{M}_n(\mathbb{C}) \longrightarrow \mathbb{C}$ une fonction polynomiale satisfaisant $\varphi(AB) = \varphi(BA)$. Soit $f_i : A \longmapsto \chi_A^i$ le i-ième coefficient de χ_A. Montrer que φ est un polynôme en $f_0, \dots f_{n-1}$.

R On a $\sigma_i(\lambda_1, \dots, \lambda_n) = (-1)^n f_{n-i}(A)$.
Soit $\psi : (\lambda_1, \dots, \lambda_n) \longmapsto \varphi(\mathrm{diag}(\lambda_1, \dots, \lambda_n))$. On a

$$\psi((\lambda_{\sigma(i)})_i) = \varphi(\mathrm{diag}((\lambda_{\sigma(i)})_i)) = P\,\mathrm{diag}((\lambda_i)_i)P^{-1} = \varphi(\mathrm{diag}((\lambda_i)_i))$$

ψ est symétrique, donc fonction des $(\sigma_i)_i$, donc des $(f_i)_i$ … Ainsi φ est un polynôme en les $(f_i)_i$ sur l'ensemble des matrices diagonales. Pour une matrice quelconque, on l'approche par des matrices diagonales et on conclut par continuité.

Q Soit I un intervalle de $\mathbb{R}$. Déterminer les sous-algèbres de dimension finie de $\mathcal{C}^0(I, \mathbb{R})$.

R Soit $\mathcal{C}$ une telle algèbre. Soit $f \in \mathcal{C}$. Pour tout i, $f^i \in \mathcal{C}$ donc $(1, f, \dots f^n)$ est liée, et il existe $P \in \mathbb{R}_n[X]$ annulateur de f. Si f est non constante, P est nul, absurde. Donc $\mathcal{C} = \{0\}$ ou $\mathcal{C} = \{f \text{ constante}\}$.

Q Montrer que si $\mathrm{Tr}(A^k) = 0$ pour tout k, alors A est nilpotente ($\mathbb{K} = \mathbb{C}$).

R En utilisant le polynôme caractéristique de A, on a que $\mathrm{Tr}(\chi_A(A)) = 0 = na_0$ où a_0 est le coefficient constant de χ_A, donc $a_0 = 0$. Ainsi $0 \in \mathrm{Sp}(A)$ et on conclut par récurrence.
Variante : la relation donne que les sommes de Newton sont toutes nulles, donc que les fonctions symétriques sont nulles, donc que les racines sont nulles : le polynôme est nilpotent.

BIBLIOGRAPHIE

[AK02] G. Allaire et S.-M. Kaber : *Algèbre linéaire numérique*. Ellipses, 2002.

[CG13] P. Caldero et J. Germoni : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[FGN07a] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[FGN07b] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 2*. Cassini, 2007.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

[Ser01] D. Serre : *Les Matrices*. Dunod, 2001.

[Tau07] P. Tauvel : *Mathématiques générales pour l'agrégation*. Masson, 2007.

150 EXEMPLES D'ACTIONS DE GROUPES SUR LES ESPACES DE MATRICES.

Soit $\mathbb{K}$ un corps commutatif. Soient n, p des entiers non nuls.

I. Action par translations et pivot de Gauss [CG13, ChIV, p127]

I. A. Généralités

Définition 1. [Action par translation]
On définit les actions par translation/multiplication à gauche et à droite :

$$\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ (P, M) & \longmapsto & PM \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathcal{GL}_p(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ (P, M) & \longmapsto & MP^{-1} \end{array}$$

Définition 2. [Matrices de dilatation, transvection, permutation élémentaire]
Une matrice de dilatation est une matrice $D_{i,\alpha} \in \mathcal{GL}_n(\mathbb{K})$ pour un $\alpha \in \mathbb{K}^*$. Une matrice de transvection est une matrice $T_{i,j,\beta} = I_n + \beta E_{i,j} \in \mathcal{GL}_n(\mathbb{K})$ pour un $\beta \in \mathbb{K}^*$ et $i \neq j$. Une matrice de permutation élémentaire est une matrice $P_{i,j} \in \mathcal{GL}_n(\mathbb{K})$ pour un $i < j$.

$$D_{i,\alpha} = \begin{pmatrix} I_{i-1} & & \\ & \alpha & \\ & & I_{n-i} \end{pmatrix} \qquad P_{i,j} = \begin{pmatrix} I_{i-1} & & & & \\ & 0 & & 1 & \\ & & I_{j-i-1} & & \\ & 1 & & 0 & \\ & & & & I_{n-j} \end{pmatrix}$$

Proposition 3. *Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. Les opérations élémentaires sur les lignes (resp. colonnes) de M sont obtenues par multiplication à gauche (resp. à droite) par les matrices précédemment introduites :*

Matrice	$D_{i,\alpha}M$	$T_{i,j,\beta}M$	$P_{i,j}M$	$MD_{i,\alpha}$	$\dots$
Opération	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \beta L_j$	$L_i \leftrightarrow \alpha L_j$	$C_i \leftarrow \alpha C_i$	$\dots$

I. B. Caractérisation des orbites et pivot de Gauss [CG13, ChI, p2]

Définition 4. On appelle :
- pivot d'une ligne son coefficient non nul le plus à gauche.
- 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 (resp. réduite) en colonnes.

Exemple 5. $\begin{pmatrix} 1 & 2 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ est réduite en lignes, $\begin{pmatrix} 2 & 0 & 0 \\ 1 & 3 & 0 \\ 2 & 4 & 0 \end{pmatrix}$ est échelonnée en colonnes.

Théorème 6. [Orbites de l'action par multiplication à gauche]
Pour l'action par multiplication à gauche :
- *deux matrices A et A' sont dans la même orbite si et seulement si $\ker(A) = \ker(A')$,*
- *toute matrice est dans l'orbite d'une unique matrice réduite en lignes.*

Théorème 7. [Orbites de l'action par multiplication à droite]
Pour l'action par multiplication à droite :
- *deux matrices A et A' sont dans la même orbite si et seulement si $\mathrm{Im}(A) = \mathrm{Im}(A')$,*
- *toute matrice est dans l'orbite d'une unique matrice réduite en colonnes.*

Théorème 8. *$\mathcal{SL}_n(\mathbb{K})$ est engendré par les transvections, $\mathcal{GL}_n(\mathbb{K})$ est engendré par les transvections et les dilatations.*

Application 9. [Algorithme du pivot de Gauss]
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.

Exemple 10. $\begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 0 \\ 0 & 5 & 2 \end{pmatrix}$ a pour matrice réduite associée $\begin{pmatrix} 1 & 2 & 1/2 \\ 0 & 1 & -1/2 \\ 0 & 0 & 1 \end{pmatrix}$.

I. C. Application à la décomposition polaire
[CG13, ChVI, p201] [Rom17, Ch22, p697]

On se place sur $\mathbb{K} = \mathbb{R}$, $n = p$ et on considère l'action à gauche restreinte à $\mathcal{O}_n(\mathbb{R})$.

Théorème 11. [Décomposition polaire]
L'application $\mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) \longrightarrow \mathcal{GL}_n(\mathbb{R}), (O, S) \longmapsto OS$ est un homéomorphisme.

Théorème 12. *L'orbite de toute matrice M contient une matrice symétrique positive. Si M est inversible, l'orbite contient une matrice symétrique définie positive.*

Application 13. $\mathcal{O}_n(\mathbb{R})$ est le seul sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ contenant $\mathcal{O}_n(\mathbb{R})$.

Application 14. Pour $A \in \mathcal{M}_n(\mathbb{R})$, on a $\|\|A\|\|_2 = \sqrt{\rho(A^\top A)}$.

II. Action de Steinitz [CG13, ChI, p2]

Définition 15. [Action de Steinitz]
On appelle action de Steinitz l'action $\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{GL}_p(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ ((P,Q),M) & \longmapsto & PMQ^{-1} \end{array}$.
Les orbites pour cette action sont appelées classes d'équivalence.

Théorème 16. *Si M est de rang r, M est équivalente à $J_r = \begin{pmatrix} I_r & \\ & 0_{n-r,p-r} \end{pmatrix}$.*

Remarque 17. L'algorithme du pivot total permet d'obtenir J_r.

Corollaire 18. *Deux matrices sont équivalentes si et seulement si elles ont même rang. Ainsi $\mathcal{O} = \{O_r \,|\, 0 \leq r \leq \min(m,n)\}$ où $O_r = \{M \in \mathcal{M}_{n,p}(\mathbb{K}) \mid \mathrm{rg}(M) = r\}$.*

Exemple 19. $\begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 0 \\ 0 & 5 & 2 \end{pmatrix}$ est équivalente à I_3.

Corollaire 20. $\mathrm{rg}(M^\top) = \mathrm{rg}(M)$.

Proposition 21. *Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Alors $\overline{O_r} = \bigsqcup_{0 \leq k \leq r} O_k$.*

Corollaire 22. *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 $n = p$, $O_n = \mathcal{GL}_n(\mathbb{K})$ est un ouvert dense de $\mathcal{M}_n(\mathbb{K})$.*

III. Action par conjugaison [CG13, ChIII, p83]

III. A. Généralités

Définition 23. [Action par conjugaison]
On considère l'action par conjugaison $\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ (P,M) & \longmapsto & PMP^{-1} \end{array}$.
Deux matrices d'une même orbite sont dites semblables.

Remarque 24. On considère un $\mathbb{K}$-espace vectoriel E de dimension finie n, et $u \in \mathcal{L}(E)$. Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, P la matrice de passage de $\mathcal{B}$ vers $\mathcal{B}'$. Alors si $A = M_{\mathcal{B}}(u)$ et $A' = M_{\mathcal{B}'}(u)$, on a $A' = PAP^{-1}$.

Proposition 25. *Deux matrices semblables ont même rang, déterminant, trace, valeurs propres, polynôme minimal, polynôme caractéristique.*

Remarque 26. Dans aucun des cas il ne s'agit d'une caractérisation. Par exemple pour le polynôme minimal considérer $\mathrm{diag}(1,1,2)$ et $\mathrm{diag}(1,2,2)$ et pour le polynôme caractéristique, considérer I_2 et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

III. B. Applications à la trigonalisabilité/diagonalisabilité [MM16]

Définition 27. Une matrice est trigonalisable (resp. diagonalisable) si elle est dans l'orbite d'une matrice triangulaire (resp. diagonale).

Théorème 28. *Une matrice est trigonalisable (resp. diagonalisable) si et seulement si son polynôme minimal est scindé (resp. scindé à racines simples).*

Proposition 29. *Dans $\mathbb{K} = \mathbb{C}$, $M \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si et seulement si sa classe de similitude est fermée dans $\mathcal{M}_n(\mathbb{K})$.*

Application 30. [Cardinal de $\mathcal{D}_n(\mathbb{F}_q)$] [Rom17, §5.6, p148–151]
Soit $n \in \mathbb{N}$, $q = p^r$ où p premier, $r \neq 0$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1+\cdots+n_q=n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

III. C. Action de $\mathcal{O}_n(\mathbb{R})$ et de $\mathcal{U}_n(\mathbb{C})$ [CG13, ChV, p149] [Rom17, Ch22]

Si $\mathbb{K} = \mathbb{R}$ (resp. $\mathbb{C}$), restreignons l'action par conjugaison à $\mathcal{O}_n(\mathbb{R})$ (resp. $\mathcal{U}_n(\mathbb{C})$).

Remarque 31. Avec le contexte de la remarque précédente, l'action de $\mathcal{O}_n(\mathbb{R})$ (resp. $\mathcal{U}_n(\mathbb{C})$) équivaut à un changement de base orthonormée pour E euclidien (resp. hermitien).

Fixons donc un endormorphisme $u \in \mathcal{L}(E)$ euclidien. On suppose u normal, c'est-à-dire que sa matrice M dans une base orthonormée fixée vérifie :

Définition 32. $M \in \mathcal{M}_n(\mathbb{K})$ est dite normale si $M^*M = MM^*$ où $M^* = \overline{M^\top}$.

Proposition 33. *Les valeurs propres (complexes) de M normale sont des racines de l'unité.*

Lemme 34.
- *Si F est un sous-espace vectoriel stable par u, alors $F^\perp$ est stable par u,*
- *Il existe un sous-espace vectoriel stable par u de dimension 1 ou 2.*

Théorème 35. [Réduction des endomorphismes normaux]
Il existe une base orthonormée $\mathcal{B}$ de E telle que

$$M_{\mathcal{B}}(u) = \begin{pmatrix} \mathrm{diag}(\lambda_1, \dots, \lambda_p) & & & \\ & R_1 & & \\ & & \ddots & \\ & & & R_r \end{pmatrix}$$

où $p + 2r = n$, $(\lambda_i)_{1 \le i \le p} \in \mathbb{R}^p$ et pour $1 \le k \le r$, $R_k = \begin{pmatrix} a_k & -b_k \\ b_k & a_k \end{pmatrix}$ avec $b_k \neq 0$.

Application 36. [Réduction d'un endomorphisme antisymétrique]
Supposons u antisymétrique. Alors il existe une base orthonormée $\mathcal{B}$ de E telle que $M_{\mathcal{B}}(u)$ est de la forme précédente, avec $\lambda_1 = \dots = \lambda_p = 0$, $2r \le n$ et $R_k = \begin{pmatrix} 0 & -b_k \\ b_k & 0 \end{pmatrix}$.

IV. Action par congruence

[Rom17, Ch15, p463]

IV. A. Généralités

On suppose dans cette section que $\mathrm{car}(\mathbb{K}) \neq 2$.

Définition 37. [Action par congruence]
On appelle action par congruence l'action sur $\mathcal{S}_n(\mathbb{K})$: $\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) & \longrightarrow & \mathcal{S}_n(\mathbb{K}) \\ (P, S) & \longmapsto & PSP^\top \end{array}$.
Deux matrices d'une même orbite sont dites congruentes.

Remarque 38. On considère un $\mathbb{K}$-espace vectoriel E de dimension finie n, q une forme bilinéaire symétrique sur E, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, P la matrice de passage de $\mathcal{B}$ vers $\mathcal{B}'$. Alors si $S = M_{\mathcal{B}}(q) \in \mathcal{S}_n(\mathbb{K})$ et $S' = M_{\mathcal{B}'}(q) \in \mathcal{S}_n(\mathbb{K})$, on a $S' = PSP^\top$.

Définition 39. [Discriminant]
On définit le discriminant de $S \in \mathcal{S}_n(\mathbb{K})$ par $\overline{\det(S)} \in \mathbb{K}^*/(\mathbb{K}^*)^2$ si S est inversible, 0 sinon.

Proposition 40. *Deux matrices congruentes ont même discriminant.*

IV. B. Classification des formes quadratiques

[CG13, ChV.B, p179]

Théorème 41. [Classification sur $\mathbb{K} = \mathbb{C}$]
Soit $S \in \mathcal{S}(\mathbb{C})$. Alors S est congruente à J_r où $r = \mathrm{rg}(S)$.
Deux matrices de $\mathcal{S}_n(\mathbb{C})$ sont congruentes si et seulement si elles ont même rang.

Théorème 42. [Classification sur $\mathbb{K} = \mathbb{R}$]
Soit $S \in \mathcal{S}(\mathbb{R})$. Il existe $(s, t) \in \mathbb{N}^2$ tels que S soit congruente à $\begin{pmatrix} I_s & & \\ & -I_t & \\ & & 0_{n-s-t} \end{pmatrix}$.

Proposition 43. *On a $s = \max(\{\dim(F) \mid F \text{ sev de } E \text{ sur lequel } q \text{ est définie positive}\})$ et $t = \max(\{\dim(F) \mid F \text{ sev de } E \text{ sur lequel } q \text{ est définie négative}\})$.*

Corollaire 44. *Deux matrices de $\mathcal{S}_n(\mathbb{R})$ sont congruentes si et seulement si elles ont même signature.*

On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 45. *$\mathbb{F}_p^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^*$.*

Application 46. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

Théorème 47. [Classification sur $\mathbb{K} = \mathbb{F}_q$]
Soit $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$. Alors toute matrice $S \in \mathcal{S}_n(\mathbb{F}_q)$ est congruente à $\begin{pmatrix} I_{r-1} & & \\ & \delta & \\ & & 0_{n-r} \end{pmatrix}$
où $\delta \in \{1, \alpha\}$ et $r = \mathrm{rg}(S)$.

Application 48. [Loi de réciprocité quadratique]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Exemple 49. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

SPEECH

Les matrices sont des objets mathématiques assez anciens, dont la structure a été formalisée par son lien avec l'algèbre linéaire (opérations sur les lignes et colonnes, endomorphismes, formes quadratiques). Les actions de groupes permettent de synthétiser tout cela.
Dans un premier temps, on regarde les multiplications de matrices qui nous mènent au pivot de GAUSS et aux décompositions LU et polaire.
Ensuite on étudie l'action de STEINITZ et la caractérisation des orbites par le rang.
Enfin la troisième partie s'intéresse à l'action par conjugaison, qui correspond à la notion de matrices représentant un même endomorphisme et donne un grand nombre d'invariants par similitude. On applique cela à la diagonalisabilité et à la réduction de FROBENIUS.
Enfin on parle de l'action par congruence qui correspond à la relation de représentation d'une même forme quadratique. Sur $\mathbb{C}$ on a une caractérisation simple des orbites, sur $\mathbb{R}$ on utilise la signature. Enfin on donne la classification sur $\mathbb{F}_q$ avec application à la loi de réciprocité quadratique.

QUESTIONS

Q Montrer le premier point du Théorème 15.

R Voir [CG13, §IV.2, p131].

Q Soit $S \in \mathcal{S}_n(\mathbb{C})$ telle que $\det(S+X) = \det(X)$ pour tout $X \in \mathcal{S}_n(\mathbb{C})$. Que dire de S ?

R On a $0 = \det(S-S) = \det(-S) = (-1)^n \det(S)$ dons S est non inversible.
Pour tout $P \in \mathcal{GL}_n(\mathbb{C})$, on a $\det(PSP^\top + PXP^\top) = \det(P)^2 \det(S+X) = \det(P)^2 \det(X) = \det(PXP^\top)$. On peut donc remplacer S par sa forme réduite. Quand X décrit $\mathcal{S}_n(\mathbb{C})$, $PXP^\top$ décrit $\mathcal{S}_n(\mathbb{C})$ donc le problème se réécrit : $\det(S'+X') = \det(X')$ pour $X' \in \mathcal{S}_n(\mathbb{C})$, où $S' = J_r$. Prenant alors $X' = \mathrm{Id}$, on obtient $\det(S'+X') = \det(X')$, ce qui n'est possible que si $\mathrm{rg}(S') = 0$, c'est-à-dire $S' = 0$, ou encore $S = 0$.

BIBLIOGRAPHIE

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[MM16] R. MANSUY et R. MNEIMNÉ : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

151 DIMENSION D'UN ESPACE VECTORIEL (ON SE LIMITERA AU CAS DE LA DIMENSION FINIE). RANG. EXEMPLES ET APPLICATIONS.

I. Espaces vectoriels et dimension

[Gou09, §3.1, p109–111]

Soit $\mathbb{K}$ un corps commutatif. Soit E un $\mathbb{K}$-espace vectoriel dont on rappelle la définition :

Définition 1. [Espace vectoriel, sous-espace vectoriel]
- $(E,+,.)$ est un $\mathbb{K}$-espace vectoriel si $(E,+)$ est un groupe commutatif et si la loi externe satisfait pour tout $\lambda,\mu \in \mathbb{K}$ et $x,y \in E$, $(\lambda+\mu).x = \lambda.x + \mu.x$, $\lambda.(x+y) = \lambda.x + \lambda.y$, $\lambda.(\mu.x) = (\lambda\mu).x$, $1_{\mathbb{K}}.x = x$,
- Un sous-ensemble non vide F de E est un sous-espace vectoriel de E s'il est stable par les lois de E, c'est-à-dire si pour tout $\lambda \in \mathbb{K}$ et $x,y \in F$, on a $\lambda.x + y \in F$.

Exemple 2. Une intersection et une somme de sous-espaces vectoriels de E est un s.e.v. de E. On peut donc définir $\mathrm{Vect}(A)$.

Définition 3. [Famille génératrice, libre, base, dimension finie]
Soit $(e_i)_{i\in I}$ une famille d'éléments de E.
- $(e_i)_{i\in I}$ est dite génératrice de E lorsque $\mathrm{Vect}((e_i)_{i\in I}) = E$. Lorsque E possède une famille génératrice finie, on dit que E est de dimension finie,
- $(e_i)_{i\in I}$ est dite libre lorsque $\forall (\lambda_i)_{i\in I} \in \mathbb{K}^I, \sum_{i\in I}\lambda_i e_i = 0 \Longrightarrow \forall i \in I, \lambda_i = 0$. Si ce n'est pas le cas, la famille est dite liée,
- Si $(e_i)_{i\in I}$ est libre et génératrice, on dit que c'est une base de E.
- Soient $(E_i)_{i\in I}$ des s.e.v de E. On dit que E est la somme directe des $(E_i)_{i\in I}$ si $\sum_{i\in I} E_i = E$ et que la décomposition de tout vecteur de E dans $(E_i)_{i\in I}$ est unique.

Exemple 4.
- $\{1,\sqrt{2},\sqrt{3}\}$ est libre sur le $\mathbb{Q}$-espace vectoriel $\mathbb{R}$.
- La base canonique de $E = \mathbb{K}^n$,
- Une sous-famille (/sur) d'une famille libre (/génératrice) de E est libre (/génératrice),
- $\mathbb{K}[X]$ n'est pas de dimension finie,
- Unicité de la décomposition de $x \in \mathrm{Vect}((e_i)_{i\in I})$ lorsque $(e_i)_{i\in I}$ est libre.

Théorème 5. [Théorème de la base incomplète]
Soient $\mathcal{L}$ une famille libre et $\mathcal{G}$ une famille génératrice de E. Alors il existe une base $\mathcal{B}$ de telle que $\mathcal{L} \subset \mathcal{B} \subset \mathcal{L}\cup\mathcal{G}$.

Corollaire 6. *Si E est de dimension finie, il admet une base. De plus, toute base de E a même cardinal appelé dimension de E, et noté $\dim(E)$.*
Toute famille libre (resp. génératrice) est de cardinal inférieur (resp. supérieur) ou égal à $\dim(E)$ et en cas d'égalité, c'est une base.

Proposition 7. [Propriétés des sous-espaces vectoriels de E]
Soient E de dimension finie n, et F_1, F_2 des sous-espaces vectorielsde E.
- *F_1 est de dimension finie et $\dim(F_1) \leq \dim(E)$, et $\dim(F_1) = \dim(E) \iff F_1 = E$.*
- **[Formule de Grassman]** *On a $\dim(F_1+F_2) + \dim(F_1\cap F_2) = \dim(F_1) + \dim(F_2)$.*
- *F_1 et F_2 sont supplémentaires dans E (c'est-à-dire $E = F_1 \oplus F_2$) si et seulement si au moins 2 des propriétés suivantes sont vérifiées :*

$$\dim(E) = \dim(F_1) + \dim(F_2) \quad F_1 \cap F_2 = \{0\} \quad E = F_1 + F_2$$

II. Rang d'une application linéaire

[Gou09, §3.2–3.3, p113–122]

Soient E, G des espaces vectoriels de dimension finie n et m.

II. A. Applications linéaires

Définition 8. [Application linéaire]
$f : E \longrightarrow G$ est linéaire si $f(\lambda.x + \mu.y) = \lambda.f(x) + \mu.f(y)$ pour $\lambda,\mu \in \mathbb{K}$ et $x,y \in E$.
$\mathcal{L}(E,G)$ est l'ensemble des applications linéaires de E dans G et $\mathcal{L}(E) = \mathcal{L}(E,E)$.

Remarque 9. $\mathrm{Im}(f)$ et $\ker(f)$ sont des s.e.v. et $\dim(\mathrm{Im}(f)) \leq \dim(E) < +\infty$.
Une application linéaire est entièrement déterminée par ses valeurs sur une base de E.

Définition 10. [Rang d'une application linéaire]
Pour $f \in \mathcal{L}(E,G)$, on note $\mathrm{rg}(f)$ et on appelle rang de f l'entier $\dim(\mathrm{Im}(f))$.

Théorème 11. [Théorème du rang]
Soit $f \in \mathcal{L}(E,G)$. Alors $\dim(\ker(f)) + \mathrm{rg}(f) = \dim(E)$.

Application 12. [MM16, §2.1, p16] Pour $f \in \mathcal{L}(E)$:
- $(\mathrm{rg}(f^k))_{k\in\mathbb{N}}$ est décroissante stationnaire et $(\mathrm{rg}(f^k) - \mathrm{rg}(f^{k+1}))_{k\in\mathbb{N}}$ est décroissante.
- il existe $P \in \mathbb{K}_{\dim(E)^2+1}[X]$ tel que $P(f) = 0_{\mathcal{L}(E)}$.

Corollaire 13. *Lorsque $n = m$, on a f bijective $\iff$ f surjective $\iff$ f injective.*

Application 14. [BMP05, p154] Existence et unicité du polynôme interpolateur de Lagrange.
[Gri15, §3.3, p63] Contre-exemple en dimension infinie : $P \longmapsto P'$.

II. B. Représentations matricielles d'une application linéaire

Définition 15. [Matrice d'une application linéaire]
Soit $f \in \mathcal{L}(E,G)$. Si $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{C}$ sont des bases de E et G, on définit la matrice $M_{\mathcal{B},\mathcal{C}}(f) \in \mathcal{M}_{m,n}(\mathbb{K})$ de f dans les bases $\mathcal{B}$ et $\mathcal{C}$ comme la matrice de vecteurs colonnes les $(f(e_i))_{1\leq i\leq n}$ exprimés dans la base $\mathcal{C}$.

Définition 16. [Rang d'une famille de vecteurs et d'une matrice]
On définit $\mathrm{rg}(A)$ le rang de $A \in \mathcal{M}_{m,n}(\mathbb{K})$ comme le rang de la famille de ses vecteurs colonnes $(x_1, \dots, x_n)$, c'est-à-dire l'entier $\dim(\mathrm{Vect}((x_i)_{1\leq i\leq n}))$.

Proposition 17. *Si $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est de rang r, alors A est équivalente à $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.*

Corollaire 18. *Deux matrices sont équivalentes si et seulement si elles ont même rang.*

Proposition 19. *Le rang d'une matrice est l'ordre du plus grand mineur non nul.*

Proposition 20. [Liens entre rangs]
- *Pour tout $A \in \mathcal{M}_{n,m}(\mathbb{K})$, il existe E, G, f et $\mathcal{B}, \mathcal{C}$ tels que $A = M_{\mathcal{B},\mathcal{C}}(f)$.*
- *Deux matrices de $\mathcal{M}_{n,m}(\mathbb{K})$ représentent une même application linéaire $f \in \mathcal{L}(E,G)$ dans des bases différentes si et seulement si elles sont équivalentes.*
- *$\mathrm{rg}(A) = \mathrm{rg}(f)$ lorsque A est une matrice de f.*

Application 21. [Gou09, §2/3, p37/90]
- La méthode du pivot de Gauss permet d'obtenir le rang d'une matrice,
- Soient $M \in \mathcal{M}_n(\mathbb{K})$ et $N \in \mathcal{GL}_n(\mathbb{K})$. Alors $\mathrm{rg}(MN) = \mathrm{rg}(NM) = \mathrm{rg}(M)$.

III. Les conséquences de la dimension finie

III. A. Espaces vectoriels normés

[Gou08, §1.5/1.6, p50/56]

Soit $(E, \|.\|)$ un espace vectoriel normé réel ou complexe de dimension quelconque (on suppose la notion de norme connue).

Théorème 22. [Théorème de Riesz]
E est de dimension finie si et seulement si $\overline{\mathbb{B}_E(0,1)}$ est compacte.

Théorème 23. *Si E est de dimension finie, alors toutes les normes sur E sont équivalentes.*

Exemple 24. Contre-exemple en dimension infinie : $\|.\|_1$ et $\|.\|_\infty$ sur $\mathcal{C}([0,1],\mathbb{R})$.
Contre-exemple sur un corps non complet : $\mathbb{Q}[\sqrt{2}]$, $N_1(a+b\sqrt{2}) = |a| + |b|$ et $N_2 = |.|$.

Corollaire 25. *Si E est de dimension finie, les compacts de E sont les fermés bornés.*

Théorème 26. [Orthonormalisation de Gram-Schmidt] *[Rom17, §22.1, p699–700]*
Supposons que $\|.\|$ dérive d'un produit scalaire $\langle . \mid . \rangle$ (E est alors un espace euclidien). Pour toute famille libre $(x_i)_{1\leq i\leq p}$ de E, il existe une unique famille orthonormée $(e_i)_{1\leq i\leq p}$ telle que pour tout $k \in [\![1,p]\!]$, $\mathrm{Vect}(e_1,\dots,e_k) = \mathrm{Vect}(x_1,\dots,x_k)$ et $\langle x_k \mid e_k \rangle > 0$.

III. B. Dualité

[Rom17, Ch14, p443–456]

Définition 27. [Espace dual]
On note $E^* = \mathcal{L}(E,\mathbb{K})$ l'espace dual de E.
A toute base $\mathcal{B} = (e_1,\dots,e_n)$ de E, on associe la famille $\mathcal{B}^* = (e_1^*,\dots,e_n^*)$ de E^* où e_i^* est la projection sur $\mathrm{Vect}(e_i)$ parallèlement à $\mathrm{Vect}((e_j)_{j\neq i})$.

Proposition 28. *$\mathcal{B}^*$ est une base de E^*, appelée base duale de $\mathcal{B}$. Ainsi, E^* est de dimension finie et $\dim(E^*) = \dim(E)$.*
Par ailleurs, toute base de E^* est la base duale d'une unique base $\mathcal{B}$ de E.

Application 29. [Théorème du rang]
Si $\phi \in E^*$ est non identiquement nulle, son noyau est un hyperplan H.
Si $\phi_1,\dots,\phi_p \in E^*$, alors $\dim(\cap_{i=1}^p \ker(\phi_i)) = \dim(\cap_{i=1}^p H_i) \geq n-p$.

Définition 30. [Orthogonal]
- L'othogonal dans E^* de $\{0\} \subset X \subset E$ est $X^\perp = \{\phi \in E^* \mid \forall x \in X, \phi(x) = 0\}$,
- L'othogonal dans E de $\{0\} \subset Y \subset E^*$ est $Y^\circ = \{x \in E \mid \forall \phi \in E, \phi(x) = 0\}$.

Ce sont des sous-espaces vectoriels de E^* et E respectivement.

Proposition 31. *Si F est un sous-espace vectoriel de E, alors $\dim(F) + \dim(F^\perp) = \dim(E)$. De même si G est un sous-espace vectoriel de E^*, $\dim(G) + \dim(G^\circ) = \dim(E)$.*

Définition 32. [Transposée]
Pour $f \in \mathcal{L}(E,F)$, on définit l'application transposée ${}^tf : F^* \longrightarrow E^*, \phi \longmapsto \phi \circ f$.

Application 33. Si $A = M_{\mathcal{B},\mathcal{C}}(f)$, alors $M_{\mathcal{B}^*,\mathcal{C}^*}({}^tf) = A^\top$.
On en déduit que ${}^t(v \circ u) = {}^tu \circ {}^tv$.

IV. Applications des espaces vectoriels de dimension finie

IV. A. Réduction d'endomorphismes [MM16]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. On suppose les notions de polynôme d'endomorphisme et de valeurs/vecteurs/espaces propres connues.

Lemme 34. [Lemme des noyaux]
Soit $(P_k)_{1\leq k\leq N}$ une famille de polynômes deux à deux premiers entre eux et $f \in \mathcal{L}(E)$. Alors en posant $P = \prod_{k=1}^N P_k$, on a $\ker(P(f)) = \bigoplus_{k=1}^N \ker(P_k(f))$.
De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Exemple 35. En pratique, on utilise souvent ce lemme avec P tel que $\ker(P(f)) = E$. On obtient alors une décomposition de E en sous-espaces stables, car $\ker(Q(f))$ est stable par f pour tout polynôme Q.

Définition 36. [Polynôme caractéristique]
On définit le polynôme caractéristique de $A \in \mathcal{M}_n(\mathbb{K})$ par $\chi_A(X) = \det(XI_n - A)$.
On définit le polynôme caractéristique de $f \in \mathcal{L}(E)$ comme le polynôme caractéristique d'une matrice de f dans n'importe quelle base de E (en remarquant que χ_A est invariant par similitude). On le note χ_f.

Théorème 37. [Théorème de Cayley-Hamilton]
Pour tout $f \in \mathcal{L}(E)$, $\chi_f(f) = 0$.

Théorème 38. [Caractérisation d'un polynôme trigonalisable]
Un endomorphisme $f \in \mathcal{L}(E)$ est trigonalisable si et seulement si χ_f est scindé.

Théorème 39. [Décomposition de Jordan] *[Rom17, Ch21, p672–675]*
Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Soient $\lambda_1, \dots, \lambda_m$ les valeurs propres de f.
Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,r_j}$ pour $j \in [\![1, m]\!]$ tels que dans une certaine base $\mathcal{B}$ de E, $M_{\mathcal{B}}(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{\substack{1\leq j\leq m \\ 1\leq k\leq r_j}}$, où $B_{j,k} = \lambda_j I_{d_{j,k}} + J_{d_{j,k}}$

en notant $J_d = \begin{pmatrix} 0 & & \dots & & 0 \\ 1 & 0 & & & \\ & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 0 & \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_d(\mathbb{K})$.

IV. B. Extensions de corps et nombres algébriques [Per96, §3.1, p65–66]

On ne considère que des corps commutatifs.

Définition 40. [Extension de corps, degré]
Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$.
$\mathbb{L}$ est alors un $\mathbb{K}$-e.v.. Lorsque $\dim(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est finie.

Exemple 41. $\mathbb{R} \subset \mathbb{C}, \mathbb{Q} \subset \mathbb{Q}(i)$.

Théorème 42. [Théorème de la base télescopique]
Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.
En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 43. [Élément algébrique, transcendant]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\phi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\phi_{|\mathbb{K}} = \mathrm{id}$ et $\phi(T) = \alpha$.
Si ϕ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\phi) = (P)$. P est appelé polynôme minimal de α.

Exemple 44. $\sqrt{2}, i$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants sur $\mathbb{Q}$.

Théorème 45. [Caractérisation d'un algébrique]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty$$

Application 46. Pour tout entier $n \in \mathbb{N}$ et toute famille $p_1, \dots, p_n$ d'entiers supérieurs ou égaux à 2, tous sans facteur carré, et premiers deux à deux, on a :

$$[\mathbb{Q}[\{\sqrt{p_i}\}_{1\leq i\leq n}] : \mathbb{Q}] = 2^n$$

ANNEXE

Exemple(s) du pivot de Gauss, schémas de degrés d'extensions de corps ...

SPEECH

La théorie de l'algèbre linéaire en dimension finie est fondamentale en mathématiques dans de nombreux domaines via les propriétés de réduction. Il y a deux visions possibles : d'un côté voir les applications linéaires dans des bases adaptées, en visualisant l'image de la base, et de l'autre les matrices associées qui permettent des calculs matriciels et des algorithmes. On va voir qu'il faut savoir jongler entre les deux !
Dans la première partie, on insiste sur la propriété d'existence de base en dimension finie et le théorème de la base incomplète.
Ensuite, la théorie du rang avec les deux visions et leurs liens (dernier théorème). On regardera les applications à l'étude d'endomorphismes.
Dans un troisième temps, on se demandera ce que la dimension finie apporte dans un espace vectoriel normé. Une conséquence notable est le procédé d'orthogonalisation de Gram-Schmidt. On introduira également la notion de dualité qui est très importante de par ses propriétés intéressantes que l'on va pouvoir notamment appliqué dans la partie suivante.
Enfin on regardera le cas particulier de l'étude des endomorphismes. On introduit des résultats classiques où la dimension finie joue un rôle important, notamment la décomposition de Jordan proposée en développement où l'on va raisonner par récurrence sur la dimension (classique) et utiliser des propriétés de dualité. Notons également des résultats en théorie des corps qui utilisent des théorèmes vus dans la leçon.

COMMENTAIRES

C'est une leçon très dense, qui se complète très bien avec des morceaux d'autres leçons. Il faut faire des choix.

QUESTIONS

Q Quelle est la première utilisation du théorème de la base incomplète ?
R Il existe des bases en dimension finie.
Q Calcul de rangs de matrices.
Q Quelle est la dimension de E/F ?
R Utiliser le théorème du rang appliqué à la projection.

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Gri15] J. Grifone : *Algèbre linéaire*. Cépaduès, 5ème édition, 2015.

[MM16] R. Mansuy et R. Mneimné : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

152 DÉTERMINANT. EXEMPLES ET APPLICATIONS.

I. Définitions et propriétés générales [Gou09, §3.5, p134–137]

I. A. Formes n-linéaires alternées, déterminant d'une famille de vecteurs

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n où $\mathbb{K}$ est un corps commutatif.

Définition 1. [Application n-linéaire, alternée]
Soit $f : E^n \longrightarrow \mathbb{K}$ une application.
- On dit que f est n-linéaire si en tout point les n applications partielles sont linéaires. L'ensemble des applications n-linéaires est noté $\mathcal{L}_p(E, \mathbb{K})$.
- Si $f \in \mathcal{L}_p(E, \mathbb{K})$, on dit que f est alternée si $f(x_1, \dots, x_p) = 0$ dès que deux des $\{x_i\}_{1 \leq i \leq p}$ sont égaux.

Théorème 2. [Propriétés de $\Lambda_n(E)$]
L'ensemble $\Lambda_n(E)$ des formes n-linéaires alternées de E est un espace vectoriel de dimension 1. Il existe une unique forme n-linéaire alternée égale à 1 sur une base donnée de $\mathcal{B}$.

Définition 3. [Déterminant dans une base]
Soit $\mathcal{B}$ une base de E. On appelle déterminant dans la base $\mathcal{B}$, et on note $\det_{\mathcal{B}}$, l'unique forme n-linéaire alternée égale à 1 sur $\mathcal{B}$.

Corollaire 4. [Expression de $\det_{\mathcal{B}}$]
Soient $x_1, \dots, x_n$ des vecteurs de E. En notant $(x_{i,1}, \dots, x_{i,n})$ les coordonnées de x_i dans une base $\mathcal{B}$ de E, on a :

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

Corollaire 5. [Changement de base]
Soit $\mathcal{B}$ une base de E. Pour $f \in \Lambda_n(E)$, on a $f = f(\mathcal{B}) \det_{\mathcal{B}}$.
En particulier, si $\mathcal{B}'$ est une autre base de E, on a $\det_{\mathcal{B}'} = \det_{\mathcal{B}'}(\mathcal{B}) \det_{\mathcal{B}}$.

Proposition 6. [Caractérisation d'une famille liée, libre]
Soient $x_1, \dots, x_n \in E$. On a équivalence entre :
(i) la famille $\{x_1, \dots, x_n\}$ est liée,
(ii) pour toute base $\mathcal{B}$ de E, on a $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$,
(iii) il existe une base $\mathcal{B}$ de E telle que $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$.

I. B. Déterminant d'une matrice carrée et d'un endomorphisme

Soit $A = (a_{i\,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$. Soit $f \in \mathcal{L}(E)$.

Définition 7. [Déterminant d'une matrice]
On appelle déterminant de A le déterminant des vecteurs colonnes de A dans la base canonique de $\mathbb{K}^n$. On le note $\det(A)$.

Proposition 8. *Soient $\lambda \in \mathbb{K}$ et $B \in \mathcal{M}_n(\mathbb{K})$. On a les propriétés suivantes :*
i) on ne change pas la valeur du déterminant lorsque l'on ajoute à une colonne une combinaison linéaire des autres colonnes,
ii) $\det(A^\top) = \det(A)$ et $\det(\lambda A) = \lambda^n \det(A)$,
iii) $\det(AB) = \det(A)\det(B)$.
iv) Si A et B sont semblables, alors $\det(A) = \det(B)$.
v) $A \in \mathcal{GL}_n(\mathbb{K}) \iff \det(A) \neq 0$. Dans ce cas, $\det(A^{-1}) = \det(A)^{-1}$.

Définition 9. [Déterminant d'un endomorphisme]
On note $\det(f)$ le déterminant de la matrice de f dans une base de E.

Remarque 10. On transpose les propriétés de la Proposition 8 aux endomorphismes.

II. Méthodes de calcul de déterminants

Exemple 11. Déterminant en dimensions 2 et 3 (règle de Sarrus).

II. A. Mineurs et cofacteurs [Gou09, §3.5, p136–137]

Définition 12. [Mineur, cofacteur, comatrice]
Soit $i, j \in [\![1, n]\!]$. On appelle mineur d'indice (i, j) le déterminant $\Delta_{i\,j}$ de la matrice d'ordre $n-1$ déduite de A en supprimant la ligne i et la colonne j. On appelle cofacteur d'indice (i, j) le scalaire $A_{i\,j} = (-1)^{i+j}\Delta_{i\,j}$.
On définit la comatrice de A par $\mathrm{Com}(A) = (A_{i\,j})_{1 \leq i,j \leq n}$.

Théorème 13. [Développement par rapport ...]
- **[À une colonne]** *Pour tout $j \in [\![1, n]\!]$, on a $\det(A) = \sum_{i=1}^n a_{i\,j} A_{i\,j}$.*
- **[À une ligne]** *Pour tout $i \in [\![1, n]\!]$, on a $\det(A) = \sum_{j=1}^n a_{i\,j} A_{i\,j}$.*

Théorème 14. [Formule de la comatrice]
On a $A\,\mathrm{Com}(A)^\top = \mathrm{Com}(A)^\top A = \det(A) I_n$.
En particulier, si A *est inversible, alors* $A^{-1} = \frac{1}{\det(A)}\mathrm{Com}(A)^\top$.

II. B. Matrices triangulaires par blocs

[Rom17, §17.2, p542–543]

Lemme 15. *Si* A *est une matrice triangulaire, alors* $\det(A) = \prod_{i=1}^n a_{i\,i}$.

Application 16. [Pivot de Gauss]
La formule du Théorème 13 est impraticable en réalité (trop d'opérations). Via des opérations sur les lignes et les colonnes, on transforme toute matrice en une matrice triangulaire supérieure dont on peut facilement calculer le déterminant.

Théorème 17. [Déterminant par blocs]
Supposons A *de la forme :*

$$A = \begin{pmatrix} A_1 & \star & \star & \dots & \star \\ 0 & A_2 & \star & \dots & \star \\ 0 & 0 & A_3 & \dots & \star \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & A_p \end{pmatrix}$$

où les $(A_i)_{1\le i\le p}$ *sont des matrices carrées et* $\star$ *des matrices quelconques de tailles adéquates. Alors* $\det(A) = \prod_{i=1}^p \det(A_i)$.

II. C. Exemples classiques

[Gou09, §3.5, p143–147]

Exemple 18. [Déterminant circulant]
Soient $a_1, \dots, a_n \in \mathbb{C}$. Alors :

$$\det\left(\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}\right) = \prod_{0\le k\le n-1} P(\omega^k) \quad \text{où} \quad \begin{cases} P(X) = \sum_{i=0}^{n-1} a_{i+1} X^i \\ \omega = \exp(2i\pi/n) \end{cases}$$

Proposition 19. [Convergence d'une suite de polygones vers l'isobarycentre]
On définit par récurrence une suite $(P^{(k)})_{k\in\mathbb{N}}$ *par* $P^{(0)} = (z_1^{(0)}, \dots, z_n^{(0)}) \in \mathbb{C}^n$ *et* $P^{(k+1)} = \left(\frac{z_1^{(k)}+z_2^{(k)}}{2}, \dots, \frac{z_{n-1}^{(k)}+z_n^{(k)}}{2}, \frac{z_n^{(k)}+z_1^{(k)}}{2}\right)$ *pour* $k \in \mathbb{N}$.
Alors $P^{(k)} \underset{k\to+\infty}{\longrightarrow} (g, g, \dots, g)$ *où* $g = \mathrm{Isobar}(z_1^{(0)}, \dots, z_n^{(0)})$.

Exemple 20. [Déterminant de Vandermonde]
Soient $a_1, \dots, a_n \in \mathbb{C}$. Alors $\det((a_i^j)_{1\le i,j\le n}) = \prod_{1\le i<j\le n} (a_j - a_i)$. **[voir annexe]**

Exemple 21. [Déterminant de Cauchy]
Soient $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{C}$ tels que $a_i + b_i \neq 0$. Alors :

$$\det\left(\left(\frac{1}{a_i+b_j}\right)_{1\le i,j\le n}\right) = \frac{\prod_{1\le i<j\le n}(a_j-a_i)(b_j-b_i)}{\prod_{1\le i,j\le n}(a_i+b_j)}$$

III. Applications des déterminants en analyse

III. A. Propriétés du déterminant

[Rou99, §2.3, p74–76]

Proposition 22. $\det : \mathcal{M}_n(\mathbb{R}) \longrightarrow \mathbb{R}$ *est* $\mathcal{C}^\infty$ *et on a :*

$$\forall M, H \in \mathcal{M}_n(\mathbb{R}),\ d\det_M(H) = \mathrm{Tr}(\mathrm{Com}(M)^\top H)$$

Application 23. [Wronskien]
Soient $A \in \mathcal{C}^0(\mathbb{R}, \mathcal{M}_n(\mathbb{R}))$ et $y_1, \dots, y_n \in \mathbb{R}^n$ des solutions de l'équation différentielle linéaire $y' = A(t)y$. On définit leur déterminant wronskien $w(t) = \det(y_1(t), \dots, y_n(t))$. Alors $w'(t) = \mathrm{Tr}(A(t))w(t)$. De plus si A est constante alors on a $\det(\exp(tA)) = \exp(t\,\mathrm{Tr}(A))$.

Application 24. On se place sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
i) $\mathcal{GL}_n(\mathbb{K})$ est un ouvert de $\mathcal{M}_n(\mathbb{K})$. De plus, $\mathcal{GL}_n(\mathbb{R})$ a deux composantes connexes,
ii) Deux matrices réelles semblables sur $\mathbb{C}$ sont semblables sur $\mathbb{R}$.

III. B. Changement de variables

[Gou08, §5.4, p334–335]

Théorème 25. [Changement de variables]
Soit U, V *deux ouverts de* $\mathbb{R}^n$ *et* ϕ *un* $\mathcal{C}^1$*-difféomorphisme de* U *sur* V. *Alors pour toute fonction borélienne* $f : V \longrightarrow \mathbb{R}_+$, *on a :*

$$\int_V f(v)dv = \int_U f(\phi(u))\,|J_\phi(u)|\,du \quad \text{où} \quad J_\phi(u) = \det(d\,\phi_u)$$

Application 26. [Passage en coordonnées polaires]
Pour $f : \mathbb{R}^2 \longrightarrow \mathbb{R}_+$ borélienne, on a $\int_{\mathbb{R}^2} f(x,y)dxdy = \int_{\mathbb{R}_+^* \times]-\pi,\pi[} f(r\cos(\theta), r\sin(\theta))rdrd\theta$.

IV. Applications des déterminants en algèbre

IV. A. Polynôme caractéristique

[Gou09, §4.1/4.2, p162/176] [BMP05, §4.3.3/4.6, p179/217]

REMARQUE 27. On étend la formule explicite du Corollaire 4 à une matrice à coefficients dans un anneau A quelconque (le déterminant est un polynôme). Si A est intègre, les propriétés du déterminant restent vraies car A se plonge dans $\mathrm{Frac}(A)$.

DÉFINITION 28. [POLYNÔME CARACTÉRISTIQUE]
On définit le polynôme caractéristique de $A \in \mathcal{M}_n(\mathbb{K})$ par $\chi_A(X) = \det(XI_n - A)$.
On définit le polynôme caractéristique de $f \in \mathcal{L}(E)$ comme le polynôme caractéristique d'une matrice de f dans n'importe quelle base de E.

APPLICATION 29.
- Les valeurs propres de A sont les racines de χ_A,
- L'ensemble des matrices nilpotentes est fermé dans $\mathcal{M}_n(\mathbb{K})$,
- Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on a $\chi_{AB} = \chi_{BA}$.

IV. B. Systèmes linéaires

[Gou09, §3.5, p137–138] [Rom17, p547–548]

Soient p et q deux entiers et $A = (a_{i\,j})_{1\leq i\leq p,\ 1\leq j\leq q} \in \mathcal{M}_{p\,q}(\mathbb{K})$. On s'intéresse à la résolution du système $(\mathscr{S}_B) \quad AX = B$, d'inconnue $X \in \mathcal{M}_{q\,1}(\mathbb{K})$ et de paramètre $B \in \mathcal{M}_{p\,1}(\mathbb{K})$.

THÉORÈME 30. *$\mathrm{rg}(A)$ est l'ordre du plus grand mineur extrait de A qui est non nul.*

EXEMPLE 31. Soit la matrice $M = \begin{pmatrix} a & 2 & -1 & b \\ 3 & 0 & 1 & -4 \\ 5 & 4 & -1 & 2 \end{pmatrix}$ où a et b sont des paramètres réels.
Alors $\mathrm{rg}(M) \geq 2$ et on a $\mathrm{rg}(M) = 2 \iff (a,b) = (1,3)$. [Gri15, §4, p136]

THÉORÈME 32. [SYSTÈME DE CRAMER]
Lorsque $p = q$, alors $(\mathscr{S}_B)$ admet une unique solution pour tout paramètre B si et seulement si $\det(A) \neq 0$. Dans ce cas, la solution X_B de $(\mathscr{S}_B)$ est le vecteur de coordonnées :

$$\forall i \in [\![1,p]\!], x_i = \frac{\det(A_1,\dots,A_{i-1},B,A_{i+1},\dots,A_n)}{\det(A)}$$

V. Applications des déterminants en géométrie

V. A. Volume d'un parallélépipède

[BMP05, §4.4.1, p184] [Gri15, p127]

On munit $\mathbb{R}^n$ de sa base canonique. Pour $n = 2$, on a :

THÉORÈME 33. [AIRE D'UN PARALLÉLOGRAMME] **[voir annexe]**
Soit $\mathcal{A}(v,w)$ l'aire du parallélogramme engendré par v et w. Alors $\mathcal{A}(v,w) = |\det(v,w)|$.

On peut généraliser en dimension quelconque :

THÉORÈME 34. [VOLUME D'UN PARALLÉLÉPIPÈDE]
Soient $v_1,\dots,v_n$ des vecteurs de $\mathbb{R}^n$. En notant $\mathcal{V}(v_1,\dots,v_n)$ le volume du parallélépipède engendré par les vecteurs $v_1,\dots,v_n$. Alors $\mathcal{V}(v_1,\dots,v_n) = |\det(v_1,\dots,v_n)|$.

V. B. Déterminant de GRAM et inégalité de HADAMARD

[Gou09, §5.4, p262–263] [Rom17, §17.4.7, p560]

Soit $(E, \langle . \mid . \rangle)$ un espace préhilbertien (réel ou complexe).

DÉFINITION 35. [MATRICE ET DÉTERMINANT DE GRAM]
Soient $x_1,\dots,x_n$ des vecteurs de E. On appelle matrice de GRAM de $x_1,\dots,x_n$ la matrice $M_G(x_1,\dots,x_n) = (\langle x_i \mid x_j \rangle)_{1\leq i,j\leq n}$ et déterminant de GRAM de $x_1,\dots,x_n$ le déterminant de la matrice de GRAM, noté $G(x_1,\dots,x_n)$.

THÉORÈME 36. [DISTANCE À UN SOUS-ESPACE VECTORIEL]
Soit F un sous-espace vectoriel de dimension finie n de E, muni d'une base $(e_1,\dots,e_n)$. 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 37. [INÉGALITÉS DE HADAMARD] **[voir annexe]**
(i) Soient $x_1,\dots,x_n$ des vecteurs de E. Alors $G(x_1,\dots,x_n) \leq \prod_{i=1}^n \|x_i\|^2$.
(ii) Soient $x_1,\dots,x_n$ des vecteurs de $\mathbb{C}^n$. Alors $|\det(x_1,\dots,x_n)| \leq \prod_{i=1}^n \|x_i\|_2$, où $\|.\|_2$ désigne la norme hermitienne standard sur $\mathbb{C}^n$.
Dans les deux points, on a égalité si et seulement si la famille $\{x_i\}_{1\leq i\leq n}$ est orthogonale ou l'un des vecteurs est nul.

APPLICATION 38. Interprétation géométrique de l'inégalité de HADAMARD dans $\mathbb{R}^n$.

ANNEXE

* Exemple 17 : illustration des opérations élémentaires sur le déterminant de VANDERMONDE

$$V_{1,n} = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} \qquad V_{2,n} = \begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & a_n & \cdots & a_n^{n-2} \end{vmatrix}$$

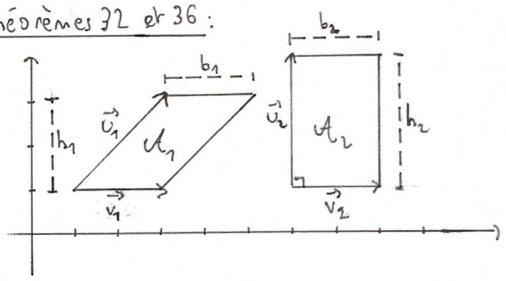
On fait $C_n \leftarrow C_n - a_1 C_{n-1}$, $C_{n-1} \leftarrow C_{n-1} - a_1 C_{n-2}$, etc ...

$$V_{1,n} = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & a_2-a_1 & a_2^2-a_1a_2 & \cdots & a_2^{n-1}-a_1a_2^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n-a_1 & a_n^2-a_1a_n & \cdots & a_n^{n-1}-a_1a_n^{n-2} \end{vmatrix}$$ prop 8.iii)

$$= \begin{vmatrix} a_2-a_1 & a_2^2-a_1a_2 & \cdots & a_2^{n-1}-a_1a_2^{n-2} \\ \vdots & \vdots & & \vdots \\ a_n-a_1 & a_n^2-a_1a_n & \cdots & a_n^{n-1}-a_1a_2^{n-2} \end{vmatrix}$$ développement selon ligne 1 (thm 12)

$$= (a_2-a_1)\cdots(a_n-a_1)\, V_{2,n}$$ linéarité selon les lignes (déf 3 et prop 8.i))

* Théorèmes 32 et 36 :



$$b_i \times h_i = \mathcal{A}_i = |\det(\vec{v}_i, \vec{v}_i)|$$

† interprétation de l'inégalité de HADAMARD.

SPEECH

Je vais vous présenter la leçon intitulée « Déterminant. Exemples et applications. ». Pourquoi étudie-t-on les déterminants ? Il y a deux motivations principales : d'un côté l'aspect pratique du déterminant (caractérisations simples de la liberté, méthodes de calculs nombreuses) et de l'autre le fait qu'il possède de nombreuses applications (on pense à l'étude de systèmes linéaires, d'endomorphismes, etc). Cela rend donc cet outil puissant.
Avant de revenir à ses applications, commençons par le définir. Dans la première partie on se place sur un corps $\mathbb{K}$ et on considère un $\mathbb{K}$-espace vectoriel E de dimension finie n. On observe que les formes n-linéaires alternées de E forment un espace vectoriel de dimension 1, ce qui permet de définir le déterminant d'une famille de vecteurs dans une base $\mathcal{B}$ comme l'unique forme n-linéaire alternée qui vaut 1 sur cette base. On a de plus une formule explicite dépendant des coefficients. On définit également le déterminant d'une matrice à coefficients dans $\mathbb{K}$ et d'un endomorphisme de $\mathcal{L}(E)$. La n-linéarité et le caractère alterné donnent alors des premiers résultats ($\det(AB) = \det(A)\det(B)$, stabilité par ajouts d'une combinaison linéaire de colonnes et surtout condition d'inversibilité d'une matrice) qui ouvrent la voie à des méthodes explicites de calculs de déterminants, comme le développement d'un déterminant par rapport à une ligne ou une colonne. Ce développement est en général intéressant pour des matrices plutôt creuses (ou pour obtenir des relations de récurrence), mais dans la pratique ce sont les déterminants de matrices triangulaires ou triangulaires par blocs qui sont les plus simples à calculer, c'est pour cela qu'on essaye de s'y ramener via la méthode du pivot de Gauss qui transforme une matrice en matrice triangulaire. On peut citer des applications classiques de ces méthodes (Vandermonde, circulant, Cauchy).
Donc les méthodes de calculs sont nombreuses et variées, ce qui tombe bien parce qu'il y a plein de domaines d'applications du déterminant, c'est l'objet de la suite de la leçon. Tout d'abord en analyse, on remarque que l'application $\det$ est un polynôme et est donc $\mathcal{C}^\infty$, l'expression de sa différentielle permet par exemple l'étude du wronskien d'un système de solutions d'une équation différentielle, ce qui constitute mon premier développement. En théorie de l'intégration, le déterminant joue un rôle fondamental dans la formule du changement de variables. Ensuite en algèbre, on peut étudier le polynôme caractéristique d'une matrice A défini comme $\det(XI_n - A)$. Cette définition est possible puisque le déterminant est un polynôme et ne fait pas intervenir d'inverses donc on peut le définir sur un anneau. Lorsque cet anneau est intègre, on conserve les propriétés vues précédemment. Ce polynôme caractéristique contient notamment des informations sur les valeurs propres de A. Toujours concernant l'étude d'une matrice, on peut s'intéresser à la résolution d'un système de type $AX = B$. Les formules de Cramer donnent alors la solution explicite unique dans le cas où $\det(A) \neq 0$. Enfin, on peut aussi souligner le rôle du déterminant en géométrie. Le déterminant de n vecteurs dans la base canonique de $\mathbb{R}^n$ s'interprète en effet comme le volume du parallélépipède engendré par ses n vecteurs. Plus généralement, dans un espace pré-hilbertien E, on peut définir le déterminant de Gram qui va être relié à la distance d'un point à un sous-espace vectoriel de E. Ce déterminant permet de démontrer l'inégalité de Hadamard, qui, dans le cas de $\mathbb{R}^n$, s'interprète comme le fait que le volume d'un parallélépipède de longueurs de côtés fixés est maximisé lorsqu'il est un rectangle, ou un hyperrectangle. Cela fait l'object de mon deuxième développement.

QUESTIONS

Q Quelle est l'application principale du procédé d'orthogonalisation de Gram-Schmidt ?
R L'existence d'une base orthonormée.
Q Calculs de déterminants dans $\mathcal{M}_n(\mathbb{Z})$. Liens entre $\mathcal{M}_n(\mathbb{Z})$, $\mathcal{M}_n(\mathbb{Q})$ et $\mathcal{M}_n(\mathbb{Z}/n\mathbb{Z})$.
Q Calculer $\det((i \wedge j)_{i\,j})$.
Q Calculer le déterminant de l'application $M \longmapsto M^\top$.

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Gri15] J. Grifone : *Algèbre linéaire*. Cépaduès, 5ème édition, 2015.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

153 POLYNÔMES D'ENDOMORPHISME EN DIMENSION FINIE. RÉDUCTION D'UN ENDOMORPHISME EN DIMENSION FINIE. APPLICATIONS.

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.
Soit $f \in \mathcal{L}(E)$. Pour $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$, on définit $P(f) = \sum_{k=0}^{p} a_k f^k \in \mathcal{L}(E)$.

I. Polynômes d'endomorphisme

I. A. L'algèbre $\mathbb{K}[f]$ et polynôme minimal [MM16, ChI/IV]

Définition 1. [POLYNÔME MINIMAL] L'application $\varphi_f : \mathbb{K}[X] \longrightarrow \mathcal{L}(E), P \longmapsto P(f)$ est un morphisme d'algèbres. Son noyau, l'ensemble des polynômes annulateurs de f, est un idéal de $\mathbb{K}[f]$ principal donc est engendré par un unique polynôme unitaire π_f appelé polynôme minimal de f. Son image $\mathbb{K}[f]$ est une sous-algèbre de $\mathcal{L}(E)$.

Remarque 2. Le noyau est non réduit à $\{0\}$ puisque $\mathcal{L}(E)$ est de dimension infinie n^2. En dimension finie, c'est faux (considérer par exemple l'opérateur de dérivation).

Proposition 3. *On a $\dim(\mathbb{K}[f]) = \deg(\pi_f)$.*

Exemple 4. Polynômes minimaux usuels [VOIR ANNEXE]

Remarque 5. Se donner $f \in \mathcal{L}(E)$ revient à se donner sa matrice M dans une base de E. On a donc les mêmes résultats pour les matrices, et si M est une matrice de f dans une certaine base, on a $\pi_f = \pi_M$ (donc deux matrices semblables ont même polynôme minimal).

I. B. Polynôme caractéristique [MM16, ChV/VII] [Gou09, Ch4] [BMP05, §4.6, p217]

Définition 6. [POLYNÔME CARACTÉRISTIQUE]
On définit le polynôme caractéristique de $M \in \mathcal{M}_n(\mathbb{K})$ par $\chi_M(X) = \det(XI_n - M)$.

Exemple 7. En dimension 2, on a $\chi_M = X^2 - \mathrm{Tr}(M)X + \det(M)$ et $\chi_M(M) = 0$. En dimension quelconque, si $\chi_M = \sum_{k=0}^{n} a_k X^k$, on a $a_n = 1$, $a_{n-1} = -\mathrm{Tr}(M)$ et $a_0 = (-1)^n \det(M)$.

Proposition 8. *Deux matrices semblables ont même polynôme caractéristique. On peut donc définir le polynôme caractéristique de f.*

Exemple 9. Polynômes caractéristiques usuels [VOIR ANNEXE]

Proposition 10. *Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on a $\chi_{AB} = \chi_{BA}$.*

Proposition 11. *Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $M \longmapsto \chi_M$ est continue.*

Application 12. L'ensemble des matrices nilpotentes est fermé pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I. C. Polynômes d'endomorphisme et sous-espaces stables [MM16, ChI/IV]

Proposition 13. *Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\ker(f)$ et $\mathrm{Im}(f)$ sont stables par g. En particulier $\ker(P(f))$ et $\mathrm{Im}(P(f))$ sont stables par f pour tout $P \in \mathbb{K}[X]$.*

Lemme 14. [LEMME DES NOYAUX]
Soit $(P_i)_{1 \leq i \leq r}$ une famille de polynômes deux à deux premiers entre eux. Alors en posant $P = \prod_{i=1}^{r} P_i$, on a $\ker(P(f)) = \bigoplus_{i=1}^{r} \ker(P_i(f))$. De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Application 15. Soit P annulateur de f. Si $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ où les $(P_i)_{1 \leq i \leq r}$ sont deux à deux premiers, alors on a la décomposition en sous-espaces f-stables $E = \bigoplus_{i=1}^{r} \ker(P_i^{\alpha_i}(f))$.

Exemple d'un projecteur, d'une symétrie

I. D. Liens entre polynômes et valeurs propres [MM16, ChV/VII]

Proposition 16. *Soit F un sous-espace f-stable de E. On pose f_F l'endomorphisme induit sur F par f. Alors :*

$$\pi_{f_F} \mid \pi_f \qquad \text{et} \qquad \chi_{f_F} \mid \chi_f$$

Si $E = \bigoplus_{i=1}^{r} E_i$ est une décomposition en sous-espaces stables de E, alors $\chi_f = \prod_{i=1}^{r} \chi_{f_{E_i}}$.

Exemple 17. Ce dernier résultat n'est pas vrai pour le polynôme minimal ! Si $f = \mathrm{Id}_E$ et $(e_1, \dots, e_n)$ est une base de E, alors $E = \bigoplus_{i=1}^{n} \mathrm{Vect}(e_i)$, $\pi_{f_{\mathrm{Vect}(e_i)}} = X - 1$ mais $\pi_f = X - 1$.

Proposition 18. [LIENS ENTRE VALEURS PROPRES]
$\lambda \in \mathbb{K}$ est une valeur propre de f si et seulement si $\chi_f(\lambda) = 0$ si et seulement si $\pi_f(\lambda) = 0$.

Exemple 19. Pour $P = X^n + \sum_{k=0}^{n-1} a_k X^k$, on définit $\mathcal{C}(P) = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$
la matrice compagnon de P. On a alors $\chi_{\mathcal{C}(p)} = \pi_{\mathcal{C}(p)} = P$.

Théorème 20. [Théorème de Cayley-Hamilton]
χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f \mid \chi_f$.

II. Application à la réduction d'endomorphismes

II. A. Trigonalisation et diagonalisation [MM16, ChVIII/IX/X] [Gou09, §4.4, p193]

Définition 21. [Multiplicités]
Soit $\lambda \in \mathbb{K}$ une valeur propre de f. On appelle :
- multiplicité géométrique de λ la dimension de $E_\lambda = \ker(f - \lambda \mathrm{Id})$, notée $m_g(\lambda)$,
- multiplicité algébrique de λ la multiplicité de λ en tant que racine de χ_f, notée $m_a(\lambda)$,
- multiplicité minimale de λ la multiplicité de λ en tant que racine de π_f, notée $m_m(\lambda)$.

Proposition 22. *On a $m_m(\lambda) \leq m_g(\lambda)$ et $m_a(\lambda) \leq m_g(\lambda)$.*

Définition 23. On dit que f est trigonalisable (resp. diagonalisable) s'l existe une base de E telle que la matrice de f dans cette base soit triangulaire (resp. diagonale).

Théorème 24. *f est trigonalisable si et seulement si χ_f est scindé si et seulement si π_f est scindé si et seulement si f admet un polynôme annulateur scindé.*

Exemple 25. Un endomorphisme nilpotent est trigonalisable. Dans une base adéquate, la matrice est même triangulaire supérieure puisque les valeurs propres d'un endomorphisme trigonalisable sont les coefficients diagonaux de sa matrice dans une base de trigonalisation.

Théorème 26. *f est diagonalisable si et seulement si π_f est scindé à racines simples ($m_m(\lambda) = 1$ pour λ valeur propre de f) si et seulement si f admet un polynôme annulateur scindé à racines simples si et seulement si $m_a(\lambda) = m_g(\lambda)$ pour toute valeur propre λ.*

Exemple 27. Un endomorphisme trigonalisable ayant des valeurs propres deux à deux distinctes ($m_g(\lambda) = 1$) est diagonalisable.

Exemple 28. Si A est diagonalisable, la matrice $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ l'est aussi, mais la matrice $\begin{pmatrix} A & A \\ 0 & A \end{pmatrix}$ ne l'est que si de plus A est nulle.

Théorème 29. [Décomposition de Dunford]
Supposons f de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n.
De plus, d et n sont des polynômes en f.

Application 30. Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \dots, \mu_n$ les n racines de χ_M (par nécessairement distinctes). Soit (D, N) la décomposition de Dunford de M. Soit $P \in \mathcal{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \dots, \mu_n)$ soit diagonale. Alors on a :

$$\exp(A) = P\,\mathrm{diag}(\mathrm{e}^{\mu_1}, \dots, \mathrm{e}^{\mu_n})P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}$$

Exemple 31.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = I_3 + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\exp\left(\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} \mathrm{e} & \mathrm{e} & \mathrm{e}/2 \\ 0 & \mathrm{e} & \mathrm{e} \\ 0 & 0 & \mathrm{e} \end{pmatrix}$$

Application 32. Résolution de l'équation différentielle $Y' = AY$ pour $A \in \mathcal{M}_n(\mathbb{C})$.

II. B. Décompositions en sous-espaces stables [MM16, ChX/XI]

Théorème 33. [Décomposition de Jordan]
Supposons f de polynôme caractéristique scindé. Notons $\lambda_1, \dots, \lambda_r$ ses valeurs propres. Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,\ell_j}$ pour $j \in [\![1, r]\!]$ tels que dans une certaine base $\mathcal{B}$ de E, $M_{\mathcal{B}}(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{\substack{1 \leq j \leq r \\ 1 \leq k \leq \ell_j}}$, où $B_{j,k} = \lambda_j I_{d_{j,k}} + J_{d_{j,k}}$ avec $J_d = \mathcal{C}(X^d) \in \mathcal{M}_d(\mathbb{K})$.

Exemple 34. Dans le cas d'un endomorphisme nilpotent, la donnée de la décomposition de Jordan (c'est-à-dire $d_1 \geq \cdots \geq d_\ell$) équivaut à la donnée du tableau de Young de l'endomorphisme. Voir des exemples en annexe. Lecture de l'image, du noyau de l'endomorphisme, etc.

Application 35. Deux endomorphismes scindés sont semblables si et seulement si ils ont même décomposition de Jordan.

Définition 36. **[Polynôme minimal local, endomorphisme cyclique]**
Soit $x \in E$. $\varphi_{f,x} : \mathbb{K}[X] \longrightarrow E, P \longmapsto P(f)(x)$ est un morphisme d'espaces vectoriels. Son noyau est un idéal de $\mathbb{K}[f]$ engendré par un unique polynôme unitaire $\pi_{f,x}$ appelé polynôme minimal local de f en x. On note $E_{f,x}$ son image.
Lorsque $E = E_{f,x}$ pour au moins un $x \in E$, on dit que f est cyclique.

Proposition 37. *Pour tout $x \in E$, $E_{f,x}$ est un sous-espace f-stable et $\mathcal{B}_x = (x, f(x), \dots, f^p(x))$ où $p = \dim(E_{f,x})$ en est une base.*

Exemple 38. En dimension 2, un endomorphisme est soit cyclique soit une homothétie.

Proposition 39. *Il existe $x \in E$ tel que $\mu_{f,x} = \mu_f$. Pour un tel x, $E_{f,x}$ admet alors un supplémentaire f-stable.*

Théorème 40. **[Décomposition de Frobenius]**
Il existe une unique suite finie de polynômes unitaires $P_1, \dots, P_r$, appelés invariants de similitude et une décomposition $E = \bigoplus_{i=1}^r E_i$ en sous-espaces stables de E telles que :
- *$P_{i+1} \mid P_i$ pour tout $1 \leq i \leq r-1$,*
- *f_{E_i} est cyclique de polynôme minimal P_i pour tout $1 \leq i \leq r$.*

Remarque 41. f est quelconque ici (contrairement à la décomposition de Jordan). On a $P_1 = \pi_f$ et $\prod_{i=1}^r P_i = \chi_f$.

Application 42. Deux endomorphismes sont semblables si et seulement si ils ont les mêmes invariants de similitudes.

Exemple 43. La réduite de $\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ est $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$.

III. Calculs pratiques avec des polynômes d'endomorphismes

III. A. Calculs d'inverses, de puissances

[MM16, §I.4, p5]

Proposition 44. *Si f admet un polynôme annulateur $P = \sum_{k=0}^p a_k X^k$ tel que $a_0 = P(0) \neq 0$, alors f est inversible et $f^{-1} = -\frac{1}{a_0} \sum_{k=0}^p a_k f^{k-1} \in \mathbb{K}[f]$.*

Corollaire 45. *f est inversible si et seulement si 0 n'est pas valeur propre de π_f.*

Proposition 46. *Pour $P \in \mathbb{K}[X]$, on a $P(f) = R(f)$ si R est le reste dans la division euclidienne de P par n'importe quel polynôme annulateur de f.*

Application 47. Si $p = \deg(\pi_f)$, on a $f^m \in \mathrm{Vect}((f^k)_{0 \leq k < p})$.

Exemple 48. Si $P = (X-a)(X-b)$ annule f (avec $a, b \in \mathbb{C}$ distincts), alors :

$$\forall m \in \mathbb{N}, f^m = \frac{a^m - b^m}{a-b} f + \frac{ba^m - ab^m}{b-a} \mathrm{Id}_E$$

III. B. Application aux matrices stochastiques

[MM16, ChXIV]

Définition 49. On dit que $Q \in \mathcal{M}_m(\mathbb{R})$ est stochastique si ses coefficients sont à valeurs dans $[0,1]$ et si pour tout $i \in [\![1, m]\!]$, on a $\sum_{j=1}^m q_{i,j} = 1$.

Application 50. Soit $(X_n)_{n \in \mathbb{N}}$ une chaîne de Markov sur $E = [\![1, m]\!]$ de mesure initiale ν_0 et de noyau de transition la matrice stochastique Q. Si ν_n est la loi de X_n, alors $\nu_n = \nu_0 Q^n$ et donc si l'on a un polynôme annulateur de Q, on peut simplifier le calcul de ν_n.

Définition 51. On dit que $(X_n)_{n \in \mathbb{N}}$ (ou Q) est irréductible si $\forall i, j \in E, \exists n \in \mathbb{N} \mid q_{i,j}^n > 0$.

Rajouter quelques lemmes …

Théorème 52. **[Théorème de Perron-Frobenius]**
Soit A est une matrice positive irréductible, alors $\rho(A) = \max_{\lambda \in \mathrm{Sp}(A)} |\lambda|$ est une valeur propre de A, de sous-espace propre de dimension 1 admettant un vecteur propre positif.

Application 53. On a $\rho(Q) = 1$ donc si Q est irréductible, $Q^\top$ admet un unique vecteur propre ν associé à 1 qui est l'unique mesure invariante par Q, c'est-à-dire telle que $\nu Q = \nu$.

Application 54. Si $(X_n)_{n \in \mathbb{N}}$ est une chaîne de Markov sur $E = [\![1, m]\!]$ de mesure initiale ν_0 et de noyau de transition la matrice stochastique Q irréductible, alors elle admet une unique mesure invariante, c'est-à-dire une mesure ν telle que $\nu^n = \nu$ si $\nu_0 = \nu$.

ANNEXE

Polynômes minimaux et caractéristiques usuels
Soit F un sous-espace vectoriel de dimension $1 \leq p \leq n-1$.

f	π_f	χ_f
nilpotent d'indice k	X^k	X^n
homothétie de rapport λ	$X-\lambda$	$(X-\lambda)^n$
projecteur sur F	X^2-X	$(X-1)^p X^{n-p}$
symétrie par rapport à F	X^2-1	$(X-1)^p(X+1)^{n-p}$

Tableaux de Young
Chaîne réductible/irréductible, périodique/apériodique

QUESTIONS

Q Que nous dit la décomposition de Dunford ?

R À un nilpotent près, un endomorphisme trigonalisable est diagonalisable.

Q A-t-on existence et/ou unicité de la décomposition de Dunford pour un endomorphisme non trigonalisable ?

Q Montrer que $\deg(\mu_A) \leq 1 + \mathrm{rg}(A)$.

Q Si $AB - BA = B$, que peut-on dire de B ?

R On montre que $AB^k - B^k A = kB^k$ pour tout k. On en déduit que $\mathrm{Tr}(B^k) = 0$ pour tout k, et donc que B est nilpotent.

Q Trouver A telle que la matrice $D = \begin{pmatrix} A & A \\ 0 & A \end{pmatrix}$ soit diagonalisable.

R S'il existe un polynôme scindé à racines simples annulateur de D, alors il annule A et donc A est diagonalisable. On vérifie qu'alors seule la matrice nulle convient …

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[MM16] R. Mansuy et R. Mneimné : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

154 SOUS-ESPACES STABLES PAR UN ENDOMORPHISME OU UNE FAMILLE D'ENDOMORPHISMES D'UN ESPACE VECTORIEL DE DIMENSION FINIE. APPLICATIONS.

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.
Soit $f \in \mathcal{L}(E)$.

I. Sous-espaces stables par un endomorphisme

I. A. Définitions et premières propriétés [MM16, ChII]

Définition 1. F sous-espace vectoriel de E est dit f-stable si $f(F) \subset F$. On note alors $f_F : F \longrightarrow F, x \longmapsto f(x)$ l'induit de f sur F.

Proposition 2. *Soit $g \in \mathcal{L}(E)$ commutant avec f. Alors $\mathrm{Im}(f), \ker(f)$ et $\ker(P(f))$ pour tout $P \in \mathbb{K}[X]$ sont g-stables.*

Exemple 3. En particulier $E_\lambda = \ker(f - \lambda \mathrm{id}_E)$ est f-stable pour tout $\lambda \in \mathbb{K}$. E_λ est le sous-espace propre associé à λ. S'il est non réduit à $\{0\}$, on dit que λ est valeur propre de f.

Exemple 4. Soit p un projecteur de $\mathcal{L}(E)$ et F un sous-espace p-stable. Alors F est somme directe d'un sous-espace de $\ker(p)$ et d'un sous-espace de $\mathrm{Im}(p)$.

Exemple 5. Soit $g \in \mathrm{Aut}(E)$ et F f-stable. Alors $g(F)$ est stable pour $g \circ f \circ g^{-1}$.

Proposition 6. *Si F est f-stable, alors $\pi_{f_F} \mid \pi_f$ et $\chi_{f_F} \mid \chi_f$.*

I. B. Sous-espaces cycliques [MM16, ChI/II]

Soit $x \in E$.

Définition 7. [polynôme minimal local, sous-espace cyclique]
L'application $\varphi_{f,x} : \mathbb{K}[X] \longrightarrow E, P \longmapsto P(f)(x)$ est un morphisme d'espaces vectoriels. Son noyau est un idéal de $\mathbb{K}[f]$. Il est engendré par un unique polynôme unitaire $\pi_{f,x}$ appelé polynôme minimal local de f en x. On note $E_{f,x}$ son image.

Proposition 8. *$E_{f,x}$ est f-stable et $E_{f,x} = \mathbb{K}[f](x) = \mathrm{Vect}(\mathcal{B}_x)$ où $d = \deg \pi_{f,x}$ et $\mathcal{B}_x = \{x, f(x), \dots, f^{d-1}(x)\}$ est une base de $E_{f,x}$.*

Définition 9. On dit que f est cyclique s'il existe $x \in E$ tel que $E = E_{f,x}$.

Exemple 10. Si $n = 2$, tout endomorphisme est soit cyclique, soit une homothétie.

Proposition 11. *Supposons f cyclique et soit x tel que $E = E_{f,x}$.*
Alors $M_{\mathcal{B}_x}(f) = \mathcal{C}(\pi_{f,x}) = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$ où $\pi_{f,x} = X^n + \sum_{k=0}^{n-1} a_k X^k$.
C'est une matrice appelée matrice compagnon de $\pi_{f,x}$. On a alors $\chi_f = \pi_f = \pi_{f,x}$.

Proposition 12. *Si f est cyclique, l'ensemble des endomorphismes commutants avec f est $\mathbb{K}[f]$.*

Théorème 13. [théorème de Cayley-Hamilton]
χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f \mid \chi_f$.

II. Détermination de sous-espaces stables et réduction

II. A. Lemme des noyaux et décomposition de Dunford [MM16, ChIV]

Lemme 14. [lemme des noyaux]
Soit $(P_i)_{1 \le i \le r}$ une famille de polynômes deux à deux premiers entre eux. Alors en posant $P = \prod_{i=1}^r P_i$, on a $\ker(P(f)) = \bigoplus_{i=1}^r \ker(P_i(f))$. De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Application 15. Il existe $x \in E$ tel que $\pi_{f,x} = \pi_f$. Donc si $\deg(\pi_f) = n$, alors f est cyclique.

Théorème 16. [décomposition de Dunford]
Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n.
De plus, d et n sont des polynômes en f.

Application 17. Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \dots, \mu_n$ les n racines de χ_M (comptées sans leur multiplicité). Soit (D, N) la décomposition de Dunford de M. Soit $P \in \mathcal{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \dots, \mu_n)$ soit diagonale. Alors on a $\exp(A) = P \,\mathrm{diag}(\mathrm{e}^{\mu_1}, \dots, \mathrm{e}^{\mu_n}) P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}$.

Exemple 18.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = I_3 + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\exp\left(\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} \mathrm{e} & \mathrm{e} & \mathrm{e}/2 \\ 0 & \mathrm{e} & \mathrm{e} \\ 0 & 0 & \mathrm{e} \end{pmatrix}$$

Exemple 19. Un endomorphisme nilpotent et diagonalisable est nul.

Application 20. Résolution de l'équation différentielle $Y' = AY$ pour $A \in \mathcal{M}_n(\mathbb{C})$.

II. B. Utilisation de la dualité dans la recherche de sous-espaces propres

[Rom17, Ch21, p672]

Définition 21. Pour $A \subset E$ on définit $A^\perp = \{\varphi \in E^* \,|\, \forall x \in A, \varphi(x) = 0\}$ et pour $B \subset E^*$, on définit $B^\circ = \{x \in E \,|\, \forall \varphi \in B, \varphi(x) = 0\}$.

Définition 22. On définit ${}^tf : E^* \longrightarrow E^*, \varphi \longmapsto \varphi \circ f$.

Proposition 23. *Si $\mathcal{B}^*$ est la base duale de $\mathcal{B}$, on a $M_{\mathcal{B}^*}({}^tf) = M_{\mathcal{B}}(f)^\top$.*

Proposition 24. *F est f-stable si et seulement si $F^\perp$ est ${}^tf$-stable.*

Proposition 25. *Soit $x \in E$ tel que $\pi_{f,x} = \pi_f$. Alors $E_{f,x}$ admet un supplémentaire f-stable.*

II. C. Sous-espaces stables et trigonalisabilité / diagonalisabilité

[MM16, ChVIII–IX]

Théorème 26. *f est trigonalisable si et seulement si χ_f est scindé si et seulement si π_f est scindé si et seulement si f admet un polynôme annulateur scindé.*

Exemple 27. [Endomorphisme trigonalisable]
Si f est trigonalisable et $(e_1, \dots, e_n)$ est une base de trigonalisation (supérieure), alors $F_k = \mathrm{Vect}(e_1, \dots, e_k)$ est f-stable.

Théorème 28. *f est diagonalisable si et seulement si π_f est scindé à racines simples si et seulement si f admet un polynôme annulateur scindé à racines simples.*

Proposition 29. *Si f est diagonalisable, soit $\mathrm{Sp}(f)$ l'ensemble de ses valeurs propres. Alors l'ensemble des sous-espaces stables de f sont les $\oplus_{\lambda \in \mathrm{Sp}(f)} F_\lambda$ où F_λ est un sous-espace de E_λ.*

Application 30. Sous-espaces propres d'un projecteur, d'une symétrie.

II. D. Autour des nilpotents et de la décomposition de Jordan

[MM16, ChX] [Rom17, Ch21, p672–675]

Application 31. [Endomorphisme nilpotent]
Si f est nilpotent d'indice n alors les sous-espaces stables de f sont exactement les $(\ker(f^k))_{0 \leq k \leq n}$.

Lemme 32. [Décomposition de Jordan d'un endomorphisme nilpotent]
Supposons f nilpotent. Il existe des entiers $d_1 \geq \cdots \geq d_\ell$ tels que dans une certaine base $\mathcal{B}$ de E, $M_{\mathcal{B}}(f)$ soit diagonale par blocs avec les blocs $(J_{d_k})_{1 \leq k \leq \ell}$ où $J_d = \mathcal{C}(X^d)$.

Théorème 33. [Décomposition de Jordan]
Supposons f de polynôme caractéristique scindé (trigonalisable). Notons $\lambda_1, \dots, \lambda_r$ ses valeurs propres distinctes. Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,\ell_j}$ pour $j \in [\![1, r]\!]$ tels que dans une certaine base $\mathcal{B}$ de E, $M_{\mathcal{B}}(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{\substack{1 \leq j \leq r \\ 1 \leq k \leq \ell_j}}$, où $B_{j,k} = \lambda_j I_{d_{j,k}} + J_{d_{j,k}}$.

Exemple 34. $\begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 2 & 0 & -1 \\ 0 & 2 & 2 & 3 \end{pmatrix}$ est semblable à $\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$.

Théorème 35. *Deux endomorphismes trigonalisables sont semblables si et seulement si ils ont même réduction de Jordan.*

Exemple 36. On déduit de la réduction de Jordan tout un ensemble de sous-espaces stables. Le cas d'un nilpotent est traité en annexe, en utilisant le tableau de Young associé à l'endomorphisme. Le cas général s'en déduit.

II. E. Décomposition de Frobenius [MM16, ChXI]

Théorème 37. [Décomposition de Frobenius]
Il existe une unique suite finie de polynômes unitaires $P_1, \dots, P_s$, appelés invariants de similitude et une décomposition $E = \bigoplus_{i=1}^{s} E_i$ en sous-espaces stables de E tels que :
- *$P_{i+1} \mid P_i$ pour tout $1 \leq i \leq s-1$,*
- *f_{E_i} est cyclique de polynôme minimal P_i pour tout $1 \leq i \leq s$.*

Corollaire 38. *Dans des bases adéquates la matrice de f est diagonale par blocs avec pour blocs les matrices compagnons $(\mathcal{C}(P_i))_{1\leq i\leq s}$. On dit que c'est la forme réduite de f.*

Exemple 39. La réduite de $\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ est $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$.

III. Autres propriétés autour des sous-espaces stables

III. A. Co-trigonalisabilité et co-diagonalisabilité [MM16, CHVIII/IX]

Rappel 40. Les sous-espaces propres de f sont stables par tout endomorphisme commutant avec f.

Proposition 41. *Soit $(f_k)_{1\leq k\leq N}$ une famille d'endomorphismes trigonalisables commutant deux à deux. Alors il existe une base commune de trigonalisation (on dit que les $(f_k)_{1\leq k\leq N}$ sont co-trigonalisables).*

Application 42. Des endomorphismes trigonalisables commutant deux à deux possèdent au moins $n+1$ sous-espaces stables en commun.

Proposition 43. *Soit $\mathbb{K} = \mathbb{C}$. Soient $f, g \in \mathcal{L}(E)$ trigonalisables tels que $fg = 0$. Alors f et g sont co-trigonalisables.*

Proposition 44. *Soit $(f_k)_{1\leq k\leq N}$ une famille d'endomorphismes diagonalisables commutant deux à deux. Alors il existe une base commune de diagonalisation (on dit que les $(f_k)_{1\leq k\leq N}$ sont co-diagonalisables).*

Application 45. Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ diagonalisables. Alors $\Theta \in \mathcal{L}(\mathcal{M}_n(\mathbb{R}))$ définit par $\Theta(M) = AMB$ est diagonalisable.

Exemple 46. Soit G un sous-groupe fini abélien de $\mathcal{GL}_n(\mathbb{C})$. Alors les éléments de G sont co-diagonalisables, et donc G est conjugué à un sous-groupe de matrices diagonales.

Corollaire 47. *Si de plus chaque endomorphisme possède n valeurs propres distinctes, les sous-espaces stables sont les mêmes pour chaque endomorphisme.*

Exemple 48. Si les valeurs propres ne sont pas nécessairement distinctes, c'est faux : on peut considérer pour f_1 une homothétie et pour f_2 un endomorphisme diagonalisable qui n'est pas une homothétie.

III. B. Semi-simplicité [BMP05, §4.2.1, p158–161] [Gou09, §5.4, p224–226]

Définition 49. [Endomorphisme semi-simple]
f est dit semi-simple si tout sous-espace f-stable admet un supplémentaire f-stable.

Théorème 50. *f est semi-simple si et seulement si π_f est sans facteur carré.*

Application 51. Sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, f est semi-simple si et seulement si f est diagonalisable sur $\mathbb{C}$.

Exemple 52. Si f est nilpotente, alors f est semi-simple si et seulement si $f = 0$.

Exemple 53. Les rotations de $\mathbb{R}^2$ sont semi-simples.

Application 54. Supposons f semi-simple et soit F un sous-espace f-stable. Alors u_F et $\overline{u} : E/F \longrightarrow E/F$ sont aussi semi-simples.

ANNEXE

Lecture de sous-espaces stables sur un tableau de YOUNG

SPEECH

On veut illustrer le rôle des sous-espaces stables dans la théorie des endomorphismes : trouver des sous-espaces stables permet par exemple de simplifier l'étude en se restreignant à un sous-espace stable, cela va amener vers la réduction des endomorphismes.
Dans chaque partie, on se demande à quoi servent les sous-espaces stables, et comment les identifier.
D'abord, pour les endomorphismes cycliques, on a un vecteur dont le sous-espace stable minimal et l'espace tout entier, on va donc parcourir l'espace entièrement grâce à ce vecteur. Ces sous-espaces sont importants car ils permettent de montrer le théorème de CAYLEY-HAMILTON très important en théorie des endomorphismes.
Ensuite, l'idée de la réduction de JORDAN est d'obtenir des sous-espaces propres donnés par le lemme des noyaux via le polynôme caractéristique. Pour la décomposition de FROBENIUS, on s'intéresse aux sous-espaces cycliques associés aux x tel que $\pi_f = \pi_{f,\,x}$.
Enfin, on s'intéresse aux propriétés autour des sous-espaces propres et de la (co-)trigonalisabilité/diagonabilité. La trigonalisation revient par exemple à trouver une famille imbriquée de sous-espaces stables.

QUESTIONS

Q Soit f cyclique. Montrer qu'il y a un nombre fini de sous-espaces f-stables.

R Soit $x \in E$ tel que $E = E_{f,\,x}$. Fixons F un sous-espace f-stable et considérons $\{P \in \mathbb{K}[X] \mid P(f)(x) \in F\}$. Comme F est f-stable, il est facile de vérifier qu'il s'agit d'un idéal de $\mathbb{K}[X]$. Il est donc engendré par un unique polynôme unitaire Q. Si $y = Q(f)(x)$, on a $\mathbb{K}[f](y) \subset F$ par stabilité mais réciproquement, si $z = P(f)(x) \in F$, alors nécessairement $P = QR$ pour un R et donc $z = R(f)(y)$. Ainsi $F = E_{f,y}$ est cyclique. Comme $\pi_f(f)(x) = 0 \in F$, on remarque alors que $Q \mid \pi_f$, et on a donc une injection de l'ensemble des sous-espaces f-stables de E dans les polynômes unitaires diviseurs de π_f. Ainsi il y a un nombre fini de sous-espaces f-stables.

Q Qu'en est-il de la réciproque lorsque $\mathbb{K}$ est infini ?

R Soit f ayant un nombre fini de sous-espaces stables. Alors E ne peut être réunion de sous-espaces stables stricts de E. En effet, si $E = \cup_{i=1}^{k} E_i$ avec $E_1 \not\subset \cup_{i>1} E_i$. Prenons donc $x \in E_1 \setminus \cup_{i>1} E_i$ et $y \in \cup_{i>1} E_i \setminus E_1$. Pour tout $\lambda \in \mathbb{K}$, $y + \lambda x \notin E_1$ donc il existe i tel que $y + \lambda x \in E_i$. Comme $\mathbb{K}$ est infini, il existe $\lambda \neq \mu$ tels que $y + \lambda x, y + \mu x \in E_i$ pour un certain i. Alors $(\lambda - \mu)x = y + \lambda x - (y + \mu x) \in E_i$, donc $x \in E_i$, ce qui est absurde.
Notons maintenant $(F_i)_{1 \leq i \leq k}$ les sous-espaces stricts de E f-stables. Choisissons $x \notin \cup_i F_i$. Alors $G = \{x, f(x), \dots, f^{n-1}(x)\}$ est une famille libre sinon $\mathrm{Vect}(\{x, f(x), \dots, f^{n-2}(x)\})$ serait f stable et de dimension inférieure à $n - 2$, donc strictement inclus dans E donc égal à l'un des E_i, ce qui est faux par définition de x. Ainsi $\pi_{f,\,x}$ est de dimension n, et donc f est cyclique.

Q Soit f tel que tout sous-espace est f-stable. Que peut-on dire de f ?

R Les sous-espaces de dimension 1 sont f-stables donc chaque vecteur est vecteur propre. Puis pour $x, y \in E$ de valeur propre $\lambda_x \neq \lambda_y$, on a $\lambda_{x+y}(x+y) = f(x+y) = f(x)+f(y) = \lambda_x x + \lambda_y y$, donc comme (x, y) est libre on a $\lambda_x = \lambda_{x+y} = \lambda_y$, ce qui est absurde. Ainsi f est une homothétie.

Q Montrer la décroissance des sauts de dimension dans la suite des noyaux itérés.

R Plusieurs possibilités, on peut quotienter.

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[MM16] R. MANSUY et R. MNEIMNÉ : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

155 ENDOMORPHISMES DIAGONALISABLES EN DIMENSION FINIE.

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.
Soit $f \in \mathcal{L}(E)$.

I. Généralités

I. A. Eléments propres

[MM16, ChI/IV]

Définition 1. On dit que $\lambda \in \mathbb{K}$ est valeur propre de f si $E_\lambda = \ker f - \lambda \mathrm{id}_E$ est non réduit à $\{0\}$. E_λ est appelé sous-espace propre de f associé à λ et ses éléments non nuls sont les vecteurs propres associés à λ. On note $\mathrm{Sp}(f)$ l'ensemble des valeurs propres de f.

Proposition 2. *Les sous-espaces propres de f sont f-stables et en somme directe.*

Exemple 3. Supposons que $n = 3$ et qu'il existe une base $\mathcal{B} = (e_1, e_2, e_3)$ telle que :

$$M_{\mathcal{B}}(f) = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{pmatrix} \qquad \text{où } \alpha \neq \beta \in \mathbb{K}^2$$

Alors $\mathrm{Sp}(f) = \{\alpha, \beta\}$, $E_\alpha = \mathrm{Vect}(e_1)$, $E_\beta = \mathrm{Vect}(e_2, e_3)$ et $E = E_\alpha \oplus E_\beta$.

I. B. Polynômes d'endomorphismes

[MM16, ChI/IV]

Pour $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$, on pose $P(f) = \sum_{k=0}^{p} a_k f^k \in \mathcal{L}(E)$.

Définition 4. [Polynôme minimal]
L'application $\varphi_f : \mathbb{K}[X] \longrightarrow \mathcal{L}(E), P \longmapsto P(f)$ est un morphisme d'algèbres. Son noyau, l'ensemble des polynômes annulateurs de f, est un idéal de $\mathbb{K}[f]$ donc est engendré par un unique polynôme unitaire π_f appelé polynôme minimal de f.

Proposition 5. *On a $\dim(\mathbb{K}[f]) = \deg(\pi_f)$.*

Exemple 6. Polynômes minimaux usuels [voir annexe]

Remarque 7. Se donner un endomorphisme $f \in \mathcal{L}(E)$ revient à se donner sa matrice M dans une base de E. On a donc les mêmes résultats pour les matrices.

Proposition 8. *Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\ker(f)$ et $\mathrm{Im}(f)$ sont stables par g. En particulier $\ker(P(f))$ et $\mathrm{Im}(P(f))$ sont stables par f pour tout $P \in \mathbb{K}[X]$.*

Lemme 9. [Lemme des noyaux]
Soit $(P_i)_{1 \leq i \leq r}$ une famille de polynômes deux à deux premiers entre eux. Alors en posant $P = \prod_{i=1}^{r} P_i$, on a $\ker(P(f)) = \bigoplus_{i=1}^{r} \ker(P_i(f))$. De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Application 10. Soit P annulateur de f. Si $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ où les $(P_i)_{1 \leq i \leq r}$ sont deux à deux premiers, alors on a la décomposition en sous-espaces f-stables $E = \bigoplus_{i=1}^{r} \ker(P_i^{\alpha_i}(f))$.

I. C. Polynôme caractéristique

[MM16, ChV/VII] [Gou09, Ch4]

Définition 11. [Polynôme caractéristique]
On définit le polynôme caractéristique de $M \in \mathcal{M}_n(\mathbb{K})$ par $\chi_M(X) = \det(XI_n - M)$.

Proposition 12. *Deux matrices semblables ont même polynôme caractéristique. On peut donc définir le polynôme caractéristique de f.*

Exemple 13. En dimension 2, on a $\chi_M = X^2 - \mathrm{Tr}(M)X + \det(M)$ et $\chi_M(M) = 0$.
En dimension quelconque, si $\chi_M = \sum_{k=0}^{n} a_k X^k$, on a $a_n = 1$, $a_{n-1} = -\mathrm{Tr}(M)$ et $a_0 = (-1)^n \det(M)$.
Polynômes caractéristiques usuels [voir annexe]

I. D. Liens entre polynômes et valeurs propres

[MM16, ChV/VII]

Proposition 14. *Soit F un sous-espace f-stable de E. On pose f_F l'endomorphisme induit sur F par f. Alors $\pi_{f_F} \mid \pi_f$ et $\chi_{f_F} \mid \chi_f$.*
Si $E = \bigoplus_{i=1}^{r} E_i$ est une décomposition en sous-espaces stables de E, alors $\chi_f = \prod_{i=1}^{r} \chi_{f_{E_i}}$.

Proposition 15. [Liens entre valeurs propres]
$\lambda \in \mathbb{K}$ est une valeur propre de f si et seulement si $\chi_f(\lambda) = 0$ si et seulement si $\pi_f(\lambda) = 0$.

Théorème 16. [Théorème de Cayley-Hamilton]
χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f \mid \chi_f$.

Définition 17. [Multiplicités]
Soit $\lambda \in \mathrm{Sp}(f)$ une valeur propre de f. On appelle :
- multiplicité géométrique de λ la dimension de E_λ, notée $m_g(\lambda)$,
- multiplicité algébrique de λ la multiplicité de λ en tant que racine de χ_f, notée $m_a(\lambda)$,
- multiplicité minimale de λ la multiplicité de λ en tant que racine de π_f, notée $m_m(\lambda)$.

On a $m_m(\lambda) \leq m_g(\lambda)$ et $m_a(\lambda) \leq m_g(\lambda)$.

II. Diagonalisabilité [MM16, ChVIII]

II. A. Critères de diagonalisabilité

Définition 18. f est diagonalisable s'il existe une base de E formée de vecteurs propres de f (c'est-à-dire si la matrice dans une certaine base de E est diagonale).

Application 19. Les valeurs propres de f sont alors les coefficients diagonaux d'une matrice diagonale associée à f (voir Exemple 3).

Théorème 20. *On a équivalence :*
- *f est diagonalisable,*
- *$E = \bigoplus_{\lambda \in \mathrm{Sp}(f)} E_\lambda$,*
- *π_f est scindé à racines simples,*
- *il existe un polynôme annulateur de f scindé à racines simples,*
- *χ_f est scindé et pour tout $\lambda \in \mathrm{Sp}(f)$, $m_g(\lambda) = m_a(\lambda)$.*

Application 21.
- Si f admet n valeurs propres distinctes, f est diagonalisable.
- Si f n'a qu'une valeur propre, f est diagonalisable si et seulement si f est une homothétie.
- Un projecteur et une symétrie sont diagonalisables.
- Un endomorphisme nilpotent et diagonalisable est nul.
- $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est diagonalisable sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.
- Si $\mathrm{rg}(f) = 1$, alors f est diagonalisable si et seulement si $\mathrm{Tr}(f) \neq 0$.

Corollaire 22. *Si F est f-stable et f est diagonalisable, alors $f_{|F}$ est diagonalisable.*

Application 23. [Cardinal de $\mathcal{D}_n(\mathbb{F}_q)$] [Rom17, p148–151]
Soit $n \in \mathbb{N}$, $q = p^r$ où p est premier et $r \in \mathbb{N}^*$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1+\cdots+n_q=n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

II. B. Co-diagonalisabilité

Proposition 24. *Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\mathrm{Im}(f)$ et les sous-espaces propres de f sont stables par g.*

Proposition 25. *Soit $(f_k)_{1\leq k\leq N}$ une famille d'endomorphismes diagonalisables commutant deux à deux. Alors il existe une base commune de diagonalisation (on dit que les $(f_k)_{1\leq k\leq N}$ sont co-diagonalisables).*

Application 26. Soient $A, B \in \mathcal{M}_n(\mathbb{R})$ diagonalisables. Alors $\Theta \in \mathcal{L}(\mathcal{M}_n(\mathbb{R}))$ définit par $\Theta(M) = AMB$ est diagonalisable.

Exemple 27. Soit G un sous-groupe fini abélien de $\mathcal{GL}_n(\mathbb{C})$. Alors les éléments de G sont co-diagonalisables. Donc G est conjugué à un sous-groupe de matrices diagonales.

II. C. Topologie pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ [BMP05, §4.3.3/4.6, p179/217]

Proposition 28. *Pour $\lambda \in \mathrm{Sp}(f)$, $|\lambda| \leq |||f|||$ où $|||.|||$ est la norme subordonnée à n'importe quelle norme sur E.*

Proposition 29. *Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on a $\chi_{AB} = \chi_{BA}$.*

Proposition 30. *$M \longmapsto \chi_M$ est continue.*

Application 31. L'ensemble des matrices nilpotentes est fermé.

Proposition 32. *$\overline{\mathcal{D}_n(\mathbb{K})} = \mathcal{T}_n(\mathbb{K})$. En particulier $\mathcal{D}_n(\mathbb{C})$ est dense dans $\mathcal{M}_n(\mathbb{C})$.*

II. D. Liens avec les endomorphismes semi-simples [BMP05, §4.2.1, p158–161]

Définition 33. [endomorphisme semi-simple]
f est dit semi-simple si tout sous-espace f-stable admet un supplémentaire f-stable.

Théorème 34. *f est semi-simple si et seulement si π_f est sans facteur carré.*

Application 35. Sur $\mathbb{K} = \mathbb{C}$, f est semi-simple si et seulement si f est diagonalisable. Sur $\mathbb{K} = \mathbb{R}$, f est semi-simple si et seulement si f est diagonalisable sur $\mathbb{C}$.

Exemple 36. Si f est nilpotente, alors f est semi-simple si et seulement si $f = 0$.

Exemple 37. Les rotations de $\mathbb{R}^2$ sont semi-simples.

Application 38. Supposons f semi-simple et soit F un sous-espace f-stable. Alors u_F et $\overline{u} : E/F \longrightarrow E/F$ sont aussi semi-simples.

III. Décomposition de Dunford

[MM16, Ch10] [Gou09, §4.4, p193]

Théorème 39. [Décomposition de Dunford]
Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d+n$ et d commute avec n. De plus, d et n sont des polynômes en f.

Application 40. Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \dots, \mu_n$ les n racines de χ_M (comptées sans leur multiplicité). Soit (D,N) la décomposition de Dunford de M. Soit $P \in \mathcal{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \operatorname{diag}(\mu_1,\dots,\mu_n)$ soit diagonale. Alors on a :

$$\exp(A) = P \operatorname{diag}(\mathrm{e}^{\mu_1},\dots,\mathrm{e}^{\mu_n}) P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}$$

Exemple 41.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = I_3 + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\exp\left(\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} \mathrm{e} & \mathrm{e} & \mathrm{e}/2 \\ 0 & \mathrm{e} & \mathrm{e} \\ 0 & 0 & \mathrm{e} \end{pmatrix}$$

Exemple 42. Un endomorphisme nilpotent et diagonalisable est nul.

Application 43. Résolution de l'équation différentielle $Y' = AY$ pour $A \in \mathcal{M}_n(\mathbb{C})$.

Remarque 44. Sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, on n'a pas continuité de $f \longmapsto (d,n)$: considérer $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & \alpha \end{pmatrix}$.

IV. Théorèmes spectraux

[Rom17, Ch22, p697]

On se place sur $\mathbb{K} = \mathbb{R}$ (resp. $\mathbb{C}$) et on considère E euclidien (resp. hermitien) de dimension finie. On note $M^* = \overline{M}^{\top}$ la transconjuguée de M. On note f^* l'adjoint de $f \in \mathcal{L}(E)$.

Définition 45. On dit que f est une isométrie (resp. un endomorphisme unitaire) si f préserve la norme ($\forall x \in E, \|f(x)\| = \|x\|$).

Définition 46. On dit que f est auto-adjoint si $f^* = f$. On dit que f est normal si $f^* f = f f^*$.

Exemple 47. On a les mêmes définitions pour les matrices. Une matrice symétrique ou orthogonale (resp. hermitienne ou unitaire) est normale.

Lemme 48. *Si F est f-stable et f est normal alors $f^{\perp}$ est f-stable et f^*-stable.*

Application 49. Les sous-espaces propres de f normal ont un orthogonal f-stable.

Théorème 50. [Réduction des endomorphismes normaux, cas complexe]
Si E est hermitien, tout endomorphisme normal est diagonalisable dans une base orthonormée.

Lemme 51. *Toute matrice symétrique réelle admet une valeur propre réelle. De plus les sous-espaces propres associés sont deux à deux orthogonaux.*

Théorème 52. [Réduction des endomorphismes auto-adjoints]
Tout endomorphisme auto-adjoint admet une base orthonormale de diagonalisation.

Application 53. Pour déterminer les valeurs propres $\mu_0 < \mu_1 < \dots < \mu_r$ de f auto-adjoint, on procède par récurrence en posant :

$$\mu_i = \min(\{\langle f(x) \mid x\rangle \mid \|x\| = 1 \text{ et } x \in (E_{\mu_0} \oplus \dots \oplus E_{\mu_{i-1}})^{\perp}\})$$

ANNEXE

Polynômes minimaux et caractéristiques usuels
Soit F un sous-espace vectoriel de dimension $1 \leq p \leq n-1$.

f	π_f	χ_f
nilpotent d'indice k	X^k	X^n
homothétie de rapport λ	$X-\lambda$	$(X-\lambda)^n$
projecteur sur F	X^2-X	$(X-1)^p X^{n-p}$
symétrie par rapport à F	X^2-1	$(X-1)^p(X+1)^{n-p}$

SPEECH

La diagonalisation permet de trouver une base de vecteurs propres, dans laquelle il est souvent beaucoup plus aisé de faire des manipulations !

QUESTIONS

Q Que peut-on dire des sous-espaces stables de f diagonalisable ?

R Ils admettent un supplémentaire stable, par le théorème de la base incomplète.

Q Comment montrer le Corollaire 22 ?

Q Le Théorème 52 est-il le même résultat que la propriété de réduction des formes quadratiques ? (l'un découle-t-il de l'autre ?)

R Ils n'ont rien à voir, en revanche il y a un résultat sur les formes quadratiques équivalent à ce résultat.

Q Soit $\mathcal{D}$ l'ensemble des matrices diagonales de $\mathcal{GL}_n(\mathbb{C})$. Que dire de $\mathcal{D}$?

R C'est un groupe abélien. Il n'est pas distingué car il existe des matrices diagonalisables non diagonales. Son commutateur est lui-même. Son normalisateur N vérifie $N/\mathcal{D} \simeq \mathfrak{S}_n$. En effet, soit $P \in N$. Pour $M = \mathrm{diag}(\mu_1, \dots, \mu_n) \in \mathcal{D}$ avec tous les coefficients distincts, on a que $M' = PMP^{-1}$ est diagonale. Notant $(\lambda_i)_{1\leq i\leq n}$ ses coefficients diagonaux, il existe $\sigma \in \mathfrak{S}_n$ telle que $\lambda_i = \mu_{\sigma(i)}$ pour $1 \leq i \leq n$, ou encore $M' = P_\sigma M$. On en déduit que $P \in P_\sigma E$.

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[MM16] R. Mansuy et R. Mneimné : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

156 EXPONENTIELLE DE MATRICES. APPLICATIONS.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On munit $\mathcal{M}_n(\mathbb{K})$ d'une norme d'algèbre $\|.\|$.

I. Convergence et propriétés algébriques de l'exponentielle de matrices

[Rom17, Ch23, p745] [Ave97, Ch5, p47]

Définition de la série exponentielle
Convergence normale sur tout compact, donc convergence de $\exp(A)$
Exemple : $\exp(0), \exp(I)$
Exponentielle de la somme de matrices qui commutent, contre-exemple. On en déduit que $\exp(A)$ est inversible et l'expression de $\exp(A)^{-1}$
$\exp(PAP^{-1}) = P\exp(A)P^{-1}$, $\exp(A^\top) = \exp(A)^\top$, $\exp(\overline{A}) = \overline{\exp(A)}$, $\det(\exp(A)) = \exp(\mathrm{Tr}(A))$
$\exp(A) \in \mathbb{K}[A]$ commute avec A

II. Calcul pratique de l'exponentielle

[Rom17, Ch23, p745] [Gou09, §4.4, p193]

Matrice diagonale, nilpotente, puis utilisation de la décomposition de DUNFORD ou de la décomposition de JORDAN

THÉORÈME 1. [DÉCOMPOSITION DE DUNFORD]
Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n.
De plus, d et n sont des polynômes en f.

APPLICATION 2. Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\lambda_1, \dots, \lambda_r$ de multiplicités $\alpha_1, \dots, \alpha_r$ ou $\mu_1, \dots, \mu_n$ les racines de χ_M. Soit (D, N) la décomposition de DUNFORD de M. Soit $P \in \mathcal{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \dots, \mu_n)$ soit diagonale. Soit p_i le projecteur sur $\ker(f - \lambda_i \mathrm{Id})^{\alpha_i}$ parallèlement à $\bigoplus_{j \neq i} \ker(f - \lambda_j \mathrm{Id})^{\alpha_j}$. Alors on a :

$$\exp(M) = P\,\mathrm{diag}(\mathrm{e}^{\mu_1}, \dots, \mathrm{e}^{\mu_n})P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!} = \sum_{i=1}^{r} \mathrm{e}^{\lambda_i} \left[\sum_{p=0}^{\alpha_i - 1} \frac{(A - \lambda_i \mathrm{Id})^k}{k!}\right] P_i$$

Si χ_A est scindé, A est diagonalisable si et seulement si son exponentielle l'est
Utilisation de la décomposition de JORDAN

III. Propriétés analytiques de l'exponentielle

III. A. Différentiabilité

[Ave97, Ch5/7, p57/79] [Rom17, Ch23, p745]

$\exp$ est $\mathcal{C}^\infty$ (admis), expression de la différentielle
$\exp$ est un $\mathcal{C}^1$-difféo local de 0 sur I_n

III. B. Injectivité et surjectivité

[Rom17, §23.4, p752] [CG13, §VI.2.5, p357–358]

Fonction log définie sur $\mathbb{B}(I_n, 1)$, qui vérifie $\exp \circ \log = \mathrm{Id}$
$\ln$ bien définie sur les matrices unipotentes
Homéomorphisme de N_p sur U_p, d'inverse le logarithme
$\exp$ est surjective (sur $\mathcal{GL}_n(\mathbb{C})$) si $\mathbb{K} = \mathbb{C}$: il existe même $Q \in \mathbb{C}[X]$ tel que $\exp(Q(A)) = A$
Connexité par arcs de $\mathcal{GL}_n(\mathbb{C})$
$\exp$ est non injective, de noyau les matrices diagonalisables de spectre inclus dans $2i\pi\mathbb{Z}$ [FGN07, §4.25, p417]
Sur $\mathbb{R}$, on a injectivité, mais plus surjectivité : $\exp(A) = \exp(A/2)^2$ donc $\exp$ est à valeurs dans $\mathcal{GL}_n^+(\mathbb{C})$

THÉORÈME 3. *$\exp : \mathcal{S}_n(\mathbb{R}) \longrightarrow \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.*

PROPOSITION 4. *$\exp : \mathcal{H}_n(\mathbb{C}) \longrightarrow \mathcal{H}_n^{++}(\mathbb{C})$ est un homéomorphisme.*

Décomposition polaire : on déduit les homéomorphismes $\mathcal{GL}_n(\mathbb{R}) \simeq \mathcal{O}_n \times \mathbb{R}^{n(n+1)/2}$ et $\mathcal{GL}_n(\mathbb{C}) \simeq \mathcal{U}_n \times \mathbb{R}^{n^2}$

IV. Application aux équations différentielles linéaires

[Ber17, Ch2/6, p46/233]

Remarque : la fonction $t \longmapsto \mathrm{e}^{tA}$ est $\mathcal{C}^\infty$ sur $\mathbb{R}$ et de dérivée $t \longmapsto A\,\mathrm{e}^{tA}$
Étude de $Y' = AY$ [Dem96]
Remarque : on peut toujours se ramener à une équation différentielle matricielle d'ordre 1 !
Solutions sous forme intégrale
Théorèmes de stabilité selon les valeurs propres de A
Exemples

QUESTIONS

Q A-t-on $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}$ dans $\exp(\mathcal{M}_2(\mathbb{R}))$?

R La première matrice a pour déterminant -1, donc n'est pas un carré dans $\mathcal{GL}_2(\mathbb{R})$. Or si $A = \exp(B)$, on a $A = \exp(B/2)^2$ donc A est un carré.
Pour la deuxième, on regarde le spectre de la matrice et on aboutit à une contradiction.

Q Soit M ayant une seule valeur propre, qui est réelle et strictement positive. A-t-on $M \in \exp(\mathcal{M}_n(\mathbb{R}))$?

R On a $\chi_M = (X-\lambda)^n$ est scindé. Écrivons sa décomposition de DUNFORD : on a $M = D+N$, avec $D = \lambda I_n$ et donc $\frac{1}{\lambda}M = I_n + \frac{1}{\lambda}N$. Si $A = \mathrm{Log}(I_n + \frac{1}{\lambda}N)$, on a $\exp(A) = M$.

Q $\exp$ est-elle injective sur $\mathcal{D}(\mathbb{R})$ l'ensemble des matrice diagonalisables de $\mathbb{R}$?

R Soit A, B diagonalisables telles que $\exp(A) = \exp(B)$. On vérifie que A, B commutent, et donc sont co-diagonalisables, ce qui implique alors que $A = B$ en regardant ce que donne $\exp(A) = \exp(B)$ dans une base de co-diagonalisation.
Pour montrer le commutativité, on montre que A est un polynôme en B.

Q Montrer que $\mathcal{GL}_n(\mathbb{C})$ est connexe par arcs.

Q Montrer que $\exp$ de $\{A \in \mathcal{M}_n(\mathbb{R}) \mid \mathrm{e}^{\mathrm{Sp}(A)} \cap \mathbb{R} = \varnothing\}$ est à valeurs dans $\mathcal{GL}_n(\mathbb{R})$.

R Penser à utiliser la réduction de JORDAN.

BIBLIOGRAPHIE

[Ave97] A. AVEZ : *Calcul différentiel*. Masson, 1997.

[Ber17] F. BERTHELIN : *Equations différentielles*. Cassini, 2017.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Dem96] J.-P. DEMAILLY : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 2*. Cassini, 2007.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

157 ENDOMORPHISMES TRIGONALISABLES. ENDOMORPHISMES NILPOTENTS.

Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

I. Généralités

I. A. Rappels sur l'étude d'endomorphismes [MM16]

Soit $f \in \mathcal{L}(E)$.

Définition 1. [Polynôme minimal]
$\varphi_f : \mathbb{K}[X] \longrightarrow \mathbb{K}[f], P \longmapsto P(f)$ est un morphisme d'algèbres. Son noyau est un idéal de $\mathbb{K}[f]$ engendré par un unique polynôme unitaire π_f appelé polynôme minimal de f.

Proposition 2. *On a* $\dim(\mathbb{K}[f]) = \deg(\pi_f)$.

Exemple 3. Polynômes minimaux usuels **[voir annexe]**

Proposition 4. *Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors $\ker(f)$ et $\mathrm{Im}(f)$ sont stables par g. En particulier $\ker(P(f))$ et $\mathrm{Im}(P(f))$ sont stables par f pour tout $P \in \mathbb{K}[X]$.*

Lemme 5. [Lemme des noyaux]
Soit $(P_i)_{1\leq i\leq r}$ une famille de polynômes deux à deux premiers entre eux et $f \in \mathcal{L}(E)$. Alors en posant $P = \prod_{i=1}^r P_i$, on a $\ker(P(f)) = \bigoplus_{i=1}^r \ker(P_i(f))$.
De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Application 6. Soit P annulateur de f. Si $P = \prod_{i=1}^r P_i^{\alpha_i}$ où les $(P_i)_{1\leq i\leq r}$ sont deux à deux premiers, alors on a la décomposition en sous-espaces f-stables $E = \bigoplus_{i=1}^r \ker(P_i^{\alpha_i}(f))$.

Définition 7. [Polynôme caractéristique]
On définit le polynôme caractéristique de $M \in \mathcal{M}_n(\mathbb{K})$ par $\chi_M(X) = \det(XI_n - M)$. Deux matrices semblables ayant même polynôme caractéristique, on définit le polynôme caractéristique de f.

Exemple 8. Polynômes caractéristiques usuels **[voir annexe]**

Proposition 9. [Liens entre valeurs propres]
$\lambda \in \mathbb{K}$ est une valeur propre de f si et seulement si $\chi_f(\lambda) = 0$ si et seulement si $\pi_f(\lambda) = 0$.

Théorème 10. [Théorème de Cayley-Hamilton]
χ_f est un polynôme annulateur de f. Autrement dit, $\pi_f \mid \chi_f$.

I. B. Noyaux itérés [MM16, ChII/IV, p46]

Proposition 11. *La suite $(\ker(f^k))_{k\in\mathbb{N}}$ est croissante stationnaire et on a :*

$$\forall k \in \mathbb{N}, \dim(\ker(f^{k+1})) = \dim(\ker(f^k)) + \dim(\ker(f) \cap \mathrm{Im}(f^k))$$

Corollaire 12. *La suite $(\dim(\ker(f^{k+1})) - \dim(\ker(f^k)))_{k\in\mathbb{N}}$ est décroissante.*

Définition 13. $p = \min(\{q \in \mathbb{N} \mid \forall k \in \mathbb{N}, \ker(f^{q+k}) = \ker(f^q)\})$ est appelé indice de f.

Proposition 14. *$p \leq n$ et on a $E = \ker(f^p) \oplus \mathrm{Im}(f^p)$.*

II. Endomorphismes nilpotents [MM16, ChI/II/IX/X, p3/23/102/113]

Définition 15. $f \in \mathcal{L}(E)$ est nilpotent si $f^p = 0$, où p est l'indice (de nilpotence) de f.

Soit f nilpotent d'indice r.

Application 16. On a alors $\pi_f = X^p$ et $\chi_f = X^n$.

Proposition 17. *On a $p \leq n$ et on a égalité si et seulement si $\dim(\ker(f)) = 1$.*

Application 18. Si f est nilpotent d'incide n, il existe une base $\mathcal{B}$ de E telle que :

$$M_{\mathcal{B}}(f) = J_n = \begin{pmatrix} 0 & & \cdots & & 0 \\ 1 & 0 & & & \\ & \ddots & \ddots & & \vdots \\ & & \ddots & \ddots & 0 \\ 0 & \cdots & & 1 & 0 \end{pmatrix}$$

En particulier, f est trigonalisable.

Exemple 19. Si $n = 3$:
- soit $p = 1$, alors $f = 0$,
- soit $p = 2$, alors $\dim(\ker(f)) = 2$,
- soit $p = 3$, alors $\dim(\ker(f)) = 1$.

Proposition 20. *f est trigonalisable, avec une diagonale de 0.*

Proposition 21. *Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $g \in \mathcal{L}(E)$ est nilpotent si et seulement si $\forall k \in \mathbb{N}^*, \mathrm{Tr}(g^k) = 0$.*

Exemple 22. Si $\mathbb{K} = \mathbb{F}_p$, le résultat est faux, prenant $g = \mathrm{Id}_{(\mathbb{F}_p)^p}$.

III. Trigonalisation

[MM16, ChIX]

III. A. Caractérisation

Définition 23. $f \in \mathcal{L}(E)$ est trigonalisable s'il existe une base de E dans laquelle la matrice de f soit triangulaire.

Proposition 24. *Si f est trigonalisable, les coefficients diagonaux de sa matrice dans une base adaptée sont les valeurs propres de f. Notant $(\lambda_i)_{1\leq i\leq r}$ ses valeurs propres, chacune de multiplicité algébrique $m_a(\lambda_i)$, on a :*

$$\mathrm{Tr}(f) = \sum_{i=1}^{r} m_a(\lambda_i)\lambda_i \qquad \text{et} \qquad \det(f) = \prod_{i=1}^{r} \lambda_i^{m_a(\lambda_i)}$$

Théorème 25. *f est trigonalisable si et seulement si χ_f est scindé si et seulement si π_f est scindé si et seulement si f admet un polynôme annulateur scindé.*

Corollaire 26. *Si $\mathbb{K} = \mathbb{C}$ ou est algébriquement clos, tout endomorphisme de $\mathcal{L}(E)$ est trigonalisable.*

Exemple 27. La matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est trigonalisable sur $\mathbb{C}$ mais par sur $\mathbb{R}$.

Application 28. Pour $A \in \mathcal{M}_n(\mathbb{C})$, on a $\det(\exp(A)) = \exp(\mathrm{Tr}(A))$.

Corollaire 29. *Si f est trigonalisable et si F est un sous-espace f-stable de E, alors f_F est trigonalisable.*

III. B. Co-trigonalisation

Lemme 30. *Soient $f, g \in \mathcal{L}(E)$ tels que f et g commutent. Alors les sous-espaces propres de f sont g-stables.*

Proposition 31. *Soit $(f_k)_{1\leq k\leq N}$ une famille d'endomorphismes trigonalisables commutant deux à deux. Alors il existe une base commune de trigonalisation (on dit que les $(f_k)_{1\leq k\leq N}$ sont co-trigonalisables).*

Exemple 32. Soient $(f_k)_{1\leq k\leq n}$ des endomorphismes nilpotents qui commutent deux à deux. Alors $f_1 \dots f_n = 0$.

Proposition 33. *Soit $\mathbb{K} = \mathbb{C}$. Soient $f, g \in \mathcal{L}(E)$ trigonalisables tels que $fg = 0$. Alors f et g sont co-trigonalisables.*

Proposition 34. *Soit $\mathbb{K} = \mathbb{C}$. Soient $f, g \in \mathcal{L}(E)$ trigonalisables tels que $fg - gf = \alpha f + \beta g$ pour un couple $(\alpha, \beta) \in \mathbb{K}^2$. Alors f et g sont co-trigonalisables.*

IV. Utilisations d'endomorphismes nilpotents/trigonalisables

IV. A. Décomposition de Dunford

[MM16, Ch10] [Gou09, §4.4, p193]

Théorème 35. [Décomposition de Dunford]
Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Alors il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $f = d + n$ et d commute avec n.
De plus, d et n sont des polynômes en f.

Application 36. Soit $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique scindé. On note $\mu_1, \dots, \mu_n$ les n racines de χ_M (comptées sans leur multiplicité). Soit (D, N) la décomposition de Dunford de M. Soit $P \in \mathcal{GL}_n(\mathbb{K})$ telle que $P^{-1}DP = \Delta = \mathrm{diag}(\mu_1, \dots, \mu_n)$ soit diagonale. Alors on a :

$$\exp(A) = P\,\mathrm{diag}(\mathrm{e}^{\mu_1}, \dots, \mathrm{e}^{\mu_n})P^{-1} \sum_{k=0}^{n-1} \frac{N^k}{k!}$$

Exemple 37.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = I_3 + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\exp\left(\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} \mathrm{e} & \mathrm{e} & \mathrm{e}/2 \\ 0 & \mathrm{e} & \mathrm{e} \\ 0 & 0 & \mathrm{e} \end{pmatrix}$$

Exemple 38. Un endomorphisme nilpotent et diagonalisable est nul.

Application 39. Résolution de l'équation différentielle $Y' = AY$ pour $A \in \mathcal{M}_n(\mathbb{C})$.

IV. B. Réduction de Jordan

[MM16, ChX] [Rom17, Ch21, p672–675]

Lemme 40. *Soit f nilpotent d'indice r. Soit $x \notin \ker(f^{r-1})$. Posons $F_x = \mathrm{Vect}(\{x, f(x), \dots, f^{r-1}(x)\})$.*
- *F_x est f-stable et $\mathcal{B}_x = \{x, f(x), \dots, f^{r-1}(x)\}$ en est une base,*
- *F_x admet un supplémentaire f-stable.*

Proposition 41. [Décomposition de Jordan d'un endomorphisme nilpotent] *Soit $f \in \mathcal{L}(E)$ nilpotent. Il existe des entiers $d_1 \geq \cdots \geq d_\ell$ tels que dans une certaine base $\mathcal{B}$ de E, $M_{\mathcal{B}}(f)$ soit diagonale par blocs avec les blocs $(J_{r_k})_{1 \leq k \leq \ell}$.*

Théorème 42. [Décomposition de Jordan] *Soit $f \in \mathcal{L}(E)$ de polynôme caractéristique scindé. Notons $\lambda_1, \dots, \lambda_r$ ses valeurs propres. Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,\ell_j}$ pour $j \in [\![1, r]\!]$ tels que dans une certaine base $\mathcal{B}$ de E, $M_{\mathcal{B}}(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{\substack{1 \leq j \leq r \\ 1 \leq k \leq \ell_j}}$, où $B_{j,k} = \lambda_j I_{d_{j,k}} + J_{d_{j,k}}$ avec $J_d = \mathcal{C}(X^d) \in \mathcal{M}_d(\mathbb{K})$.*

Exemple 43. $\begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 2 & 0 & -1 \\ 0 & 2 & 2 & 3 \end{pmatrix}$ est semblable à $\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$.

Théorème 44. *Deux endomorphismes trigonalisables sont semblables si et seulement si ils ont même réduction de* Jordan.

Définition 45. [Tableau de Young]
Le tableau de Young associé à une suite d'entiers $d_1 \geq \cdots \geq d_\ell$ est un tableau à ℓ lignes telles que chaque ligne i comporte d_i cases.
A un endomorphisme nilpotent f, on peut donc associer un unique tableau de Young associé à cet endomorphisme via sa réduction de Jordan.
Plus généralement, si f est trigonalisable, de valeurs propres $\lambda_1, \dots, \lambda_r$, on lui associe les r tableaux de Young associés aux r valeurs propres comme le tableau de Youngde $f_{N_i} - \lambda_i \mathrm{Id}_{N_i}$ où $N_i = \ker(f - \lambda_i \mathrm{id})^{m_a(\lambda_i)}$.

Proposition 46. *Deux endomorphismes nilpotents (resp. trigonalisables) sont semblables si et seulement si ils ont même tableau de* Young *(resp. ils ont même valeurs propres et mêmes tableaux de* Young *associés à chacune des valeurs propres).*

Exemple 47. [Lecture d'un tableau de Young]
Soit f nilpotent. Regardons son tableau de Young :
- les cases du tableau s'interprètent comme les éléments d'une base dans laquelle la matrice de f est la forme réduite de Jordan.
  La i-ième ligne est associée au bloc de Jordan de taille d_i. Si on prend x tel que F_x est le sous-espace associé à ce bloc, alors les cases de la ligne i parcourues de gauche à droite sont associées à la base $f^{d_i-1}(x), \dots, f(x), x$ de F_x,
- pour trouver les sous-espaces associés à $\mathrm{Im}(f^k)$, il suffit d'enlever les k dernières cases de chaque ligne,
- pour trouver les sous-espaces associés à $\ker(f^k)$, on garde les k premières cases de chaque ligne,
- de ces deux dernières observations on déduit facilement $\dim(\mathrm{Im}(f^k))$ et $\dim(\ker(f^k))$,
- l'indice de nilpotence est le nombre maximal de cases sur une ligne.

Application 48. Soient $f, g \in \mathcal{L}(E)$ nilpotents ayant même polynôme minimal et même rang. Alors si $n \leq 6$, f et g sont semblables. En dimension 7, on a un contre-exemple : considérer les tableaux $(3,2,2)$ et $(3,3,1)$.

Application 49. Il y a autant de classes de similitudes de matrices nilpotentes que de partitions de n.

ANNEXE

Polynômes minimaux et caractéristiques usuels
Soit F un sous-espace vectoriel de dimension $1 \leq p \leq n-1$.

f	π_f	χ_f
nilpotent d'indice k	X^k	X^n
homothétie de rapport λ	$X-\lambda$	$(X-\lambda)^n$
projecteur sur F	X^2-X	$(X-1)^p X^{n-p}$
symétrie par rapport à F	X^2-1	$(X-1)^p(X+1)^{n-p}$

Tableaux de YOUNG

SPEECH

Les endomorphismes trigonalisables sont très intéressants à étudier car leur structure permet une simplification des manipulations (le produit de matrices triangulaires supérieures reste une matrice triangulaire supérieure, on a les valeurs propres sur la diagonales, …).
Leur étude nous amène d'abord à regarder le cas des endomorphismes nilpotents. Le lien entre les deux arrive avec la décomposition de DUNFORD.

COMMENTAIRES

Cette leçon est sensée amener vers JORDAN.

QUESTIONS

Q Soient $f, g \in \mathcal{L}(E)$. Montrer que si $[[f,g],f]=0$, alors $[f,g]$ est nilpotent.

R On a :

$$\begin{aligned}\mathrm{Tr}([f,g]^n) &= \mathrm{Tr}([f,g]^{n-1}[f,g]) = \mathrm{Tr}([f,g]^{n-1}(fg-gf)) \\ &= \mathrm{Tr}([f,g]^{n-1}fg) - \mathrm{Tr}([f,g]^{n-1}gf) \\ &= \mathrm{Tr}(gf[f,g]^{n-1}) - \mathrm{Tr}([f,g]^{n-1}gf) = 0\end{aligned}$$

Il reste à appliquer la proposition 21.

Q À quoi correspond l'espace vectoriel engendré par les nilpotents ?

R Cet espace ne contient pas d'élément inversible, car 0 est valeur propre de chacun de ses éléments. Tous les éléments de l'ensemble ont une trace nulle, car $\mathrm{Tr}(n_1+n_2)=0$. On va montrer qu'en fait ce sont tous les éléments de trace nulle. En effet, matriciellement, les matrices de trace nulle sont de dimension n^2-1, et la dimension de notre espace vectoriel est au moins n^2-n car $(E_{i\,j})_{i\neq j}$ est une famille libre de notre espace, tout comme les matrices $(\mathrm{diag}(0,\dots,0,\begin{pmatrix}1 & -1\\ 1 & -1\end{pmatrix},0,\dots,0))_{1\leq i\leq n-1}$ où le bloc non nul est en position i, et les deux familles considérées sont libres entre elles. On a donc une famille libre de dimension n^2-1, ce qui conclut.

Q Montrer que la décomposition de DUNFORD reste valable pour toute matrice réelle, et qu'alors D et N sont réelles.

R Soit $M \in \mathcal{M}_n(\mathbb{R})$. Elle est trigonalisable sur $\mathbb{C}$, donc on écrit $M=D+N$ sa décomposition de DUNFORD. On a alors $\overline{D}+\overline{N}=\overline{M}=M=D+N$ donc par unicité D et N sont bien réelles.

Q Trigonaliser $M=\begin{pmatrix}2 & 2 & -3\\ 5 & 1 & -5\\ -3 & 4 & 0\end{pmatrix}$.

R On calcule $\chi_M=(X-1)^3$. On trouve $e_1=(1,1,1)^\top \in \ker(M-I_3)$ et $e_2=(1,1,0)^\top \in \ker(M-I_3)^2$. Complétant en une base (e_1,e_2,e_3), la matrice dans cette base est triangulaire.

BIBLIOGRAPHIE

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[MM16] R. MANSUY et R. MNEIMNÉ : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

158 MATRICES SYMÉTRIQUES RÉELLES, MATRICES HERMITIENNES.

Soit $n \in \mathbb{N}^*$. Pour $M \in \mathcal{M}_n(\mathbb{K})$, on note $M^* = \overline{M}^\top$.

I. Généralités [Gou09, §5.1, p227]

I. A. Définitions et premières propriétés

Définition 1. [Matrice symétrique réelle, matrice hermitienne]
Soit $M \in \mathcal{M}_n(\mathbb{R})$. On dit que M est symétrique (resp. anti-symétrique) si $M = M^\top$ (resp. $M = -M^\top$). On note $\mathcal{S}_n(\mathbb{R})$ (resp. $\mathcal{A}_n(\mathbb{R})$) l'ensemble des matrices symétriques (resp. anti-symétriques) réelles.
Soit $M \in \mathcal{M}_n(\mathbb{C})$. On dit que M est hermitienne si $M = \overline{M}^\top$. On note $\mathcal{H}_n(\mathbb{C})$ l'ensemble des matrices hermitiennes.

Exemple 2. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix} \in \mathcal{S}_n(\mathbb{R})$ et $\begin{pmatrix} 1 & -i & 3+2i \\ i & 1 & 1+i \\ 3-2i & 1-i & 6 \end{pmatrix} \in \mathcal{H}_n(\mathbb{C})$.

Remarque 3. $\mathcal{H}_n(\mathbb{C})$ est un $\mathbb{R}$-espace vectoriel mais pas un $\mathbb{C}$-espace vectoriel.

Proposition 4. *$\dim(\mathcal{S}_n(\mathbb{R})) = \frac{n(n+1)}{2}$, $\dim(\mathcal{A}_n(\mathbb{R})) = \frac{n(n-1)}{2}$ et $\dim_{\mathbb{R}}(\mathcal{H}_n(\mathbb{C})) = n^2$.*

Proposition 5. *On a $\mathcal{M}_n(\mathbb{R}) = \mathcal{S}_n(\mathbb{R}) \oplus \mathcal{A}_n(\mathbb{R})$ et $\mathcal{H}_n(\mathbb{C}) = \mathcal{S}_n(\mathbb{R}) \oplus i\mathcal{A}_n(\mathbb{R})$.*

Exemple 6. $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 \\ 3 & 5 & 7 \\ 5 & 7 & 9 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 1 \\ -2 & -1 & 0 \end{pmatrix}$.

Proposition 7. *Pour $A \in \mathcal{S}_n(\mathbb{R})$ ou $\mathcal{H}_n(\mathbb{R})$, on a $\mathrm{Sp}(A) \subset \mathbb{R}$.*

Définition 8. On définit :
- $\mathcal{S}_n^+(\mathbb{R})$ l'ensemble des $S \in \mathcal{S}_n(\mathbb{R})$ telles que $X^\top SX \geq 0$ pour $X \in \mathbb{R}^n$,
- $\mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des $S \in \mathcal{S}_n^+(\mathbb{R})$ telles que $X^\top SX = 0 \Longrightarrow X = 0$,
- $\mathcal{H}_n^+(\mathbb{C})$ l'ensemble des $H \in \mathcal{H}_n(\mathbb{C})$ telles que $\overline{X}^\top HX \geq 0$ pour $X \in \mathbb{C}^n$,
- $\mathcal{H}_n^+(\mathbb{C})$ l'ensemble des $H \in \mathcal{H}_n^+(\mathbb{C})$ telles que $\overline{X}^\top HX = 0 \Longrightarrow X = 0$.

I. B. Liens avec les formes bilinéaires symétriques / hermitiennes

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ selon le contexte.

Définition 9. Soit $\mathbb{K} = \mathbb{R}$. Soit $\varphi : E \times E \longrightarrow \mathbb{R}$ une forme bilinéaire.
- φ est dite symétrique si $\varphi(x,y) = \varphi(y,x)$ pour $x, y \in E$,
- si φ est symétrique, l'application $\Phi : E \longrightarrow \mathbb{R}, x \longmapsto \varphi(x,x)$ est appelée forme quadratique associée à φ. φ est appelée forme polaire associée à Φ (elle est unique).

Définition 10. Soit $\mathbb{K} = \mathbb{C}$. Soit $\varphi : E \times E \longrightarrow \mathbb{C}$ une forme sesquilinéaire (pour tout $x \in E$, $\varphi(x,.)$ est linéaire et $\varphi(.,x)$ est anti-linéaire).
- φ est dite hermitienne si $\varphi(x,y) = \overline{\varphi(y,x)}$ pour $x, y \in E$,
- si φ est hermitienne, l'application $\Phi : E \longrightarrow \mathbb{R}, x \longmapsto \varphi(x,x)$ est appelée forme hermitienne associée à φ. φ est appelée forme polaire associée à Φ (elle est unique)

Exemple 11. Dans $\mathcal{C}([0,1],\mathbb{C})$, l'application $\varphi : (f,g) \longmapsto \int_0^1 f\overline{g}$ est hermitienne, et induit sur $\mathcal{C}([0,1],\mathbb{R})$ une forme bilinéaire symétrique.
Sur $\mathbb{K}^n$, $(X,Y) \longmapsto \overline{X}^\top.Y$ est bilinéaire symétrique ou sesquilinéaire hermitienne.

Proposition 12. *Soit $\mathcal{B}_E = (e_1, \dots, e_n)$ une base de E et $\varphi : E \times E \longrightarrow \mathbb{K}$ une forme bilinéaire ou sesquilinéaire. Alors*
- *si $\mathbb{K} = \mathbb{R}$, φ est symétrique si et seulement si $A = M_{\mathcal{B}_E}(\varphi) = (\varphi(e_i,e_j))_{1 \leq i,j \leq n} \in \mathcal{S}_n(\mathbb{R})$,*
- *si $\mathbb{K} = \mathbb{C}$, φ est hermitienne si et seulement si $A \in \mathcal{H}_n(\mathbb{R})$.*

Pour $x, y \in E$, on note X et Y leurs coordonnées dans $\mathcal{B}_E$. Dans les deux cas on a alors $\forall x, y \in E, \varphi(x,y) = \overline{X}^\top AY$.

Proposition 13. *Si $\mathcal{B}'_E$ est une autre base de E, et P est la matrice de passage de $\mathcal{B}_E$ vers $\mathcal{B}'_E$, alors $M_{\mathcal{B}'_E}(f) = P^\top AP$.*

II. Réduction et applications [Gou09, §5.1, p227]

II. A. Orthogonalité et théorème spectral [Rom17, Ch22, p697]

Soit Φ une forme quadratique (resp. hermitienne) de forme polaire φ.

Définition 14. Une base $\mathcal{B}$ de E est dite Φ-orthogonale si $\varphi(e,e') = 0$ pour $e \neq e' \in \mathcal{B}$.

Proposition 15. *Il existe une base Φ-orthogonale de E.*

Théorème 16. [Théorème spectral]
Soit $M \in \mathcal{S}_n(\mathbb{R})$ (resp. $M \in \mathcal{H}_n(\mathbb{C})$). Alors il existe une matrice P orthogonale (resp. unitaire) telle que $P^{-1}MP = P^*MP$ est diagonale réelle.

Application 17. Soit $S \in \mathcal{S}_n(\mathbb{R})$. Alors $S \in \mathcal{S}_n^+(\mathbb{R})$ (resp. $S \in \mathcal{S}_n^{++}(\mathbb{R})$) si et seulement si $\mathrm{Sp}(S) \subset \mathbb{R}_+$ (resp. $\mathrm{Sp}(S) \subset \mathbb{R}_+^*$).

Proposition 18. *Soit $A \in Sc_n^{++}(\mathbb{R})$ et $B \in \mathcal{S}_n(\mathbb{R})$, alors il existe $P \in \mathcal{GL}_n(\mathbb{R})$ telle que $P^\top AP$ et $P^\top BP$ soient diagonales.*

II. B. Signature d'une forme quadratique/hermitienne et réduction de Gauss [Rom17, Ch15, p463]

Théorème 19. [Réduction de Gauss]
Pour toute forme quadratique (resp. hermitienne) Φ sur E, il existe $r \in \mathbb{N}$, $(\lambda_i)_{1\leq i\leq r} \in (\mathbb{R}^*)^r$ et $(\ell_i)_{1\leq i\leq r} \in (E^*)^r$ indépendantes telles que $\Phi = \sum_{i=1}^r \lambda_i \ell_i^2$ (resp. $\Phi = \sum_{i=1}^r \lambda_i |\ell_i|^2$).

Exemple 20. $\Phi((x,y,z,t)) = xy + yz + zt + tx = \frac{1}{4}[(x+z+y+t)^2 - (x+z-y-t)^2]$.

Théorème 21. *Il existe un unique couple (s,t) d'entiers naturels tels que pour toute base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ Φ-orthogonale, alors il y a exactement s vecteurs de $\mathcal{B}$ en lesquels $\Phi > 0$, t vecteurs de $\mathcal{B}$ en lesquels $\Phi < 0$ et $n-s-t$ vecteurs de $\mathcal{B}$ en lesquels $\Phi = 0$. On a $s+t = \mathrm{rg}(\Phi)$.*

Définition 22. Le couple s,t est appelé signature de Φ.

Exemple 23. $\Phi((x,y,z,t)) = xy + yz + zt + tx$ a pour signature $(1,1)$ et pour rang 2.

Corollaire 24. *Si $A \in \mathcal{S}_n(\mathbb{R})$ (resp. $A \in \mathcal{H}_n(\mathbb{R})$) est de rang r, il existe $s,t \in \mathbb{N}$ tels que $s+t=r$ et $P \in \mathcal{GL}_n(\mathbb{R})$ (resp $P \in \mathcal{GL}_n(\mathbb{C})$) telle que $P^\top AP$ (resp. P^*AP) est diagonale par blocs avec pour blocs I_s, $-I_t$ et 0_{n-r}.*

III. Propriétés topologiques en lien avec les matrices symétriques réelles [CG13]

Proposition 25. *$\mathcal{S}_n^{++}(\mathbb{R}) = \mathcal{S}_n^+(\mathbb{R}) \subset \mathcal{GL}_n(\mathbb{R})$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.*

Lemme 26. *Soit $A \in \mathcal{S}_n^+(\mathbb{R})$. Alors il existe $S \in \mathcal{S}_n^+(\mathbb{R})$ unique telle que $A = S^2$.*

Théorème 27. [Décomposition polaire]
L'application $\begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O,S) & \longmapsto & OS \end{array}$ *est un homéomorphisme.*

Application 28. $\mathcal{O}_n(\mathbb{R})$ est le seul sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ contenant $\mathcal{O}_n(\mathbb{R})$.

Application 29. Pour $A \in \mathcal{M}_n(\mathbb{R})$, on a $|||A|||_2 = \sqrt{\rho(A^\top A)}$.

Définition 30. Pour $A \in \mathcal{M}_n(\mathbb{R})$, on pose $\exp(A) = \sum_{n\geq 0} \frac{A^n}{n!}$.

Exemple 31. On a $\exp(\mathrm{diag}(\lambda_1,\dots,\lambda_n)) = \mathrm{diag}(\mathrm{e}^{\lambda_1},\dots,\mathrm{e}^{\lambda_n})$.

Théorème 32. *$\exp : \mathcal{S}_n(\mathbb{R}) \longrightarrow \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme.*

Corollaire 33. *$\mathcal{GL}_n(\mathbb{R})$ est homéomorphe à $\mathcal{O}_n(\mathbb{R}) \times \mathbb{R}^{n(n+1)/2}$.*

IV. Applications

IV. A. Différentielle seconde d'une fonction $\mathcal{C}^2$ [Rou99, p327] [Gou08, §5.2, p315]

Théorème 34. [Théorème de Schwarz]
Soit f une fonction de classe $\mathcal{C}^2$ définie sur un ouvert U de $\mathbb{R}^n$. Alors $D^2f \in \mathcal{M}_n(\mathbb{R})$ est une matrice symétrique.

Lemme 35. *Soit $A_0 \in \mathcal{S}_n(\mathbb{R}) \cap \mathcal{GL}_n(\mathbb{R})$. Alors il existe $V \in \mathcal{V}(A_0)$ et $g \in \mathcal{C}^1(V, \mathcal{GL}_n(\mathbb{R}))$ telle que $\forall A \in V, A = g(A)^\top A_0 g(A)$.*

Théorème 36. [Lemme de Morse]
Soit $f : U \longrightarrow \mathbb{R}$ 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 $d^2f(0)$ est non dégénérée, de signature $(p, n-p)$.
Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine de $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = \varphi(x)_1^2 + \cdots + \varphi(x)_p^2 - \varphi(x)_{p+1}^2 - \cdots - \varphi(x)_n^2$ au voisinage de 0.

Application 37. Soit x_0 un point critique de f tel que la hessienne de f est non dégénérée. Alors c'est un minimum (resp. maximum) local si et seulement si la hessienne est de signature $(n,0)$ (resp. $(0,n)$).
De plus, si la hessienne est de signature $(p,n-p)$ pour $1 \leq p \leq n-1$, alors on a des directions v pour lesquelles x_0 sera minimum local de $h \longmapsto f(x+hv)$ et d'autres pour lesquelles x_0 sera maximum local.

Exemple 38. **[cas $n=2$]** Soit x_0 un point critique de f telle que $D^2 f(x_0) = \begin{pmatrix} r & s \\ s & t \end{pmatrix}$. Alors

- si $rt - s^2 > 0$ et $r+t>0$, x_0 est un minimum local,
- si $rt - s^2 > 0$ et $r+t<0$, x_0 est un maximum local,
- si $rt - s^2 < 0$, x_0 n'est pas un extremum,
- si $rt - s^2 = 0$, on ne peut pas conclure.

Exemple 39. Pour le dernier cas, on peut considérer :

$$f(x,y) = x^4 \qquad f(x,y) = -x^4 \qquad f(x,y) = x^4 - y^4$$

IV. B. Analyse matricielle numérique

[AK02, PIII/Ch7, p105/135]

Théorème 40. **[factorisation LU]**
Soit $A \in \mathcal{GL}_n(\mathbb{R})$ une matrice dont tous les mineurs principaux sont non nuls. Alors il existe un unique couple (L,U) de matrices tel que L est triangulaire inférieure avec diagonale de 1, U est triangulaire supérieure et $A = LU$.

Exemple 41. $$= \begin{pmatrix} 3 & 1 & 4 \\ 12 & 6 & 19 \\ 24 & 14 & 42 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 8 & 3 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 \\ 0 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Corollaire 42. *Si de plus $A \in \mathcal{S}_n(\mathbb{R})$, il existe L triangulaire inférieure à diagonale de 1 et D diagonale telle que $A = LDL^\top$.*

Théorème 43. **[factorisation de Cholesky]**
Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$. Alors il existe une unique matrice B triangulaire inférieure telle que tous ses éléments diagonaux soient positifs et $A = BB^\top$.

Application 44. **[moindres carrés]**
Soient $n,p \in \mathbb{N}$ et $A \in \mathcal{M}_{n,p}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On cherche un vecteur $x \in \mathbb{R}^p$ tel que $\|b - Ax\|_2 = \inf_{y \in \mathbb{R}^p} \|b - Ay\|_2$.

(i) Il existe toujours une solution au problème,
(ii) x est solution si et seulement si $A^\top Ax = A^\top b$,
(iii) Si $n \geq p$ et $\mathrm{rg}(A) = p$, $A^\top A$ est inversible et il existe une unique matrice réelle B triangulaire inférieure, à diagonale positive, telle que $A^\top A = BB^\top$, et alors $x = (BB^\top)^{-1}A^\top b$ est une solution.

IV. C. Vecteurs gaussiens

[BL07, §IV.4, p98]

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé. Soit $d \in \mathbb{N}^*$.

Définition 45. **[vecteur gaussien]**
Une variable aléatoire $X = (X_1, \dots, X_d)$ à valeurs dans $\mathbb{R}^d$ est un vecteur gaussien si toute combinaison linéaire des $(X_i)_{1 \leq i \leq d}$ suit une loi gaussienne.

Exemple 46. Si les $(X_i)_{1 \leq i \leq d}$ sont indépendantes et identiquement distribuées de loi $\mathcal{N}(0,1)$, alors X est un vecteur gaussien. On note alors $X \sim \mathcal{N}(0, I_d)$.

Proposition 47. *La loi d'un vecteur gaussien X est entièrement déterminée par sa moyenne $m = \mathbb{E}[X]$ et sa matrice de covariance $\Sigma = (\mathrm{Cov}(X_i, X_j))_{1 \leq i,j \leq d} \in \mathcal{S}_d^+(\mathbb{R})$. On note alors $X \sim \mathcal{N}(m, \Sigma)$.*

Proposition 48. *Soit $m \in \mathbb{R}^d, \Sigma \in \mathcal{S}_n^+(\mathbb{R})$. Soit $X \sim \mathcal{N}(0, I_d)$.*
Il existe $A \in \mathcal{M}_d(\mathbb{R})$ telle que $\Sigma = AA^\top$ et alors $m + AX \sim \mathcal{N}(m, \Sigma)$.

Proposition 49. *Soit $X \sim \mathcal{N}(m, \Sigma)$. Alors Σ est inversible si et seulement si il n'existe pas de relation affine entre les $(X_i)_{1 \leq i \leq d}$ presque surement.*
Dans ce cas, X admet pour densité $f : x \longmapsto \frac{1}{(2\pi)^{\frac{d}{2}}\sqrt{\det(\Sigma)}} \exp\left(-\frac{1}{2}\,{}^t(x-m)\Sigma^{-1}(x-m)\right)$.

COMMENTAIRES

On peut parler de probabilités avec la notion de covariance, les vecteurs gaussiens et le théorème de COCHRAN (cf [Ouv09]).

QUESTIONS

Q Montrer que $\mathcal{GL}_2(\mathbb{R})$ a exactement 2 composantes connexes.

R Il y en a au moins 2 en considérant le déterminant. Ensuite on utilise l'homéomorphisme $\mathcal{O}_2(\mathbb{R}) \times \mathbb{R}^3$ lorsque $A \in \mathcal{SO}_2(\mathbb{R})$ et

Q Donner une réduction de GAUSS de $f(x,y,z,t) = 2xy - y^2 + z^2 + t^2$.

R $f(x,y,z,t) = -(y - 1/2(2x-3t))^2 + \frac{1}{4}(2x-3t)^2 + z^2 + t^2$.

BIBLIOGRAPHIE

[AK02] G. ALLAIRE et S.-M. KABER : *Algèbre linéaire numérique*. Ellipses, 2002.

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Ouv09] J.-Y. OUVRARD : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

159 FORMES LINÉAIRES ET DUALITÉ EN DIMENSION FINIE. EXEMPLES ET APPLICATIONS.

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

I. Formes linéaires et espace dual [Gou09, §3.4, p126] [Rom17, Ch14, p443]

I. A. Généralités sur les formes linéaires

Définition 1. [Forme linéaire, espace dual]
Une forme linéaire sur E est une application linéaire de E dans $\mathbb{K}$. On note $E^* = \mathcal{L}(E, \mathbb{K})$ l'ensemble des formes linéaires, appelé espace dual de E.

Exemple 2.
- Dans $\mathbb{K}^n$, l'application $(x_1, \dots, x_n) \longmapsto x_k$ pour un $k \in [\![1, n]\!]$ est une forme linéaire,
- Soit $A \in \mathcal{M}_n(\mathbb{K})$. L'application $f_A : M \longmapsto \mathrm{Tr}(AM)$ est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$,
- Si $\mathbb{K} = \mathbb{R}$ et $f : E \longrightarrow \mathbb{R}$ est différentiable en un point a, alors df_a est une forme linéaire.
- Le morphisme d'évaluation $\mathrm{ev}_a : P \longmapsto P(a)$ en un point $a \in \mathbb{K}$ est une forme linéaire sur $\mathbb{K}_n[X]$.

Proposition 3. *Le noyau d'une forme linéaire non nulle est un hyperplan de E, c'est-à-dire un sous-espace vectoriel de E de dimension $n-1$. Dans ce cas, elle est surjective. Réciproquement, tout hyperplan de E est le noyau d'une forme linéaire non nulle.*

Exemple 4. Si A est non nulle, $\{M \in \mathcal{M}_n(\mathbb{K}) \mid \mathrm{Tr}(AM) = 0\}$ est un hyperplan de $\mathcal{M}_n(\mathbb{K})$.

I. B. Espace dual et base duale
[FGN07, §7.8/7.9, p239] [Gou08, An.B, p407–416] [Bre99, Ch5, p79–82]

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

Définition 5. [Base duale]
On appelle base duale de $\mathcal{B}$ la base $\mathcal{B}^* = (e_1^*, \dots, e_n^*)$ où chaque e_i^*, défini par $e_i^*(e_j) = \delta_{i,j}$ pour tout j, est l'application i-ième coordonnée dans la base $\mathcal{B}$.

Exemple 6.
- $\mathcal{B} = ((1,0),(0,1))$ est une base de $\mathbb{K}^2$. Sa base duale est composée de $(x,y) \longmapsto x$ et $(x,y) \longmapsto y$.
- Soit $\mathcal{B} = (E_{i\,j})_{1 \le i \le j \le n}$. La base duale de $\mathcal{B}$ est $\mathcal{B}^* = (f_{E_j\,i})_{1 \le i \le j \le n}$.

Proposition 7. *Toute base duale est une base de E^*. En particulier $\dim(E) = \dim(E^*)$ et pour tout $\varphi \in E^*$, on a $\varphi = \sum_{i=1}^n \varphi(e_i) e_i^*$.*

Corollaire 8. *$x = \sum_i x_i e_i \longmapsto \varphi = \sum_i x_i e_i^*$ est un isomorphisme de E dans E^*. Il n'est cependant pas canonique car dépend de la base $\mathcal{B}$ choisie.*

Théorème 9. [Théorème de Riesz-Fréchet]
Soit H un espace de Hilbert. Alors pour toute application $\phi \in H' = H^*$, il existe un unique $f \in H$ tel que $\forall v \in H, \phi(v) = \langle f \mid v \rangle$.
De plus $\phi \longmapsto f$ est une isométrie ($\|f\|_H = \|\phi\|_{H'}$).

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 $E^* : x \longmapsto \langle x \mid . \rangle$.

Proposition 11. [Isomorphisme canonique sur $\mathcal{M}_n(\mathbb{K})$]
L'application $f : A \longmapsto f_A$ 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 $f(XY) = f(YX)$ est colinéaire à la trace.

Application 12. Si $n \ge 2$, tout hyperplan de $\mathcal{M}_n(\mathbb{K})$ coupe $\mathcal{GL}_n(\mathbb{K})$.

I. C. Espace bidual et base antéduale

Définition 13. $E^{**} = (E^*)^*$ est appelé espace bidual de E^*.

Proposition 14. *On a un isomorphisme de E dans E^{**} donné par*

$$\begin{array}{rccc} \Theta : & E & \longrightarrow & E^{**} \\ & x & \longmapsto & f \mapsto f(x) \end{array}$$

Proposition 15. [Base antéduale]
Soit $\mathcal{B}^* = (f_1, \dots, f_n)$ une base de E^*. Alors il existe une unique base $\mathcal{B} = (e_1, \dots, e_n)$ de E dont $\mathcal{B}^*$ est la base duale. $\mathcal{B}$ est alors appelée base antéduale.

Exemple 16. Soient $(a_i)_{0 \le i \le n}$ une famille de points de $\mathbb{K}$ deux à deux distincts. Notons $\ell_i = \prod_{j \ne i} \frac{X - x_j}{x_i - x_j} \in \mathbb{K}_n[X]$ et $\mathcal{B}^* = (\ell_0, \dots, \ell_n)$ la base (de $\mathbb{K}_n[X]^*$) des polynômes de Lagrange. Alors la base antéduale de $\mathcal{B}$ est $(\mathrm{ev}_{a_0}, \dots, \mathrm{ev}_{a_n})$.

II. Autour de l'orthogonalité

[Gou09, §3.4, p126] [Rom17, Ch14, p443]

II. A. Notion d'orthogonalité

Définition 17. [Orthogonalité]
- On dit que $\varphi \in E^*$ et $x \in E$ sont orthogonaux si $\varphi(x) = 0$.
- Pour $A \subset E$ on définit $A^\perp = \{\varphi \in E^* \mid \forall x \in A, \varphi(x) = 0\}$ l'orthogonal de A.
- Pour $B \subset E^*$, on définit l'orthogonal de B par $B^\circ = \{x \in E \mid \forall \varphi \in B, \varphi(x) = 0\}$.

Proposition 18.
- *Si $A_1 \subset A_2 \subset E$, on a $A_2^\perp \subset A_1^\perp$.*
- *Si $B_1 \subset B_2 \subset E^*$, on a $B_2^\circ \subset B_1^\circ$.*
- *Si $A \subset E$, on a $A^\perp = \mathrm{Vect}(A)^\perp$ et si $B \subset E^*$, on a $B^\circ = \mathrm{Vect}(B)^\perp$.*

Théorème 19. *Soit F (resp. G) un sous-espace vectoriel de E (resp. E^*).*
- *On a $\dim(F) + \dim(F^\perp) = \dim(E)$ et $(F^\perp)^\circ = F$.*
- *On a $\dim(G) + \dim(G^\circ) = \dim(E)$ et $(G^\circ)^\perp = G$.*

Application 20.
- Soient $(f_i)_{1\leq i\leq k} \in (E^*)^k$ de rang r. Alors $F = \cap_{1\leq i\leq k} \ker(f_i)$ est de dimension $n - r$.
- Réciproquement, si G est un sous-espace vectoriel de dimension $n - r$, il existe r formes linéaires indépendantes dont G est l'intersection des noyaux.

Exemple 21. L'ensemble des applications linéaires qui s'annulent sur un hyperplan de E forme une droite de E^*.

Exemple 22. Soit $E = \mathbb{R}^4$ et $(e_i)_{1\leq i\leq 4}$ les vecteurs de la base canonique. Soit $F = \mathrm{Vect}(e_1 + e_2 + e_3, e_2 - e_4)$. Alors $F = \ker(\varphi_1) \cap \ker(\varphi_2)$, où

$$\varphi_1(a,b,c,d) = a - c \quad \text{et} \quad \varphi_2(a,b,c,d) = b + d - a$$

II. B. Transposée d'une application linéaire

[Rom17, §14.5, p453]

Soit F un autre $\mathbb{K}$-espace vectoriel de dimension finie p et $u \in \mathcal{L}(E,F)$.

Définition 23. On définit l'application transposée de u par

$$\begin{array}{rccc} {}^tu : & F^* & \longrightarrow & E^* \\ & f & \longmapsto & f \circ u \end{array}$$

Proposition 24.
- *$u \longmapsto {}^tu$ est linéaire et injective de $\mathcal{L}(E,F)$ dans $\mathcal{L}(F^*,E^*)$,*
- *$\mathrm{Im}({}^tu) = \ker(u)^\perp$,*
- *$\mathrm{Im}(u^\perp) = \ker({}^tu)$,*
- *Si $v \in \mathcal{L}(F,G)$ où G est un $\mathbb{K}$-espace vectoriel, alors ${}^t(v \circ u) = {}^tu \circ {}^tv$.*

Proposition 25. *Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E et F, de bases duales $\mathcal{B}^*$ et $\mathcal{B}'^*$. Alors $M_{B'^*,B^*}(u) = M_{B,B'}({}^tu)^\top$.*
En particulier $\mathrm{rg}({}^tu) = \mathrm{rg}(u)$.

Proposition 26. *Si P est la matrice de passage d'une base $\mathcal{B}$ de E vers une base $\mathcal{B}'$, alors la matrice de passage de $\mathcal{B}^*$ vers $\mathcal{B}'^*$ est $(P^{-1})^\top$.*

III. Applications

III. A. Utilisation de la dualité dans la recherche de sous-espaces propres

[Rom17, Ch21, p672]

Soit $f \in \mathcal{L}(E)$. On suppose connues les notions de polynôme minimal (noté π_f) et de polynôme minimal local (noté $\pi_{f,x}$ en un point x).

Proposition 27. *F est f-stable si et seulement si $F^\perp$ est ${}^tf$-stable.*

Proposition 28. *Soit $x \in E$ tel que $\pi_{f,x} = \pi_f$. Alors $E_{f,x} = \mathbb{K}[f](x)$ admet un supplémentaire f-stable.*

Application 29. [Décomposition de Jordan]
Supposons f de polynôme caractéristique scindé (trigonalisable). Notons $\lambda_1, \dots, \lambda_r$ ses valeurs propres distinctes. Il existe des entiers $d_{j,1} \geq \cdots \geq d_{j,\ell_j}$ pour $j \in [\![1,r]\!]$ tels que dans une certaine base $\mathcal{B}$ de E, $M_{\mathcal{B}}(f)$ soit diagonale par blocs avec les blocs $(B_{j,k})_{\substack{1\leq j\leq r \\ 1\leq k\leq \ell_j}}$, où

$$B_{j,k} = \begin{pmatrix} \lambda_j & 0 & \dots & \dots & 0 \\ 1 & \lambda_j & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda_j & 0 \\ 0 & \dots & 0 & 1 & \lambda_j \end{pmatrix} \in \mathcal{M}_{d_{j,k}}(\mathbb{K}).$$

III. B. Calcul différentiel

[BMP05, §1, p20] [Gou09, §5.2/3, p317/327] [Rou99, Ch7, p380]

On se place sur $\mathbb{K} = \mathbb{R}$ et on considère $(E, \langle . \mid . \rangle)$ un espace euclidien.

Proposition 30. *Si $f : E \longrightarrow \mathbb{R}$ 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 :*

$$\forall h \in E, df_a(h) = \langle \nabla f(a) \mid h \rangle$$

Application 31. Géométriquement, le gradient s'interprète comme la direction de plus grande pente de f autour de a. C'est l'idée utilisée dans de nombreux algorithmes d'optimisation.

Théorème 32. [Théorème des extrema liés]
Soit $f, g_1, \dots, g_r : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ des fonctions de classe $\mathcal{C}^1$ définies sur U ouvert. Notons $\Gamma = \{x \in U \mid g_1(x) = \dots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum local en $a \in \Gamma$ et si les formes linéaires $(dg_1(a), \dots, dg_r(a))$ sont libres, alors il existe des réels (uniques) $\lambda_1, \dots, \lambda_r$, appelés multiplicateurs de Lagrange, tels que

$$df(a) = \sum_{i=1}^{r} \lambda_i dg_i(a)$$

Application 33. Tout endomorphisme symétrique de E admet une valeur propre réelle.

Application 34. [Inégalité de Hadamard]

(i) Soient $x_1, \dots, x_n$ des vecteurs de $(E, \langle . \mid . \rangle)$ un espace préhilbertien (réel ou complexe). . Alors $|\det((\langle x_i \mid x_j \rangle)_{1 \leq i,j \leq n})| \leq \prod_{i=1}^n \|x_i\|^2$.

(ii) Soient $x_1, \dots, x_n$ des vecteurs de $\mathbb{C}^n$. Alors $|\det(x_1, \dots, x_n)| \leq \prod_{i=1}^n \|x_i\|_2$, où $\|.\|_2$ désigne la norme hermitienne standard sur $\mathbb{C}^n$.

Dans les deux points, on a égalité si et seulement si la famille $\{x_i\}_{1 \leq i \leq n}$ est orthogonale ou l'un des vecteurs est nul.

ANNEXE

Interprétation géométrique du gradient, interprétation géométrique de l'inégalité de Hadamard.

QUESTIONS

Q Montrer que tout endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie admet un hyperplan stable.

R Soit u un endomorphisme d'un $\mathbb{C}$-ev E. Si $f \in E^*, \ker(f)$ est un hyperplan. On veut trouver f tel que $u(\ker(f)) \subset \ker f$.
Si x est tel que $f(x) = 0$ alors $f \circ u(x) = 0$. On a $f(x) = 0 \Longrightarrow {}^t u(f)(x) = 0$.
Si ${}^t u$ est diagonale dans une base $(f_1, \dots, f_n)$, on a ${}^t u(f) = {}^t u(\sum a_i f_i) = 0$. Ce qui donne $f = 0$ ...

Q Posons $a = (1,2,3)^\top, b = (3,2,1)^\top, c = (4,5,6)^\top$ et $d_\ell = (6,5,4+\ell)^\top$ pour un h quelconque. Trouver une base de $E \cap F$ où $E = \mathrm{Vect}(a,b)$ et $F = \mathrm{Vect}(c, d_\ell)$

R Distinguer selon les valeurs de h ...

Q Peut-on trouver deux formes linéaires non nulles sur E dont le produit est nul ?

R Soit $H_i = \ker(\varphi_i)$. Si $H_1 \cup H_2 \neq E$, on prend $x_1 \in H_1 \setminus H_2$ et $x_2 \in H_2 \setminus H_1, x_1 + x_2 \notin H_1 \cup H_2$ et $(\varphi_1 \varphi_2)(x_1 + x_2) = 0$.

Q Calculer la dimension de $E = \{M \in \mathcal{M}_n(\mathbb{K}) \mid \forall i, \sum_j x_{ij} = 0\}$.

R On pose $\varphi_i : M \longmapsto \sum_{j=1}^n m_{ij}$. On a $E = \cap_{i=1}^n \ker(\varphi_i)$.
Soient $(\lambda_i)_i$ tels que $\sum_i \lambda_i \varphi_i = 0$. Prenons $M_i = E_{ii}$, ce qui donne $\lambda_i = 0$.
Donc $\dim(E) = n^2 - n$.

Q Soit $F = \{M \in \mathcal{M}_n(\mathbb{K}) \mid \forall j, \sum_i x_{ij} = 0\}$. Calculer la dimension de $E \cap F$.

R $E = \cap_{i=1}^n \ker(\varphi_i)$ et $F = \cap_{j=1}^n \ker(\psi_j)$.

Q Soit $E = \mathcal{M}_n(\mathbb{K})$. Montrer $F = \mathrm{Vect}(\{MN - NM \mid M, N \in E\}) = \ker \mathrm{Tr}$.

R Si $M \in F$, Alors $\mathrm{Tr}(M) = 0$. Montrons qu'on a égalité des dimensions. La trace est une forme linéaire non nulle, il faut donc montrer que F est un hyperplan. Regardons $F^\perp = \{f \in E^* \mid \forall M \in F, f(M) = 0\}$. On a $\mathrm{Tr} \in F^\perp$ et si $f \in F^\perp$, on a $\forall X, Y, f(XY - YX) = 0$ donc $f(XY) = f(YX)$ puis on conclut par la proposition 11 : $F^\perp$ est de dimension 1.

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bre99] H. Brezis : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

160 ENDOMORPHISMES REMARQUABLES D'UN ESPACE VECTORIEL EUCLIDIEN (DE DIMENSION FINIE).

Soit $(E, \langle . \mid . \rangle)$ un espace euclidien de dimension finie $n \in \mathbb{N}^*$. On note $\|.\|$ la norme issue du produit scalaire. Soit $u \in \mathcal{L}(E)$.

I. Endomorphismes d'un espace euclidien [Rom17, Ch22, p697]

I. A. Adjoint d'un endomorphisme

Théorème 1. [Adjoint d'un endomorphisme]
Il existe un unique endomorphisme $u^* \in \mathcal{L}(E)$ tel que :

$$\forall x, y \in E, \langle u(x) \mid y \rangle = \langle x \mid u^*(y) \rangle$$

u^* est appelé adjoint de u.

Proposition 2. *Soit $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E et $S = (\langle e_i \mid e_j \rangle)_{1 \leq i,j \leq n}$ la matrice du produit scalaire dans la base $\mathcal{B}$. Si $A = M_{\mathcal{B}}(u)$, alors $M_{\mathcal{B}}(u^*) = S^{-1} A^\top S$.*
En particulier si $\mathcal{B}$ est orthonormée, $M_{\mathcal{B}}(u^*) = A^\top$.

Proposition 3. [Propriétés de l'adjoint]
Pour $v, w \in \mathcal{L}(E)$ et $\lambda \in \mathbb{R}$, on a :
(i) $(v^*)^* = v$,
(ii) $(v \circ w)^* = w^* \circ v^*$,
(iii) $\ker(v^*) = \mathrm{Im}(v)^\perp$ *et* $\mathrm{Im}(v^*) = \ker(v)^\perp$,
(iv) $\mathrm{rg}(v) = \mathrm{rg}(v^*)$,
(v) Si F est un sous-espace vectoriel stable par v, alors $F^\perp$ est stable par v^*,
(vi) $|||u^*||| = |||u|||$.

I. B. Exemples d'endomorphismes remarquables

Définition 4. [Endomorphisme orthogonal]
u est un endomorphisme orthogonal (ou isométrie) de E si $u^* = u^{-1}$, autrement dit si u conserve le produit scalaire :

$$\forall x, y \in E, \langle u(x) \mid u(y) \rangle = \langle x \mid y \rangle$$

On note $\mathcal{O}(E)$ l'ensemble des isométries de E.

Proposition 5. *$v : E \longrightarrow E$ est orthogonale si et seulement si v est linéaire et conserve la norme.*

Exemple 6.
- Id_E et $-\mathrm{Id}_E$ sont des endomorphismes orthogonaux. Ce sont les seuls en dimension 1,
- les rotations et les symétries orthogonales sont des isométries,
- les valeurs propres d'une isométrie ne peuvent être que ± 1.

Proposition 7. *u est une isométrie de E si et seulement si u est inversible et $u^* = u^{-1}$.*
Dans une base $\mathcal{B}$ orthonormée de E, si $A = M_{\mathcal{B}}(u)$, on a $A^\top = A^{-1}$.

Définition 8.
- On dit que u est symétrique (ou auto-adjoint) si $u^* = u$, ou encore si

$$\forall x, y \in E, \langle u(x) \mid y \rangle = \langle x \mid u(y) \rangle$$

  On note $\mathcal{S}(E)$ l'ensemble des endomorphismes symétriques de E.
- On dit que u est anti-symétrique si $u^* = -u$. On note $\mathcal{A}(E)$ l'ensemble des endomorphismes symétriques de E.

Exemple 9. $u + u^* \in \mathcal{S}(E)$. Un projecteur orthogonal est symétrique.

Définition 10. u est dit normal si $u^* u = u u^*$.

Exemple 11. Un endomorphisme auto-adjoint, antisymétrique ou orthogonal est normal.

Proposition 12. *Soit $\mathcal{B}$ une base orthonormée de E et $A = M_{\mathcal{B}}(u)$. On a les caractérisations matricielles des endomorphismes remarquables vus précédemment :*

u	*définition*	$M_{\mathcal{B}}(u^*)$
symétrique	$u^* = u$	$A^\top = A$
anti-symétrique	$u^* = -u$	$A^\top = -A$
orthogonal	$u^* = u^{-1}$	$A^\top A = I$
normal	$u^* u = u u^*$	$A^\top A = A A^\top$

II. Endomorphismes normaux [Rom17, Ch22, p697] [Gou09, §5.3, p258]

Dans cette partie u désigne un endomorphisme normal ($u^* u = u u^*$).

Proposition 13. *On a $\|u(x)\| = \|u^*(x)\|$ pour tout $x \in E$.*

Application 14. Les valeurs propres (complexes) de u sont des racines de module 1.

Lemme 15. *Si F est un sous-espace vectoriel stable par u, alors $F^\perp$ est stable par u.*

Lemme 16. *Il existe un sous-espace vectoriel stable par u de dimension 1 ou 2.*

Proposition 17. *Supposons $n = \dim(E) = 2$. Alors :*
- *soit u a une valeur propre réelle, et alors u est diagonalisable dans une b.o.n.,*
- *soit la matrice de u dans une b.o.n. est de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.*

Théorème 18. [Réduction des endomorphismes normaux]
Il existe une base orthonormée $\mathcal{B}$ de E telle que

$$M_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_p & & & \\ & & & R_1 & & \\ & & & & \ddots & \\ & & & & & R_r \end{pmatrix}$$

où $p + 2r = n$, $(\lambda_i)_{1\le i\le p} \in \mathbb{R}^p$ et pour $1 \le k \le r$, $R_k = \begin{pmatrix} a_k & -b_k \\ b_k & a_k \end{pmatrix}$ avec $b_k \neq 0$.

Application 19. [Réduction d'un endomorphisme antisymétrique]
Supposons u antisymétrique. Alors il existe une base orthonormée $\mathcal{B}$ de E telle que

$$M_{\mathcal{B}}(u) = \begin{pmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & R_1 & & \\ & & & & \ddots & \\ & & & & & R_r \end{pmatrix} \quad \text{où} \quad 2r \le n \quad \text{et} \quad R_k = \begin{pmatrix} 0 & -b_k \\ b_k & 0 \end{pmatrix}$$

III. Endomorphismes auto-adjoints

III. A. Premières propriétés

[Rom17, Ch22, p697] [AK02, Ch7, p135]

Proposition 20. *$\mathcal{S}(E)$ est un sous-espace vectoriel de dimension $n(n+1)/2$.*

Définition 21. u est dit symétrique positif (resp. défini positif) s'il est symétrique avec $\langle x \mid u(x)\rangle \ge 0$ pour tout $x \in E$ (resp. $\langle x \mid u(x)\rangle > 0$ pour $x \in E\backslash\{0\}$). On note $\mathcal{S}^+(E)$ (resp. $\mathcal{S}^{++}(E)$) l'ensemble des endomorphismes symétriques positifs (resp. définis positifs).

Exemple 22. La matrice du produit scalaire dans une base de E est définie positive.

Proposition 23. *On a $\mathrm{Sp}(u) \subset \mathbb{R}$ pour $u \in \mathcal{S}(E)$, $\mathrm{Sp}(u) \subset \mathbb{R}_+$ pour $u \in \mathcal{S}^+(E)$ et $\mathrm{Sp}(u) \subset \mathbb{R}_+^*$ pour $u \in \mathcal{S}^{++}(E)$.*

Lemme 24. *Si $\lambda \neq \mu$, les sous-espaces propres associés $E_\lambda = \ker(u - \lambda \mathrm{id}_E)$ et $E_\mu = \ker(u - \mu \mathrm{id}_E)$ sont orthogonaux.*

Proposition 25. *Soit $A \in \mathcal{M}_{n,p}(\mathbb{R})$ avec $n \ge p$ telle que $\mathrm{rg}(A) = p$ (ou encore $\ker(A) = \{0\}$). Alors $A^\top A \in \mathcal{S}_p^{++}(\mathbb{R})$.*

Application 26. [Moindres carrés]
Soient $n, p \in \mathbb{N}$ et $A \in \mathcal{M}_{n,p}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On cherche un vecteur $x \in \mathbb{R}^p$ tel que $\|b - Ax\|_2 = \inf_{y\in\mathbb{R}^p} \|b - Ay\|_2$.
(i) Il existe toujours une solution au problème,
(ii) x est solution si et seulement si $A^\top Ax = A^\top b$,
(iii) Si $n \ge p$ et $\mathrm{rg}(A) = p$, $A^\top A$ est inversible et il existe une unique matrice réelle B triangulaire inférieure, à diagonale positive, telle que $A^\top A = BB^\top$, et alors $x = (BB^\top)^{-1}A^\top b$ est une solution.

III. B. Autour du théorème spectral

[Rom17, Ch22, p697]

Théorème 27. [Théorème spectral]
Tout endomorphisme de $\mathcal{S}(E)$ est diagonalisable dans une b.o.n.

Corollaire 28. *Soit $A \in \mathcal{S}_n(\mathbb{R})$. Alors il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que $P^\top AP$ soit diagonale.*

Corollaire 29. *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 $\mathrm{Sp}(u) \subset \mathbb{R}_+^*$.*

Application 30. Pour $A \in \mathcal{S}_n(\mathbb{R})$, on a $|||A|||_2 = \rho(A)$.

Application 31. 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 32. $\exp : \mathcal{S}_n(\mathbb{R}) \longrightarrow \mathcal{S}_n^{++}(\mathbb{R})$ *est un homéomorphisme.*

IV. Endomorphismes orthogonaux

IV. A. Propriétés et réductions

[Rom17, Ch22, p697]

Proposition 33. *Soit $u \in \mathcal{O}(E)$.*
- $\mathrm{Sp}(u) \subset \mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$,
- $\det(u) = \pm 1$. *En particulier u est inversible.*

Proposition 34. *Soit $u \in \mathcal{L}(E)$.*
(i) Si $u \in \mathcal{O}(E)$, u transforme toute b.o.n. en une b.o.n.,
(ii) $u \in \mathcal{O}(E)$ si et seulement si u transforme une b.o.n. en une b.o.n..

Théorème 35. [Réduction des endomorphismes orthogonaux]
Soit $u \in \mathcal{O}(E)$. Il existe une base orthonormée $\mathcal{B}$ telle que

$$M_{\mathcal{B}}(u) = \begin{pmatrix} I_{p_1} & & & & \\ & -I_{p_2} & & & \\ & & R_1 & & \\ & & & \ddots & \\ & & & & R_r \end{pmatrix}$$

où $p_1 + p_2 + 2r = n$ et pour $1 \leq k \leq r$, $R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$ pour un $\theta_k \notin \pi\mathbb{Z}$.

IV. B. Structure de groupe de $\mathcal{O}_n(\mathbb{R})$

[Per96, §V.4/ChVI, p125/141]

Proposition 36. *$\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$ et $\mathcal{O}_n^+(\mathbb{R}) = \{A \in \mathcal{O}_n(\mathbb{R}) \mid \det(A) = 1\}$ est un sous-groupe distingué de $\mathcal{O}_n(\mathbb{R})$.*

Définition 37. Soit u une symétrie orthogonale. On note $E^+ = \ker(u - \mathrm{Id}_E)$ et $E^- = \ker(u - \mathrm{Id}_E)$ qui vérifient $E = E^+ \oplus E^-$. Si $\dim E^- = 1$, on dit que u est une réflexion. Si $\dim E^- = 2$, on dit que u est un renversement.

Théorème 38. [Générateurs de $\mathcal{O}_n(\mathbb{R})$ et $\mathcal{O}_n^+(\mathbb{R})$]
- *$\mathcal{O}_n(\mathbb{R})$ est engendré par les réflexions orthogonales. Plus précisément, si $A \in \mathcal{O}_n(\mathbb{R})$, A est produit d'au plus n réflexions.*
- *Pour $n \geq 3$, $\mathcal{O}_n^+(\mathbb{R})$ est engendré par les réflexions orthogonales. Plus précisément, si $A \in \mathcal{O}_n^+(\mathbb{R})$, A est produit d'au plus n renversements.*

IV. C. Etude en dimensions 2 et 3

[Gri15, §7.10, p241] [Per96, §V.5, p148]

Proposition 39. [Étude en dimension 2]
Soit $u \in \mathcal{O}(\mathbb{R}^2)$ et A la matrice de u dans la base canonique de $\mathbb{R}^2$. On a deux cas :
- *soit $u \in \mathcal{O}^+(\mathbb{R}^2)$ et 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,*
- *soit $u \notin \mathcal{O}^+(\mathbb{R}^2)$ et 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 $\theta/2$.*

Proposition 40. [Étude en dimension 3]
Soit $u \in \mathcal{O}(\mathbb{R}^3)$. Il existe une base $\mathcal{B}$ de $\mathbb{R}^3$ telle que la matrice de u dans la base $\mathcal{B}$ soit :

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}$$

pour un $\theta \in [0, 2\pi[$ et où $\varepsilon = \pm 1$ vaut :
- *1 si $u \in \mathcal{O}^+(\mathbb{R}^3)$ (u est alors une rotation d'angle θ autour d'une droite),*
- *-1 si $u \notin \mathcal{O}^+(\mathbb{R}^3)$ (u est alors la composée d'une rotation d'angle θ autour d'une droite D puis d'une symétrie orthogonale par rapport à $D^\perp$).*

IV. D. Topologie du groupe orthogonal

[CG13, ChVI, p201] [Rom17, Ch22.3, p697]

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 $\mathcal{O}^+(E)$ et $\mathcal{O}^-(E)$.*

Théorème 43. [Décomposition polaire]
L'application $\begin{array}{ccc} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \longrightarrow & \mathcal{GL}_n(\mathbb{R}) \\ (O, S) & \longmapsto & OS \end{array}$ *est un homéomorphisme.*

Application 44. $\mathcal{O}_n(\mathbb{R})$ est le seul sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ contenant $\mathcal{O}_n(\mathbb{R})$.

Application 45. Pour $A \in \mathcal{M}_n(\mathbb{R})$, on a $|||A|||_2 = \sqrt{\rho(A^\top A)}$.

ANNEXE

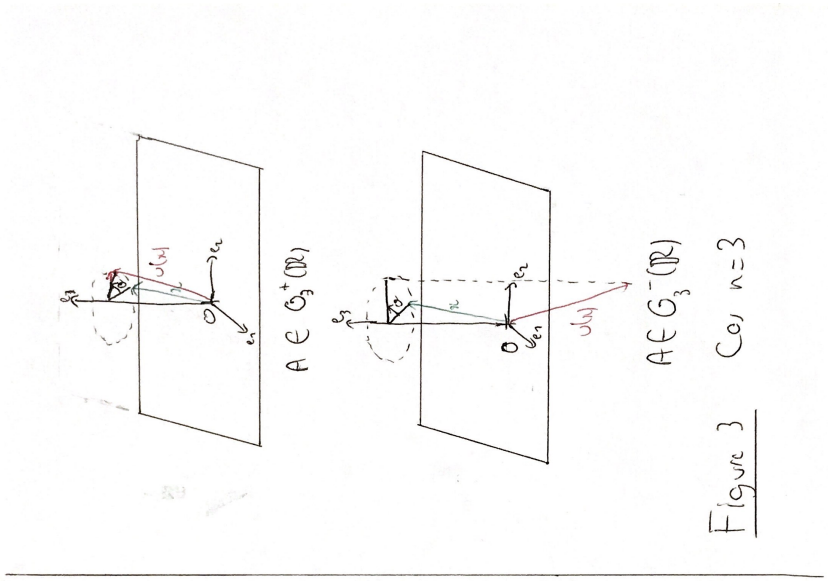


Figure 3 Cas n=3

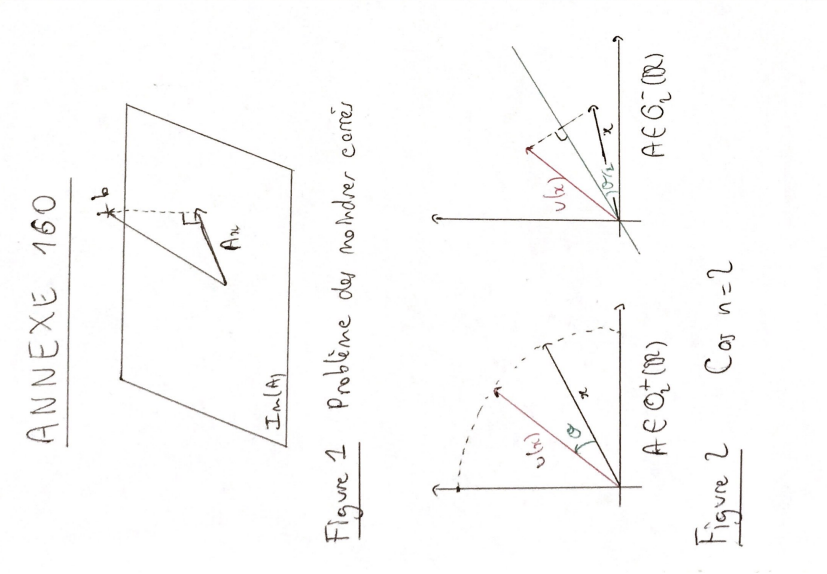


Figure 1 Problème des moindres carrés

Figure 2 Cas n=2

QUESTIONS

Q Montrer que $|||u|||_2 = |||u^*|||_2$.

R On a $\|u^*(x)\|_2^2 = \langle u^*(x) \mid u^*(x)\rangle = \langle x \mid uu^*(x)\rangle \leq \|x\| \, \|uu^*\|$, donc $|||u^*|||^2 \leq |||uu^*||| \leq |||u^*||| \, |||u|||$. Puis on procède de même pour montrer que $|||u|||^2 \leq |||u^*||| \, |||u|||$.

Q Quelle sont les utilisations des moindres carrés ?

R Enlever des dimensions à notre système (système surdéterminé). Faire une régression linéaire. On peut aussi évoquer le théorème de COCHRAN en probabilités (modèle de régression linéaire gaussien).

Q Un endomorphismes orthogonal conserve-t-il l'angle orienté ?

R Non, regarder les symétries.

Q Que font les projecteurs orthogonaux concernant les angles ?

R Ils annulent les angles.

Q Montrer par récurrence sur n que si M est nilpotente est non nulle, alors $\varphi_M(\mathbb{R}^n) = \mathbb{R}$ où $\varphi_M : X \longmapsto X^\top M X$.

R Pour $n = 1$, il n'y a rien à montrer, car toute matrice nilpotente est nulle.

Si $M \in \mathcal{M}_{n+1}(\mathbb{R})$ est nilpotente, elle est semblable à $\begin{pmatrix} A & C \\ 0 & 0 \end{pmatrix}$ où $A \in \mathcal{M}_n(\mathbb{R})$ est nilpotente. Si elle est non nulle, par hypothèse de récurrence φ_A est surjective, et donc φ_M aussi (à X on associe $(X\,0)$, leur image par A et M sont identiques. Sinon, A est nulle, et par réduction de JORDAN on peut supposer $C = (0, \dots, 0, 1)^\perp$. Prenant $X = \lambda(0, \dots, \alpha, \beta)$, on a $\varphi_M(X) = X^\top(0, \dots, 0, \beta, 0) = \alpha\beta$: c'est dont bien surjectif.
Sinon, on prend l'endomorphisme canoniquement associé à M, …

BIBLIOGRAPHIE

[AK02] G. ALLAIRE et S.-M. KABER : *Algèbre linéaire numérique*. Ellipses, 2002.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Gri15] J. GRIFONE : *Algèbre linéaire*. Cépaduès, 5ème édition, 2015.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

161 DISTANCES ET ISOMÉTRIES D'UN ESPACE AFFINE EUCLIDIEN.

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n, et $\mathcal{E}$ un espace affine dirigé par E.

I. Distances d'un espace affine euclidien

I. A. Définitions et premières propriétés [Aud06, ChII, p51]

On munit E d'un produit scalaire : E est un espace vectoriel euclidien, $\mathcal{E}$ est un espace affine euclidien
Distance entre deux points de $\mathcal{E}$, c'est bien une distance (inégalité triangulaire ...)
Distance à un sous-espace affine, lien avec le projeté orthogonal

I. B. Matrice et déterminant de Gram [Gou09, §5.4, p262] [Rom17, §17.4.7, p560]

Définition 1. [Matrice et déterminant de Gram]
Soient $x_1, \dots, x_n$ des vecteurs de E. On appelle matrice de Gram de $x_1, \dots, x_n$ la matrice $M_G(x_1, \dots, x_n) = (\langle x_i \mid x_j \rangle)_{1 \leq i,j \leq n}$ et déterminant de Gram de $x_1, \dots, x_n$ le déterminant de la matrice de Gram, noté $G(x_1, \dots, x_n)$.

Lemme 2. *$G(x_1, \dots, x_n) \geq 0$ et $G(x_1, \dots, x_n) = 0$ si et seulement si $(x_i)_{1 \leq i \leq n}$ est liée.*

Théorème 3. [Distance à un sous-espace vectoriel]
Soit F un sous-espace vectoriel de dimension finie n de E, muni d'une base $(e_1, \dots, e_n)$. 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 4. [Inégalités de Hadamard] **[voir annexe]**
(i) Soient $x_1, \dots, x_n$ des vecteurs de E. Alors $G(x_1, \dots, x_n) \leq \prod_{i=1}^n \|x_i\|^2$.
(ii) Soient $x_1, \dots, x_n$ des vecteurs de $\mathbb{R}^n$. Alors $|\det(x_1, \dots, x_n)| \leq \prod_{i=1}^n \|x_i\|_2$, où $\|.\|_2$ désigne la norme euclidienne standard sur $\mathbb{R}^n$.
Dans les deux points, on a égalité si et seulement si la famille $\{x_i\}_{1 \leq i \leq n}$ est orthogonale ou l'un des vecteurs est nul.

Application 5. Interprétation géométrique de l'inégalité de Hadamard dans $\mathbb{R}^n$.

Corollaire 6. *Expression de la projection de x sur F à l'aide de matrices de Gram.*

II. Isométries d'un espace affine euclidien [Aud06, ChII, p51]

II. A. Définitions et premières propriétés [Tau06, Ch6, p91]

Isométrie vectorielle, isométrie affine, example des translations, des symétries orthogonales (par rapport à un sous-espace vectoriel F de E ou un sous-espace affine $\mathcal{F}$ de $\mathcal{E}$) $\rightarrow$ réflexion
Groupe $\mathcal{O}(E)/\operatorname{Isom}(\mathcal{E})$ des isométries vectorielles/affines
F sous-espace vectoriel f-stable implique $F^\perp$ sous-espace vectoriel f-stable

II. B. Structure des isométries

Cas où $\mathcal{E} = \mathcal{P}$: selon le nombre de points fixes de l'isométrie, on l'écrit comme composée d'une, deux ou trois réflexions.
Les réflexions engendrent $\mathcal{O}(E), \operatorname{Isom}(\mathcal{E})$
Déplacement, anti-déplacement
Les isométries sont des bijections, $\operatorname{Isom}^+(\mathcal{E})$ est un sous-groupe distingué, déplacements préservent les orientations de l'espace
Forme réduite des isométries affines
Réduction des isométries affines, écriture matricielle
Connexité par arcs de $\mathcal{O}_n^+(\mathbb{R})$. $\mathcal{O}_n(\mathbb{R})$ a deux composantes connexes par arcs homéomorphes
$\operatorname{Isom}^+(\mathcal{E})$ est connexe par arcs

III. Isométries en dimension 2 et 3

III. A. Classification des isométries [Gri15, §7.10, p241] [Per96, §V.5, p148]

En dimension 2, les isométries vectorielles sont les rotations et les réflexions

Proposition 7. [Étude en dimension 2]
Soit $u \in \mathcal{O}(\mathbb{R}^2)$ et A la matrice de u dans la base canonique de $\mathbb{R}^2$. On a deux cas :
- *soit $u \in \mathcal{O}^+(\mathbb{R}^2)$ et 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,*
- *soit $u \notin \mathcal{O}^+(\mathbb{R}^2)$ et 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 $\theta/2$.*

Les isométries affines sont les translations, les rotations, les réflexions et les symétries glissées.
En dimension 3, les isométries vectorielles sont les réflexions, les rotations autour d'un axe et les antirotations :

Proposition 8. **[Étude en dimension 3]**
Soit $u \in \mathcal{O}(\mathbb{R}^3)$. Il existe une base $\mathcal{B}$ de $\mathbb{R}^3$ telle que la matrice de u dans la base $\mathcal{B}$ soit :

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}$$

pour un $\theta \in [0, 2\pi[$ et où $\varepsilon = \pm 1$ vaut :
- *1 si $u \in \mathcal{O}^+(\mathbb{R}^3)$ (u est alors une rotation d'angle θ autour d'une droite),*
- *-1 si $u \notin \mathcal{O}^+(\mathbb{R}^3)$ (u est alors la composée d'une rotation d'angle θ autour d'une droite D puis d'une symétrie orthogonale par rapport à $D^\perp$).*

Classification des isométries affines selon la partie linéaire et l'existence de point fixe : réflexion, symétrie glissée, rotation, vissage, anti-rotation

III. B. Similitudes et figures stables en dimension 2 [Aud06, §III.3, p89]

Similitudes, exemples des isométries, des homothéties
Point invariant d'une similitude
Les similitudes directes conservent les angles, envoient droites et cercles sur droites et cercles

III. C. Isométries préservant des parties de $\mathcal{E}$
[Rom17, §3.4, p84] [Aud06, ChIII/V, p360] [Szp09, §8.II.6/8.III.3, p410/421]

Dans le plan : on définit le sous-groupe D_{2n} de $\mathcal{O}_2(\mathbb{R})$ des isométries préservant un polygone régulier à n sommets
D_{2n} est engendré par la symétrie et la rotation d'angle $\frac{2\pi}{n}$, d'ordre 2 et 4, ce qui donne la liste des éléments de D_{2n}

Application 9. D_{2n} s'injecte naturellement dans $\mathcal{GL}_2(\mathbb{C})$, envoyant la rotation d'angle $2\pi/n$ et la symétrie sur

$$R = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Enumérations des isométries positives, des isométries négatives du groupe diédral
Dans l'espace, regardons les isométries préservant certaines figures
Définition d'un polyèdre.
L'isobarycentre est conservé par une isométrie (en particulier un potentiel centre de symétrie)
Bijection isométries positives/négatives
Isométries préservant le tétraèdre régulier

Théorème 10. $\mathrm{Isom}(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ *et* $\mathrm{Isom}^+(\mathcal{C}) \simeq \mathfrak{S}_4$.

Lien entre les isométries du tétraèdre et du cube

ANNEXE

interprétation du déterminant de Gram comme volume
rotations, vissage, anti-rotations, etc
similitudes,
groupes diédraux, cube, tétraèdre

QUESTIONS

Q Que dire de $M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in \mathcal{O}_3(\mathbb{R})$?

R La matrice permutte les vecteurs de la base. C'est une isométrie positive, donc une rotation. On remarque que $(1,1,1)$ est invariant donc on connaît l'axe de la droite. Puis en prenant la trace, on a $1 + 2\cos(\theta) = \mathrm{Tr}(M) = 0$ donc $\theta = \frac{2\pi}{3}$.

Q Soit $\varphi_{\theta,b} : z \longmapsto \mathrm{e}^{i\theta} z + b$ et $\psi_{\theta,b} : z \longmapsto \mathrm{e}^{i\theta} \overline{z} + b$. Ce sont des similitudes (directes pour φ, indirectes pour ψ). Parmi celles-ci, lesquelles sont des symétries ? Des symétries glissées ?

R On regarde les conditions sur θ, b pour que ψ soit une réflexion.
On doit tomber sur $\mathrm{e}^{i\theta}\,\overline{b} + b = 0$.

Q Soit $a_1, \dots, a_n \in \mathbb{R}^p$. A quelle condition sur ces points existe-t-il $M_1, \dots M_n$ tels que $A_i = \frac{M_i + M_{i+1}}{2}$ pour tout i.

R On a $M_{i+1} = 2A_i - M_i = f_i(M_i)$ où f_i est la symétrie de centre A_i fixe. Donc si l'on a M_1, on a tous les autres points et il faut que $M_1 = f_n(f_{n-1}(\dots(M_1))) = f(M_1)$.
Or $\vec{f_i} = -\mathrm{id}$ donc si n est impair, f est une symétrie centrale de centre M_1.

BIBLIOGRAPHIE

[Aud06] M. Audin : *Géométrie*. EDP Sciences, 2006.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Gri15] J. Grifone : *Algèbre linéaire*. Cépaduès, 5ème édition, 2015.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Szp09] A. Szpriglas : *Algèbre L3*. Pearson Education, 2ème édition, 2009.

[Tau06] P. Tauvel : *Analyse complexe pour la Licence 3*. Dunod, 2006.

162 SYSTÈMES D'ÉQUATIONS LINÉAIRES ; OPÉRATIONS ÉLÉMENTAIRES, ASPECTS ALGORITHMIQUES ET CONSÉQUENCES THÉORIQUES.

Soit $\mathbb{K}$ un corps et n, p des entiers non nuls.
On considère le système de n équations à p inconnues à coefficients dans $\mathbb{K}$ défini par :

$$(\mathscr{S}_B) \quad \begin{cases} a_{1\,1}\,x_1 + \cdots + a_{1\,p}\,x_p = b_1 \\ \vdots \\ a_{n\,1}\,x_1 + \cdots + a_{n\,p}\,x_p = b_n \end{cases}$$

où les $(a_{i\,j})_{1\leq i\leq n,\,1\leq j\leq p}$ et les $(b_i)_{1\leq i\leq n}$ sont des éléments de $\mathbb{K}$.

I. Généralités

[CG13, ChIV, p127]

I. A. Conditions d'existence et d'unicité de solutions

Définition 1. On appelle solution de $(\mathscr{S}_B)$ tout vecteur $x = (x_1, \ldots, x_p) \in \mathbb{K}^p$ satisfaisant les n équations. On dira que $(\mathscr{S}_B)$ est compatible s'il admet au moins une solution. On notera alors S_B l'ensemble des solutions.
Lorsque $b_1 = \cdots = b_n = 0$, on dit que $(\mathscr{S}_B)$ est homogène.

Exemple 2. Le système $\begin{cases} x + y = 2 \\ x - y = 0 \\ 2x + y = 0 \end{cases}$ n'est pas compatible.

En notant $A = (a_{i\,j})_{1\leq i\leq n,\,1\leq j\leq p} \in \mathcal{M}_{n\,p}(\mathbb{K})$, $B = (b_1 \ldots b_n)^\top \in \mathcal{M}_{n\,1}(\mathbb{K})$ et $X = (x_1, \ldots, x_p)^\top \in \mathcal{M}_{p\,1}(\mathbb{K})$, le système $(\mathscr{S}_B)$ se réécrit $AX = B$.

Théorème 3. *Le système est compatible si et seulement si $B \in \mathrm{Im}(A)$. Dans ce cas, S_B est un espace affine dirigé par $\ker(A)$ et de dimension $p - \mathrm{rg}(A)$.*

Définition 4. [Système de Cramer]
Lorsque $n = p$ et $A \in \mathcal{GL}_n(\mathbb{K})$, on dit que $(\mathscr{S}_B)$ est un système de Cramer.

Théorème 5. [Système de Cramer]
Si $(\mathscr{S}_B)$ est un système de Cramer, il admet une unique solution, égale à $X = A^{-1}B$. De plus, on a les formules de Cramer :

$$\forall i \in [\![1, p]\!],\ x_i = \frac{\det(C_1, \ldots, C_{i-1}, B, C_{i+1}, \ldots, C_n)}{\det(A)}$$

où les $(C_j)_{1\leq j\leq n}$ sont les colonnes de A.

I. B. Cas de matrices triangulaires

Application 6. [Méthode des remontées]
Si $A \in \mathcal{GL}_n(\mathbb{K}) \cap \mathcal{TS}_n(\mathbb{K})$, le système se résout en résolvant chacune des équations de la dernière à la première : on calcule x_n solution de $x_n = \frac{1}{a_{n\,n}} b_n$, puis $x_{n-1} = \frac{1}{a_{n-1\,n-1}}(b_{n-1} - a_{n-1\,n}x_n)$, …, jusqu'à $x_1 = \frac{1}{a_{1\,1}}(b_1 - \sum_{j=2}^{n} a_{1\,j}x_j)$.

Remarque 7. Lorsque A n'est plus inversible, on peut toujours effectuer la méthode des remontées : les étapes i telles que $a_{i\,i} = 0$ constituent alors des équations de compatibilité.

Exemple 8. Résolution de $\begin{cases} 2x - z = 0 \\ my + 3z = 12 \\ 2z = 8 \end{cases}$ où $m \in \mathbb{R}$ est un paramètre.

II. Résolution pratique d'un système linéaire

[CG13, ChI, p2]

II. A. Algorithme du pivot de Gauss

Proposition 9. *L'ensemble des solutions de $(\mathscr{S}_B)$ ne change pas si l'on effectue les opérations élémentaires suivantes :*
- *si l'on ajoute à une équation une combinaison linéaire des autres,*
- *si l'on multiplie une équation par un scalaire non nul,*
- *si l'on change l'ordre des équations.*

Définition 10. [Matrices de dilatation, transvection, permutation élémentaire]
Une matrice de dilatation est une matrice $D_{i,\alpha} \in \mathcal{GL}_n(\mathbb{K})$ pour un $\alpha \in \mathbb{K}^*$. Une matrice de transvection est une matrice $T_{i,j,\beta} = I_n + \beta E_{i,j} \in \mathcal{GL}_n(\mathbb{K})$ pour un $\beta \in \mathbb{K}^*$ et $i \neq j$. Une matrice de permutation élémentaire est une matrice $P_{i,j} \in \mathcal{GL}_n(\mathbb{K})$ pour un $i < j$.

$$D_{i,\alpha} = \begin{pmatrix} I_{i-1} & & \\ & \alpha & \\ & & I_{n-i} \end{pmatrix} \qquad P_{i,j} = \begin{pmatrix} I_{i-1} & & & & \\ & 0 & & 1 & \\ & & I_{j-i-1} & & \\ & 1 & & 0 & \\ & & & & I_{n-j} \end{pmatrix}$$

Proposition 11. *Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. Les opérations élémentaires sur les lignes (resp. colonnes) de M sont obtenues par multiplication à gauche (resp. à droite) par les matrices précédemment introduites :*

Matrice	$D_{i,\alpha}M$	$T_{i,j\beta}M$	$P_{i,j}M$	$MD_{i,\alpha}$	$\dots$
Opération	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \beta L_j$	$L_i \leftrightarrow \alpha L_j$	$C_i \leftarrow \alpha C_i$	$\dots$

Définition 12. On appelle :
- pivot d'une ligne son coefficient non nul le plus à gauche.
- 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 (resp. réduite) en colonnes.

Exemple 13. $\begin{pmatrix} 1 & 2 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ est réduite en lignes, $\begin{pmatrix} 2 & 0 & 0 \\ 1 & 3 & 0 \\ 2 & 4 & 0 \end{pmatrix}$ est échelonnée en colonnes.

Définition 14. [Action par translation]
On définit les actions par translation/multiplication à gauche et à droite :

$$\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ (P, M) & \longmapsto & PM \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathcal{GL}_p(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ (P, M) & \longmapsto & MP^{-1} \end{array}$$

Théorème 15. [Orbites de l'action par multiplication à gauche]
Pour l'action par multiplication à gauche :
- *deux matrices A et A' sont dans la même orbite si et seulement si $\ker(A) = \ker(A')$,*
- *toute matrice est dans l'orbite d'une unique matrice réduite en lignes.*

Théorème 16. [Orbites de l'action par multiplication à droite]
Pour l'action par multiplication à droite :
- *deux matrices A et A' sont dans la même orbite si et seulement si $\mathrm{Im}(A) = \mathrm{Im}(A')$,*
- *toute matrice est dans l'orbite d'une unique matrice réduite en colonnes.*

Application 17. [Algorithme du pivot de Gauss]
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.

Exemple 18. $\begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 0 \\ 0 & 5 & 2 \end{pmatrix}$ a pour matrice réduite associée $\begin{pmatrix} 1 & 2 & 1/2 \\ 0 & 1 & -1/2 \\ 0 & 0 & 1 \end{pmatrix}$.

Remarque 19.
- Il y a $\mathrm{rg}(A)$ pivots. Les $n - r$ dernières lignes de la forme réduite donnent alors des équations de compatibilité du système sur le second membre.
- Lorsque $n = p$ et A est inversible, la forme réduite est triangulaire supérieure avec coefficients non nuls et on peut via des opérations élémentaires sur les colonnes se ramener à la matrice identité, ce qui permet un calcul pratique de l'inverse de A.
- Lorsque $p \geq n$ et la matrice est de rang n, on peut définir des inconnues principales associées aux colonnes des pivots, les autres inconnues devenant alors des paramètres.

Exemple 20. On cherche à résoudre le système $(\mathscr{S}_B)$, de paramètre $a \in \mathbb{R}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 6 & 10 \\ -1 & -2 & -2 \end{pmatrix} X = \begin{pmatrix} 4 \\ 17 \\ 1+a \end{pmatrix}$, équivalent au système $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} X = \begin{pmatrix} 4 \\ 5 \\ a \end{pmatrix}$.
On a donc une condition de compatibilité pour avoir existence d'une solution : il faut que $a = 0$. Si c'est le cas, on peut par exemple paramétrer les solutions selon x_2 en résolvant $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4 - 2x_2 \\ 5 \end{pmatrix}$ qui admet bien une unique solution (à x_2 fixé).

II. B. Applications

[AK02, PIII/Ch7, p105/135]

Théorème 21. *$\mathcal{SL}_n(\mathbb{K})$ est engendré par les transvections, $\mathcal{GL}_n(\mathbb{K})$ est engendré par les transvections et les dilatations.*

Théorème 22. [Factorisation LU]
Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice dont tous les mineurs principaux sont non nuls. Alors il existe un unique couple (L, U) de matrices tel que L est triangulaire inférieure avec diagonale de 1, U est triangulaire supérieure et $A = LU$.

Théorème 23. [Factorisation de Cholesky]
Soit A une matrice symétrique réelle définie positive. Alors il existe une unique matrice B triangulaire inférieure telle que tous ses éléments diagonaux soient positifs et $A = BB^*$.

Exemple 24. $\begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & 0 \\ 3 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

$$\begin{pmatrix} 16 & 8 & 20 \\ 8 & 13 & 10 \\ 20 & 10 & 26 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 2 & 3 & 0 \\ 5 & 0 & 1 \end{pmatrix} \begin{pmatrix} 4 & 2 & 5 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Application 25. [Résolution de $(\mathscr{S}_B)$]
Si $A \in \mathcal{GL}_n(\mathbb{K})$ admet une décomposition $A = LU$, on résout $(\mathscr{S}_B)$ en résolvant $LY = B$ puis $UX = Y$. Ces deux systèmes étant triangulaires, ils ont un coût moins important.
De même dans le cas de la factorisation de Cholesky.

Exemple 26. $\begin{pmatrix} 16 & 8 & 20 \\ 8 & 13 & 10 \\ 20 & 10 & 26 \end{pmatrix} X = \begin{pmatrix} 0 \\ 27 \\ -2 \end{pmatrix}$ donne $Y = \begin{pmatrix} 0 \\ 9 \\ -2 \end{pmatrix}$ puis $X = \begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix}$.

III. Résolution numérique

III. A. Minimisation de fonctionnelle

[FGN12, §1.21, p39–41]

On suppose dans cette section que $n = p$ et $A \in \mathcal{S}_n^{++}(\mathbb{R})$ est une matrice symétrique définie positive. On pose $\langle . \mid . \rangle$ le produit scalaire usuel sur $\mathbb{R}^n$.

Proposition 27. *La résolution de $(\mathscr{S}_B)$ est équivalente au problème de minimisation de $f : x \longmapsto \frac{1}{2}\langle AX \mid X\rangle - \langle B \mid X\rangle$: f admet en effet un unique minimum X_0, caractérisé par $AX_0 = B$.*

Théorème 28. [Méthode de gradient à pas optimal]
Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$ elliptique, c'est-à-dire f est $\mathcal{C}^1$ et telle qu'il existe $\alpha > 0$ satisfaisant

$$\forall x, y \in \mathbb{R}^p, \langle \nabla f(x) - \nabla f(y) \mid x - y\rangle \geq \alpha \|x - y\|^2$$

Alors la suite $(x_n)_{n\in\mathbb{N}}$ définie par $x_0 \in \mathbb{R}^p$ et $x_{n+1} = x_n - \rho_n \nabla f(x_n)$ où $\rho_n = \operatorname{argmin}_{\rho>0} f(x_n - \rho\nabla f(x_n))$ converge vers l'unique minimum global de f.

Application 29. Prenant f la fonctionnelle quadratique définie précédemment, on obtient la convergence de toute suite $(x_n)_{n\in\mathbb{N}}$ définie par $x_0 \in \mathbb{R}^p$ et $x_{n+1} = x_n - \rho_n \nabla f(x)$

III. B. Méthode des moindres carrés

[AK02, Ch7, p135]

Proposition 30. *Soit $A \in \mathcal{M}_{n,\,p}(\mathbb{R})$ avec $n \geq p$ telle que $\operatorname{rg}(A) = p$ (ou encore $\ker(A) = \{0\}$). Alors $A^\top A \in \mathcal{S}_p^{++}(\mathbb{R})$.*

Application 31. [Moindres carrés]
Soient $n, p \in \mathbb{N}$ et $A \in \mathcal{M}_{n,\,p}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On cherche un vecteur $x \in \mathbb{R}^p$ tel que $\|b - Ax\|_2 = \inf_{y\in\mathbb{R}^p} \|b - Ay\|_2$.

(i) Il existe toujours une solution au problème,
(ii) x est solution si et seulement si $A^\top Ax = A^\top b$,
(iii) Si $n \geq p$ et $\operatorname{rg}(A) = p$, $A^\top A$ est inversible et il existe une unique matrice réelle B triangulaire inférieure, à diagonale positive, telle que $A^\top A = BB^\top$, et alors $x = (BB^\top)^{-1}A^\top b$ est une solution.

Application 32. [Régression linéaire en statistiques]
Etant donnés des points $(x_i, y_i)_{1\leq i\leq n}$, on souhaite tester si les points sont plus ou moins alignés. Pour cela, on cherche la droite $y = ax + b$ de meilleure approximation, c'est-à-dire on cherche a et b minimisant $\sum_{1\leq i\leq n} |y_i - ax_i - b|^2$. On se ramène donc au problème précédent en posant $A = \begin{pmatrix} 1 & x_1 \\ \vdots & \vdots \\ 1 & x_n \end{pmatrix}$ et $X = \begin{pmatrix} b \\ a \end{pmatrix}$.

ANNEXE

Moindres carrés

SPEECH

La formule de CRAMER permet la résolution de systèmes linéaires mais est beaucoup trop complexe en pratique, on envisage d'autres méthodes de résolution. Dans le cas d'une matrice triangulaire, par exemple, on a une complexité en n^2 avec la méthode des remontées.

QUESTIONS

Q Soit $n \geq 2$ et $a_1, \dots, a_n \in \mathbb{K}$. Soient $P_1, \dots, P_n \in \mathbb{R}[X]$ tels que $\deg P_k = k-1$. Calculer $\det(P_i(a_j))_{i,j}$.

R Notons M la matrice en question. On suppose les polynômes unitaires pour simplifier. La famille est une base car est échelonnée en degrés.
On se ramène à la base canonique par transvections (ou par procédé d'orthogonalisation de GRAM-SCHMIDT), ce qui donne le déterminant de VANDERMONDE, soit $\prod_{i<j}(a_j - a_i)$.

Q Calculer le déterminant de $\begin{pmatrix} \alpha_1 & a & \dots & a \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a \\ b & \dots & b & \alpha_n \end{pmatrix}$.

R Regardons le polynôme $x \longmapsto \det((m_{ij} + x))$ de degré au plus n. Par des opérations sur les lignes, on enlève les x de chaque ligne sauf la première, ce qui montre en fait que le polynôme est de degré 1.
Appliquons ceci à la matrice. En évaluant en $-a$ et en $-b$, on obtient deux points d'annulation si $a \neq b$, et donc le déterminant est nul.
Si $a = b$, on utilise la continuité du déterminant par rapport aux coefficients. On pose $f(x) = u(a,b)x + v(a,b)$ où $u, v \in \mathcal{C}^\infty$.

Q Montrer que $\mathcal{SL}_n(\mathbb{R})$ est connexe par arcs.

R Utiliser le fait que $\mathcal{SL}_n(\mathbb{R})$ est engendré par les transvections.

Q Montrer que $\mathcal{GL}_n(\mathbb{R})$ est engendré par les inversibles diagonalisables.

BIBLIOGRAPHIE

[AK02] G. ALLAIRE et S.-M. KABER : *Algèbre linéaire numérique*. Ellipses, 2002.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[FGN12] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

170 FORMES QUADRATIQUES SUR UN ESPACE VECTORIEL DE DIMENSION FINIE. ORTHOGONALITÉ, ISOTROPIE. APPLICATIONS.

E est un $\mathbb{K}$-espace vectoriel de dimension finie n, où $\mathbb{K}$ est un corps de caractéristique différente de 2.

I. Généralités sur les formes quadratiques

[Rom17, Ch15, p463] [De 11, ChI–IV, p6]

I. A. Formes bilinéaires et formes quadratiques

Forme bilinéaire (symétrique), matrice d'une forme bilinéaire dans une base, expression en produit matriciel
Forme quadratique, forme polaire associée. Matrice d'une forme quadratique, expression en produit matriciel
Exemples : polynômes homogènes de degré 2, exemple de $M \longmapsto \mathrm{Tr}(M^2)$ sur $\mathcal{M}_n(\mathbb{R})$.
En fait si on fixe une base, q est un polynôme homogène de degré 2 explicité par la matrice de q dans la base
Exemples

Proposition 1. *Soit q une forme quadratique. L'ensemble des matrices représentant q dans des bases de E est exactement l'une des orbites de l'action par congruence sur $\mathcal{S}_n(\mathbb{K})$:*

$$\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) & \longrightarrow & \mathcal{S}_n(\mathbb{K}) \\ (P, S) & \longmapsto & PSP^\top \end{array}$$

Définition 2. [discriminant]
On définit le discriminant de $S \in \mathcal{S}_n(\mathbb{K})$ par $\overline{\det(S)} \in \mathbb{K}^*/(\mathbb{K}^*)^2$ si S est inversible, 0 sinon.

Proposition 3. *Deux matrices congruentes ont même discriminant. Ainsi on peut donc définir le discriminant d'une forme quadratique.*

I. B. Objets associés aux formes quadratiques

Vecteurs orthogonaux, propriétés, noyau d'une forme quadratique, lien avec le noyau de la matrice de la forme quadratique, rang, forme dégénérée
Vecteurs isotropes, cône isotrope, orthogonal
Exemples
Théorème d'existence d'une base formée de vecteurs isotropes sous conditions

II. Réduction des formes quadratiques

[Rom17, Ch15, p463] [De 11, ChV.3, p93] [CG13, ChV.D, p97]

Théorème 4. [réduction de Gauss]
Pour toute forme quadratique réelle q sur E, il existe un entier r, $\lambda_1, \dots, \lambda_r \in \mathbb{R}^*$ et $\ell_1, \dots, \ell_r$ des formes linéaires indépendantes tels que $q(x) = \sum_{i=1}^r \lambda_i \ell_i$.

Corollaire 5. *La forme polaire associée à q est alors $\varphi(x, y) = \sum_{i=1}^r \lambda_i \ell_i(x)\ell_i(y)$.*

Exemple 6. $q(x, y, z) = -x^2 - y^2 - z^2 + 2(xy + xz + yz) = -(x - y - z)^2 + (y + z)^2 + (y - z)^2$

Corollaire 7. *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 $i > r$. En particulier $r = \mathrm{rg}(q)$ et $\ker(q) = \cap_{i=1}^r \ker \ell_i$.*

Regardons maintenant plus en détail le cas $\mathbb{K} = \mathbb{R}$.

Corollaire 8. *Notons $s = \mathrm{card}(\{i \mid \lambda_i > 0\})$ et $t = \mathrm{card}(\{i \mid \lambda_i < 0\})$. Alors la matrice de q dans une certaine base est $\mathrm{diag}(I_s, -I_t, 0_{n-(s+t)})$.*

Forme (définie) positive, inégalité de Cauchy-Schwarz pour une forme quadratique positive

Proposition 9. [loi d'inertie de Sylvester]

- *s et t sont uniques (ne dépendent par de la décomposition de Gauss choisie) et déterminés par :*

$$s = \max\{\dim(F) \mid F \in \mathcal{P}\} \qquad t = \max\{\dim(F) \mid F \in \mathcal{N}\}$$

  où $\mathcal{P}$ (resp. $\mathcal{N}$) désigne l'ensemble des sous-espaces de $\mathbb{R}^n$ sur lesquels la restriction de q est définie positive (resp. définie négative). De plus $r = s + t$.
- *Soit $(e_i)_{1 \le i \le n}$ une base de $\mathbb{R}^n$ orthogonale pour q. Alors s est le nombre de vecteurs $(e_i)_{1 \le i \le n}$ tels que $q(e_i) > 0$ et t est le nombre de vecteurs $(e_i)_{1 \le i \le n}$ tels que $q(e_i) < 0$.*

Définition 10. (s, t) s'appelle la signature de q.

Exemple 11. La signature de $M \longmapsto \mathrm{Tr}(M^2)$ est $(n(n+1)/2, n(n-1)/2)$.

Application 12. [Forme de Hankel]
Soit $P \in \mathbb{R}[X]$ de degré n et $x_1, \dots, x_t$ ses racines distinctes, de multiplicité $m_1, \dots, m_t$. On définit $s_k = \sum_{\ell=1}^{t} m_\ell x_\ell^k$ pour $k \in \mathbb{N}$ puis on pose

$$\forall (X_0, \dots, X_{n-1}) \in \mathbb{C}^n, s(X_1, \dots, X_n) = \sum_{0 \leq i,j \leq n-1} s_{i+j} X_i X_j$$

Alors $s_{\mathbb{R}}$ (la restriction de s à $\mathbb{R}^n$) est une forme quadratique sur $\mathbb{R}^n$, de signature (p, q) où $p + q = t$ et $p - q$ est le nombre de racines réelles de P.

III. Classification des formes quadratiques

[Rom17, Ch15, p463] [CG13, ChV.B, p179] [De 11, ChV/VI, p87/100]

Remarque 13. Classifier les formes quadratiques revient à chercher les orbites l'action par congruence l'action.

Soit q une forme quadratique sur E de rang r.

III. A. Sur $\mathbb{C}$

Théorème 14. [classification sur $\mathbb{K} = \mathbb{C}$ (ou $\mathbb{K}$ algébriquement clos)]
La matrice de q dans une certaine base est $J_r = \mathrm{diag}(I_r, 0_{n-r})$. Dans cette base on a donc $q(x_1, \dots, x_n) = x_1^2 + \cdots + x_r^2$.

Corollaire 15. *Deux formes quadratiques sur un $\mathbb{C}$-espace vectoriel sont congruentes si et seulement si elles ont même rang.*

Application 16. Il y a $n + 1$ classes de congruences de formes quadratiques sur E.

III. B. Sur $\mathbb{R}$

Notons (s, t) la signature de q.

Théorème 17. [classification sur $\mathbb{K} = \mathbb{R}$]
La matrice de q dans une certaine base est $\begin{pmatrix} I_s & & \\ & -I_t & \\ & & 0_{n-r} \end{pmatrix}$. Dans cette base on a donc $q(x_1, \dots, x_n) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_r^2$.

Corollaire 18. *Deux formes quadratiques sur un $\mathbb{R}$-espace vectoriel sont congruentes si et seulement si elles ont même signature.*

Application 19. Il y a $r + 1$ classes de congruences de formes quadratiques de rang r sur E.

III. C. Sur $\mathbb{F}_q$

On suppose $\mathbb{K} = \mathbb{F}_q$ où $q = p^\ell$ pour un p premier impair et $\ell \in \mathbb{N}^*$.
On note $\mathbb{F}_q^2 = \left\{x^2 \,|\, x \in \mathbb{F}_q\right\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 20. *$\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.*

Théorème 21. [classification sur $\mathbb{K} = \mathbb{F}_q$]
Soit $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$.
La matrice de q dans une certaine base est $\begin{pmatrix} I_{r-1} & & \\ & \delta & \\ & & 0_{n-r} \end{pmatrix}$ où $\delta \in \{1, \alpha\}$.

Application 22. Il y a $2n + 1$ classes de congruences de formes quadratiques sur E.

Théorème 23. [loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \quad \text{où} \quad \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } x = 0 \\ -1 & \text{sinon} \end{cases}$$

Exemple 24. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

COMMENTAIRES

Autres références : [Gou09, Per96].
Attention à la caractéristique 2 qui est un cas particulier, pour lequel les résultats sont rapidement faux

QUESTIONS

Q À quoi servent les formes de HANKEL ?

R Cela permet de calculer la forme de GAUSS sans connaître les racines.

Q Soit $A \in \mathcal{M}_n(\mathbb{K})$ et $q(x) = X^\top AX$. Trouver la forme polaire associée.

R Soit $\varphi(X,Y) = X^\top AY$. On a $A = \frac{A+A^\top}{2} + \frac{A-A^\top}{2}$. On vérifie que $\phi(X,Y) = X^\top(\frac{A+A^\top}{2})Y$ fonctionne.

Q La matrice d'une forme quadratique correspond-elle à la matrice d'une autre application ?

R On introduit les fonctions $\varphi_g : E \longrightarrow E^*, x \longmapsto \varphi(x,.)$ et $\varphi_d : E \longrightarrow E^*, x \longmapsto \varphi(.,x)$. A est alors la matrice de ces applications dans la base duale de la base associée à la matrice A.

Q $\det : \mathcal{M}_2(\mathbb{K}) \longrightarrow \mathbb{K}$ est-elle une forme quadratique ? Quel est son rang ? Son discriminant ? Quelle est la signature si $\mathbb{K} = \mathbb{R}$? Sur un corps fini, à quelle matrice est-elle congruente ?

R C'est un polynôme homogène de degré 2 en les coordonnées des matrices, donc c'est une forme quadratique.
Pour trouver son rang, soit on utilise la forme bilinéaire associée, soit on calcule sa réduction de GAUSS. On a :

$$\det = E_1E_4 - E_2E_3 = \frac{1}{4}((E_1+E_4)^2 - (E_1-E_4)^2 - (E_2+E_3)^2 + (E_2-E_3)^2)$$

Donc $\mathrm{rg}(\det) = 4$.
Par ailleurs, la matrice associée dans une bonne base est :

$$\begin{pmatrix} 0 & 0 & 0 & 1/2 \\ 0 & 0 & -1/2 & 0 \\ 0 & -1/2 & 0 & 0 \\ 1/2 & 0 & 0 & 0 \end{pmatrix}$$

On obtient le (un) discriminant $1/16$, donc 1. Une autre manière de l'obtenir est d'utiliser la base de la réduction de GAUSS.
Si $\mathbb{K} = \mathbb{R}$, on aurait pour signature $(2,2)$. Sur $\mathbb{F}_q$, elle est congruente à l'identité.

Q Questions sur le plan hyperbolique.

Q Exemple concret de hessienne.

BIBLIOGRAPHIE

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[De 11] C. DE SEGUINS PAZZIS : *Invitation aux formes quadratiques*. Calvage et Mounet, 2011.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

171 FORMES QUADRATIQUES RÉELLES. CONIQUES. EXEMPLES ET APPLICATIONS.

I. Formes quadratiques réelles

[Rom17, Ch15, p463] [De 11, §X.2, p181]

I. A. Définitions générales

Forme quadratique, forme polaire associée
Exemple de $M \longmapsto \mathrm{Tr}(M^2)$ sur $\mathcal{M}_n(\mathbb{R})$
Vecteurs orthogonaux, noyau d'une forme quadratique, lien avec le noyau de la matrice de la forme quadratique, rang, forme dégénérée
Exemples

I. B. Propriétés de réduction

Théorème 1. [Réduction de Gauss]
Pour toute forme quadratique réelle q sur $\mathbb{R}^n$, il existe, si $r = \mathrm{rg}(q)$, $\lambda_1, \dots, \lambda_r \in \mathbb{R}^*$ et $\ell_1, \dots, \ell_r$ des formes linéaires indépendantes tels que $q(x) = \sum_{i=1}^r \lambda_i \ell_i$.

Corollaire 2. *La forme polaire associée à q est alors $\varphi(x,y) = \sum_{i=1}^r \lambda_i \ell_i(x)\ell_i(y)$.*

Exemple 3. $q(x,y,z) = -x^2-y^2-z^2+2(xy+xz+yz) = -(x-y-z)^2+(y+z)^2+(y-z)^2$

Corollaire 4. *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 5. *Notons $s = \mathrm{card}(\{i \mid \lambda_i > 0\})$ et $t = \mathrm{card}(\{i \mid \lambda_i < 0\})$. Alors la matrice de q dans une certaine base est $\mathrm{diag}(I_s, -I_t, 0_{n-(s+t)})$.*

Forme (définie) positive, inégalité de Cauchy-Schwarz pour une forme quadratique positive

Proposition 6. [Loi d'inertie de Sylvester]
- *s et t sont uniques (ne dépendent par de la décomposition de Gauss choisie) et déterminés par :*

$$s = \max\{\dim(F) \mid F \in \mathcal{P}\} \qquad t = \max\{\dim(F) \mid F \in \mathcal{N}\}$$

  où $\mathcal{P}$ (resp. $\mathcal{N}$) désigne l'ensemble des sous-espaces de $\mathbb{R}^n$ sur lesquels la restriction de q est définie positive (resp. définie négative). De plus $r = s + t$.
- *Soit $(e_i)_{1\le i\le n}$ une base de $\mathbb{R}^n$ orthogonale pour q. Alors s est le nombre de vecteurs $(e_i)_{1\le i\le n}$ tels que $q(e_i) > 0$ et t est le nombre de vecteurs $(e_i)_{1\le i\le n}$ tels que $q(e_i) < 0$.*

Définition 7. (s,t) s'appelle la signature de q.

Exemple 8. La signature de $M \longmapsto \mathrm{Tr}(M^2)$ est $(n(n+1)/2, n(n-1)/2)$.

Corollaire 9. [Réduction d'une forme quadratique réelle]
Il existe des formes linéaires $(\ell_i)_{1\le i\le r}$ indépendantes telles que $q = \sum_{i=1}^s \ell_i^2 - \sum_{i=s+1}^r \ell_i^2$. Pour $A \in \mathcal{M}_n(\mathbb{R})$, il existe s,t uniques et $P \in \mathcal{GL}_n(\mathbb{R})$ tels que $PAP^\top = \mathrm{diag}(I_s, -I_t, 0_{n-(s+t)})$.

Théorème 10. [Théorème spectral] [Aud06, §VII.7.8]
Soient q, q' des formes quadratiques avec q définie positive. Alors il existe une base orthonormée pour q et orthogonale pour q'.

I. C. Applications

[Rou99, §5.5, p327] [CG13, §V.D, p197]

Exemple 11. La différentielle seconde est une forme quadratique sur $\mathbb{R}^n$.

Lemme 12. *Soit $A_0 \in \mathcal{S}_n(\mathbb{R}) \cap \mathcal{GL}_n(\mathbb{R})$. Alors il existe $V \in \mathcal{V}(A_0)$ et $g \in \mathcal{C}^1(V, \mathcal{GL}_n(\mathbb{R}))$ telle que $\forall A \in V, A = g(A)^\top A_0 g(A)$.*

Théorème 13. [Lemme de Morse]
Soit $f : U \longrightarrow \mathbb{R}$ 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 $d^2 f(0)$ est non dégénérée, de signature $(p, n-p)$.
Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine de $\mathbb{R}^n$ tel que $\varphi(0) = 0$ et $f(x) - f(0) = \varphi(x)_1^2 + \cdots + \varphi(x)_p^2 - \varphi(x)_{p+1}^2 - \cdots - \varphi(x)_n^2$ au voisinage de 0.

Remarque 14. Un polynôme homogène de degré 2 est une forme quadratique.

Proposition 15. [Forme de Hankel]
Soit $P \in \mathbb{R}[X]$ de degré n et $x_1, \dots, x_t$ ses racines distinctes, de multiplicité $m_1, \dots, m_t$. On définit $s_k = \sum_{\ell=1}^t m_\ell x_\ell^k$ pour $k \in \mathbb{N}$ puis on pose

$$\forall (X_0, \dots, X_{n-1}) \in \mathbb{C}^n, s(X_1, \dots, X_n) = \sum_{0\le i,j\le n-1} s_{i+j} X_i X_j$$

Alors $s_{\mathbb{R}}$ (la restriction de s à $\mathbb{R}^n$) est une forme quadratique sur $\mathbb{R}^n$, de signature (p,q) où $p+q = t$ et $p-q$ est le nombre de racines réelles de P.

II. Application à l'étude des coniques

II. A. Vocabulaire

[Aud06, §VII.1, p221]

On se place dans un plan affine euclidien $\mathcal{P}$, muni d'un repère orthonormé $(O, \vec{i}, \vec{j})$.

Définition 16. Une conique $\mathcal{C}$ est l'ensemble des points (x, y) de $\mathcal{P}$ satisfaisant l'équation :

$$(\mathcal{E}) \quad ax^2 + 2bxy + cy^2 + dx + ey + f = 0$$

où $a, b, c, d, e, f \in \mathbb{R}$ sont des paramètres, avec $(a, b, c) \neq (0, 0, 0)$.
$q(x, y) = ax^2 + bxy + cy^2$ est la forme quadratique associée à $\mathcal{E}$, supposée non nulle, et $\ell(x, y) = dx + ey$ est la forme linéaire associée à $\mathcal{E}$.

Remarque 17. q ne dépend pas du point d'origine O choisi.

Définition 18. Un point Ω est centre de symétrie de $\mathcal{C}$ si dans le repère $(\Omega, \vec{i}, \vec{j})$, la partie linéaire de l'équation définissant $\mathcal{C}$ est nulle.
$\mathcal{C}$ est dite à centre si elle admet un unique centre de symétrie.

Proposition 19. *$\mathcal{C}$ est à centre si et seulement si q est non dégénérée.*

Exemple 20. $\Omega = (a, b)$ est l'unique centre de la conique définie par $(x - a)^2 + (y - b)^2 = c$ dans $(O, \vec{i}, \vec{j})$.
Une conique de type $ax^2 + dx + ey + f = 0$ n'est pas à centre.

Proposition 21. *Si $\mathcal{C}$ est à centre, il existe un repère orthonormé de $\mathcal{P}$, d'origine Ω, dans lequel l'équation de $\mathcal{C}$ est du type $\alpha x^2 + \beta y^2 = \gamma$ avec $\alpha, \beta \neq 0$.*

Définition 22. On définit $Q(x, y, z) = q(x, y) + \ell(x, y)z + fz^2$ la forme quadratique sur $\mathbb{R}^3$ appelée forme homogénéisée de q. $\mathcal{C}$ est dite propre si Q est non dégénérée.

Exemple 23. Les coniques propres sont de « vraies » coniques : ce ne sont pas des droites.

II. B. Classification

[Aud06, §VII.2, p228]

Théorème 24. [Classification des coniques propres]
On peut classifier les coniques propres en fonction des signatures de Q et de q :

$\mathrm{sgn}(Q)$	$\mathrm{sgn}(q)$	*Classe*	*Exemple*
$(3,0)/(0,3)$	$(2,0)/(0,2)$	$\varnothing$	$x^2 + y^2 = -1$
$(2,1)/(1,2)$	$(2,0)/(0,2)$	*ellipse*	$x^2 + y^2 = 1$
$(2,1)/(1,2)$	$(1,1)$	*hyperbole*	$x^2 - y^2 = 1$
$(2,1)/(1,2)$	$(1,0)/(0,1)$	*parabole*	$x^2 + y = 0$

Théorème 25. [Classification des coniques impropres]

$\mathrm{sgn}(Q)$	$\mathrm{sgn}(q)$	*Classe*	*Exemple*
$(2,0)/(0,2)$	$(2,0)/(0,2)$	*point*	$x^2 + y^2 = 0$
$(2,0)/(0,2)$	$(1,0)/(0,1)$	$\varnothing$	$x^2 = -1$
$(1,1)$	$(1,1)$	*droites sécantes*	$x^2 - y^2 = 0$
$(1,1)$	$(1,0)/(0,1)$	*droites parallèles*	$x^2 = 1$
$(1,0)/(0,1)$	$(1,0)/(0,1)$	*droite double*	$x^2 = 0$

II. C. Point de vue géométrique

[Rom17, Ch16, p497] [Aud06, §VII.2, p232]

Théorème 26. *Soit $\mathcal{C}$ une conique propre non vide qui n'est pas un cercle. Alors il existe un point $F \in \mathcal{P}$ appelé foyer, une droite $\mathcal{D}$ ne contenant pas F, appelée directrice et un réel $e > 0$ appelé excentricité tels que $\mathcal{C} = \{M \in \mathcal{P} \mid d(M, F) = ed(M, \mathcal{D})\}$.*
Si $e < 1$, $\mathcal{C}$ est une ellipse. Si $e = 1$, $\mathcal{C}$ est une parabole. Enfin si $e > 1$, $\mathcal{C}$ est une parabole.

Définition 27. La perpendiculaire à $\mathcal{D}$ passant par F est appelée axe focal. C'est un axe de symétrie de $\mathcal{C}$.

Théorème 28. *Dans le repère $(F, \vec{i}, \vec{j})$ où $\vec{i}$ unitaire dirige l'axe focal et $\vec{j}$ unitaire dirige $\mathcal{D}$, l'équation de $\mathcal{C}$ est, en notant p l'abscisse de $\mathcal{D}$:*

$$(1 - e^2)x^2 + y^2 + 2pe^2x - p^2e^2 = 0$$

Proposition 29. *Si $\mathcal{C}$ est à centre ($e \neq 1$), le centre a pour coordonnées $(-\frac{pe^2}{1-e^2}/, 0)$ dans le repère $(F, \vec{i}, \vec{j})$.*
Par symétrie, $\mathcal{C}$ est aussi la conique caractérisée par le foyer F' et la directrice $\mathcal{D}'$, symétriques de F et $\mathcal{D}$ par rapport au centre.

PROPOSITION 30. [DÉFINITION BIFOCALE DES CONIQUES PROPRES À CENTRE]

- *Si $\mathcal{C}$ est une ellipse (qui n'est pas un cercle), alors $\mathcal{C} = \{M \in \mathcal{P} \mid MF + MF' = 2a\}$ pour un réel $2a$ appelé grand axe de $\mathcal{C}$,*
- *Si $\mathcal{C}$ est une hyperbole, alors $\mathcal{C} = \{M \in \mathcal{P} \mid |MF - MF'| = 2a\}$ pour un réel $2a$ appelé grand axe de $\mathcal{C}$.*

ANNEXE

Différentes coniques et leurs éléments associés : foyers, directrices ...

QUESTIONS

Q Quelles sont les orbites fermées de $\mathcal{S}_n(\mathbb{R})$ pour l'action de congruence ? (voir [CG13]).

R Montrons que 0 est toujours dans l'adhérence d'une orbite (et alors seule $\{0\}$ est une orbite fermée). On prend pour cela une suite de matrices qui tend vers 0 ...

Q Réduire $q(x,y,z,t) = xy + yz + zt$.

R Par exemple $q(x,y,z,t) = \frac{1}{4}\left[(x+y)^2 - (x-y)^2 + (y+z-t)^2 - (z-y-t)^2\right]$. Ainsi q est de signature $(2,2)$.

Q Montrer que $M \longmapsto \mathrm{Tr}(M^2)$ est une forme quadratique. Quelle est sa signature ?

Q Que se passe-t-il dans le cas d'une forme quadratique définie positive avec la réduction de GAUSS ?

R On obtient la signature $(n,0)$.

Q Montrer que les mineurs principaux d'une matrice définie positive sont tous non nuls (question similaire à la précédente).

Q Montrer que $\det(\mathcal{S}_n^{++}(\mathbb{R})) = \mathbb{R}_+^*$.

Q Par quelles opérations le cône isotrope est-il stable ? Contient-il des sous-espaces vectoriels ? Calculer la dimension maximale d'un sous-espace contenu dans le cône.

R Par multiplication par un scalaire (surtout pas par somme !). Il contient des droites (multiplication par un scalaire), il contient $\ker E$.
Si q est non dégénérée, prenons $F \subset C_q$ le cône isotrope. On a $\dim F + \dim F^\perp = \dim E$, d'où $F \subset F^\perp$ puisque si $x \in F$, alors $\forall y \in F$, $\varphi(x,y) = 0$ en développant $0 = q(x+y) = q(x) + 2\varphi(x,y) + q(y) = 2\varphi(x,y)$. Ainsi $\dim(F) \leq n/2$.
Dans le cas où q n'est pas dégénérée, écrivons $E = \ker q \oplus G$. q_G est non dégénérée, donc on applique ce qui précède et $\dim(F \cap G) \leq \dim(G)/2$ si $F \subset C_q$. Puis $\dim(F \cap \ker q) \leq \dim(\ker(q))$ donc $\dim(F) \leq \dim(G)/2 + \dim(\ker q) \leq \frac{n - \dim(\ker q)}{2}$.

Q Soit E un espace vectoriel de dimension $2n$, et F un sous-espace vectoriel de dimension n, q une forme quadratique non dégénérée sur E. On suppose q nulle sur F. Quelle est la signature de q ?

R La signature est (n,n). En prenant une base de F, on peut compléter en une base telle que la matrice à une forme par blocs 2×2 particulière, et on peut alors la réduire ...

BIBLIOGRAPHIE

[Aud06] M. AUDIN : *Géométrie*. EDP Sciences, 2006.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[De 11] C. DE SEGUINS PAZZIS : *Invitation aux formes quadratiques*. Calvage et Mounet, 2011.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

181 BARYCENTRES DANS UN ESPACE AFFINE RÉEL DE DIMENSION FINIE, CONVEXITÉ. APPLICATIONS.

Soit $(\mathcal{E}, E)$ un $\mathbb{R}$-espace affine.

I. Définitions, coordonnées barycentriques

I. A. Premières propriétés [Aud06, §I.5, p29]

Définition barycentre, isobarycentre : exemple du milieu d'un segment, de la paramétrisation d'un segment comme barycentres
Associativité du barycentre, application au centre de gravité

Proposition 1. [Convergence d'une suite de polygones vers l'isobarycentre]
On définit par récurrence une suite $(P^{(k)})_{k\in\mathbb{N}}$ par $P^{(0)} = (z_1^{(0)}, \dots, z_n^{(0)}) \in \mathbb{C}^n$ et $P^{(k+1)} = (\frac{z_1^{(k)}+z_2^{(k)}}{2}, \dots, \frac{z_{n-1}^{(k)}+z_n^{(k)}}{2}, \frac{z_n^{(k)}+z_1^{(k)}}{2})$ pour $k \in \mathbb{N}$.
Alors $P^{(k)} \underset{k\to+\infty}{\longrightarrow} (g, g, \dots, g)$ où $g = \mathrm{Isobar}(z_1^{(0)}, \dots, z_n^{(0)})$.

I. B. Barycentres et structure affine [Tau00, Ch3, p27]

Une fonction est affine si et seulement si elle conserve les barycentres
Un sous-espace est affine si et seulement si il contient tous les barycentres
Description de l'espace affine défini par une partie de $\mathcal{E}$

I. C. Coordonnées barycentriques [Aud06, ChI/V, p42/150]

Repère affine, coordonnées barycentriques, uniques à renormalisation près
Lien entre repère affine et base vectorielle de $\mathcal{E}_a$ où a est le premier point du repère affine
Exemples du centre de gravité d'un triangle
Application : la seule application affine qui fixe $n+1$ points indépendants de $\mathcal{E}$ est l'identité

Proposition 2. *Soit A, B, C trois points non alignés. Les coordonnées barycentriques d'un point M dans le repère affine (A, B, C) sont proportionnelles aux aires orientées des triangles MBC, MCA, MAB. Plus précisément*

$$\mathcal{A}(MBC)\overrightarrow{MA} + \mathcal{A}(MCA)\overrightarrow{MB} + \mathcal{A}(MAB)\overrightarrow{MC} = \vec{0}$$

Théorèmes de Ménélaüs et de Ceva

Proposition 3. *Soient $k+1$ points $A_0, \dots, A_k$ affinement libres, de coordonnées dans un repère affine $(a_{ij})_{0\le i\le n, 0\le j\le k}$. Alors $M = (x_0, \dots, x_n) \in \mathrm{Aff}(A_0, \dots, A_k)$ si et seulement si $\det(A|M) = 0$.*

Exemple 4. Dans un repère affine du plan, A, B, C sont alignés si et seulement si $\det \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = 0$.

II. Convexité

On suppose E euclidien.

II. A. Définitions et enveloppe convexe [Aud06, §I.6, p31] [Gou08, §1.5, p54]

Partie convexe
Exemples des intervalles, d'une boule convexe, intersection de convexe
Conservation des convexes par une application affine ou par l'image réciproque
Exemples : hyperplans comme noyaux d'une application affine, hyperplans d'appuis, demis-espaces
Enveloppe convexe d'une partie
Exemples : intersection de semis-plans $\to$ polytopes
Un convexe est stable par barycentres à coefficients positifs. Description de l'enveloppe convexe par barycentres à coefficients positifs
Application : l'enveloppe convexe d'une partie finie de X est compacte

Théorème 5. [Théorème de Carathéodory]
Soit X un espace affine de dimension finie n. Alors pour tout $S \subset X$, $\mathrm{conv}(S)$ est l'ensemble des barycentres à coefficients positifs d'au plus $n+1$ points de S. Autrement dit :

$$\mathrm{conv}(S) = \left\{ \sum_{i=1}^{n+1} \lambda_i x_i \,|\, (x_i, \lambda_i)_{1\le i\le n+1} \in (S \times \mathbb{R}_+)^{n+1} \right\}$$

Corollaire 6. *Soit S un compact de X euclidien. Alors $\mathrm{conv}(S)$ est compact.*

Application 7. Soit $M \in \mathcal{M}_n(\mathbb{Z})$. Notons $(C_j)_{1\le j\le n}$ ses colonnes. L'équation diophantienne $MX = 0$ admet une solution non nulle dans $\mathbb{N}^n$ si et seulement si $0 \in \mathrm{conv}(\{C_1, \dots, C_n\})$.

II. B. Topologie des convexes [Tau00, §5.4, p78]

S convexe implique $\overline{S}$ et S° convexes
S d'intérieur non vide si et seulement si $\mathrm{Aff}(S) = \mathcal{E}$.

S convexe compact implique $S = \mathrm{conv}(\partial S)$

II. C. Points extrémaux d'un convexe, sommets

[Tau00, §5.8, p86] [Gou09, §4.2, p180]

Points extrémaux, définition équivalente : la partie privée du point reste convexe
Exemples des points extrémaux de la boule fermée : la frontière
Polygones/polyèdres ... les sommets sont les points extrémaux
Théorème de KREIN-MILMAN

ANNEXE

Tout un tas de dessins ...

QUESTIONS

Q Quel est le lien, s'il y en a, entre les polytopes et les polyèdres ?

R Le polyèdre a un intérieur non vide en général. C'est juste une question de convention.

Q Qu'est-ce qu'une forme affine ?

R C'est la donnée d'une forme linéaire et de coordonnées barycentriques.

Q Soit C un convexe de X affine, avec $\dim(X) < +\infty$. Soit $f : X \longrightarrow X$ affine telle que $f(C) = C$. Montrer que f permute les points extrémaux.

Q Soit A, B, C un triangle et M un point du triangle ABC, de coordonnées (α, β, γ) dans (A, B, C). Exprimer α, β, γ en fonction d'aires de certains triangles.

R On a $\alpha\vec{AM} + \beta\vec{BM} + \gamma\vec{CM} = \vec{0}$. On a $\mathcal{A}(AMC) = \frac{1}{2}\det(\vec{MA}, \vec{MC})$ et

$$\begin{aligned} 0 &= \det(\alpha\vec{AM} + \beta\vec{BM} + \gamma\vec{CM}, \vec{CM}) = \alpha\mathcal{A}(AMC) - \beta\mathcal{A}(BMC) \\ &= -\alpha\mathcal{A}(AMB) + \gamma\mathcal{A}(BMC) = \beta\mathcal{A}(AMB) - \gamma\mathcal{A}(AMC) \end{aligned}$$

Donc $\mathcal{A}(AMB) = \gamma, \mathcal{A}(BMC) = \alpha, \mathcal{A}(AMC) = \beta$.

BIBLIOGRAPHIE

[Aud06] M. AUDIN : *Géométrie*. EDP Sciences, 2006.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Tau00] P. TAUVEL : *Cours de géométrie*. Dunod, 2000.

182 APPLICATIONS DES NOMBRES COMPLEXES À LA GÉOMÉTRIE.

I. Géométrie euclidienne du plan [Rom17, Ch4, p101]

I. A. Généralités [Rom17, Ch4, p101]

Représentation du plan euclidien $\mathcal{P}$ par les complexes
Identifications points, affixe, produit scalaire, déterminant, condition d'alignement des points, équation d'une droite
Lien entre argument et angle orienté
Exemples : équations de droites / de cercles
Équivalence entre la distance et du module

I. B. Applications [Aud06, §I.5, p29]

Barycentres :
Définition barycentre, isobarycentre : exemple du milieu d'un segment, de la paramétrisation d'un segment comme barycentres
Associativité du barycentre, application au centre de gravité
Théorème de GAUSS-LUCAS

PROPOSITION 1. [CONVERGENCE D'UNE SUITE DE POLYGONES VERS L'ISOBARYCENTRE]
On définit par récurrence une suite $(P^{(k)})_{k\in\mathbb{N}}$ *par* $P^{(0)} = (z_1^{(0)}, \dots, z_n^{(0)}) \in \mathbb{C}^n$ *et* $P^{(k+1)} = \left(\frac{z_1^{(k)}+z_2^{(k)}}{2}, \dots, \frac{z_{n-1}^{(k)}+z_n^{(k)}}{2}, \frac{z_n^{(k)}+z_1^{(k)}}{2}\right)$ *pour* $k \in \mathbb{N}$.
Alors $P^{(k)} \underset{k\to+\infty}{\longrightarrow} (g, g, \dots, g)$ *où* $g = \mathrm{Isobar}(z_1^{(0)}, \dots, z_n^{(0)})$.

Critère de cocyclicité : théorème de PTOLÉMÉE, de l'angle moitié
Aire maximale d'un triangle, caractérisation des triangles équilatéraux

II. Transformations du plan

II. A. Autour des similitudes [Tau00, §7.2, p108] [Aud06, §II.3, p89]

Isométries : isomorphisme $\mathcal{O}_2^+(\mathbb{R}) \simeq \mathbb{U}$. Forme analytique des isométries
Translations, homothéties $\to$ similitude = composée
Similitudes directes, indirectes
Application : définition d'un polygone convexe

II. B. Inversions [Rom17, §4.8, p120]

Définition, expression en terme de nombre complexes, involution du plan privé d'un point, cercle des points fixes

II. C. Autour des homographies [Aud06, ChVI.5, p194]

Isomorphisme entre $\mathbb{C} \cup \{+\infty\}$ et la sphère de RIEMANN S
Définitions, groupe des bijections de S
Birapport, propriété de conservation par une homographie

III. Applications des nombres complexes à la géométrie de l'espace : les quaternions [CG13, ChVII, p232]

Groupe des quaternions sous forme matricielle, conjugué, norme d'un quaternion, produit scalaire associé, la base $(1, \mathrm{i}, \mathrm{j}, \mathrm{k})$ est orthonormée, $\mathbb{H} = \mathbb{I} \oplus^{\perp} \mathbb{R}$
On définit $\mathrm{SU}_2(\mathbb{C}) = \{h \in \mathbb{H} \,|\, N(h) = 1\}$

THÉORÈME 2. *On a* $\mathrm{SU}_2(\mathbb{C})/\{\pm I_2\} \simeq \mathrm{SO}_3(\mathbb{R})$.

ANNEXE

Transformations de base, sphère de RIEMANN

SPEECH

Utiliser les nombres complexes pour faire de la géométrie permet notamment d'utiliser une structure de corps qui enrichit la structure d'espace vectoriel.

QUESTIONS

Q Montrer que $Z(H) = \mathbb{R}.1$.

R On prend $h \in Z(H)$, disons $h = w.1+x.i+y.j+z.k$. On a $hi = ih$, ce qui donne $y = z = 0$, puis en utilisant $jh = hj$, on obtient de même $w = 0$.

Q Pourquoi $\mathbb{R}.1$ et les quaternions imaginaires purs sont-ils orthogonaux ?

R Le produit scalaire est lié à la trace ($1, i, j, k$ forme une base orthonormée).
Ou : on a $\langle 1 \mid i \rangle = 1\bar{i} + i\bar{1} = 0, \ldots$

Q Montrer que les deux définitions données du biraport coïncident.

R Soient $a, b, c, d \in \mathbb{C}$. On a :

$$[a, b, c, d] = \frac{a-c}{b-c}\frac{b-d}{a-d} = \frac{ab-ad-bc+cd}{ab-bd-ac+cd} = \frac{(c-a)d+ab-bc)}{(c-b)d+ab-ac}$$

Soit donc $M = \begin{pmatrix} c-a & ab-bc \\ c-b & ab-ac \end{pmatrix}$. On a $\det(M) = \ldots = (c-a)(a(b-c)+b(c-b))$.
On regarde $h_M : z \longmapsto \frac{a-c}{b-c}\frac{b-z}{a-z}$ l'homographie associée.

BIBLIOGRAPHIE

[Aud06] M. AUDIN : *Géométrie*. EDP Sciences, 2006.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Tau00] P. TAUVEL : *Cours de géométrie*. Dunod, 2000.

183 UTILISATION DES GROUPES EN GÉOMÉTRIE.

Soit $\mathcal{E}$ espace affine dirigé par E (action transitive de $(E,+)$ sur $\mathcal{E}$).

I. Transformations d'un espace affine
[Rom17, Ch3, p75] [Aud06, §I.3/4, p16/26]

I. A. Espace et applications affines

Définition espace affine, exemple du plan, de l'espace
Application affine. Préservation de l'alignement, du parallélisme, des barycentres
Exemple d'une translation
Ensemble des points fixes. Exemple de l'homothétie affine

I. B. Le groupe affine

Définition de $\mathrm{GA}(\mathcal{E})$. C'est un groupe
Bijection entre $\mathrm{GL}(E)$ et $\mathrm{GA}_P(\mathcal{E})$ le sous-ensemble de $\mathrm{GA}(\mathcal{E})$ fixant P
Écriture sous la forme $f = t_u \circ g = h \circ t_v$
Action transitive du groupe affine sur les repères affines de $\mathcal{E}$
Groupe $D(\mathcal{E}) = L^{-1}(Z(\mathrm{GL}(E)))$ formé des dilatations : sous-groupe distingué
Relations de conjugaison pour les homothéties

I. C. Utilisation du groupe affine

Théorèmes de THALÈS et de DESARGUES

II. Géométrie euclidienne, groupe d'isométries
[Aud06, ChII/III/V, p51/73/143]

II. A. Groupe des isométries affines [Rom17]

Isométrie affine, exemple : homothétie de rapport ± 1
Réflexion affine : σ telle que $\vec{\sigma}$ est une réflexion vectorielle et σ a un point fixe $\to$ isométrie
$\mathrm{Isom}(\mathcal{E})$ sous-groupe de $\mathrm{GA}(\mathcal{E})$. L morphisme surjectif de noyau $T(\mathcal{E})$
Déplacements, anti-déplacements
Engendrement de $O(E)$ (resp. $\mathrm{Isom}(\mathcal{E})$) par les réflexions vectorielles (resp. affines). Toute isométrie est produit d'au plus n (resp. $n+1$) réflexions.

II. B. Angles orientés en dimension 2 et similitudes [Aud06, §III.1, p73]

Définition de l'angle par une action de groupes. Groupe des similitudes : une application linéaire est une similitude directe si et seulement si elle préserve les angles orientés

II. C. Isométries planes, isométries de l'espace [Aud06, §III.2, p85]

Décomposition d'une isométrie affine
Classification des isométries du plan et de l'espace

II. D. Quaternions et géométrie de l'espace [CG13, ChVII, p232]

Groupe des quaternions sous forme matricielle, conjugué, norme d'un quaternion, produit scalaire associé, la base $(1, \mathrm{i}, \mathrm{j}, \mathrm{k})$ est orthonormée, $\mathbb{H} = \mathbb{I} \oplus^{\perp} \mathbb{R}$
On définit $\mathrm{SU}_2(\mathbb{C}) = \{h \in \mathbb{H} \,|\, N(h) = 1\}$

THÉORÈME 1. *On a* $\mathrm{SU}_2(\mathbb{C})/\{\pm I_2\} \simeq \mathrm{SO}_3(\mathbb{R})$.

III. Groupes des isométries fixant une partie

III. A. Généralités [Rom17, §3.4, p84]

Groupe des isométries préservant une partie de $\mathcal{E}$. Isométries positives/négatives …
L'isobarycentre est conservé par une isométrie (en particulier un potentiel centre de symétrie)
Bijection isométries positives/négatives

III. B. Polygones et polyèdres convexes [Rom17, §3.4, p88], [CG13, §XII.3, p365]

On se place dans le plan affine.
Définition d'un polygone.

EXEMPLE 2. Le groupe des isométries du plan préservant un polygone régulier à n côtés de centre O contient :
i) n rotations de centre O et d'angle $\frac{k2\pi}{n}$ pour $k \in [\![0, n-1]\!]$,
ii) n symétries d'axe 2 sommets opposés ou 2 milieux de côtés opposés si n est pair, 1 sommet et le milieu du côté opposé si n est impair.
C'est le groupe diédral D_{2n}.

On se place maintenant dans un espace affine de dimension 3.
Définition d'un polyèdre.
Isométries préservant le tétraèdre régulier.

THÉORÈME 3. $\mathrm{Isom}(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ *et* $\mathrm{Isom}^+(\mathcal{C}) \simeq \mathfrak{S}_4$.

APPLICATION 4. La formule de BURNSIDE (si G groupe fini agit lui-même par conjugaison alors $|\mathcal{O}| = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}(g)|$) permet de montrer que l'on peut colorier les 6 faces du cube avec 3 couleurs de 57 manières différentes.

IV. Applications des groupes à la classification de coniques réelles

[Aud06, §VII.2, p228]

Définition des coniques, exemples
Par l'action de $\mathrm{GA}(\mathcal{E})$ sur l'ensemble des coniques par $g.f = f \circ g^{-1}$, les orbites permettent de classifier les coniques

ANNEXE

Translations, homothéties, théorèmes de THALÈS et de DESARGUES, rotations, réflexions, symétrie glissée, isométries de l'espace, groupe diédral, isoméries du tétraèdre, types de coniques

QUESTIONS

Q Est-ce une coïncidence de retrouver le groupe des isométries du tétraèdre dans celui du cube modulo 2 en quelque sorte ?

R Pour le tétraèdre, on ne peut que agir sur les sommets.
On peut inscrire deux tétraèdres réguliers dans le cube : partant d'un sommet on prend les sommets diamétralement opposés sur chaque face adjacente. Alors une isométrie du cube envoie tous les points d'un des tétraèdre soit sur lui même, soit sur l'autre tétraèdre. Dans les deux cas ($\mathbb{Z}/2\mathbb{Z}$), on retrouve les permutations $\mathfrak{S}_4$.

Q Montrer que $\mathrm{Isom}(\mathcal{C}) = \mathrm{Isom}(\mathrm{conv}(\mathcal{C}))$.

R Dans un sens, utiliser la conservation des barycentres.

Q Autre définition de l'ellipse de STEINER ?

R Ellipse de rayon maximal parmi les ellipses inscrites dans le triangle ?

Q Soit $h = h(O, \lambda)$ et $h' = h(O, \lambda')$. Que vaut hh' ?

R Si $\lambda\lambda' = 1$, $hh' = t_{\vec{u}}$ où $\vec{u} = \overrightarrow{At_{\vec{u}}(A)}$ pour tout A. Prenant $A = O$, on obtient $\vec{u} = (1 - \lambda')\vec{OO'}$.
Sinon, $h \vec{\circ} h' = \lambda'\lambda\,\mathrm{Id}$ donc $hh' = h(O'', \lambda\lambda')$. Montrons que O, O', O'' sont colinéaires. Pour cela, on part de $\vec{O'O''}$, et on obtient $(1 - \lambda\lambda')\vec{O'O''} = (1 - \lambda)\vec{OO'}$.

BIBLIOGRAPHIE

[Aud06] M. AUDIN : *Géométrie*. EDP Sciences, 2006.

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

190 MÉTHODES COMBINATOIRES, PROBLÈMES DE DÉNOMBREMENT.

I. Notion de dénombrement et de combinatoire [Tau07, ChII, p5]

I. A. Bijections entre cardinaux

Ensemble fini, exemples, cardinal, $\mathrm{card}(F) \leq \mathrm{card}(E)$ si $F \subset E$, deux ensembles de même cardinal sont en bijection
Union d'ensembles disjoints finis, ensemble privé d'une partie.
Exemple : pour $n \in \mathbb{N}^*$, on appelle dérangement de n une permutation de $[\![1, n]\!]$ sans point fixe. On note d_n le nombre de dérangements de n. On a $n! = \sum_{k=0}^{n} \binom{n}{k} d_k$
Cardinal de $A \cup B$ dans le cas général, de $A \times B$, lemme des bergers
Cardinal de l'ensemble des fonctions (injectives, surjectives) de E dans F
Parties de E

I. B. Coefficients binomiaux et combinatoire

Définition, formules classiques (somme des coefficients binomiaux, formule de PASCAL, de VANDERMONDE)

II. Dénombrement en algèbre

II. A. Dénombrement sur un corps fini
[Rom17, §13.6–7, p429–435] [Per96, §III.2/IV.5, p72/105]

Soit $p \in \mathcal{P}$ et $q = p^n$ où $n \in \mathbb{N}^*$. On note $\mathbb{F}_q$ le corps à q éléments.
Cardinaux de $\mathcal{GL}_n(\mathbb{F}_q), \mathcal{SL}_n(\mathbb{F}_q), \mathcal{PGL}_n(\mathbb{F}_q), \mathcal{PSL}_n(\mathbb{F}_q)$
On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

PROPOSITION 1. *Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon, on a $\left|\mathbb{F}_q^2\right| = \frac{q+1}{2}$.*

APPLICATION 2. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p^2$.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

DÉFINITION 3. [SYMBOLE DE LEGENDRE]
Soit $a \in \mathbb{Z}$, on appelle symbole de LEGENDRE (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

On suppose dans la suite p impair.

PROPOSITION 4. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

EXEMPLE 5. -1 est un carré modulo q si et seulement si $q \mid 1 \mod 4$.

THÉORÈME 6. [LOI DE RÉCIPROCITÉ QUADRATIQUE]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

PROPOSITION 7. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

EXEMPLE 8. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

II. B. Actions de groupes [Rom17, §1.6–10/5.6, p19/148]

Soit $(G, .)$ un groupe et X un ensemble.

DÉFINITION 9. [ACTION D'UN GROUPE SUR UN ENSEMBLE]
On dit que G opère à gauche sur X si on a une application $G \times X \longrightarrow X, (g, x) \longmapsto g.x$ telle que $\forall g, h \in G, \forall x \in X, g.(h.x) = (gh).x$ et $\forall x \in X, 1.x = x$.

On considère . une action de G sur X.

EXEMPLE 10.
- G opère sur lui-même par translation à gauche ($g.h = gh$), par conjugaison ($g.h = ghg^{-1}$),
- $\mathfrak{S}(X)$ opère naturellement sur X : $\sigma.x = \sigma(x)$.

DÉFINITION 11. [ORBITES, TRANSITIVITÉ, FIDÉLITÉ]
- Pour $x \in X$, on appelle orbite de x et on note $O(x)$ l'ensemble $G.x = \{g.x \mid x \in X\}$. On note $\mathcal{O}$ l'ensemble des orbites de X. C'est une partition de X.
- On dit que l'action est transitive s'il n'y a qu'une seule orbite pour l'action de G sur X, c'est-à-dire si $\forall x \in X, O(x) = X$.

DÉFINITION 12. [STABILISATEUR, ACTION LIBRE]
On appelle stabilisateur de $x \in X$ le groupe $\mathrm{Stab}(x) = \{g \in G \mid g.x = x\}$.
On dit que G opère librement sur X si $\mathrm{Stab}(x) = \{e\}$ pour tout $x \in X$.

Proposition 13. *Soit $x \in X$. L'application $g \in G \longmapsto g.x \in O(x)$ a pour noyau $\mathrm{Stab}(x)$. L'application quotient est alors une bijection de $G/\mathrm{Stab}(x)$ dans $O(x)$.*
En particulier, si $|G| < +\infty$, on a $\forall x \in X, |O(x)| = [G : \mathrm{Stab}(x)] = \frac{|G|}{|\mathrm{Stab}(x)|}$.

Application 14. [Classes de conjugaisons de $\mathfrak{S}_n$]
Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type.
Le nombre de classes de conjugaison est le nombre de partitions de n.
Calcul du cardinal de la classe de conjugaison associée au type $(\ell_1, \dots, \ell_m)$. Deux calculs proposés, où l'on note $p_k = \mathrm{card}(\{i \mid \ell_i = k\})$:

$$\left(\prod_{i=1}^{m} \binom{n - \sum_{j<i} \ell_j}{\ell_i} (\ell_i - 1)!\right) \times \left(\prod_{k=1}^{n} \frac{1}{p_k!}\right) = \frac{n!}{\prod_{k=1}^{n} k^{p_k} p_k!}$$

Dans la suite de cette partie on suppose G et X finis.

Corollaire 15. [Équation aux classes]
Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Application 16. [Cardinal de $\mathcal{D}_n(\mathbb{F}_q)$]
Soit $n \in \mathbb{N}$, $q = p^r$ où p premier, $r \neq 0$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1 + \dots + n_q = n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

Corollaire 17. [Formule de Burnside]

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Application 18. On peut colorier les 6 faces (toutes identiques) d'un cube avec 3 couleurs de 57 manières différentes.

III. Dénombrement en analyse

III. A. Utilisation des probabilités [Ouv08]

Lien entre probabilité uniforme sur un ensemble fini et cardinal d'une partie
Application à la probabilité de retour en 0 au bout de $2n$ pas de la marche aléatoire simple $\to$ application à la récurrence/transience
Formule du crible, nombre de dérangements

Application 19. On a $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

III. B. Séries génératrices [FGN07, §I.2–6, p6] [Rom17, Ch2, p53–55/73]

Série génératrice ordinaire, exponentielle
Équivalent du nombre de solutions S_n de $\sum \alpha_i n_i = n$ [Gou08, §4.4, p249]
Idée : relation de récurrence lors d'un dénombrement $\to$ introduction de la série génératrice ordinaire ou exponentielle pour obtenir une équation fonctionnelle, différentielle, et déterminer la fonction associée. On vérifie que le rayon de convergence est positif, puis on identifie les coefficients

Corollaire 20. *Le nombre de permutations de $\mathfrak{S}_n$ ayant exactement r points fixes est $\binom{r}{n} d_{n-r} = \frac{n!}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$.*

Application 21. En utilisant un déterminant circulant, on montre qu'il y a plus (resp. moins) de dérangements impairs que de dérangements pairs dans $\mathfrak{S}_n$ lorsque n est pair (resp $n > 1$ impair).

Nombres de Catalan, nombres de Bell

COMMENTAIRES

Il faut aller piocher dans plusieurs références pour cette leçon. Voir aussi [FGN07, BMP05].

QUESTIONS

Q Questions autour de la loi de réciprocité quadratique : où intervient l'hypothèse p et q impairs ? Caractérisation des carrés, à la fin comment passer de l'inégalité modulo p à celle dans $\mathbb{Z}$, réduction des formes quadratiques en caractéristique différente de 2. Que se passe-t-il si $p = 2$? À quoi sert la loi de réciprocité quadratique ? À quoi ça sert de savoir si un élément est un carré dans $\mathbb{F}_q$?

Q Quelle est la probabilité que deux entiers soient premiers entre eux ?

R $6/\pi^2$.

Q Soit $\mathcal{H}_{d,n}$ l'ensemble des polynômes homogènes de degré d à n variables. Quelle est sa dimension ?

R Une base de $\mathcal{H}_{d,n}$ est $(X_{i_1} \dots X_{i_d})_{i_1,\dots,i_d \in [\![1,n]\!]}$, ou encore $(X_1^{\alpha_1} \dots X_n^{\alpha_n})_{\sum_i \alpha_i = d}$.
On cherche donc le nombre de $(\alpha_i)_i$ tels que $\sum_i \alpha_i = d$.
Prenons d points alignés, que l'on veut séparer en n morceaux. Pour cela on rajoute $n-1$ points à ces points aux endroits de séparation. Finalement la dimension est :

$$\binom{d+n-1}{n-1}$$

Q Montrer que $\varphi(n) = \sum_{d|n} \frac{\mu(d)}{d}$. Ou plutôt montrer que si $g(n) = \sum_{d|n} f(d)$ alors $f(n) = \sum_{d|n} g(d)\mu(n/d)$.

Q Dénombrer les polynômes de degré 3 à 3 variables.

Q Dénombrer les permutations de $\mathfrak{S}_n$ sans point fixe (voir aussi la formule de Pascal dans le [Rom17]).

Q Sur $\mathfrak{S}_n$, on dit qu'une permutation σ est un zig-zag si pour $i \in [\![1, n-1]\!]$, $\sigma(i) \notin [\![\sigma(i-1), \sigma(i+1)]\!]$. Montrer qu'il y a autant de zig-zag descendants qu'ascendants (faire une réflexion ...). Donner une relation de récurrence sur le cardinal des zig-zags (on regarde les ascendants ...).

Q Interpréter de manière combinatoire la formule du triangle de Pascal.

Q Dénombrer le nombre de mots bien parenthésés de longueur $2n$?

R On trouve les nombres de Catalan. On peut par exemple utiliser les chemins sous-diagonaux pour trouver la relation de récurrence $c_{n+1} = \sum_{d=0}^{n} c_d c_{n-d}$.

Q Combien y a-t-il de droites / de plans dans $\mathbb{F}_q^n$?

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Ouv08] J.-Y. Ouvrard : *Probabilités : Tome 1*. Cassini, 2ème édition, 2008.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Tau07] P. Tauvel : *Mathématiques générales pour l'agrégation*. Masson, 2007.

Deuxième partie

Leçons d’Analyse et de Probabilités

201 ESPACES DE FONCTIONS. EXEMPLES ET APPLICATIONS.

I. Espaces de fonctions continues

I. A. Fonctions continues et norme uniforme

Fonctions continues, norme uniforme, une limite simple de fonctions continues est continue, interversion de limites, exemples et contre-exemples
L'espace des fonctions bornées est un BANACH

I. B. Fonctions continues sur un compact
[Gou08, §1.3/4.3, p31/228] [HL09, Ch1, p37]

L'image d'un compact par une application continue est un compact. Les fonctions continues sont donc bornées, $\mathcal{C}(K)$ est un espace de de BANACH.
Minimisation sur un compact, application : si f est coercive continue et minorée alors elle admet un minimum qui est atteint.
Théorème de HEINE. Application aux fonctions 2π-périodiques, théorème de DINI. Contre-exemple si l'on n'est plus sur un compact
Autre application : une limite simple continue de fonctions continues sur un compact est une limite uniforme
X compact. Définition de l'(uniforme) équicontinuité d'une partie de $\mathcal{C}(X)$, exemple des fonctions lipschitziennes
Théorème d'ARZELA-ASCOLI, application aux opérateurs à noyaux $\to$ opérateurs compacts

I. C. Densités de familles de fonctions
[HL09, Ch1, p26–30]

Soit (X,d) un compact non vide.

THÉORÈME 1. [THÉORÈME DE STONE-WEIERSTRASS]
Soit H une sous-algèbre de $\mathcal{C}(X,\mathbb{R})$ séparante et unitaire. Alors H est dense dans $\mathcal{C}(X,\mathbb{R})$.

Application : théorème de WEIERSTRASS (dans le cas où l'on est sur $\mathbb{R}$, la limite est nécessairement un polynôme), base de FOURIER des fonctions 2π-périodiques
Application : une fonction continue f telle que $\int_a^b f(x)x^n dx = 0$ pour tout n est nulle

II. Espaces de LEBESGUE
[BP15, Ch9, p157–194] [Bre99, ChIV, p54]

Soit $(E,\mathcal{A},\mu)$ un espace mesuré. Soit $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$. Soit Ω un ouvert de $\mathbb{R}^d$, muni de sa tribu borélienne et de la restriction à Ω de la mesure de LEBESGUE, dont on suppose la construction connue. Soit $p\in[1,+\infty]$ et q son exposant conjugué ($\frac{1}{p}+\frac{1}{q}=1$).

II. A. Construction

DÉFINITION 2. [APPLICATION $\|.\|_p$, ESPACE $\mathcal{L}^p$]
Pour $f:E\longrightarrow\mathbb{K}$ mesurable, on définit $\|f\|_p=\left(\int_E|f|^p\,d\mu\right)^{\frac{1}{p}}$ lorsque p est fini, et $\|f\|_\infty=\inf\{M>0\,|\,|f|\leq M\ \mu\text{-p.p.}\}$. On définit l'espace vectoriel :

$$\mathcal{L}^p(E,\mathcal{A},\mu)=\{f:E\longrightarrow\mathbb{K}\text{ mesurable}\,|\,\|f\|_p<+\infty\}$$

THÉORÈME 3. [INÉGALITÉ DE HÖLDER]
Pour toutes fonctions $f,g:E\longrightarrow\mathbb{K}$ mesurables, on a $\|fg\|_1\leq\|f\|_p\|g\|_q$.

COROLLAIRE 4. [INÉGALITÉ DE MINKOWSKI]
Pour toutes fonctions $f,g:E\longrightarrow\mathbb{K}$ mesurables, on a $\|f+g\|_p\leq\|f\|_p+\|g\|_p$.

DÉFINITION 5. On note $L^p(E,\mathcal{A},\mu)=\mathcal{L}^p(E,\mathcal{A},\mu)/\{\|.\|_p=0\}$ (ou $L^p(E)$, ou L^p) l'ensemble des fonctions de $\mathcal{L}^p(E,\mathcal{A},\mu)$ quotienté par la relation d'égalité μ-p.p.. L'application $\|.\|_p$ passe au quotient et définit ainsi une application sur $L^p(E,\mathcal{A},\mu)$ notée également $\|.\|_p$.

COROLLAIRE 6. *$\|.\|_p$ est une norme et l'espace $(L^p(E),\|.\|_p)$ est un espace vectoriel normé.*

APPLICATION 7. [INCLUSION ENTRE ESPACES L^p] Soient $p,p'\in[1,+\infty]$.
- lorsque $\mu(E)<+\infty$, on a $p<p'\Longrightarrow L^{p'}\subset L^p$,
- contre-exemple dans le cas où $\mu(E)=+\infty$: $f:x\longrightarrow(1+x)^{-1}\mathbb{1}_{\mathbb{R}_+^*}(x)\in L^2\setminus L^1$.
- on a $p'<p\Longrightarrow\ell^{p'}\subset\ell^p$.

Dans le cas général il n'y a pas d'inclusion (contre-exemple).

II. B. Propriétés des espaces L^p

THÉORÈME 8. [THÉORÈME DE RIESZ-FICHER]
L'espace $(L^p(E,\mathcal{A},\mu),\|.\|_p)$ est un espace de BANACH.

COROLLAIRE 9. *Toute suite convergente dans L^p admet une sous-suite qui converge μ-p.p..*

EXEMPLE 10. Contre-exemple de non-convergence de la suite μ-p.p. : les bosses roulantes.

Théorème 11. *Lorsque $p < \infty$:*
(i) l'ensemble des fonctions en escalier à support compact est dense dans L^p,
(ii) l'ensemble des fonctions continues à support compact est dense dans L^p,
(iii) L^p est séparable.

Application 12. Uniforme continuité de l'opérateur par translation : pour tout $f \in L^p$, $a \longmapsto \tau_a f$ est uniformément continue sur $\mathbb{R}$.

II. C. Approximation de l'unité et régularisation par convolution

[BP15, Ch14, p291–314] [QZ13, ChIX.III, p318]

On se place sur $E = \mathbb{R}^d$ où d est un entier quelconque.

Définition 13. On appelle convolution de f et g la fonction $f \star g : x \longmapsto \int_{\mathbb{R}^d} f(y)g(x-y)dy$, lorsque celle-ci est bien définie.

Définition 14. [Approximation de l'unité et suite régularisante]
Une suite $(\alpha_n)_{n\geq 1}$ de fonctions positives de L^1 est une approximation de l'unité si :
- pour tout $n \in \mathbb{N}$, on a $\int_{\mathbb{R}^d} \alpha_n d\lambda_d = 1$,
- pour tout $\varepsilon > 0$, on a $\lim_{n\to+\infty} \int_{\{x\geq\varepsilon\}} \alpha_n d\lambda_d = 0$.

Si de plus les $(\alpha_n)_{n\geq 1}$ sont de classe $\mathcal{C}_c^\infty$, alors on dit que c'est une suite régularisante.

Exemple 15. [Existence d'une suite régularisante]
On considère $\phi : x \longmapsto \exp(\frac{1}{\|x\|^2-1})\mathbb{1}_{]0,1]}(\|x\|)$ puis $\alpha : x \longmapsto \frac{\phi(x)}{\int_{\mathbb{R}^d}\phi d\lambda_d}$.
Alors la suite $\alpha_n : x \longmapsto n^d\alpha(nx)$ est une suite régularisante.

Théorème 16.
(i) Si $f \in L^1$ et $g \in L^p$, alors $f \star g$ existe μ-p.p. et $\|f \star g\|_p \leq \|f\|_1 \|g\|_p$.
(ii) Si $p < +\infty$, soient $f \in L^p$ et $(\alpha_n)_{n\in\mathbb{N}}$ une approximation de l'unité. Alors $f * \alpha_n \xrightarrow[n\to+\infty]{L^p} f$.

Application 17. [Construction de fonctions plateaux]
Soit K un compact de $\mathbb{R}^d$ et Ω un ouvert contenant K. Alors il existe $\theta \in \mathcal{C}^\infty(\mathbb{R}^d)$ telle que $\theta = 1$ sur K, $\theta = 0$ sur $\mathbb{R}^d \setminus \Omega$ et $0 \leq \theta \leq 1$.

Théorème 18. *$\mathcal{C}_c^\infty(\mathbb{R}^d)$ est dense dans L^p pour $1 \leq p < +\infty$.*

III. Fonctions holomorphes

[Tau06]

Soit U un ouvert de $\mathbb{C}$

Fonction holomorphe, stabilité, exemple, une série entière est holomorphe $\mathcal{C}^\infty$
Formule de Cauchy, contre-exemple avec le lemme de l'indice
Fonction holomorphe si et seulement si analytique, principe du maximum, théorème des zéros isolés
Limite d'une suite uniforme de fonctions holomorphes

QUESTIONS

Q Soit K un compact. Montrer que $(\mathcal{C}(K,\mathbb{R}), \|.\|_\infty)$ est séparable.

R Il s'agit du théorème de Stone-Weierstrass ! Si K est un compact de $\mathbb{R}$, les polynômes sont en effet denses dans $(\mathcal{C}(K,\mathbb{R}), \|.\|_\infty)$.

Sinon, K est séparable, considérons $(U_n)_n$ une base dénombrable d'ouverts et soit $f_n : x \longmapsto d(x, U_n^c)$. On pose alors $X = \{P((f_n)_n) \mid P \in \mathbb{Q}[(X_n)_n]\}$ qui est un ensemble dénombrable et dense par le théorème de Stone-Weierstrass.

BIBLIOGRAPHIE

[BP15] M. Briane et G. Pagès : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Bre99] H. Brezis : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[HL09] F. Hirsch et G. Lacombe : *Eléments d'analyse fonctionnelle*. Dunod, 2009.

[QZ13] H. Queffélec et C. Zuily : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Tau06] P. Tauvel : *Analyse complexe pour la Licence 3*. Dunod, 2006.

202 EXEMPLES DE PARTIES DENSES ET APPLICATIONS.

Soit (E,d) un espace métrique, A une partie de E
Adhérence de A, définition de A dense

I. En dimension finie

I. A. Densité sur $\mathbb{R}$

[Gou08, §1.1, p10] [FGN07, §1.13, p29]

A est dense si et seulement si $A \cap]a,b[\neq \varnothing$ pour tout $a<b$
Exemples de $\mathbb{Q}$ et $\mathbb{R}\setminus\mathbb{Q}$, application : le seul morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{R}$ est l'identité
Un sous-groupe de $\mathbb{R}$ est soit dense soit de la forme $a\mathbb{Z}$
$a\mathbb{Z}+b\mathbb{Z}$est dense si et seulement si a et b sont commensurables, $(\mathrm{e}^{in\theta})_n$ est dense dans $\mathbb{U}$ si et seulement si $\theta \notin 2\pi\mathbb{Q}$
Densité dans $\mathbb{C}$, dans $\mathbb{R}^n$

I. B. Densité dans les espaces de matrices

[BMP05, §4.3.3/4.6, p179/217] [MM16, §VII.3, p76]

Densité de $\mathrm{GL}_n(\mathbb{K})$, application : $\chi_{AB}=\chi_{BA}$, différentielle du déterminant
Densité des matrices diagonalisables dans les trigonalisables, donc dans $\mathcal{M}_n(\mathbb{C})$ en particulier
Application au théorème de Cayley-Hamilton, non continuité du polynôme minimal, de la décomposition de Dunford

II. Densités dans les fonctions continues sur un compact

II. A. Généralités

[HL09, Ch1, p26–30]

Soit (X,d) un compact non vide. Espace des fonctions continues sur un compact, muni de la norme uniforme

Théorème 1. [Théorème de Stone-Weierstrass]
Soit H une sous-algèbre de $\mathcal{C}(X,\mathbb{R})$ séparante et unitaire. Alors H est dense dans $\mathcal{C}(X,\mathbb{R})$.

Application : théorème de Weierstrass (dans le cas où l'on est sur $\mathbb{R}$, la limite est nécessairement un polynôme), polynôme de Bernstein, densité des fonctions lipschitziennes
Application : une fonction continue f telle que $\int_a^b f(x)x^n dx=0$ pour tout n est nulle

II. B. Fonctions périodiques

[Gou08, Ch4.5, p256–270] [QZ13, ChIV, p68–135] [BMP05, §3.3.3/3.3.4, p127]

Densité des polynômes trigonométriques dans les fonctions 2π-périodiques continues $\to$ base de Fourier des fonctions 2π-périodiques
On note $\mathbb{T}=\mathbb{R}/2\pi\mathbb{Z}$, $e_n=\mathrm{e}^{in\cdot}$ pour $n\in\mathbb{Z}$. On définit lorsque cela a un sens $\langle f \mid g\rangle = \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{g(t)}dt$ et $\|f\|_1=\sqrt{\langle f\mid f\rangle}$.

Définition 2. [coefficient de Fourier]
Pour $f\in L^1(\mathbb{T})$, on définit $c_n(f)=\frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{-int}\,dt=\langle f\mid e_n\rangle$ le n-ième coefficient de Fourier de f, où $n\in\mathbb{Z}$.

Définition 3. [somme partielles de Fourier, de Fejér]
On appelle somme partielle de Fourier d'ordre $N\in\mathbb{N}$ la quantité $S_N(f)=\sum_{n=-N}^{N} c_n(f)e_n$.
On appelle somme partielle de Fejér d'ordre $N\in\mathbb{N}$ la quantité $\sigma_N(f)=\frac{1}{N}\sum_{n=0}^{N-1} S_N(f)$.

Définition 4. [noyaux de Dirichlet, de Fejér]
On appelle noyau de Dirichlet à l'ordre $N\in\mathbb{N}$ la fonction $D_N=\sum_{n=-N}^{N} e_n$.
On appelle noyau de Fejér à l'ordre $N\in\mathbb{N}$ la fonction $K_N=\frac{1}{N}\sum_{n=0}^{N-1} D_n=\sum_{n=-N}^{N}(1-|n|/N)e_n$.

Théorème 5. [théorème de Fejér]
Soit $f\in\mathcal{C}(\mathbb{T})$. Alors $\|\sigma_N(f)\|_\infty\leq\|f\|_\infty$ pour tout $N\geq 1$ et $\sigma_N(f)=f*K_N \xrightarrow[N\to+\infty]{u} f$.

Remarque 6. On peut retrouver le théorème de Weierstrass à partir de ce résultat.

Application 7. $\mathcal{F}:\mathcal{C}(\mathbb{T})\longrightarrow c_0(\mathbb{Z}), f\longmapsto (c_n(f))_{n\in\mathbb{Z}}$ est injective.

Théorème 8. *$(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L^2(\mathbb{T})$. En particulier, pour $f\in L^2(\mathbb{T})$:*

$$f=\sum_{n\in\mathbb{Z}} c_n(f)e_n \qquad \text{et} \qquad \|f\|_{L^2}^2=\sum_{n\in\mathbb{Z}}|c_n(f)|^2$$

Application 9. [calculs de séries]
On peut reprendre l'Exemple 41 pour calculer les normes des applications dans L^2 : pour $a\in[\![0,2\pi]\!]$: $\sum_{n\in\mathbb{N}^*}\frac{\sin(na)}{n}=\frac{\pi-a}{2}$ (première fonction) et $\sum_{n\in\mathbb{N}^*}\frac{1}{n^4}=\frac{\pi^4}{90}$ (deuxième fonction).
On peut aussi calculer classiquement $\sum_{n\in\mathbb{N}^*}\frac{1}{n^2}=\frac{\pi^2}{6}$ et $\sum_{n\in\mathbb{N}^*}\frac{1}{(2n-1)^2}=\frac{\pi^2}{8}$.

Théorème 10. *Si $f\in\mathcal{C}(\mathbb{T})\cap\mathcal{C}^1_{pm}(\mathbb{T})$, alors $(S_N(f))_{N\in\mathbb{N}}$ converge normalement vers f.*

Exemple 11. Contre-exemple sans l'hypothèse $\mathcal{C}^1_{pm}$: il existe une fonction $f\in\mathcal{C}(\mathbb{T})$ telle que $(S_N(f)(0))_{N\in\mathbb{N}}$ ne converge pas (c'est un corollaire du théorème de Banach-Steinhaus).

III. Espaces L^p

[BP15, Ch9, p157–194] [Bre99, ChIV, p54] [QZ13, ChIX.III, p318]

Soit $(E, \mathcal{A}, \mu)$ un espace mesuré. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On se place sur $\mathbb{R}^d$ muni de la mesure de Lebesgue, dont on suppose la construction connue. Soit $p \in [1, +\infty]$ et q son exposant conjugué ($\frac{1}{p} + \frac{1}{q} = 1$).
On suppose connue la construction des espaces L^p, des normes $\|.\|_p$, la complétude de L^p pour $p < +\infty$.

Théorème 12. *Lorsque $p < \infty$:*
(i) l'ensemble des fonctions en escalier à support compact est dense dans L^p,
(ii) l'ensemble des fonctions continues à support compact est dense dans L^p,
(iii) L^p est séparable.

Application 13. Uniforme continuité de l'opérateur par translation : pour tout $f \in L^p$, $a \longmapsto \tau_a f$ est uniformément continue sur $\mathbb{R}$.

Définition 14. On appelle convolution de f et g la fonction $f \star g : x \longmapsto \int_{\mathbb{R}^d} f(y)g(x-y)dy$, lorsque celle-ci est bien définie.

Définition 15. [Approximation de l'unité et suite régularisante]
Une suite $(\alpha_n)_{n\geq 1}$ de fonctions positives de L^1 est une approximation de l'unité si :
- pour tout $n \in \mathbb{N}$, on a $\int_{\mathbb{R}^d} \alpha_n d\lambda_d = 1$,
- pour tout $\varepsilon > 0$, on a $\lim_{n\to+\infty} \int_{\{x\geq\varepsilon\}} \alpha_n d\lambda_d = 0$.

Si de plus les $(\alpha_n)_{n\geq 1}$ sont de classe $\mathcal{C}_c^\infty$, alors on dit que c'est une suite régularisante.

Exemple 16. [Existence d'une suite régularisante]
On considère $\phi : x \longmapsto \exp(\frac{1}{\|x\|^2-1})\mathbb{1}_{]0,1]}(\|x\|)$ puis $\alpha : x \longmapsto \frac{\phi(x)}{\int_{\mathbb{R}^d}\phi d\lambda_d}$.
Alors la suite $\alpha_n : x \longmapsto n^d\alpha(nx)$ est une suite régularisante.

Théorème 17.
(i) Si $f \in L^1$ et $g \in L^p$, alors $f \star g$ existe μ-p.p. et $\|f \star g\|_p \leq \|f\|_1 \|g\|_p$.
(ii) Si $p < +\infty$, soient $f \in L^p$ et $(\alpha_n)_{n\in\mathbb{N}}$ une approximation de l'unité. Alors $f * \alpha_n \xrightarrow[n\to+\infty]{L^p} f$.

Application 18. [Construction de fonctions plateaux]
Soit K un compact de $\mathbb{R}^d$ et Ω un ouvert contenant K. Alors il existe $\theta \in \mathcal{C}^\infty(\mathbb{R}^d)$ telle que $\theta = 1$ sur K, $\theta = 0$ sur $\mathbb{R}^d \setminus \Omega$ et $0 \leq \theta \leq 1$.

Théorème 19. *$\mathcal{C}_c^\infty(\mathbb{R}^d)$ est dense dans L^p pour $1 \leq p < +\infty$.*

IV. Densité dans les espaces de Hilbert

[BMP05, §3.1.5, p110] [Dem96, §II.5, p51]

Soit H un espace de Hilbert.
Critères de densité dans un espace de Hilbert. Théorème d'existence d'une base hilbertienne
Formules de Parseval, exemple
Cas de L^2 : c'est un espace de Hilbert avec le produit scalair associé ...
Soit I un intervalle de $\mathbb{R}$.

Définition 20. Soit $\rho : I \longrightarrow \mathbb{R}$ une fonction mesurable, strictement positive et telle que pour tout $n \in \mathbb{N}$, $\int_I |x|^n \rho(x)dx < +\infty$. On dit alors que ρ est une fonction de poids.

Définition 21. On définit $L^2(I,\rho) = \left\{f : I \longrightarrow \mathbb{C} \text{ mesurable} \mid \int_I |f(x)|^2 \rho(x)dx < +\infty\right\}$.

Proposition 22. *$L^2(I,\rho)$ est un espace de Hilbert pour le produit du scalaire $\langle f \mid g\rangle_\rho = \int_I f(x)\overline{g(x)}\rho(x)dx$.*

Proposition 23. *Il existe une unique famille $(P_n)_{n\in\mathbb{N}}$ de polynômes unitaires deux à deux orthogonaux pour $\langle . \mid .\rangle_\rho$ et tels que $\deg(P_n) = n$ pour tout n.*

Exemple 24. Voir les dessins en annexe :
- Pour $I = \mathbb{R}$ et $\rho : x \longmapsto \mathrm{e}^{-x^2}$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de Hermite,
- Pour $I = [-1,1]$ et $\rho : x \longmapsto 1$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de Legendre.

Théorème 25. [Base hilbertienne de polynômes orthogonaux]
Soit ρ une fonction de poids. S'il existe $\alpha > 0$ tel que $\int_I \mathrm{e}^{\alpha|x|}\rho(x)dx < +\infty$, alors la famille $(P_n)_{n\in\mathbb{N}}$ est une base hilbertienne de $L^2(I,\rho)$.

Exemple 26. Sans l'hypothèse on a le contre-exemple suivant : soit la fonction de poids $w : x \longmapsto x^{-\ln(x)}$ sur $I = \mathbb{R}_+$. Alors $(P_n)_{n\in\mathbb{N}}$ ne forme pas une base de $L^2(I,w)$.

Application 27. Si I est borné, on a donc nécessairement une base hilbertienne.
La famille $(P_n \exp(-.^2/2))_n$, pour $(P_n)_{n\in\mathbb{N}}$ les polynômes de Hermite, est une base hilbertienne de $L^2(\mathbb{R})$.

QUESTIONS

Q Soit $f \in \mathcal{C}^0(\mathbb{R}, \mathbb{R})$ telle que $f_{|\mathbb{Q}} = 0$. Montrer que $f = 0$.

Q Soit H un hyperplan d'un espace vectoriel normé. Que dire de ses propriétés topologiques ?

R Soit H est dense, soit H est fermé. En effet, $H \subset \overline{H} \subset E$, donc soit $\overline{H} = H$, soit $\overline{H} = E$.

Q Donner des exemples d'hyperplans denses/fermés.

R Soit $\varphi_1 : f \longmapsto \int f$ et $\varphi_2 : f \longmapsto f(0)$ sur $(\mathcal{C}([0,1], \mathbb{R}), \|.\|_1)$. φ_1 est continue tandis que φ_2 ne l'est pas. Leur noyau respectif est donc fermé et dense.

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[BP15] M. Briane et G. Pagès : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Bre99] H. Brezis : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[Dem96] J.-P. Demailly : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[HL09] F. Hirsch et G. Lacombe : *Eléments d'analyse fonctionnelle*. Dunod, 2009.

[MM16] R. Mansuy et R. Mneimné : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[QZ13] H. Queffélec et C. Zuily : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

203 UTILISATION DE LA NOTION DE COMPACITÉ.

Soit (X, d) un espace métrique (donc séparé).

I. Caractérisations de la compacité, premières utilisations
[Gou08, §1.3, p27]

I. A. Propriété de Borel-Lebesgue

Définition par la propriété de Borel-Lebesgue, exemples d'un espace fini, contre exemple de $\mathbb{R}$, caractérisation par les fermés, fermés dans un compact, intersection (union finie) de compacts, théorème de Tychonov, théorème des fermés emboités,
Premier théorème de Dini. Contre-exemple si la fonction limite n'est pas continue : $x \longmapsto x^n$.
Remarque : un espace compact est par définition séparé ! à ne pas oublier dans la définition

I. B. Théorème de Bolzano-Weierstrass et conséquences
[Gou08, §1.4, p46] [FGN07, §2.19, p86]

X est compact si et seulement si il satisfait la propriété de Bolzano-Weierstrass.
X est précompact et complet si et seulement si X compact. Exemples des compacts d'un espace de dimension finie. X compact implique $(\mathcal{C}(X, \mathbb{R}), \|.\|_\infty)$ complet.
Procédé d'extraction diagonale

Proposition 1. *Soit (E, d) un espace métrique compact et $(u_n)_{n\in\mathbb{N}} \in E^{\mathbb{N}}$ telle que $d(u_n, u_{n+1}) \longrightarrow_{n\to+\infty} 0$.*
Alors l'ensemble Γ des valeurs d'adhérence de $(u_n)_{n\in\mathbb{N}} \in E^{\mathbb{N}}$ est connexe.

Application 2. [Lemme de la grenouille]
Soit $f : [0, 1] \longrightarrow [0, 1]$ une fonction continue et $(x_n)_{n\in\mathbb{N}} \in [0, 1]^{\mathbb{N}}$ définie par $x_0 \in [0, 1]$ et $x_{n+1} = f(x_n)$ pour $n \in \mathbb{N}$.
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

II. A. Extrema
[Gou08, §2.1, p71]

L'image d'un compact par une application continue est un compact. Pas forcément l'image réciproque. Une application continue définie sur un compact et à valeurs dans $\mathbb{R}$ est bornée et atteint ses bornes.
Si f est coercive continue et minorée alors elle admet un minimum qui est atteint.
La distance à un compact est atteinte.
Théorème de Rolle, inégalité des accroissements finis
Équivalence des normes en dimension finie, application à la continuité des applications linéaires

II. B. Théorème de Heine
[Gou08, §1.3, p31]

Théorème de Heine. Exemples : fonctions continues périodiques, ou continues avec une limite finie en $\pm\infty$, deuxième théorème de Dini

II. C. Théorème de point fixe
[Gou08, §1, p21/32]

Point fixe dans un compact, exemple de $\cos$.
Application : si X est compact, $f : X \longrightarrow X$ est telle que $d(f(a), f(b)) \geq d(a, b)$ pour tout $a, b \in X$, alors f est une isométrie bijective sur X. [FGN14, §2.3, p68]
Application : si K est compact convexe et f est 1-lipschitzienne, alors f admet au moins un point fixe.
Théorèmes du point fixe de Brouwer, de Schauder

II. D. Théorème de Stone-Weierstrass
[HL09, Ch1, p26]

Soit (X, d) un compact non vide.

Théorème 3. [Théorème de Stone-Weierstrass]
Soit H une sous-algèbre de $\mathcal{C}(X, \mathbb{R})$ séparante et unitaire. Alors H est dense dans $\mathcal{C}(X, \mathbb{R})$.

Application : théorème de Weierstrass (dans le cas où l'on est sur $\mathbb{R}$, la limite est nécessairement un polynôme), base de Fourier des fonctions 2π-périodiques

III. Compacité en dimension finie

III. A. Espaces vectoriels normés
[HL09, Ch2, p43] [FG97, §2.32, p77–78]

Théorème de Riesz
En dimension infinie : la boule unité de $(\mathcal{C}([0, 1]), \|.\|_\infty)$ n'est pas compacte : $f_n : x \longmapsto x^n$ converge vers une fonction non continue !

Proposition 4. *Soit K un espace métrique compact. Les morphismes d'anneaux de $\mathcal{C}(K, \mathbb{R})$ dans $\mathbb{R}$ sont les morphismes d'évaluation $(\mathrm{ev}_t : f \longmapsto f(t))_{t\in K}$.*

III. B. Le théorème d'Arzela-Ascoli
[HL09, Ch1, p37]

Soit X un compact. Définition de l'(uniforme) équicontinuité d'une partie de $\mathcal{C}(X)$, exemple des fonctions lipschitziennes
Théorème d'Ascoli, application aux opérateurs à noyaux $\to$ opérateurs compacts

QUESTIONS

Q Peut-on trouver une fonction continue de $\mathbb{R}$ dans $\mathbb{R}$ non limite uniforme de polynômes ?

R Oui, toute fonction continue qui n'est pas un polynôme !

Q Soit $f : [a,b] \longrightarrow \mathbb{R}$ continue telle que $\int_a^b f(t)t^n dt = 0$ pour tout $n \in \mathbb{N}$. Montrer que $f = 0$.

R On approxime f uniformément par une suite $(P_n)_n$ de polynômes. On a pour tout n, $\int_a^b f(t)P_n(t)dt = 0$, et donc $\int_a^b f(t)^2 dt = \lim_{n\to+\infty} \int_a^b f(t)P_n(t)dt = 0$.

Q Soient X, Y métriques compacts. Montrer que toute $f \in \mathcal{C}(X \times Y, \mathbb{R})$ est limite uniforme de combinaisons linéaires de fonctions produits.

Q Montrer sans le théorème de Riesz que la boule unité des polynômes n'est pas compacte.

R Considérons la norme infinie sur $[0,1]$ et la famille $(X^n)_{n\in\mathbb{N}}$. Si la boule unité était compacte, il existerait une sous-suite φ et un polynôme P tel que $X^{\varphi(n)} \underset{n\to+\infty}{\longrightarrow} P$, et alors on aurait $P(1) = 1$ et $P([0,1[) = 0$ ce qui est impossible par continuité d'un polynôme.

Q Soit $(X_n)_{n\in\mathbb{N}}$ une suite décroissante de compacts non vides. Montrer que $\cap_{n\in\mathbb{N}} X_n \neq \varnothing$.

R Prenons $x_n \in X_n$ pour tout n. Alors $(x_n)_{n\in\mathbb{N}} \in X_0^{\mathbb{N}}$ donc x_n converge vers un x quitte à extraire. Comme $(x_n)_{n\geq k} \in X_k^{\mathbb{N}}$, on a que $x \in X_k$ pour tout k, et donc $x \in \cap_{n\in\mathbb{N}} X_n$.

Q Soit E un espace vectoriel normé. Montrer que $\overline{\mathbb{B}}(0,1)$ est compacte si et seulement si $\mathbb{S}(0,1)$ l'est.

R Si $\overline{\mathbb{B}}(0,1)$ est compacte, $\mathbb{S}(0,1)$ l'est. Réciproquement, si $\mathbb{S}(0,1)$ est compacte, soit $(x_n)_n$ une suite de $\overline{\mathbb{B}}(0,1)$. Si elle ne converge pas vers 0, supposons qu'aucun des termes n'est nul quitte à extraire. Alors $\frac{x_n}{\|x_n\|} \in \mathbb{S}(0,1)$ converge quitte à extraire, et $\|x_n\| \in [0,1]$ converge quitte à extraire, donc finalement $(x_n)_n$ converge.

Q $\mathcal{O}_n(\mathbb{R}) = \left\{M \mid M^\top M = \mathrm{Id}_n\right\}$ est-il compact ?

R Il est fermé car $\mathcal{O}_n(\mathbb{R}) = f^{-1}(\{\mathrm{Id}_n\})$ où $f(M) = M^\top M$ est continue. Il est bien sûr borné.

Q Soit A un compact de $\mathcal{M}_n(\mathbb{R})$. $S = \left\{P^{-1}MP \mid M \in A, P \in \mathcal{GL}_n(\mathbb{R})\right\}$ est-il compact ?

R Non, si on prend pour A un singleton, sa classe de similitude est bornée si et seulement si c'est une homothétie !

BIBLIOGRAPHIE

[FG97] S. Francinou et H. Gianella : *Exercices de mathématiques pour l'agrégation - Algèbre 1*. Masson, 1997.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[FGN14] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 3*. Cassini, 2ème édition, 2014.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[HL09] F. Hirsch et G. Lacombe : *Eléments d'analyse fonctionnelle*. Dunod, 2009.

204 CONNEXITÉ. EXEMPLES ET APPLICATIONS.

Soient E et F des espaces topologiques.

I. Espaces et parties connexes [Gou08, §1.4, p38]

I. A. Notion de connexité

Espace connexe, caractérisation par les parties ouvertes et fermées de E, exemples de $\mathbb{R}$, d'un intervalle, contre-exemple d'un segment privé d'un point
Parties connexes, contre-exemple de $\mathbb{Q}$, $\mathbb{R} \setminus \mathbb{Q}$
Image d'un connexe par une application continue
Image d'une partie connexe par une application continue à valeurs dans $\{0, 1\}$
Application aux intervalles de $\mathbb{R}$, $\mathbb{R}$ n'est pas homéomorphe à $\mathbb{R}^2$

I. B. Propriétés topologiques [Gou08, §1.4, p46] [FGN07, §2.19, p86]

Suites dans un compact et connexité :

Proposition 1. *Soit (E, d) un espace métrique compact et $(u_n)_{n\in\mathbb{N}} \in E^{\mathbb{N}}$ telle que $d(u_n, u_{n+1}) \longrightarrow_{n\to+\infty} 0$.*
Alors l'ensemble Γ des valeurs d'adhérence de $(u_n)_{n\in\mathbb{N}} \in E^{\mathbb{N}}$ est connexe.

Application 2. [Lemme de la grenouille]
Soit $f : [0, 1] \longrightarrow [0, 1]$ une fonction continue et $(x_n)_{n\in\mathbb{N}} \in [0, 1]^{\mathbb{N}}$ définie par $x_0 \in [0, 1]$ et $x_{n+1} = f(x_n)$ pour $n \in \mathbb{N}$.
Alors $(x_n)_{n\in\mathbb{N}}$ converge si et seulement si $\lim_{n\to+\infty} x_{n+1} - x_n = 0$.

Si $A \subset B \subset \overline{A}$ avec A connexe, alors B est connexe
L'adhérence d'une partie connexe est connexe
Une union de connexes d'intersection non vide est connexe
Pour l'intersection, c'est faux $\rightarrow$ contre-exemple sur $\mathbb{R}^2$
Produit de connexes

I. C. Composantes connexes

Composante connexe, exemples, décomposition de E en composantes connexes $\rightarrow$ dès que l'on a une décomposition en fermés/ouverts connexes disjoints

I. D. Connexité par arcs

Connexité par arcs, qui implique la connexité
La réciproque est fausse en général, contre-exemples classiques
Segment, connexité par lignes brisées
Un convexe est connexe par arcs
Si Ω est ouvert, on a équivalence entre Ω connexe et Ω connexe par lignes brisées

II. Applications en analyse

II. A. Fonctions à valeurs réelles [Gou08, §1.4, p38] [FGN07, §4.28, p253]

Soit I un intervalle réel.
Théorème des valeurs intermédiaires, théorème de Darboux

Théorème 3. [Théorème de Sard]
Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction de classe $\mathcal{C}^1$ et C l'ensemble des zéros de f'.
Alors $f(C)$ est de mesure nulle.

Si $U \subset E$ connexe est tel que $df(a) = 0$ pour tout $a \in U$, alors f est constante sur U
Connexité d'une boule en toute dimension finie
Théorème de Cauchy-Lipschitz : unicité de la solution maximale

II. B. Analyse complexe [Tau06, Ch6/7, p67/84] [Rud98, Ch10, p241]

Lemme : un ouvert de $\mathbb{C}$ est connexe si et seulement si il est connexe par arcs
Arcs, chemins, intégrales le long d'un chemin, exemples de $z \longmapsto z$, $z \longmapsto \overline{z}$, $z \longmapsto z^{-1}$
f continue admet une primitive sur Ω si et seulement si pour tout chemin fermé, $\int_\gamma f(z)dz = 0$
Formule de Cauchy 1 sur un connexe : $\int_\gamma f(z)dz = 0$
Lemme de l'indice, fonction constante sur chaque composantes connexe, exemple (en annexe)
Formule de Cauchy 2, exemples

Corollaire 4. *Une fonction holomorphe est analytique. Plus précisément si $\mathbb{D}(z_0, R) \subset U$ et f est holomorphe sur U alors f est développable en série entière sur $\mathbb{D}(z_0, R)$ et on a pour tout chemin γ d'indice 1 en z_0 :*

$$\forall n \in \mathbb{N}, \frac{f^{(n)}(z_0)}{n!} = \frac{1}{2i\pi} \int_\gamma \frac{f(s)}{(s - z_0)^{n+1}} ds$$

En particulier f est $\mathcal{C}^\infty$
Chemins homotopes, espaces simplement connexes, l'intégrale sur deux chemins homotopes d'une fonction holomorphe entre les deux chemins est la même.
f holomorphe est constante ssi f est nulle sur un voisinage d'un point ssi $f^n(z) = 0$ pour tout n pour un $z \in \Omega$
Principe du maximum, application au théorème de d'Alembert-Gauss, principe des zéros isolés, prolongement holomorphe, application à la fonction Γ, aux polynômes orthogonaux

Théorème des résidus, exemples d'intégrales

III. Connexité des espaces de matrices

[Rom17, §21.8/23.2, p682/748] [CG13]

Connexité par arcs donc connexité de $\mathrm{GL}_n(\mathbb{C})$, mais pas de $\mathrm{GL}_n(\mathbb{R})$ qui a deux composantes connexes, tout comme $\mathcal{O}_n(\mathbb{R})$
Connexité de la sphère
Application : isomorphisme des quaternions
Connexité de $\mathcal{S}_n(\mathbb{R})$, de $\mathcal{S}_n^+(\mathbb{R})$, de $\mathcal{S}_n^{++}(\mathbb{R})$
Pour $A \in \mathcal{M}_n(\mathbb{C})$, $\exp(\mathbb{C}A)$ est connexe par arcs

ANNEXE

Dessins de composantes connexes, d'ensemble connexes ou non ...
Ensembles connexes non connexes par arcs.

QUESTIONS

Q Soit E un espace vectoriel normé de dimension supérieure ou égale à 2. $S_E = \{x \in E \mid \|x\| = 1\}$ est-il connexe ?

R Soient $x, y \in S_E$. Regardons le chemin $t \longmapsto \frac{ty+(1-t)x}{\|ty+(1-t)x\|}$ lorsque le segment $[x, y]$ ne contient par 0. C'est bien un chemin reliant les deux points dans S_E. Si $x = -y$ alors puisque $\dim(E) \geq 2$ on peut prendre $z \in S_E$ tel que z et x sont libres, et alors on relie par ce qui précède x à z puis z à y.

Q Soit E un espace vectoriel normé. $A \subset E$ vérifie la propriété du point fixe si toute fonction continue de A dans A admet un point fixe. Étudier le lien entre cette propriété et la connexité.

R La connexité n'implique pas la propriété. Cependant si la propriété est vraie, l'ensemble est connexe. Raisonnons par contraposée.
Si A n'est pas connexe, écrivons $A = O_1 \cup O_2$ avec $O1 \cap O_2 = \varnothing$. Posons $f(O_1) = a_2 \in O_2$ et $f(O_2) = a_1 \in O_1$: f est continue et n'a pas de point fixe. Donc A ne vérifie pas la propriété.

BIBLIOGRAPHIE

[CG13] P. Caldero et J. Germoni : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rud98] W. Rudin : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

[Tau06] P. Tauvel : *Analyse complexe pour la Licence 3*. Dunod, 2006.

205 ESPACES COMPLETS. EXEMPLES ET APPLICATIONS.

(X, d) désigne un espace métrique non vide.

I. Généralités sur la complétude

[Gou08, §1.2, p19–27]

I. A. Suites de Cauchy

Définition 1. [suite de Cauchy]
$(x_n)_{n\in\mathbb{N}} \in X^{\mathbb{N}}$ est dite de Cauchy si $\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} \,|\, \forall p, q \geq n_0, d(x_p, x_q) \leq \varepsilon$.

Proposition 2.
- *Toute suite convergente est de* Cauchy.
- *Une suite de* Cauchy *est bornée et* $\sup_{p,q} d(u_p, u_q) < +\infty$.
- *Une suite de* Cauchy *admettant une valeur d'adhérence* ℓ *converge vers* ℓ.

Définition 3. [espace complet, espace de Banach]
X est dit complet si toute suite de Cauchy de X est convergente.

Exemple 4. $(\mathbb{R}, |.|)$ est complet. $\mathbb{Q}$ n'est pas complet : considérer par exemple $u_n = \sum_{k=0}^{n} \frac{1}{k!}$ ou $u_0 > 0$ et $u_{n+1} = \frac{u_n + \frac{2}{u_n}}{2}$. [Hau07, §16.7, p312]

I. B. Premières propriétés

Théorème 5. [complété d'un espace métrique]
Il existe un espace métrique complet $(\hat{X}, \hat{d})$ *et une isométrie* $i : (X, d) \longrightarrow (\hat{X}, \hat{d})$ *d'image dense. De plus, si* $(\hat{X}', \hat{d}')$ *et* i' *convient également, alors il existe une isométrie bijective* $\varphi : \hat{X} \longrightarrow \hat{X}'$ *telle que* $\phi \circ i = i'$.

Exemple 6.
- $\hat{\mathbb{Q}} = \mathbb{R}$ pour la distance usuelle (on construit en fait $\mathbb{R}$ comme étant le complété de $\mathbb{Q}$),
- $\hat{\mathcal{P}} = \mathcal{C}([0,1])$ pour la norme uniforme, où $\mathcal{P}$ est l'ensemble des fonctions polynomiales sur $[0,1]$ **[théorème de Weierstrass]**.

Proposition 7. *Si* (X, d) *est complet et* $A \subset X$, *alors* (A, d) *est complet si et seulement si* A *est fermé dans* X.

Proposition 8. *Si* $((X_i, d_i))_{1\leq i\leq n}$ *sont des espaces métriques, alors* $\prod_{i=1}^{n} X_i$ *est complet pour la distance produit si et seulement si tous les* $((X_i, d_i))_{1\leq i\leq n}$ *sont complets.*
En particulier, un espace vectoriel normé de dimension finie est complet.

Théorème 9. [théorème des fermés emboîtés]
Si X *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, $\cap_{n\in\mathbb{N}} F_n$ *est un singleton.*

Exemple 10. $(\mathbb{R}, d)$ où $d(x, y) = |\arctan(x) - \arctan(y)|$ n'est pas complet.

Proposition 11. *Un métrique est compact si et seulement si il est précompact est complet.*

II. Exemples d'espaces vectoriels normés complets

II. A. Espaces de Banach, exemple des applications linéaires continues

[Gou08, §1.5, p47]

Définition 12. [espace de Banach]
Un espace vectoriel normé complet est un espace de Banach.

Proposition 13. $(E, \|.\|)$ *est un espace* Banach *si et seulement si toute série à termes dans* E *absolument convergente est convergente.*

Soit $(E, \|.\|)$ un espace de Banach.

Exemple 14. $(\mathcal{B}(X, E), \|.\|_\infty)$ et $(\mathcal{C}_b(X, E), \|.\|_\infty)$ sont des espaces de Banach, et donc $(\mathcal{C}(K, E), \|.\|_\infty)$ pour K compact aussi.

Proposition 15. *Si* F *est un espace de* Banach, $\mathcal{L}(E, F)$ *est complet pour* $|||f||| = \sup_{\|x\|_E \leq 1} \|f(x)\|_F$. *Ainsi, le dual topologique d'un e.v.n. est toujours complet.*

Application 16. Si $u \in \mathcal{L}(E)$ est tel que $\|u\| \leq 1$, alors $(\mathrm{Id} - u) \in \mathrm{GL}(E)$ et son inverse est $\sum_{n\geq 0} u^n$. On en déduit que $\mathrm{GL}(E)$ est un ouvert de $\mathcal{L}(E)$.

II. B. Espaces L^p

[BP15, Ch9, p157–194] [Bre99, ChIV, p54]

Soit $(E, \mathcal{A}, \mu)$ un espace mesuré. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 17. [application $\|.\|_p$, espace $\mathcal{L}^p$]
Pour $f : E \longrightarrow \mathbb{K}$ mesurable, on définit $\|f\|_p = (\int_E |f|^p \, d\mu)^{1/p}$ lorsque p est fini, et $\|f\|_\infty = \inf\{M > 0 \,|\, |f| \leq M \ \mu\text{-p.p.}\}$. On définit l'espace vectoriel :

$$\mathcal{L}^p(E, \mathcal{A}, \mu) = \{f : E \longrightarrow \mathbb{K} \text{ mesurable} \,|\, \|f\|_p < +\infty\}$$

Théorème 18. [Inégalité de Hölder]
Pour toutes fonctions $f, g : E \longrightarrow \mathbb{K}$ mesurables, on a $\|fg\|_1 \leq \|f\|_p \|g\|_q$.

Corollaire 19. [Inégalité de Minkowski]
Pour toutes fonctions $f, g : E \longrightarrow \mathbb{K}$ mesurables, on a $\|f+g\|_p \leq \|f\|_p + \|g\|_p$.

Définition 20. [Espace L^p]
On note $L^p(E,\mathcal{A},\mu) = \mathcal{L}^p(E,\mathcal{A},\mu)/\{\|.\|_p = 0\}$ (ou $L^p(E)$, ou L^p) l'ensemble des fonctions de $\mathcal{L}^p(E,\mathcal{A},\mu)$ quotienté par la relation d'égalité μ-p.p.. L'application $\|.\|_p$ passe au quotient et définit ainsi une application sur $L^p(E,\mathcal{A},\mu)$ notée également $\|.\|_p$ par abus.

Corollaire 21. *$\|.\|_p$ est une norme et l'espace $(L^p(E), \|.\|_p)$ est un espace vectoriel normé.*

Exemple 22. [Espace ℓ^p]
Cas où $E = \mathbb{N}$ et μ est la mesure de comptage.
Si p est fini, on note ℓ^p l'espace $\mathcal{L}^p = L^p = \{(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}} \mid \sum_{n=0}^{+\infty} |a_n|^p < +\infty\}$.
$\ell^\infty = \mathcal{L}^\infty = L^\infty$ est l'espace des suites bornées.

Théorème 23. [Théorème de Riesz-Ficher]
L'espace $(L^p(E,\mathcal{A},\mu), \|.\|_p)$ est un espace de Banach.

Corollaire 24. *Toute suite convergente de L^p admet une sous-suite qui converge μ-p.p..*

Contre-exemple : on n'a pas forcément convergence de la suite p.p. : bosses roulantes.

II. C. Le cas des espaces de Hilbert

[Gou08, An.B, p407–416] [Bre99, Ch5, p79–82] [BMP05, §3.1.2, p95–107]

Définition 25. [Espace de Hilbert]
H est un espace préhilbertien si c'est un espace vectoriel muni d'un produit scalaire. C'est un espace de Hilbert s'il est complet pour la norme issue du produit scalaire.

Remarque 26. Toute norme vérifiant l'identité du parallélogramme dérive d'un produit scalaire et est donc une norme hilbertienne. C'est un critère pratique : $(\mathcal{C}([a,b],\mathbb{K}), \|.\|_\infty)$ n'est pas un espace de Hilbert par exemple.

Exemple 27.
- Si $(H_n)_{n\in N}$ est une suite d'espaces de Hilbert, alors $H = \{(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} H_n \mid \sum_{n\in\mathbb{N}} \|x_n\|^2 < +\infty\}$ est un espace de Hilbert pour le produit scalaire $\langle (x_n)_{n\in\mathbb{N}} \mid (y_n)_{n\in\mathbb{N}} \rangle_H = \sum_{n\in\mathbb{N}} \langle x_n \mid y_n \rangle_{H_n}$.
- $L^2(E,\mathcal{A},\mu)$ est un espace de Hilbert pour tout espace mesuré $(E,\mathcal{A},\mu)$.

Théorème 28. [Projection sur un convexe fermé]
Soit C un convexe fermé d'un espace de Hilbert H. Alors :

$$\forall x \in H, \exists! p \in C \mid \|x-p\| = d(x,C)$$

De plus, p est l'unique élément de C satisfaisant $\forall c \in C, \Re(\langle x-p \mid c-p\rangle) \leq 0$.

Remarque 29. On a en fait juste besoin de C complet et H préhilbertien.

Corollaire 30. *Soit F un sous-espace vectoriel fermé de H. Alors $H = F \oplus F^\perp$.*

Exemple 31. Contre-exemples :
- lorsque F n'est pas fermé : prendre $H = \ell^2(\mathbb{N})$ et F l'ensemble des suites de H nulles à partir d'un certain rang. $F^\perp = \{0\}$ mais $E \neq F$,
- lorsque H est seulement un espace de Banach : $E = (\mathbb{R}^2, \|.\|_\infty)$. Les points $\{(x,0) \mid -1 \leq x \leq 1\}$ minimisent la distance de $(0,1)$ à $\mathrm{Vect}((1,0))$.

Application 32. Existence et unicité de l'espérance conditionnelle d'une variable aléatoire.

Application 33. Soit $T \in \mathcal{L}(H)$. Alors il existe un unique opérateur $U \in \mathcal{L}(H)$ tel que :

$$\forall x, y \in H, \langle T(x) \mid y\rangle = \langle x \mid U(y)\rangle$$

Théorème 34. [Théorème de Riesz-Fréchet]
Soit H un espace de Hilbert. Alors pour toute application $\phi \in H'$, il existe un unique $f \in H$ tel que $\forall v \in H, \phi(v) = \langle f \mid v\rangle$.
De plus $\phi \longmapsto f$ est une isométrie ($\|f\|_H = \|\phi\|_{H'}$).

III. Utilisation de la complétude

III. A. Prolongement d'applications

[Gou08, §1.2, p22–23]

Théorème 35. *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 36. *Soient E un espace vectoriel normé, D un sous-espace vectoriel dense de E et F un espace de* Banach. *Alors toute application linéaire continue de D dans F a un unique prolongement linéaire continu sur E.*

Application 37. Prolongement de la transformée de Fourier sur $L^2(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d), \mathrm{Leb})$.

III. B. Théorèmes de point fixe

[Gou08, §1.2, p21–23]

Théorème 38. [théorème de point fixe de Picard]
Soit (X,d) un espace métrique complet et $\phi : X \longrightarrow X$ une application k-contractante pour un $k \in]0,1[$. Alors ϕ admet un unique point fixe. De plus, toute suite à valeurs dans X définie par $u_{n+1} = \phi(u_n)$ converge vers l'unique point fixe de ϕ.

Corollaire 39. *Le résultat reste valable si l'on suppose seulement que l'une des itérées de ϕ est contractante.*

Remarque 40. Contre-exemple lorsque X n'est pas complet : $X =]0,1]$ et $\phi : x \longmapsto x/2$. Lorsque l'on a seulement $f(\phi(x),\phi(y)) < d(x,y)$, le résultat est faux dans le cas général ($\phi : x \longmapsto \sqrt{x^2+1}$) mais est vrai si X est compact.

Corollaire 41. *Soit Λ un espace métrique et $\phi : X \times \Lambda \longrightarrow X$ une application continue et uniformément contractante par rapport à Λ, c'est-à-dire il existe $k \in]0,1[$ tel que pour tout $\lambda \in \Lambda$, $\phi(.,\lambda)$ est k-contractante. Alors pour tout $\lambda \in \Lambda$, il existe un unique point fixe $x(\lambda)$ à $\phi(.,\lambda)$ et l'application $\lambda \longmapsto x(\lambda)$ est continue.*

Théorème 42. [théorème de Cauchy-Lipschitz] *[Rou99, p167]*
Soit $\|.\|$ une norme sur $\mathbb{R}^m$, I un intervalle de $\mathbb{R}$ et $f : I \times \mathbb{R}^m \longrightarrow \mathbb{R}^m$ une application continue globalement lipschtizienne en la seconde variable (c'est-à-dire pour tout $K \subset I$ compact, $\exists k > 0 \,|\, \forall t \in K, \forall y,z \in \mathbb{R}^m, \|f(t,y) - f(t,z)\| \leq k\|y-z\|$).
Alors pour $t_0 \in I$ et $x \in \mathbb{R}^m$ donnés, le problème de Cauchy $\begin{cases} y'(t) = f(t,y(t)) \\ y(t_0) = x \end{cases}$ *admet une unique solution définie sur I.*

Exemple 43. Soit $A \in \mathcal{M}_m(\mathbb{R})$. Il existe une unique solution $Y \in \mathcal{C}^1(\mathbb{R},\mathbb{R}^m)$ telle que

$$\begin{cases} Y' = AY \\ Y(t_0) = Y_0 \end{cases}$$

III. C. Autour du théorème de Baire

[Gou08, An.A, p397–406] [Rud98, Ch5, p125] [Bre99, Ch2, p15–21]

Théorème 44. [théorème de Baire]
Si $(U_n)_{n\in\mathbb{N}}$ est une suite d'ouverts denses d'un espace complet E, alors $\cap_{n\in\mathbb{N}} U_n$ l'est aussi.

Application 45. Un espace de Banach est de dimension finie ou non dénombrable. Par exemple $\mathbb{R}[X]$ n'est complet pour aucune norme.

Théorème 46. [théorème de Banach-Steinhaus]
Soit E un espace de Banach *et F un espace vectoriel normé. Soit $(u_i)_{i\in I}$ une famille d'applications de $\mathcal{L}_c(E,F)$ simplement bornée (c'est-à-dire $\forall x \in E, \sup_{i\in I} \|u_i(x)\| \leq +\infty$). Alors $\sup_{i\in I} |||u_i||| < +\infty$.*

Application 47. Existence d'une fonction continue 2π-périodique telle que sa série de Fourier diverge en 0.

Application 48. Soient E, E_1 des espaces de Banach et E_2, F des espaces vectoriels normés.
- Soit $f : E \longrightarrow F$ limite simple d'une famille d'applications de $\mathcal{L}_c(E,F)$. Alors $f \in \mathcal{L}_c(E,F)$.
- Soit $B : E_1 \times E_2 \longrightarrow F$ une application bilinéaire telle que les applications partielles soient continues. Alors $B \in \mathcal{L}_c(E_1 \times E_2, F)$.

Théorème 49. [théorème de l'application ouverte]
Une application linéaire continue surjective entre espaces de Banach *est ouverte.*

Corollaire 50. *Une application linéaire continue bijective entre espaces de* Banach *est d'inverse continue.*

Application 51. Si un espace de Banach est muni de 2 normes dont l'une est plus fine que l'autre, alors elles sont équivalentes.

Corollaire 52. [théorème du graphe fermé]
Une application linéaire $T : E \longrightarrow F$ 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.*

Application 53. (admis) Si T et U sont des applications linéaires (pas forcément continues) de H satisfaisant $\forall x,y \in H, \langle T(x) \mid y\rangle = \langle x \mid U(y)\rangle$, alors T et U sont continues (donc $T,U \in \mathcal{L}(H)$).

SPEECH

Lorsque l'on s'intéresse à des limites de familles d'éléments d'un espace, la question de l'existence de la limite peut souvent poser problème. Lorsqu'elle existe, la limite peut aussi ne pas appartenir à l'espace de départ. Les espaces complets sont alors un cadre très pratique car ce sont des espaces dans lesquels les suites convergentes admettent leur limite dans ces espaces. Travailler dans ces espaces assure donc de nombreux résultats d'existence dont nous allons parler dans cette leçon.
De plus, tout espace métrique peut être complété en un espace complet, et donc dans la pratique on peut assez facilement se placer dans ce contexte.

QUESTIONS

Q Montrer que $\mathbb{R}$ n'est pas dénombrable en utilisant le théorème des fermés emboités.

Q On veut montrer que le théorème de l'application ouverte n'est plus valable lorsque l'un des deux espaces n'est pas de Banach. Considérer $\mathrm{id} : (\ell^2, \|.\|_2) \longrightarrow (\ell^2, \|.\|_\infty)$.

R Cette fonction est bien définie, bijective, et on a que id est continue puisque $\|.\|_\infty \leq \|.\|_2$. Or, si id^{-1} était continue, on aurait l'existence de C telle que $\|.\|_2 \leq C \|.\|_\infty$ et en prenant $x^n = (\delta_{i\leq n})_{i\in\mathbb{N}}$, on aboutit à une contradiction.

Q Montrer qu'il existe $f \in \mathcal{C}([0,1], \mathbb{R})$ telle que $\sup_{n\in\mathbb{N}^*}\{|n\int_0^1 f - \sum_{k=1}^n f(k/n)|\} = +\infty$.

R On pose $u_n : f \longmapsto \left|n\int_0^1 f - \sum_{k=1}^n f(k/n)\right|$. Alors $u_n \in \mathcal{L}(E, \mathbb{R})$ et E et $\mathbb{R}$ sont complets.
A $n \in \mathbb{N}$ fixé, on peut trouver f d'intégrale $1/2$, de norme infinie 1 et nulle en les $(k/n)_{0\leq k\leq n}$ (par exemple affine par morceaux avec $f(2k + 1/2n) = 1$).
On a $|u_n(f)| \leq 2n \|f\|_\infty$ et on trouve une fonction qui atteint cette borne (1 sur les $(k/n)_k$, -1 sur les $(2k + 1/n)_k$).

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[BP15] M. Briane et G. Pagès : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Bre99] H. Brezis : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Hau07] D. Hauchecorne : *Les contre-exemples en Mathématiques*. Ellipses, 2ème édition, 2007.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

[Rud98] W. Rudin : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

207 PROLONGEMENT DE FONCTIONS. EXEMPLES ET APPLICATIONS.

Définition d'un prolongement d'une fonction définie sur $A \subset E$.

I. Prolongement par continuité [Gou08, §1.2, p23]

On considère des espaces métriques.

I. A. Prolongement ponctuel

Continuité d'une fonction continue en un point d'accumulation a implique $\lim_{x\to a} f(x) = f(a)$. On peut donc prolonger par continuité la fonction si elle n'est pas définie en a lorsque $\lim_{x\to a} f(x) = \ell \in F$.
Exemples de sinc, contre-exemple de $\sin(1/x)$ ou d'une fonction indicatrice.

I. B. Prolongement par densité

Deux fonctions continues égales sur une partie dense sont égales, exemple d'une équation fonctionnelle $f(x+y) = f(x) + f(y) \to f$ est linéaire
Prolongement par densité d'applications uniformément continues, application à la définition d'une intégrale de fonctions continues à partir des fonctions en escaliers
Prolongement d'applications linéaires continues définies sur un sous-espace dense.
Application : prolongement de la transformée de Fourier définie sur $\mathcal{S}(\mathbb{R}^d)$ dense dans $L^2(\mathbb{R}^d)$.

II. Prolongement différentiel

II. A. Prolongement $\mathcal{C}^k$ et applications [Gou08, §2.1, p74–77] [Rou99, Ch6, p328–335]

Prolongement d'une fonction continue de classe $\mathcal{C}^1$ sur $I \setminus \{a\}$ telle que $f' \underset{x\to a}{\longrightarrow} \ell \in \mathbb{R}$. Alors f est $\mathcal{C}^1$ sur I (et $f'(a) = \ell$).
Exemple de fonction $\mathcal{C}^\infty$ sur $\mathbb{R}$, nulle sur $\mathbb{R}^-$.
Fonctions plateaux, existence de fonction $\mathcal{C}^\infty$ admettant des limites à gauche fixées des dérivées à toute ordre.

II. B. Prolongement des solutions d'EDO [Ber17, Ch1/3]

Équation différentielle, solution, prolongement d'une solution, solution globale implique maximale, mais pas la réciproque, exemple de $x' = x^2$.
Prolongement d'une solution en une solution maximale
Théorème de Cauchy-Lipschitz
Théorème des bouts
Exemple de Lokta-Volterra
Si f est bornée : le théorème des bouts implique que la solution maximale est globale !
Lemme de Grönwall, application au théorème des bouts dans le cas d'un problème linéaire avec A, B fonctions continues

III. Prolongement de fonctions de la variable complexe

III. A. Prolongement de séries entières [Gou08, §4.4, p236–256] [BMP05, §2.1/2.2, p47–56]

Soit $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence R.

Définition 1. [Rayon de convergence]
On définit le rayon de convergence de la série entière par le réel $R = \sup(\{r \geq 0 \,|\, (|a_n r^n|)_{n\in\mathbb{N}} \text{ est bornée}\})$.

Exemple 2. La série entière $\sum_{n\geq 0} \frac{z^n}{n!}$ a un rayon de convergence infini.

Proposition 3. [Lemme d'Abel]
- *Si $|z| < R$, la série $\sum_{n\geq 0} a_n z^n$ converge absolument,*
- *La série entière $\sum_{n\geq 0} a_n z^n$ convergence normalement sur $\mathbb{D}_r(0)$ pour tout $r < R$. En particulier, la série entière est continue sur $\mathbb{D}_R(O)$,*

Exemple 4. On n'a pas forcément continuité sur $\overline{\mathbb{D}}_R(0)$! Considérer par exemple $\sum_{n\geq 0}(-1)^n z^n = \frac{1}{1-z}$ sur $\mathbb{D}_1(0)$, prolongeable en 1 par $1/2$ mais dont la série en 1 diverge.

Exemple 5. [différents comportements possibles sur le cercle $\mathscr{C}_R(0)$]
- $\sum_{n\geq 0} z^n$ diverge en tout point de $\mathscr{C}_1(0)$,
- $\sum_{n\geq 0} z^n/n$ converge en tout point de $\mathscr{C}_1(0)$ sauf en 1,
- $\sum_{n\geq 0} z^n/n^2$ converge en tout point de $\mathscr{C}_1(0)$.

Théorème 6. [Théorème d'Abel]
Soit $f : z \longmapsto \sum_{n\geq 0} a_n z^n$ de rayon de convergence 1. On suppose que $\sum_{n\geq 0} a_n$ converge. Alors pour tout $\alpha \in [0, \pi/2[$, on a

$$\lim_{z\to 1, z\in\Delta_\alpha} f(z) = \sum_{n\geq 0} a_n \quad \text{où} \quad \Delta_\alpha = \{1 - \rho\,\mathrm{e}^{i\theta} \in \mathbb{D}(0,1) \,|\, \rho > 0, \theta \in [-\alpha, \alpha]\}$$

Théorème 7. [Théorème taubérien faible]
Soit $f : z \longmapsto \sum_{n\geq 0} a_n z^n$ de rayon de convergence 1. On suppose que $a_n = o(1/n)$ et qu'il existe $S \in \mathbb{C}$ tel que $f(x) \longrightarrow_{x\to 1^-} S$. Alors $\sum_{n\geq 0} a_n$ converge et $\sum_{n\geq 0} a_n = S$.

III. B. Prolongement des fonctions holomorphes

[Tau06, §Ch7/8, p84/89] [BMP05, §2.7, p82]

Prolongement analytique, exemple de l'identité $\cos^2 + \sin^2 = 1$ étendue à $\mathbb{C}$ tout entier, du prolongement holomorphe de l'exponentielle
Application : base hilbertienne des polynômes orthogonaux
Principe du maximum, cas d'égalité, lemme de SCHWARZ
Types de singularité : dans le cas d'une fausse singularité prolongement par continuité holomorphe ! Exemple de sinc en 0.
Pole (simple)

PROPOSITION 8. *Γ est holomorphe sur $\{\Re(z) > 0\}$.*

APPLICATION 9. Γ admet un unique prolongement méromorphe sur $\mathbb{C}$, holomorphe sur $\mathbb{C} \setminus -\mathbb{N}$.

APPLICATION 10. $\forall x \in \mathbb{R}_+^*, \Gamma(x) = \lim_{n\to+\infty} \dfrac{n! n^x}{x(x+1)\dots(x+n)}$ **[FORMULE DE GAUSS]**

ANNEXE

Graphe de sinc, d'une fonction plateau, des solutions de $y' = y^2$, d'une solution maximale ...

SPEECH

L'objectif de cette leçon est de parvenir à prolonger des fonctions définies sur différents espaces. Par exemple la fonction sinus cardinal nous donne l'idée simple du prolongement par continuité en 0.
On comprend rapidement qu'il y a plusieurs manières de prolonger une fonction, on s'intéresse notamment aux propriétés de régularité, et à quelles conditions cela est possible. D'abord on regarde le prolongement par continuité, en utilisant une notion de densité.
Dans le cadre des équations différentielles, la notion de durée de vie des solutions amène au théorème de CAUCHY-LIPSCHITZ et au théorème des bouts. En analyse complexe, le prolongement analytique corollaire du théorème des zéros isolés permet d'assurer l'unicité.

COMMENTAIRES

Il faut savoir démontrer le théorème d'holomorphie sous le signe intégral, connaître le théorème de HAHN-BANACH : si ce n'est pas dans le plan, on peut avoir des questions dessus.

QUESTIONS

Q Soit $\alpha \in]-1,1[$ et $u_i = (\alpha^{in})_{n\in\mathbb{N}}$ pour $i \in \mathbb{N}$. Montrer que pour tout $i \in \mathbb{N}$, $u_i \in \ell^2(\mathbb{N})$ et que la famille $(u_i)_{i\in\mathbb{N}}$ est une famille totale de $\ell^2(\mathbb{N})$.

R On a $|(u_i)_n|^2 = \left|\alpha^{2i}\right|^n$ est convergente puisque $|\alpha| < 1$. Montrons que la famille est totale. Soit $v \in \mathrm{Vect}((u_i)_i)^\perp$. Regardons la série entière $f : z \longmapsto \sum_{n\in\mathbb{N}} v(n) z^n$. Son rayon de convergence est au moins 1, par critère de CAUCHY-SCHWARZ. De plus f s'annule en les α^i, donc est nulle par le théorème des zéros isolés. Donc $v = 0$.

Q Déterminer les morphismes d'algèbre continues de $(\mathcal{C}^0([0,1],\mathbb{R}), \|.\|_\infty)$ dans $(\mathbb{R}, |.|)$.

R Regarder l'image des polynômes puis utiliser le théorème de WEIERSTRASS. On obtient les morphismes d'évaluation.

Q Existe-t-il $f \in \mathcal{H}(\mathbb{D}(0,1))$ (ou $f \in \mathcal{H}(\mathbb{C} \setminus \{-i, i\})$) telle que $f_{|]-1,1[} = \arctan$?

R Considérer par exemple $f : z \longmapsto \sum_{n\geq 0} \frac{z^{2n+1}}{2n+1}$.

BIBLIOGRAPHIE

[Ber17] F. BERTHELIN : *Équations différentielles*. Cassini, 2017.

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

[Tau06] P. TAUVEL : *Analyse complexe pour la Licence 3*. Dunod, 2006.

208 ESPACES VECTORIELS NORMÉS, APPLICATIONS LINÉAIRES CONTINUES. EXEMPLES.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit E un $\mathbb{K}$-espace vectoriel.

I. Généralités sur les espaces vectoriels normés [Gou08, §1.5, p47–48]

Définition 1. [norme]
On appelle norme sur E une application $\|.\| : E \longrightarrow \mathbb{R}^+$ telle que :
- pour tout $x \in E$, $\|x\| = 0 \iff x = 0$,
- pour tout $\lambda \in \mathbb{K}$ et $x \in E$, $\|\lambda.x\| = |\lambda| \, \|x\|$,
- pour tout $x, y \in E$, $\|x + y\| \leq \|x\| + \|y\|$.

Lorsque E est muni d'une norme, on parle d'espace vectoriel normé.

Exemple 2.
1. **[sur $\mathbb{K}^n$]** pour $p \in [1, +\infty]$, $\|(x_1, \dots, x_n)\|_p = \left(\sum_{i=1}^n |x_i|^p\right)^{1/p}$ et $\|(x_1, \dots, x_n)\|_\infty = \max_{1 \leq i \leq n} |x_i|$.
2. **[sur $\mathbb{K}[X]$]** Généralisation à $\mathbb{K}[X] \simeq \mathbb{K}^{(\mathbb{N})}$.
3. **[sur $\mathcal{F}([a,b], \mathbb{K})$]** $\|f\|_\infty = \sup_{[a,b]} |f|$ **[sur $\mathcal{C}([a,b], \mathbb{K})$]** $\|f\|_p = \left(\int_a^b |f(x)|^p \, dx\right)^{1/p}$.

On suppose dans la suite E muni d'une norme $\|.\|_E$.

Proposition 3. *E est métrique pour la distance $d : (x, y) \longmapsto \|y - x\|_E$.*

Définition 4. [normes équivalentes]
Soit N_1, N_2 deux normes sur E. On dit que N_1 est plus fine que N_2 s'il existe $C > 0$ tel que $N_2 \leq C N_1$ sur E. On dit que N_1 et N_2 sont équivalentes si chacune est plus fine que l'autre.

Remarque 5. N_1 et N_2 définissent alors la même topologie, et leurs distances induites sont équivalentes.

Exemple 6. Sur $\mathbb{K}^n$, la famille $\{\|.\|_p\}_{1 \leq p \leq \infty}$ est une famille de normes équivalentes.

II. Continuité des applications linéaires [Gou08, §1.5, p48–50]

Soient $(E, \|.\|_E)$, $(F, \|.\|_F)$ et $(G, \|.\|_G)$ des espaces vectoriels normés. On note $\mathcal{L}(E, F)$ les applications linéaires de E dans F et $\mathcal{L}_c(E, F)$ son sous-ensemble d'applications continues. On note $\mathcal{L}(E \times F, G)$ les applications bilinéaires de $E \times F$ dans G.

Théorème 7. *Soit $f \in \mathcal{L}(E, F)$. Alors on a équivalence :*
(i) f est continue sur E,
(ii) f est continue en 0,
(iii) f est bornée sur la boule ou la sphère unité de E,
(iv) il existe $M > 0$ tel que $\forall x \in E$, $\|f(x)\|_F \leq M \|x\|_E$,
(v) f est lipschitzienne sur E.

Exemple 8. L'application $\begin{array}{ccc} E = \mathcal{C}^1([a,b], \mathbb{K}) & \longrightarrow & F = \mathcal{C}^0([a,b], \mathbb{K}) \\ f & \longmapsto & f' \end{array}$ est linéaire.
Si $\|f\|_F = \|f\|_\infty$, elle est continue pour $\|f\|_E = \|f\|_\infty + \|f'\|_\infty$ mais pas pour $\|f\|_E = \|f\|_\infty$.

Définition 9. [norme subordonnée]
On définit $|||f||| = \sup_{x \in E \setminus \{0\}} \frac{\|u(x)\|_F}{\|x\|_E} = \sup_{\|x\|_E \leq 1} \frac{\|u(x)\|_F}{\|x\|_E} = \sup_{\|x\|_E = 1} \|u(x)\|_F$ pour $f \in \mathcal{L}_c(E, F)$. On l'appelle la norme subordonnée à $\|.\|_E$ et $\|.\|_F$.

Proposition 10. *$|||.|||$ est une norme sur $\mathcal{L}_c(E, F)$.*
De plus, pour $f \in \mathcal{L}_c(E, F)$ et $g \in \mathcal{L}_c(F, G)$, on a $|||g \circ f|||_{E,G} \leq |||f|||_{E,F} \, |||g|||_{F,G}$.

Exemple 11. Pour $E = F = \mathbb{K}^n$, on définit des normes sur $\mathcal{M}_n(\mathbb{K})$: [AK02, §3.1, p54]
- $|||A|||_\infty = \max_{1 \leq i \leq n} \sum_{j=1}^n |a_{i,j}|$ est la norme subordonnée associée à $\|.\|_E = \|.\|_\infty$.
- $|||A|||_1 = \max_{1 \leq j \leq n} \sum_{i=1}^n |a_{i,j}|$ est la norme subordonnée associée à $\|.\|_E = \|.\|_1$.

On a $|||\mathrm{Tr}||| = n$ pour $E = F = (\mathcal{M}_n(\mathbb{K}), |||.|||_\infty)$.

Proposition 12. *Soit $f \in \mathcal{L}_2(E \times F, G)$ [a]. Alors on a équivalence :*
- *f est continue sur $E \times F$,*
- *f est continue en $(0, 0)$,*
- *il existe $M > 0$ tel que $\forall (x, y) \in E \times F$, $\|f(x, y)\|_G \leq M \|x\|_E \|y\|_F$.*

a. ensemble des applications $E \times F \longrightarrow G$ bilinéaires

Exemple 13. Un produit scalaire est une forme bilinéaire continue.
Soit $E = (\mathbb{R}^{\mathbb{N}}, \|.\|_\infty)$. L'application :

$$\begin{array}{ccc} E \times E & \longrightarrow & E \\ ((x_n)_{n \in \mathbb{N}}, (y_n)_{n \in \mathbb{N}}) & \longmapsto & (n x_n y_n)_{n \in \mathbb{N}} \end{array}$$

n'est pas continue.

III. Espaces vectoriels normés de dimension finie

[Gou08, §1.5, p50/56] [Hau07, §17.6-7, p321–322]

Soit $(E, \|.\|)$ un espace vectoriel normé réel ou complexe de dimension quelconque (on suppose la notion de norme connue).

Proposition 14. *La sphère unité de $(\mathbb{R}^n, \|.\|_\infty)$ est compacte.*

Théorème 15. *Si E est de dimension finie, alors toutes les normes sur E sont équivalentes.*

Exemple 16. Contre-exemple en dimension infinie : $\|.\|_1$ et $\|.\|_\infty$ sur $\mathcal{C}([0,1], \mathbb{R})$.
Contre-exemple sur $\mathbb{Q}$ non complet : $\mathbb{Q}[\sqrt{2}]$, $N_1(a+b\sqrt{2}) = |a| + |b|$ et $N_2 = |.|$.

Corollaire 17. *Si E est de dimension finie, les compacts de E sont les fermés bornés.*

Exemple 18. C'est faux en dimension infinie : prendre $(\mathcal{C}^0([0,1]), \|.\|_\infty)$ et considérer $(f_n = \mathbb{1}_{[0,1/n]}) \in \overline{\mathbb{B}(0,1)}^{\mathbb{N}}$.

Corollaire 19. *Si E est de dimension finie, E est complet.*

Corollaire 20. *Un sous-espace vectoriel d'un espace de dimension finie est fermé.*

Corollaire 21. *Si E et de dimension finie, alors $\mathcal{L}(E,F) = \mathcal{L}_c(E,F)$.*

Exemple 22. Contre-exemple en dimension infinie : $f \longmapsto f(0)$ sur $(\mathcal{C}([0,1], \mathbb{K}), \|.\|_1)$, ou $P \longmapsto P'$ sur $(\mathbb{K}[X], \|.\|_\infty)$.

Théorème 23. [Théorème de Riesz]
E est de dimension finie si et seulement si $\overline{\mathbb{B}_E(0,1)}$ est compacte.

IV. Propriétés des espaces de Banach

IV. A. Généralités

[Gou08, §1.5, p52]

Définition 24. [Espace et algèbre de Banach]
Un espace de Banach est un espace vectoriel normé complet. Une algèbre A est une algèbre de Banach si elle est munie d'une norme sous-multiplicative (c'est-à-dire $\forall x, y \in A, \|x.y\| \leq \|x\| \, \|y\|$).

Exemple 25.
- $\mathbb{K}^n$ et $\mathcal{F}([a,b], \mathbb{K})$ sont des espaces de Banach,
- Si F est un espace de Banach, $\mathcal{L}_c(E,F)$ est une algèbre de Banach.
- $\mathbb{K}[X]$ n'est complet pour aucune norme (considérer $P_n(x) = \sum_{k=0}^n \frac{X^k}{\|X^k\|(1+k^2)}$).

Proposition 26. *Un espace vectoriel normé est un espace de Banach si et seulement si toute série absolument convergente est convergente.*

Corollaire 27. *Soit A une algèbre de Banach.*
- *Si $\|x\| \leq 1$, $\sum_{n\in\mathbb{N}} x^n$ est inversible, d'inverse $1-x$.*
- *L'ensemble des inversibles de A est un ouvert.*

Théorème 28. [Complété d'un espace métrique]
Il existe un espace métrique complet $(\hat{X}, \hat{d})$ et une isométrie $i : (X,d) \longrightarrow (\hat{X}, \hat{d})$ d'image dense. De plus, si $(\hat{X}', \hat{d}')$ et i' convient également, alors il existe une isométrie bijective $\varphi : \hat{X} \longrightarrow \hat{X}'$ telle que $\phi \circ i = i'$.

Exemple 29.
- $\hat{\mathbb{Q}} = \mathbb{R}$ pour la distance usuelle (on construit en fait $\mathbb{R}$ comme étant le complété de $\mathbb{Q}$),
- $\hat{\mathcal{P}} = \mathcal{C}([0,1])$ pour la norme uniforme, où $\mathcal{P}$ est l'ensemble des fonctions polynomiales sur $[0,1]$ **[Théorème de Weierstrass]**.
- Pour la norme $p < +\infty$: $\mathcal{C}(\widehat{[0,1]}, \mathbb{K}) = L^p([0,1])$, $\mathcal{C}(\widehat{[0,1]}, \mathbb{K}) = \mathcal{C}([0,1], \mathbb{K})$.

IV. B. Théorème de Baire et conséquences

[Gou08, An.A, p397–406] [Rud98, Ch5, p125] [Bre99, Ch2, p15–21]

Théorème 30. [Théorème de Baire]
Si $(U_n)_{n\in\mathbb{N}}$ est une suite d'ouverts denses d'un espace complet E, alors $\cap_{n\in\mathbb{N}} U_n$ l'est aussi.

Application 31. Un espace de Banach est de dimension finie ou non dénombrable.

Théorème 32. [Théorème de Banach-Steinhaus]
Soit E un espace de Banach et F un espace vectoriel normé. Soit $(u_i)_{i\in I}$ une famille d'applications de $\mathcal{L}_c(E,F)$ simplement bornée (c'est-à-dire $\forall x \in E, \sup_{i\in I} \|u_i(x)\| \leq +\infty$). Alors $\sup_{i\in I} |||u_i||| < +\infty$.

Application 33. Existence d'une fonction continue 2π-périodique telle que sa série de Fourier diverge en 0.

Application 34. Soient E, E_1 des espaces de Banach et E_2, F des espaces vectoriels normés.
- Soit $f : E \longrightarrow F$ limite simple d'une famille d'applications de $\mathcal{L}_c(E,F)$. Alors $f \in \mathcal{L}_c(E,F)$.
- Soit $B : E_1 \times E_2 \longrightarrow F$ une application bilinéaire telle que les applications partielles soient continues. Alors $B \in \mathcal{L}_c(E_1 \times E_2, F)$.

Théorème 35. [Théorème de l'application ouverte]
Une application linéaire continue surjective entre espaces de Banach est ouverte.

Corollaire 36. *Une application linéaire continue bijective entre espaces de Banach est d'inverse continue.*

Application 37. $(\mathcal{GL}(E), \circ)$ est un groupe. C'est un ouvert de $\mathcal{L}_c(E, \circ)$.

Application 38. Si un espace de Banach est muni de 2 normes dont l'une est plus fine que l'autre, alors elles sont équivalentes.

Corollaire 39. [Théorème du graphe fermé]
Une application linéaire $T : E \longrightarrow F$ entre deux espaces de Banach est continue si et seulement si son graphe $(\{(x, T(x)) \mid x \in E\})$ est fermé pour la norme produit.

Application 40. (admis) Si T et U sont des applications linéaires (pas forcément continues) de H satisfaisant $\forall x, y \in H, \langle T(x) \mid y\rangle = \langle x \mid U(y)\rangle$, alors T et U sont continues (donc $T, U \in \mathcal{L}(H)$).

V. Le cas des espaces de Hilbert

[Gou08, An.B, p407–416] [Bre99, Ch5, p79–82] [BMP05, §3.1.2, p95–107]

Définition 41. [Espace de Hilbert]
H est un espace préhilbertien si c'est un espace vectoriel muni d'un produit scalaire. C'est un espace de Hilbert s'il est complet pour la norme issue du produit scalaire.

Remarque 42. Toute norme vérifiant l'identité du parallélogramme dérive d'un produit scalaire et est donc une norme hilbertienne. C'est un critère pratique : $(\mathbb{C}([a,b],\mathbb{K}), \|.\|_\infty)$ n'est pas un espace de Hilbert par exemple.

Exemple 43.
- Si $(H_n)_{n\in N}$ est une suite d'espaces de Hilbert, alors $H = \left\{(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} H_n \mid \sum_{n\in\mathbb{N}} \|x_n\|^2 < +\infty\right\}$ est un espace de Hilbert pour le produit scalaire $\langle (x_n)_{n\in\mathbb{N}} \mid (y_n)_{n\in\mathbb{N}}\rangle_H = \sum_{n\in\mathbb{N}} \langle x_n \mid y_n\rangle_{H_n}$.
- $L^2(X, \mathcal{A}, \mu)$ est un espace de Hilbert pour tout espace mesuré $(X, \mathcal{A}, \mu)$.

Théorème 44. [Projection sur un convexe fermé]
Soit C un convexe fermé d'un espace de Hilbert H. Alors :

$$\forall x \in H, \exists! p \in C \mid \|x - p\| = d(x, C)$$

De plus, p est l'unique élément de C satisfaisant $\forall c \in C, \Re(\langle x - p \mid c - p\rangle) \leq 0$.

Remarque 45. On a en fait juste besoin de C complet et H préhilbertien.

Corollaire 46. *Soit F un sous-espace vectoriel fermé de H. Alors $H = F \oplus F^\perp$.*

Théorème 47. [Théorème de Riesz-Fréchet]
Soit H un espace de Hilbert. Alors pour toute application $\phi \in H'$, il existe un unique $f \in H$ tel que $\forall v \in H, \phi(v) = \langle f \mid v\rangle$.
De plus $\phi \longmapsto f$ est une isométrie ($\|f\|_H = \|\phi\|_{H'}$).

Exemple 48. Contre-exemples :
- lorsque C n'est pas convexe : soit $H = \mathbb{R}$ et $C = \mathbb{R}\setminus]-1, 1[$. Alors 1 et -1 minimisent la distance de 0 à C.
- lorsque F n'est pas fermé : prendre $H = \ell^2(\mathbb{N})$ et F l'ensemble des suites de H nulles à partir d'un certain rang. $F^\perp = \{0\}$ mais $E \neq F$,
- lorsque H est seulement un espace de Banach : $E = (\mathbb{R}^2, \|.\|_\infty)$. Les points $\{(x, 0) \mid -1 \leq x \leq 1\}$ minimisent la distance de $(0,1)$ à $\mathrm{Vect}((1,0))$.

Application 49. Existence de l'espérance conditionnelle d'une variable aléatoire L^2.

Application 50. Existence et unicité de l'adjoint d'un opérateur $T \in H'$.

SPEECH

L'objectif de la leçon est de généraliser les notions d'analyse (continuité, …) dans le cadre d'espaces vectoriels.
Dans la première partie, on rappelle des généralités et exemples usuels sur les espaces vectoriels normés. La notion de distance permet de faire de la topologie. On a de nombreuses caractérisations de la continuité des applications linéaires, notamment par la norme subordonnée.
Ensuite, on regarde le cas particulier des espaces vectoriels normés de dimension finie. On se ramène en fait à l'étude de $\mathbb{K}^n$. Notion de complétude Le théorème de Rieszoffre une forte caractérisation de la dimension finie.
Puis une troisième partie se consacre aux espaces de Banach, plus restrictifs mais qui offrent en général un cadre de travail appréciable (et accessible par le théorème de complétude). On s'attarde notamment sur les théorèmes de Baire, de Banach-Steinhaus, de l'application ouverte, du graphe fermé.
Enfin on regarde le cas des espaces de Hilbert, encore plus restrictifs que les Banach, mais qui sont un cadre également très important.

COMMENTAIRES

Beaucoup de choses à mettre dans cette leçon : en profiter pour ne mettre que des choses que l'on maîtrise et partir dans les directions que l'on souhaite.
Le [QZ13] contient tout ce qu'il faut pour cette leçon.

QUESTIONS

Q Soit $f : E \times F \longrightarrow G$ bilinéaire dans un Banach, continue par rapport aux deux variables séparément. Montrer que f est continue.

R C'est un corollaire du théorème de Banach-Steinhaus.

Q Existe-t-il des applications linéaires non continues ?

R Oui, par exemple f définie par $f(p/q) = 1/q$ si $p \wedge q = 1$ et $f(x) = 0$ si $x \notin \mathbb{Q}$.

BIBLIOGRAPHIE

[AK02] G. Allaire et S.-M. Kaber : *Algèbre linéaire numérique*. Ellipses, 2002.

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bre99] H. Brezis : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Hau07] D. Hauchecorne : *Les contre-exemples en Mathématiques*. Ellipses, 2ème édition, 2007.

[QZ13] H. Queffélec et C. Zuily : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Rud98] W. Rudin : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

209 APPROXIMATION D'UNE FONCTION PAR DES POLYNÔMES ET DES POLYNÔMES TRIGONOMÉTRIQUES. EXEMPLES ET APPLICATIONS.

I. Approximation par des polynômes [Gou08, §2.1/4.4, p75/236–256]

I. A. Approximation locale de fonctions régulières

Théorème 1. [Formule de Taylor-Young]
Soient $n \in \mathbb{N}$ et f une fonction de classe $\mathcal{C}^n$ définie sur un intervalle I de $\mathbb{R}$ et à valeurs dans un $\mathbb{R}$-espace vectoriel normé E. Alors pour $a \in I$:

$$f(a+h) =_{h\to 0} \sum_{k=0}^{n} \frac{h^k}{k!} f^{(k)}(a) + o(h^n)$$

Exemple 2. On a les développements limités suivants, pour tout $n \in \mathbb{N}$:

$$\mathrm{e}^x = \sum_{k=0}^{n} \frac{x^k}{k!} + o(x^n) \quad \text{et} \quad \sin(x) = \sum_{k=0}^{n} \frac{(-1)^k x^{2k+1}}{(2k+1)!} + o(x^{2n+2})$$

Théorème 3. [Formule de Taylor avec reste intégral]
Soient $n \in \mathbb{N}$ et f une fonction de classe $\mathcal{C}^{n+1}$ définie sur un intervalle $[a,b]$ de $\mathbb{R}$ et à valeurs dans un $\mathbb{R}$-espace de Banach E. Alors :

$$f(b) = \sum_{k=0}^{n} \frac{h^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)dt$$

Théorème 4. [Théorème de Bernstein]
Soit $a > 0$ et $f :]-a,a[\longrightarrow \mathbb{R}$ une fonction $\mathcal{C}^\infty$ telle que pour tout entier k, $f^{(2k)} \geq 0$ sur $]-a,a[$. Alors f admet un développement en série entière sur $]-a,a[$.

I. B. Densité dans l'espace des fonctions continues [QZ13, §XIII.II.1, p518–519]

Théorème 5. [Théorème de Weierstrass]
$\mathbb{R}[X]$ est dense dans $\mathcal{C}([a,b],\mathbb{C},\|.\|_\infty)$ pour $a < b \in \mathbb{R}$.

Remarque 6. On a le théorème de Stone-Weierstrass : soient (X,d) un compact non vide et H une sous-algèbre de $\mathcal{C}(X,\mathbb{R})$ séparante et unitaire. Alors H est dense dans $\mathcal{C}(X,\mathbb{R})$. On retrouve ce résultat mais aussi la densité des polynômes trigonométriques dans $\mathcal{C}(\mathbb{T})$.

Application 7. Soit $f : [0,1] \longrightarrow \mathbb{C}$ continue telle que pour tout $n \in \mathbb{N}$, $\int_0^1 f(t)t^n dt = 0$. Alors f est nulle.

Application 8. Soit $f : \mathbb{R}_+ \longrightarrow \mathbb{C}$ continue telle $\int_{\mathbb{R}_+} f(t)dt$ existe et pour tout $n \in \mathbb{N}$, $\int_0^{+\infty} f(t)\,\mathrm{e}^{-nt}\,dt = 0$. Alors f est nulle.

Exemple 9. Ce résultat n'est plus vrai si l'intervalle n'est pas borné ! En effet si $f : \mathbb{R} \longrightarrow \mathbb{R}$ est limite uniforme d'une suite de polynômes alors f est un polynôme.

I. C. Densité dans L^2 [BMP05, §3.1.5, p110] [Dem96, §II.5, p51]

Soit I un intervalle de $\mathbb{R}$.

Définition 10. Soit $\rho : I \longrightarrow \mathbb{R}$ une fonction mesurable, strictement positive et telle que pour tout $n \in \mathbb{N}$, $\int_I |x|^n \rho(x)dx < +\infty$. On dit alors que ρ est une fonction de poids.

Définition 11. On définit $L^2(I,\rho) = \left\{ f : I \longrightarrow \mathbb{C} \text{ mesurable} \mid \int_I |f(x)|^2 \rho(x)dx < +\infty \right\}$.

Proposition 12. *$L^2(I,\rho)$ est un espace de Hilbert pour le produit du scalaire $\langle f \mid g \rangle_\rho = \int_I f(x)\overline{g(x)}\rho(x)dx$.*

Proposition 13. *Il existe une unique famille $(P_n)_{n\in\mathbb{N}}$ de polynômes unitaires deux à deux orthogonaux pour $\langle . \mid . \rangle_\rho$ et tels que $\deg(P_n) = n$ pour tout n.*

Exemple 14. Voir les dessins en annexe :
- Pour $I = \mathbb{R}$ et $\rho : x \longmapsto \mathrm{e}^{-x^2}$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de Hermite,
- Pour $I = [-1,1]$ et $\rho : x \longmapsto 1$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de Legendre.

Théorème 15. [Base hilbertienne de polynômes orthogonaux]
S'il existe $\alpha > 0$ tel que $\int_I \mathrm{e}^{\alpha|x|} \rho(x)dx < +\infty$, alors la famille $(P_n)_{n\in\mathbb{N}}$ est une base hilbertienne de $L^2(I,\rho)$.

Application 16. Si I est borné, on a donc nécessairement une base hilbertienne.
La famille $(P_n \exp(-.^2/2))_n$, pour $(P_n)_{n\in\mathbb{N}}$ les polynômes de Hermite, est une base hilbertienne de $L^2(\mathbb{R})$.

Exemple 17. Contre-exemple si la condition du théorème n'est pas vérifiée : considérer $I = \mathbb{R}_+$, $\rho : x \longrightarrow x^{-\ln(x)}$ et $f : x \longrightarrow \sin(2\pi\ln(x))$.

II. Interpolation polynômiale

II. A. Interpolation de LAGRANGE et erreur d'interpolation [Dem96, ChII, p21]

Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction continue. On se donne $(x_i)_{0\leq i\leq n}$ des points deux à deux distincts de $[a,b]$.

THÉORÈME 18. *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 d'interpolation de* LAGRANGE *associé à f et à $(x_i)_i$. On a $P_n = \sum_{i=0}^n f(x_i)\ell_i$ où $\ell_i = \prod_{j\neq i} \frac{X-x_j}{x_i-x_j}$.*

THÉORÈME 19. *Supposons f $(n+1)$ fois dérivable. Alors pour $x \in [a,b]$, il existe $\zeta_x \in [a,b]$ tel que $f(x) - P_n(x) = \frac{1}{(n+1)!}\Pi_{n+1}(x)f^{(n+1)}(\zeta_x)$ où $\Pi_{n+1}(x) = \prod_{j=0}^n X - x_j$. Ainsi :*

$$\|f - P_n\|_\infty \leq \frac{1}{(n+1)!}\|\Pi_{n+1}\|_\infty \left\|f^{(n+1)}\right\|_\infty$$

EXEMPLE 20. 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 ($x_i = x_0 + ih$), on a :

$$|f - P_n| \leq \frac{h^{n+1}}{n+1}\max_{0\leq i\leq n}\left|f^{(n+1)}(x_i)\right| \quad \text{et} \quad \|\Pi_{n+1}\|_\infty = O\left(\left(\frac{b-a}{\mathrm{e}}\right)^{n+1}\right)$$

APPLICATION 21. [PHÉNOMÈNE DE RUNGE]
Soit $f : x \longrightarrow \frac{1}{x^2+1}$ sur $[-1,1]$. C'est une fonction $\mathcal{C}^\infty$ mais dont les dérivées augmentent rapidement en norme infinie vers 0. Il s'en suit dans le cas de points équidistants que $\frac{1}{(n+1)!}\|\Pi_{n+1}\|_\infty \left\|f^{(n+1)}\right\|_\infty \underset{n\to+\infty}{\not\to} 0$.
On observe alors (voir annexe) que les polynômes d'interpolation ne convergent pas uniformément vers f.

DÉFINITION 22. [POLYNÔMES DE TCHEBYCHEV]
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 23. *Les racines de T_{n+1} sont les $\left(\cos\left(\frac{2k+1}{2n}\pi\right)\right)_{0\leq k\leq n}$, appelés points d'interpolation de* TCHEBYCHEV.

EXEMPLE 24. Prenant les points d'interpolation de TCHEBYCHEV (avec $[a,b] = [0,1]$), on a :

$$\|\Pi_{n+1}\|_\infty = O\left(\left(\frac{b-a}{4}\right)^{n+1}\right)$$

Comme $(\mathrm{e}/4)^{n+1} \underset{n\to+\infty}{\longrightarrow} 0$, on obtient que les polynômes d'interpolation de TCHEBYCHEV sont beaucoup plus précis que ceux associés à des points équidistants.

APPLICATION 25. Le phénomène de RUNGE n'est plus observé avec les polynômes d'interpolation de TCHEBYCHEV.

II. B. Application aux méthodes de quadrature [Dem96, ChIII, p59]

Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction continue. On cherche des formules pour approcher $I(f) = \int_a^b f(t)dt$. 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 26. [MÉTHODE DE QUADRATURE]
Une méthode de quadrature consiste, pour $0 \leq i \leq n-1$ à approcher $I_i = \int_{x_i}^{x_{i+1}} f$ par $A_i(f) = h_i\sum_{j=0}^{\ell_j}\omega_{i\,j}f(\zeta_{i\,j})$ où les $(\zeta_{i\,j})_j$ sont dans $[x_i, x_{i+1}]$ et les $(\omega_{i\,j})_{0\leq j\leq n}$ sont des réels fixés tels que $\sum_j \omega_{i\,j} = 1$.
On note alors $E(f) = I(f) - \sum_{i=0}^{n-1} A_i(f)$ l'erreur de la méthode.

DÉFINITION 27. [MÉTHODE DE QUADRATURE]
On dit qu'une méthode de quadrature est d'ordre N si elle est exacte ($E(f) = 0$) 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 28. Fixant $(\zeta_j)_j$ associés 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]**
On approxime $I(f)$ par $\sum_{i=0}^{n-1} h_i f(z_i)$ où $(z_i)_i = (x_i)_i$ ou $(x_{i+1})_i$. Méthode d'ordre 0.

(ii) **[MÉTHODE DES POINTS MILIEUX]**
De même avec $(z_i)_i = (\frac{x_{i+1}-x_i}{2})_i$. Méthode d'ordre 1 et $E(f) \leq \frac{1}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iii) **[MÉTHODE DES TRAPÈZES]**
On approxime $I(f)$ par $\sum_{i=0}^{n-1} h_i\frac{f(x_{i+1})+f(x_i)}{2}$. Méthode d'ordre 1 et $E(f) \leq \frac{2}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iv) **[MÉTHODE DE SIMPSON]**
On approxime $I(f)$ par $\sum_{i=0}^{n-1} h_i\frac{f(x_{i+1})+4f(\frac{x_{i+1}-x_i}{2})+f(x_i)}{6}$. Méthode d'ordre 3 et $E(f) = O(\left\|f^{(4)}\right\|_\infty)$ si f est $\mathcal{C}^4$.

EXEMPLE 29. Approximation de $\int_0^\pi \cos^2(x)dx = \frac{\pi}{4}$:
(i) méthode des rectangles (à gauche ou à droite) : π,
(ii) méthode des points milieux : 0,
(iii) méthode des trapèzes : π,
(iv) méthode de SIMPSON : $\frac{\pi}{3}$.

III. Approximation de fonctions périodiques

[Gou08, Ch4.5, p256–270] [QZ13, Ch4, p68–135] [BMP05, §3.3.3/3.3.4, p127]

III. A. Polynômes trigonométriques et séries de Fourier

On note $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$, $e_n = \mathrm{e}^{in\cdot}$ pour $n \in \mathbb{Z}$. On définit lorsque cela a un sens $\langle f \mid g\rangle = \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{g(t)}dt$ et $\|f\|_1 = \sqrt{\langle f \mid f\rangle}$.

Définition 30. [Polynôme, série trigonométrique]
On appelle polynôme trigonométrique une combinaison linéaire finie des $(e_n)_{n\in\mathbb{Z}}$.
On appelle série trigonométrique une combinaison linéaire des $(e_n)_{n\in\mathbb{Z}}$.

Une série trigonométrique converge-t-elle ? Ponctuellement, uniformément, dans L^p ? …

Définition 31. [Coefficient et série de Fourier]
Pour $f \in L^1(\mathbb{T})$, on définit $c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{-int}\,dt = \langle f \mid e_n\rangle$ le n-ième coefficient de Fourier de f, où $n \in \mathbb{Z}$. On définit la série de Fourier associée à f comme la série trigonométrique $S = \sum_{n\in\mathbb{Z}} c_n(f)e_n$.

Exemple 32.

- Pour $f = \mathbb{1}_{]-a,a[}$ où $0 < a < \pi$, on a $c_n(f) = \begin{cases} a/\pi & \text{si } n = 0 \\ \sin(na)/n\pi & \text{sinon} \end{cases}$.
- Pour $f : x \longmapsto 1 - \frac{x^2}{\pi^2}$, on a $c_n(f) = \frac{2(-1)^n}{\pi^2 n^2}$ si $n \neq 0$, 1 sinon.

Proposition 33. *Pour $f \in L^1(\mathbb{T})$, on a :*

(i) $c_n(\overline{f}) = \overline{c_{-n}(f)}$,
(ii) $c_n(\tau_a f) = \mathrm{e}^{ina}\,c_n(f)$,
(iii) $f * e_n = c_n(f)e_n$,
(iv) *si* $f \in \mathcal{C}(\mathbb{T}) \cap \mathcal{C}^1_{pm}(\mathbb{T})$, $c_n(f') = inc_n(f)$.

Lemme 34. [Lemme de Riemann-Lebesgue]
Si $f \in L^1(\mathbb{T})$, alors $c_n(f) \underset{n\to+\infty}{\longrightarrow} 0$.

III. B. Convergences au sens de Cesàro

Définition 35. [Somme partielles de Fourier, de Fejér]
On appelle somme partielle de Fourier d'ordre $N \in \mathbb{N}$ la quantité $S_N(f) = \sum_{n=-N}^{N} c_n(f)e_n$.
On appelle somme partielle de Fejér d'ordre $N \in \mathbb{N}$ la quantité $\sigma_N(f) = \frac{1}{N}\sum_{n=0}^{N-1} S_N(f)$.

Remarque 36. On peut voir $S_N(f)$ comme la projection sur $\mathcal{P}_N = \mathrm{Vect}((e_n)_{-N\le n\le N})$.

Définition 37. [Noyaux de Dirichlet, de Fejér]
Le noyau de Dirichlet d'ordre $N \in \mathbb{N}$ est la fonction $D_N = \sum_{n=-N}^{N} e_n$.
Le noyau de Fejér d'ordre $N \in \mathbb{N}$ est la fonction $K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n = \sum_{n=-N}^{N}(1-\frac{|n|}{N})e_n$.

Proposition 38. *On a les propriétés suivantes :*

D1) $S_N(f) = f * D_N$,
D2) D_N *est pair et* $\|D_N\|_1 = 1$,
D3) $\forall x \in \mathbb{T}, D_N(x) = \frac{\sin\left(\frac{2N+1}{2}x\right)}{\sin(x/2)}$,

F1) $\sigma_N(f) = f * K_N$,
F2) $\|K_N\|_1 = 1$,
F3) $\forall x \in \mathbb{T}, K_N(x) = \frac{1}{N}\frac{\sin^2(Nx/2)}{\sin^2(x/2)} \ge 0$,
F4) $\forall \delta \in]0,\pi], \int_{\delta\le|t|\le\pi} K_N(t)dt \underset{N\to+\infty}{\longrightarrow} 0$.

Théorème 39. [Théorème de Fejér]

- *Soit $f \in \mathcal{C}(\mathbb{T})$. Alors $\|\sigma_N(f)\|_\infty \le \|f\|_\infty$ pour tout $N \ge 1$ et $\sigma_N(f) = f * K_N \underset{N\to+\infty}{\overset{u}{\longrightarrow}} f$.*
- *Soit $f \in L^p(\mathbb{T})$ pour un $p \in [1,+\infty[$. Alors $\|\sigma_N(f)\|_p \le \|f\|_p$ pour tout $N \ge 1$ et $\lim_{N\to+\infty}\|\sigma_N(f) - f\|_p = 0$.*

Remarque 40. On peut retrouver le théorème de Weierstrass à partir du premier résultat.

Application 41. $\mathcal{F} : \mathcal{C}(\mathbb{T}) \longrightarrow c_0(\mathbb{Z}), f \longmapsto (c_n(f))_{n\in\mathbb{Z}}$ est injective.

III. C. Convergence en moyenne quadratique

Théorème 42. *$(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L^2(\mathbb{T})$. En particulier, pour $f \in L^2(\mathbb{T})$:*

$$f = \sum_{n\in\mathbb{Z}} c_n(f)e_n \qquad \text{et} \qquad \|f\|_{L^2}^2 = \sum_{n\in\mathbb{Z}} |c_n(f)|^2$$

Application 43. [Calculs de séries]
On peut reprendre l'Exemple 41 pour calculer les normes des applications dans L^2 : pour $a \in [\![0, 2\pi]\!]$: $\sum_{n\in\mathbb{N}^*}\frac{\sin(na)}{n} = \frac{\pi-a}{2}$ (première fonction) et $\sum_{n\in\mathbb{N}^*}\frac{1}{n^4} = \frac{\pi^4}{90}$ (deuxième fonction).
On peut aussi calculer $\sum_{n\in\mathbb{N}^*}\frac{1}{n^2} = \frac{\pi^2}{6}$ et $\sum_{n\in\mathbb{N}^*}\frac{1}{(2n-1)^2} = \frac{\pi^2}{8}$.

Théorème 44. *Si $f \in \mathcal{C}(\mathbb{T}) \cap \mathcal{C}^1_{pm}(\mathbb{T})$, alors $(S_N(f))_{N\in\mathbb{N}}$ converge normalement vers f.*

Exemple 45. Il existe une fonction $f \in \mathcal{C}(\mathbb{T})$ telle que $(S_N(f)(0))_{N\in\mathbb{N}}$ ne converge pas.

ANNEXE

Polynômes de Hermite et de Legendre.
Illustration des différentes méthodes numériques.

SPEECH

Il y a plusieurs types de convergences (écrire au tableau) : ponctuelle, uniforme, au sens de Cesàro, quadratique (associée à la norme L^2). On va essayer de montrer des résultats pour chaque type de convergence et de faire des liens entre eux.

QUESTIONS

Q Trouver un espace de suites sur lequel la transformée de Fourier $\mathcal{F}$ est surjective.

R Soit $\mathcal{F} : L^1(\mathbb{T}) \longrightarrow \mathbb{C}_0^{\mathbb{Z}}$.
Si $f \in L^1(\mathbb{T})$, on sait par lemme de Riemann-Lebesgue, que $c_n(f) \underset{n\to+\infty}{\longrightarrow} 0$ donc l'application est bien définie. Est-elle surjective ?

Vérifions que $(\mathbb{C}_0^{\mathbb{Z}}, \|.\|_\infty)$ est complet. On a $(\mathbb{C}_0^{\mathbb{Z}}, \|.\|_\infty) \subset (\mathbb{C}_b^{\mathbb{Z}}, \|.\|_\infty)$ complet. Soit $(u_n)_n$ une suite de Cauchy. Soient $p, q \in \mathbb{N}$. Soit $((u_n^k)_n)_k$ une suite de $\mathbb{C}_0(\mathbb{Z})$ convergent vers $(u_n)_n$. On a $\lim_{n\to+\infty} u_n = \lim_{n\to+\infty} \lim_{k\to+\infty} u_n^k$. Cette limite vaut-elle 0 ? Soit $N \in \mathbb{N}$. On a $|u_N| \leq |u_N - u_N^k| + |u_N^k| \leq \|u - u^k\|_\infty + |u_N^k|$. Donc $\limsup_N |u_N| \leq \|u - u^k\|_\infty$ pour tout k, donc $\lim_N u_N = 0$.
Si $\mathcal{F}$ est surjective, elle est bijective, linéaire et continue de $(L^1(\mathbb{T}), \|.\|_1)$ dans $(\mathbb{C}_0^{\mathbb{Z}}, \|.\|_\infty)$. Par un corollaire du théorème de Banach-Steinhaus, $\mathcal{F}^{-1}$ serait continue, donc il existerait C telle que $\|.\|_{L^1} \leq C \|\mathcal{F}(.)\|_\infty$ sur $L^1(\mathbb{T})$. On vérifie que ce n'est pas possible.

Q Soit $f \in \mathcal{C}(\mathbb{T})$. $\{f * g \mid g \in \mathcal{C}(\mathbb{T})\}$ est-il dense dans $\mathcal{C}(\mathbb{T})$ pour $\|.\|_2$?

R Montrons que $e_m = \mathrm{e}^{im.}$ n'est pas dans l'adhérence en supposant $c_m(f) = 0$.
S'il existe $(g_n)_n$ telle que $f * g_n \underset{n\to+\infty}{\longrightarrow} e_m$, alors $c_m(f * g_n) = c_m(f)c_m(g_n) = 0$ pour tout n, alors que $c_m(e_m) = 1$, ce qui donne une contradiction.
Par ailleurs, si $c_k(f) \neq 0$ pour tout k, montrons que l'ensemble est dense. Soit $h \in \mathcal{C}(\mathbb{T})$. On voudrait trouver $(g_n)_n$ telle que $c_k(g_n) \underset{n\to+\infty}{\longrightarrow} \frac{c_k(h)}{c_k(f)}$ pour tout k. Posons $g_n = \sum_{k=-n}^{n} \frac{c_k(h)}{c_k(f)} \mathrm{e}_k$. Alors par l'égalité de Parseval :

$$\|f * g_n - h\|_2^2 = \sum_{k\in\mathbb{Z}} |c_k(f * g_n - h)|^2$$

On calcule $|c_k(f * g_n - h)| = 0$ pour $n \geq k$, et $c_k(h)$ pour $n < k$, donc $\|f * g_n - h\|_2^2 = \sum_{|k|>n} |c_k(h)|^2 \underset{n\to+\infty}{\longrightarrow} 0$ en tant que reste d'une série convergente.

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Dem96] J.-P. Demailly : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[QZ13] H. Queffélec et C. Zuily : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

213 ESPACES DE HILBERT. BASES HILBERTIENNES. EXEMPLES ET APPLICATIONS.

I. Espaces préhilbertiens et de HILBERT

I. A. Généralités [HL09, Ch3, p84]

Produit scalaire, espace préhilbertien, inégalité de CAUCHY-SCHWARZ, H est alors normé
Identité du parallèlogramme

REMARQUE 1. Toute norme vérifiant l'identité du parallélogramme dérive d'un produit scalaire et est donc une norme hilbertienne. C'est un critère pratique : $(\mathcal{C}([a,b],\mathbb{K}),\|.\|_\infty)$ n'est pas un espace préhilbertien par exemple.

DÉFINITION 2. H est un espace de HILBERT s'il est complet pour la norme induite.

EXEMPLE 3.
- $\mathbb{K}^n$ muni du produit scalaire usuel, $\mathcal{M}_n(\mathbb{K})$ muni de $\langle A \mid B\rangle = \mathrm{Tr}(\overline{B^\top})$, $\mathcal{C}([0,1],\mathbb{K})$
- Si $(H_n)_{n\in N}$ est une suite d'espaces de HILBERT, alors $H = \{(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} H_n \mid \sum_{n\in\mathbb{N}} \|x_n\|^2 < +\infty\}$ est un espace de HILBERT pour le produit scalaire $\langle (x_n)_{n\in\mathbb{N}} \mid (y_n)_{n\in\mathbb{N}}\rangle_H = \sum_{n\in\mathbb{N}} \langle x_n \mid y_n\rangle_{H_n}$.

Orthogonalité, exemples

I. B. Projection sur un convexe fermé et conséquences
[Gou08, An.B, p407–416] [Bre99, Ch5, p79–82] [BMP05, §3.1.2, p95–107]

On se place sur un espace de HILBERT H.

THÉORÈME 4. [PROJECTION SUR UN CONVEXE FERMÉ]
Soit C un convexe fermé d'un espace de HILBERT *H. Alors :*

$$\forall x \in H, \exists! p \in C \mid \|x-p\| = d(x,C)$$

De plus, p est l'unique élément de C satisfaisant $\forall c \in C, \Re(\langle x-p \mid c-p\rangle) \leq 0$.

COROLLAIRE 5. *Soit F un sous-espace vectoriel fermé de H. Alors $H = F \oplus F^\perp$.*

THÉORÈME 6. [THÉORÈME DE RIESZ-FRÉCHET]
Soit H un espace de HILBERT. *Alors pour toute application $\phi \in H'$, il existe un unique $f \in H$ tel que $\forall v \in H, \phi(v) = \langle f \mid v\rangle$.*
De plus $\phi \longmapsto f$ est une isométrie ($\|f\|_H = \|\phi\|_{H'}$).

REMARQUE 7. On a en fait juste besoin de C complet et H préhilbertien dans le théorème de projection.

EXEMPLE 8. Contre-exemples :
- lorsque F n'est pas fermé : prendre $H = \ell^2(\mathbb{N})$ et F l'ensemble des suites de H nulles à partir d'un certain rang. $F^\perp = \{0\}$ mais $E \neq F$,
- lorsque H est seulement un espace de BANACH : $E = (\mathbb{R}^2, \|.\|_\infty)$. Les points $\{(x,0) \mid -1 \leq x \leq 1\}$ minimisent la distance de $(0,1)$ à $\mathrm{Vect}((1,0))$.

APPLICATION 9. Soit $T \in \mathcal{L}(H)$. Alors il existe un unique opérateur $U \in \mathcal{L}(H)$ tel que :

$$\forall x,y \in H, \langle T(x) \mid y\rangle = \langle x \mid U(y)\rangle$$

THÉORÈME 10. [THÉORÈME DE LAX-MILGRAM]
Soit $a : H^2 \longrightarrow \mathbb{R}$ une forme bilinéaire continue et coercive. Alors pour tout $\ell \in H'$, il existe un unique $u \in H$ tel que $\forall v \in H, a(u,v) = \ell(v)$.
Si de plus a est symétrique alors u est l'unique élément de H minimisant $v \longmapsto \frac{1}{2}a(v,v) - \ell(v)$.

APPLICATION 11. [PROBLÈME DE DIRICHLET FAIBLE]
Soit $I =]0,1[$ et $f \in L^2(I)$. Alors

$$\exists! u \in H_0^1(I) \mid \forall v \in H_0^1(I), \int_I u'.v' + \int_I uv = \int_I fv$$

De plus u minimise la fonction $v \longmapsto \frac{1}{2}\int_I |v'|^2 + v^2 - \int_I fv$.

II. Bases hilbertiennes et convergence faible

II. A. Bases hilbertiennes [HL09, §3.4, p107] [BMP05, §3.1.4, p107]

Soit H un espace de HILBERT.
Somme/base hilbertienne, exemples
Critères de densité dans un espace de HILBERT. Théorème d'existence d'une base hilbertienne
Formules de PARSEVAL, exemple
Coordonnées hilbertiennes, convergence dans H de $\sum x_n e_n$ dès que $\sum |x_n|^2 < +\infty$
Un espace de dimension infinie est isomorphe à ℓ^2 si et seulement si il est séparable si et seulement si il admet une base hilbertienne

II. B. Convergence faible [HL09, §3.2, p99]

Définition de la convergence faible, par linéarité il suffit de le vérifier sur une base hilbertienne

Convergence forte implique faible, réciproque vraie si de plus $\|x_n\| \underset{n\to+\infty}{\longrightarrow} \|x\|$
Exemples simples
La boule unité est faiblement compacte

III. Cas des espaces L^2 [BL07, ChVI, p149]

Soit $(E, \mathcal{A}, \mu)$ un espace mesuré.

PROPOSITION 12. *$L^2(E, \mathcal{A}, \mu)$ est un espace de* HILBERT *pour le produit scalaire $\langle . \mid . \rangle$ défini par $\langle f \mid g \rangle = \int_E f\overline{g}d\mu$.*

APPLICATION 13. Existence de l'espérance conditionnelle d'une variable aléatoire L^2.

III. A. L'espace $L^2(\mathbb{T})$
[Gou08, Ch4.5, p256–270] [QZ13, Ch4, p68–135] [BMP05, §3.3.3/3.3.4, p127]

On note $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$, $e_n = \mathrm{e}^{in.}$ pour $n \in \mathbb{Z}$. On définit lorsque cela a un sens $\langle f \mid g \rangle = \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{g(t)}dt$ et $\|f\|_1 = \sqrt{\langle f \mid f \rangle}$.

PROPOSITION 14. *La famille $(e_n)_{n\in\mathbb{Z}}$ est une famille orthonormée.*

DÉFINITION 15. [COEFFICIENT DE FOURIER]
On définit lorsque cela a un sens $c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{-int}\,dt = \langle f \mid e_n \rangle$ le n-ième coefficient de FOURIER de f, où $n \in \mathbb{Z}$.

EXEMPLE 16.
- Pour $f = \mathbb{1}_{]-a,a[}$ où $0 < a < \pi$, on a $c_n(f) = \begin{cases} a/\pi & \text{si } n = 0 \\ \sin(na)/n\pi & \text{sinon} \end{cases}$.
- Pour $f : x \longrightarrow 1 - \frac{x^2}{\pi^2}$, on a $c_n(f) = \begin{cases} 1 & \text{si } n = 0 \\ \frac{2(-1)^n}{\pi^2 n^2} & \text{sinon} \end{cases}$.

DÉFINITION 17. [SOMME PARTIELLES DE FOURIER, DE FEJÉR]
On appelle somme partielle de FOURIER d'ordre $N \in \mathbb{N}$ la quantité $S_N(f) = \sum_{n=-N}^{N} c_n(f)e_n$.
On appelle somme partielle de FEJÉR d'ordre $N \in \mathbb{N}$ la quantité $\sigma_N(f) = \frac{1}{N}\sum_{n=0}^{N-1} S_N(f)$.

REMARQUE 18. On peut voir $S_N(f)$ comme la projection sur $\mathcal{P}_N = \mathrm{Vect}((e_n)_{-N\le n\le N})$.

DÉFINITION 19. [NOYAUX DE DIRICHLET, DE FEJÉR]
On appelle noyau de DIRICHLET à l'ordre $N \in \mathbb{N}$ la fonction $D_N = \sum_{n=-N}^{N} e_n$.
On appelle noyau de FEJÉR à l'ordre $N \in \mathbb{N}$ la fonction $K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n = \sum_{n=-N}^{N}(1 - \frac{|n|}{N})e_n$.

PROPOSITION 20. *On a les propriétés suivantes :*

D1) $S_N(f) = f * D_N$,
D2) D_N *est pair et* $\|D_N\|_1 = 1$,
D3) $\forall x \in \mathbb{T}, D_N(x) = \frac{\sin\left(\frac{2N+1}{2}x\right)}{\sin(x/2)}$,

F1) $\sigma_N(f) = f * K_N$,
F2) $\|K_N\|_1 = 1$,
F3) $\forall x \in \mathbb{T}, K_N(x) = \frac{1}{N}\frac{\sin^2(Nx/2)}{\sin^2(x/2)} \ge 0$,
F4) $\forall \delta \in]0, \pi], \int_{\delta\le|t|\le\pi} K_N(t)dt \underset{N\to+\infty}{\longrightarrow} 0$.

THÉORÈME 21. [THÉORÈME DE FEJÉR]
- *Soit $f \in \mathcal{C}(\mathbb{T})$. Alors $\|\sigma_N(f)\|_\infty \le \|f\|_\infty$ pour tout $N \ge 1$ et $\sigma_N(f) = f * K_N \underset{N\to+\infty}{\overset{u}{\longrightarrow}} f$.*
- *Soit $f \in L^p(\mathbb{T})$ pour un $p \in [1, +\infty[$. Alors $\|\sigma_N(f)\|_p \le \|f\|_p$ pour tout $N \ge 1$ et $\lim_{N\to+\infty}\|\sigma_N(f) - f\|_p = 0$.*

REMARQUE 22. On peut retrouver le théorème de WEIERSTRASS à partir du premier résultat.

APPLICATION 23. $\mathcal{F} : \mathcal{C}(\mathbb{T}) \longrightarrow c_0(\mathbb{Z}), f \longmapsto (c_n(f))_{n\in\mathbb{Z}}$ est injective.

THÉORÈME 24. *$(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L^2(\mathbb{T})$. En particulier, pour $f \in L^2(\mathbb{T})$:*

$$f = \sum_{n\in\mathbb{Z}} c_n(f)e_n \qquad \text{et} \qquad \|f\|_{L^2}^2 = \sum_{n\in\mathbb{Z}} |c_n(f)|^2$$

APPLICATION 25. [CALCULS DE SÉRIES]
On peut reprendre l'Exemple 41 pour calculer les normes des applications dans L^2 : pour $a \in [\![0, 2\pi]\!]$: $\sum_{n\in\mathbb{N}^*}\frac{\sin(na)}{n} = \frac{\pi-a}{2}$ (première fonction) et $\sum_{n\in\mathbb{N}^*}\frac{1}{n^4} = \frac{\pi^4}{90}$ (deuxième fonction).
On peut aussi calculer classiquement $\sum_{n\in\mathbb{N}^*}\frac{1}{n^2} = \frac{\pi^2}{6}$ et $\sum_{n\in\mathbb{N}^*}\frac{1}{(2n-1)^2} = \frac{\pi^2}{8}$.

III. B. L'espace $L^2(\rho, I)$ [BMP05, §3.1.5, p110] [Dem96, §II.5, p51]

Soit I un intervalle de $\mathbb{R}$.

DÉFINITION 26. Soit $\rho : I \longrightarrow \mathbb{R}$ une fonction mesurable, strictement positive et telle que pour tout $n \in \mathbb{N}$, $\int_I |x|^n \rho(x)dx < +\infty$. On dit alors que ρ est une fonction de poids.

DÉFINITION 27. On définit $L^2(I,\rho) = \left\{ f : I \longrightarrow \mathbb{C} \text{ mesurable} \mid \int_I |f(x)|^2 \rho(x)dx < +\infty \right\}$.

PROPOSITION 28. *$L^2(I,\rho)$ est un espace de* HILBERT *pour le produit du scalaire $\langle f \mid g \rangle_\rho = \int_I f(x)\overline{g(x)}\rho(x)dx$.*

PROPOSITION 29. *Il existe une unique famille $(P_n)_{n\in\mathbb{N}}$ de polynômes unitaires deux à deux orthogonaux pour $\langle . \mid . \rangle_\rho$ et tels que $\deg(P_n) = n$ pour tout n.*

EXEMPLE 30. Voir les dessins en annexe :
- Pour $I = \mathbb{R}$ et $\rho : x \longmapsto \mathrm{e}^{-x^2}$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de HERMITE,
- Pour $I = [-1,1]$ et $\rho : x \longmapsto 1$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de LEGENDRE.

THÉORÈME 31. [BASE HILBERTIENNE DE POLYNÔMES ORTHOGONAUX]
Soit ρ une fonction de poids. S'il existe $\alpha > 0$ tel que $\int_I \mathrm{e}^{\alpha|x|}\rho(x)dx < +\infty$, alors la famille $(P_n)_{n\in\mathbb{N}}$ est une base hilbertienne de $L^2(I,\rho)$.

EXEMPLE 32. Sans l'hypothèse on a le contre-exemple suivant : soit la fonction de poids $w : x \longmapsto x^{-\ln(x)}$ sur $I = \mathbb{R}_+$. Alors $(P_n)_{n\in\mathbb{N}}$ ne forme pas une base de $L^2(I,w)$.

APPLICATION 33. Si I est borné, on a donc nécessairement une base hilbertienne.
La famille $(P_n \exp(-.^2/2))_n$, pour $(P_n)_{n\in\mathbb{N}}$ les polynômes de HERMITE, est une base hilbertienne de $L^2(\mathbb{R})$.

ANNEXE

Théorème de projection sur un convexe fermé
Polynômes orthogonaux

QUESTIONS

Q Soient A, B des convexes fermés disjoints d'un espace de HILBERT réel. On suppos A compact. Montrer qu'il existe un hyperplan affine G séparant A et B, c'est-à-dire $H \setminus G$ a deux composantes connexes, dont l'une contient A et l'autre B.

R Considérons $\varphi : A \longrightarrow \mathbb{R}_+, x \longmapsto d(x,B)$. On a $d(A,B) = \min(\varphi) > 0$.
Soit $a \in A$ atteignant la distance et $b = p_B(a)$. Soit $\psi : x \longmapsto \langle b-a \mid x \rangle$. Montrons que $\psi(A) < 0$ et $\psi(B) > 0$.
Si $x \in A$, on a $\langle x-a \mid b-a \rangle \leq 0$ et si $y \in B$, on a $\langle y-b \mid a-b \rangle < 0$ et donc $\psi(y) > \langle b \mid a-b \rangle$
…

BIBLIOGRAPHIE

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bre99] H. BREZIS : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[Dem96] J.-P. DEMAILLY : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[HL09] F. HIRSCH et G. LACOMBE : *Eléments d'analyse fonctionnelle*. Dunod, 2009.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

214 THÉORÈME D'INVERSION LOCALE, THÉORÈME DES FONCTIONS IMPLICITES. EXEMPLES ET APPLICATIONS EN ANALYSE ET EN GÉOMÉTRIE.

I. Théorèmes d'inversion

[Rou99, Ch5, p175] [Gou08, §5.3, p321]

TIL : on veut généraliser le fait que si f est $\mathcal{C}^1$ et monotone alors f^{-1} est $\mathcal{C}^1$
Définition d'un $\mathcal{C}^k$-difféomorphisme (local)
Théorème d'inversion locale (figure) : c'est une condition suffisante
Contre-exemple : $f(u) = u + u^2 \sin(\pi/u)$ est dérivable de dérivée non nulle mais f n'est pas localement injective en 0 car elle n'est pas $\mathcal{C}^1$
Applications : $M \longmapsto M^p$ est un $\mathcal{C}^1$-difféomorphisme local en $I_n \to$ existence d'une racine p-ième matricielle, $\exp$ est un $\mathcal{C}^1$-difféomorphisme local en I_n
Exemple [Gou08, exo2, p238]
Théorème d'inversion globale
Contre exemple sans f injective [Rou99]
Application : changement de variables en coordonnées polaires, calcul de $\int_{\mathbb{R}} \mathrm{e}^{-x^2}\, dx$
Interprétation du rôle du jacobien comme limite d'un volume, en utilisant le TIL

II. Théorème des fonctions implicites

[Rou99, Ch5, p175] [Gou08, §5.3, p321]

TFI
Exemple en dimension 2 [Gou08, p326]
Exemple : $f(h,x) = (x-a)(b-x) + hx^3$. Pour h suffisamment petit, on a trois zéros de f dont on donne un développement asymptotique
Paramètrage du cercle. Exemple d'application à la recherche de 0
Théorème : TFI et TIL sont équivalents

THÉORÈME 1. [THÉORÈME DES EXTREMA LIÉS]
Soit $f, g_1, \dots, g_r : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ des fonctions de classe $\mathcal{C}^1$ définies sur U ouvert. Notons $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum local en $a \in \Gamma$ et si les formes linéaires $(dg_1(a), \dots, dg_r(a))$ sont libres, alors il existe des réels (uniques) $\lambda_1, \dots, \lambda_r$, appelés multiplicateurs de LAGRANGE, *tels que*

$$df(a) = \sum_{i=1}^{r} \lambda_i dg_i(a)$$

Application à la diagonalisation d'un endomorphisme symétrique en base orthonormée

III. Changement de coordonnées

[Rou99, Ch5, p175]

Changement de coordonnées, application pour une EDP [Rou99, Ch5, Ex. 63]
Immersion, submersion, rang constant
Remarque : tout cela généralise le TIL

THÉORÈME. [LEMME DE MORSE]
Soit $f : U \longrightarrow \mathbb{R}$ 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 $d^2 f(0)$ est non dégénérée, de signature $(p, n-p)$.
Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine de $\mathbb{R}^n$ tel que $\phi(0) = 0$ et $f(x) - f(0) = \varphi(x)_1^2 + \cdots + \varphi(x)_p^2 - \varphi(x)_{p+1}^2 - \cdots - \varphi(x)_n^2$ au voisinage de 0.

IV. Sous-variétés de $\mathbb{R}^n$

[Rou99]

Sous-variétés, exemples, vecteurs tangents,
Exemples : ouvert de $\mathbb{R}^n$, espace discret, sphère
interprétation géométrique des extrema liés

ANNEXE

Dessins des différents théorèmes et de quelques exemples

COMMENTAIRES

Intérêt du TIL est de résoudre l'équation $y = f(x)$! Celui du TFI est de trouver une paramétrisation de $f(x, y) = 0$ au voisinage d'un point annulateur. Faire un dessin pendant le speech ! Le [Rou99, Ch5] est bien adapté mais manque de certaines preuves.

QUESTIONS

Q Résoudre $X^3 + X^2 - X = A$ où A est une matrice de $\mathcal{M}_n(\mathbb{R})$.

R On pose $f(X) = X^3 + X^2 - X$. f est différentiable et

$$df(X)H = X^2H + XHX + HX^2/XH + HX - H$$

Donc $df(I_n)H = 4H$. Sur un voisinage de I_n et A suffisamment proche de I_n, on a $X = f^{-1}(A)$.

Q Calculer la différentielle de $X \in \mathcal{M}_n(\mathbb{R}) \longmapsto X^3$.

R Soit on fait le calcul à la main, soit on introduit l'application trilinéaire $(X, Y, Z) \longmapsto XYZ$.

Q Soit $f :]0, 1[\longrightarrow \mathbb{R}^2$ injective sur son image et $\mathcal{C}^1$. Son image est-elle une sous-variété ?

R Pas forcément ! Penser au lasso.

BIBLIOGRAPHIE

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

215 APPLICATIONS DIFFÉRENTIABLES DÉFINIES SUR UN OUVERT DE $\mathbb{R}^n$. EXEMPLES ET APPLICATIONS.

I. Autour de la différentiabilité

[Rou99, Ch2, p39] [Gou08, §5.1, p303]

I. A. FRÉCHET-différentiabilité

Définition au sens de FRÉCHET, unicité, lien avec la dérivée sur $\mathbb{R}$
Cas d'une fonction linéaire, bilinéaire, constante, ...
Propriétés de linéarité, de composition, de continuité
Classe $\mathcal{C}^1$, cas d'un $\mathcal{C}^1$-difféomorphisme
Différentielle du déterminant, d'une matrice puissance p, de l'inverse d'une matrice

I. B. Dérivées directionnelles et GATEAUX-différentiabilité

Définition, GATEAUX-différentiabilité
GATEAUX implique FRÉCHET, mais la réciproque est fausse ! $\to$ contre-exemple
Caractérisation : une fonction est $\mathcal{C}^1$ si et seulement si elle admet des dérivées partielles en tout point de U qui sont continues sur U.
Gradient

I. C. Inégalités sur les applications différentiables

[Rou99, Ch3, p93] [Gou08, §5.1 p303]

Inégalité de la moyenne, cas d'un ouvert convexe et f k-lipschitzienne
Théorème des accroissements finis. Applications

II. Différentielle d'ordre quelconque

[Rou99, Ch6, p275]

Classe $\mathcal{C}^k$, théorème de SCHWARZ (contre-exemple lorsque la fonction n'est pas $\mathcal{C}^2$)
Formules de TAYLOR

III. Théorèmes d'inversion locale/globale et des fonctions implicites

[Rou99, Ch5, p175] [Gou08, §5.3, p321]

TIL : on veut généraliser le fait que si f est $\mathcal{C}^1$ et monotone sur $I \subset \mathbb{R}$, alors f^{-1} est $\mathcal{C}^1$.
Définition d'un $\mathcal{C}^k$-difféomorphisme (local)
TIL (figure) : c'est une condition suffisante
Contre-exemple : $f(u) = u + u^2 \sin(\pi/u)$ est dérivable de dérivée non nulle mais f n'est pas localement injective en 0 car elle n'est pas $\mathcal{C}^1$.
Applications : $M \longmapsto M^p$ est un $\mathcal{C}^1$-difféomorphisme local en I_n $\to$ existence d'une racine p-ième matricielle, $\exp$ est un $\mathcal{C}^1$-difféomorphisme local en I_n
Exemple [Gou08, exo2, p238]
TIG, contre-exemple sans f injective [Rou99]
Application : changement de variables en coordonnées polaires, calcul de $\int_{\mathbb{R}} \exp -x^2 dx$
Interprétation du rôle du jacobien comme limite d'un volume, en utilisant le TIL
TFI
Exemple en dimension 2 [Gou08, p326]
Exemple : $f(h, x) = (x-a)(b-x) + hx^3$. Pour h suffisamment petit, on a trois zéros de f dont on donne un développement asymptotique
Paramétrage du cercle. Exemple d'application à la recherche de 0
Théorème : TFI et TIL sont équivalents

IV. Changement de coordonnées

[Rou99, Ch5, p175]

Changement de coordonnées, application pour une EDP [Rou99, Ch5, Ex. 63]
Immersion, submersion, rang constant
Remarque : tout cela généralise le TIL

THÉORÈME 1. [LEMME DE MORSE]
Soit $f : U \longrightarrow \mathbb{R}$ 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 $d^2 f(0)$ est non dégénérée, de signature $(p, n-p)$. Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine de $\mathbb{R}^n$ tel que $\phi(0) = 0$ et $f(x) - f(0) = \varphi(x)_1^2 + \cdots + \varphi(x)_p^2 - \varphi(x)_{p+1}^2 - \cdots - \varphi(x)_n^2$ au voisinage de 0.

V. Application à la recherche d'extremums

[Rou99, Ch5, p175] [Gou08, 5.2/3, p317/327]

Conditions nécessaires du premier/deuxième ordre, liens avec la signature de $d^2 f(a)$ (lien avec le lemme de MORSE)

THÉORÈME 2. [THÉORÈME DES EXTREMA LIÉS]
Soit $f, g_1, \ldots, g_r : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ des fonctions de classe $\mathcal{C}^1$ définies sur U ouvert. Notons $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum local en $a \in \Gamma$ et si les formes linéaires $(dg_1(a), \ldots, dg_r(a))$ sont libres, alors il existe des réels (uniques) $\lambda_1, \ldots, \lambda_r$, appelés multiplicateurs de LAGRANGE, tels que

$$df(a) = \sum_{i=1}^{r} \lambda_i dg_i(a)$$

Application à la diagonalisation d'un endomorphisme symétrique en base orthonormée
Inégalité de HADAMARD
Sous-variétés : vers les extrema liés. Méthodes de gradient

ANNEXE

Interprétation des différents théorèmes (TIL, TFI). extrema …

COMMENTAIRES

Il n'est pas obligatoire de parler de sous-variétés.
Il faut expliquer les problèmes que l'on rencontre en dimension multiple : des caractérisations par les dérivées directionnelles ne suffisent pas car on peut approcher le point autrement qu'en suivant une droite ! L'objectif de la différentielle est de ne pas avoir besoin de regarder ce qu'il se passe coordonnée par coordonnée
Le théorème du rang constant permet de faire le lien avec les sous-variétés.

QUESTIONS

Q On pose $f(x,y) = \sum_{n\geq 0} 2^{-n} a(nx)b(ny)$ où a, b sont $\mathcal{C}^1$ bornées et de dérivées bornées. Montrer que f est différentiable.

R On montre que f converge normalement et donc est $\mathcal{C}^0(\mathbb{R}^2)$. Ses dérivées partielles existent et sont bornées et continues ... on en déduit que f est $\mathcal{C}^1$.

Q Soit $f : \mathbb{S}^1 \longrightarrow \mathbb{S}^1$. On considère $F : (r,\theta) \longrightarrow rf(\theta)$. F est-elle différentiable ?

R Si F est différentiable, on a $F(tr, \mathrm{e}^{i\theta}) = tr\,\mathrm{e}^{if(\theta)} = L(tr\,\mathrm{e}^{i\theta}) + o(t)$, donc $L(r\,\mathrm{e}^{if(\theta)}) = r\,\mathrm{e}^{if(\theta)}$ donc $L = F$ et F est linéaire.
Pour que F soit linéaire, on veut $F(\mathrm{e}^{i\theta} + \mathrm{e}^{i\theta'}) = F(\mathrm{e}^{i\theta}) + F(\mathrm{e}^{i\theta'}) = \mathrm{e}^{if(\theta)} + \mathrm{e}^{if(\theta')}$. C'est vrai si f est une isométrie, c'est-à-dire si $f(\theta) = \pm\theta + \theta_0$ ($+$: rotations, $-$: symétrie).

Q $\varphi : A \longmapsto \mathrm{e}^{\mathrm{Tr}(A)}\,A$ est-elle différentiable ? Si oui calculer sa différentielle.

R $\partial_{E_{ij}}\varphi(A) = \mathrm{e}^{\mathrm{Tr}(A)}\,E_{ij}$ si $i \neq j$, $\mathrm{e}^{\mathrm{Tr}(A)}(A + E_{ij})$ sinon.
Donc $d\varphi(A)(H) = \mathrm{e}^{\mathrm{Tr}(A)}(H + \sum_i h_{ii}A)$.

Q Soit $f :]0,1[\longrightarrow \mathbb{R}$ dérivable. Soit $g(x,y) = \begin{cases} \frac{f(x)-f(y)}{x-y} \text{ si } x \neq y \\ f'(x) \text{ sinon} \end{cases}$. Montrer que g est différentiable en a lorsque f est deux fois dérivable en a.

R On regarde les dérivées partielles pour intuiter la différentielle.
On peut introduire $\varphi(t) = f(t) - f(a) - (t-a)f'(a) - \frac{(t-a)^2}{2}f''(a)$.

BIBLIOGRAPHIE

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

219 EXTREMUMS : EXISTENCE, CARACTÉRISATION, RECHERCHE. EXEMPLES ET APPLICATIONS.

Soit f une fonction à valeurs réelles définie sur un $\mathbb{R}$-espace vectoriel normé E.

I. Existence et unicité d'extremums

Définition 1. On dit que f admet un minimum (resp. maximum) local en $x_0 \in E$ s'il existe un voisinage V de x_0 tel que $\forall x \in V, f(x) \geq f(x_0)$ (resp. $\forall x \in V, f(x) \leq f(x_0)$).
On dit que f admet un minimum (resp. maximum) global en $x_0 \in E$ si $\forall x \in E, f(x) \geq f(x_0)$ (resp. $\forall x \in E, f(x) \leq f(x_0)$).
Un extremum de f est un maximum ou un mimimum de f.

Remarque 2. Un extremum global est bien sur un extremum local.

Exemple 3. $x \longmapsto x^2$ admet un minimum global en 0. $\cos$ admet un maximum global en les $(2k\pi)_{k\in\mathbb{Z}}$. L'application $x \longmapsto (x-1)x(x+1)$ admet un minimum local mais pas d'extremums.

I. A. Compacité et coercivité

[Gou08, §1.3, p31] [BMP05, §1.5, p26]

Proposition 4. *Une fonction continue sur un compact est bornée et atteint ses bornes.*

Application 5. Soit K un compact de E, F un fermé de E, avec K et F disjoints. Alors $K \longrightarrow \mathbb{R}, x \longmapsto d(x,F)$ atteint son minimum noté $d(K,F)$.

Application 6. Soit f une application définie sur un compact K et contractante. Alors f admet un unique point fixe.

Définition 7. On dit que f est coercive si $\lim_{\|x\|\to+\infty} f(x) = +\infty$.

Exemple 8. Une norme est coercive. Une forme linéaire ne l'est pas.

Proposition 9. *Si $E = \mathbb{R}^n$ et f est coercive et continue, alors f est minorée et atteint son minimum global.*

I. B. Convexité

[BMP05, §1.5, p26]

Définition 10. [ensemble convexe, fonction convexe]
Un ensemble E est convexe si pour tout $x, y \in E$ et $t \in [0,1]$, on a $tx + (1-t)y \in E$.
f est dite convexe si $\forall x, y \in E, \forall t \in [0,1], f(tx+(1-t)y) \leq tf(x) + (1-t)f(y)$.
f est dite strictement convexe si $\forall x, y \in E, \forall t \in]0,1[, f(tx+(1-t)y) \leq tf(x)+(1-t)f(y)$.

Théorème 11. *En dimension finie, si f est convexe alors elle est continue.*

Exemple 12. Une norme sur E est convexe. Pour $A \in \mathcal{S}_n(\mathbb{R})$, $f : x \longmapsto \langle Ax \mid x\rangle$ est convexe si et seulement si $A \in \mathcal{S}_n^+(\mathbb{R})$, et strictement convexe si et seulement si $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

Proposition 13. *Si f convexe admet un minimum local, alors c'est une minimum global.*
De plus l'ensemble des minima est convexe.
Si de plus f est strictement convexe, alors elle admet au plus un minimum, qui est alors global.

I. C. Dans les espaces de Hilbert

[Gou08, An.B, p407–416] [Bre99, ChV/VIII, p79–82/136] [BMP05, §3.1.2, p95–107]

Soit H un espace de Hilbert.

Théorème 14. [projection sur un convexe fermé]
Soit C un convexe fermé de H. Alors :

$$\forall x \in H, \exists! p \in C \mid \|x-p\| = d(x,C)$$

De plus, p est l'unique élément de C satisfaisant $\forall c \in C, \Re(\langle x-p \mid c-p\rangle) \leq 0$.

Exemple 15. Si C n'est pas convexe : soit $H = \mathbb{R}$ et $C = \mathbb{R}\setminus]-1,1[$. Alors 1 et -1 minimisent la distance de 0 à C.

Corollaire 16. *Soit F un sous-espace vectoriel fermé de H. Alors $H = F \oplus F^\perp$.*

Application 17. [théorème de Riesz-Fréchet]
Pour toute application $\phi \in H'$, il existe un unique $f \in H$ tel que $\forall v \in H, \phi(v) = \langle f \mid v\rangle$.
De plus $\phi \longmapsto f$ est une isométrie ($\|f\|_H = \|\phi\|_{H'}$).

Application 18. Existence et unicité de l'adjoint d'un opérateur $T \in H'$.

Théorème 19. [théorème de Lax-Milgram]
Soit $a : H^2 \longrightarrow \mathbb{R}$ une forme bilinéaire continue et coercive. Alors pour tout $\ell \in H'$, il existe un unique $u \in H$ tel que $\forall v \in H, a(u,v) = \ell(v)$.
Si de plus a est symétrique alors u est l'unique élément de H minimisant $v \longmapsto \frac{1}{2}a(v,v) - \ell(v)$.

Application 20. [problème de Dirichlet faible]
Soit $I =]0,1[$ et $f \in L^2(I)$. Alors

$$\exists! u \in H_0^1(I) \mid \forall v \in H_0^1(I), \int_I u'.v' + \int_I uv = \int_I fv$$

De plus u minimise la fonction $v \longmapsto \frac{1}{2}\int_I |v'|^2 + v^2 - \int_I fv$.

I. D. Holomorphie [BMP05, §2.5.2, p72]

On se place sur $E = \mathbb{C}$ et on considère $f \in \mathcal{H}(\Omega)$ où Ω est un ouvert connexe non vide de $\mathbb{C}$.

Théorème 21. [Formule de la moyenne]
Soit $z_0 \in \Omega$ et $r > 0$ tel que $\mathbb{D}(z_0, r) \subset \Omega$. Alors $f(z_0) = \frac{1}{2\pi}\int_0^{2\pi} f(z_0 + re^{i\theta})d\theta$.

Théorème 22. [Principe du maximum local]
Soit $f \in \mathcal{H}(\Omega)$ telle que $\sup_\Omega |f|$ est atteint. Alors f est constante.

Corollaire 23. *Si f ne s'annule pas et $\inf_\Omega |f|$ est atteint, alors f est constante.*

Théorème 24. [Principe du maximum global]
Soit $f \in \mathcal{H}(\Omega) \cap \mathcal{C}(\overline{\Omega})$. Alors $\max_\Omega |f| = \max_{\partial\Omega} |f|$ et s'il existe $z_0 \in \Omega$ réalisant le maximum, alors f est constante sur Ω.

Application 25. [Théorème de d'Alembert-Gauss]
Tout polynôme de $\mathbb{C}[X]$ non constant admet au moins une racine complexe.

Application 26. [Lemme de Schwarz]
Soit $\mathbb{D} = \mathbb{D}(0,1)$. Soit $f : \mathbb{D} \longrightarrow \mathbb{D}$ holomorphe telle que $f(0) = 0$.
Alors $|f'(0)| \leq 1$ et $\forall z \in \mathbb{D} \setminus \{0\}, |f(z)| \leq |z|$.
De plus, si $|f'(0)| = 1$ ou s'il existe $z \in \mathbb{D} \setminus \{0\}$, tel que $|f(z)| \leq |z|$, alors f est une rotation.

II. Extrema et calcul différentiel [BMP05, §1.3, p15]

II. A. Conditions du premier ordre et applications
[Gou08, §2.1/5.2, p71/315] [Rou99, p327]

Soit U un ouvert de $\mathbb{R}^n$ et f définie sur U.

Définition 27. Si f est différentiable en $x_0 \in U$ et si $df(x_0) = 0$, on dit que x_0 est un point critique de f.

Proposition 28. *Si x_0 est un extremum local de f et si f est différentiable en x_0, alors x_0 est un point critique.*

Exemple 29. Attention ce n'est qu'une condition nécessaire : $x \longmapsto x^3$ n'admet pas d'extremum en 0.

Exemple 30. Etude des extremums de $f : (x,y) \longmapsto x^4 + y^4 - 2(x-y)^2$: il n'y a pas de maximum local, et les seuls minimums locaux sont globaux et sont $\pm(\sqrt{2}, -\sqrt{2})$.

Théorème 31. [Théorème de Rolle]
Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction continue sur $[a,b]$, dérivable sur $]a,b[$ et telle que $f(a) = f(b)$. Alors il existe $c \in]a,b[$ tel que $f'(c) = 0$.

Application 32. [Théorème des accroissements finis]
Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction continue sur $[a,b]$, dérivable sur $]a,b[$. Alors il existe $c \in]a,b[$ tel que $f'(c) = \frac{f(b)-f(a)}{b-a}$.

II. B. Conditions du second ordre [Rou99, p327] [Gou08, §5.2, p315]

Proposition 33. *Soit $x_0 \in U$ un point critique de f. On suppose f de classe $\mathcal{C}^2$ en x_0. Alors :*
(i) si x_0 est un minimum (resp. maximum) local, alors $d^2 f(x_0)$ est positive (resp. négative),
(ii) si $d^2 f(x_0)$ est définie positive (resp. définie négative), alors x_0 est un minimum (resp. maximum) local.

Exemple 34. Ce n'est pas une condition nécessaire : prendre $x \longmapsto x^4$.

Théorème 35. [Lemme de Morse]
Soit $f : U \longrightarrow \mathbb{R}$ 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 $d^2 f(0)$ est non dégénérée, de signature $(p, n-p)$.
Alors il existe un $\mathcal{C}^1$-difféomorphisme φ entre deux voisinages de l'origine de $\mathbb{R}^n$ tel que $\phi(0) = 0$ et $f(x) - f(0) = \varphi(x)_1^2 + \cdots + \varphi(x)_p^2 - \varphi(x)_{p+1}^2 - \cdots - \varphi(x)_n^2$ au voisinage de 0.

Application 36. Soit x_0 un point critique de f tel que la hessienne de f est non dégénérée. Alors c'est un minimum (resp. maximum) local si et seulement si la hessienne est de signature $(n,0)$ (resp. $(0,n)$).
De plus, si la hessienne est de signature $(p, n-p)$ pour $1 \leq p \leq n-1$, alors on a des directions v pour lesquelles x_0 sera minimum local de $h \longmapsto f(x+hv)$ et d'autres pour lesquelles x_0 sera maximum local.

Exemple 37. [Cas $n = 2$] Soit x_0 un point critique de f telle que $D^2 f(x_0) = \begin{pmatrix} r & s \\ s & t \end{pmatrix}$. Alors

- si $rt - s^2 > 0$ et $r + t > 0$, x_0 est un minimum local,
- si $rt - s^2 > 0$ et $r + t < 0$, x_0 est un maximum local,
- si $rt - s^2 < 0$, x_0 n'est pas un extremum,
- si $rt - s^2 = 0$, on ne peut pas conclure.

Exemple 38. Pour le dernier cas, on peut considérer :

$$f(x,y) = x^4 \qquad f(x,y) = -x^4 \qquad f(x,y) = x^4 - y^4$$

II. C. Optimisation sous contraintes

[BMP05, §1, p20] [Gou08, §5.2/3, p317/327] [Rou99, Ch7, p380]

Théorème 39. [Théorème des extrema liés]
Soit $f, g_1, \dots, g_r : U \subset \mathbb{R}^n \longrightarrow \mathbb{R}$ des fonctions de classe $\mathcal{C}^1$ définies sur U ouvert. Notons $\Gamma = \{x \in U \mid g_1(x) = \cdots = g_r(x) = 0\}$. Si $f_{|\Gamma}$ admet un extremum local en $a \in \Gamma$ et si les formes linéaires $(dg_1(a), \dots, dg_r(a))$ sont libres, alors il existe des réels (uniques) $\lambda_1, \dots, \lambda_r$, appelés multiplicateurs de Lagrange, tels que

$$df(a) = \sum_{i=1}^{r} \lambda_i dg_i(a)$$

Application 40. Tout endomorphisme symétrique de E admet une valeur propre réelle.

Application 41. [Inégalité de Hadamard]
(i) Soient $x_1, \dots, x_n$ des vecteurs de $(E, \langle . \mid . \rangle)$ un espace préhilbertien (réel ou complexe). . Alors $|\det((\langle x_i \mid x_j \rangle)_{1 \leq i,j \leq n})| \leq \prod_{i=1}^n \|x_i\|^2$.
(ii) Soient $x_1, \dots, x_n$ des vecteurs de $\mathbb{C}^n$. Alors $|\det(x_1, \dots, x_n)| \leq \prod_{i=1}^n \|x_i\|_2$, où $\|.\|_2$ désigne la norme hermitienne standard sur $\mathbb{C}^n$.
Dans les deux points, on a égalité si et seulement si la famille $\{x_i\}_{1 \leq i \leq n}$ est orthogonale ou l'un des vecteurs est nul.

III. Optimisation numérique

III. A. Méthode de Newton

[Rou99, Ch4, p140]

Théorème 42.
Soit $f : [c,d] \longrightarrow \mathbb{R}$ une fonction $\mathcal{C}^2$, où $c < d$, et telle que $f(c) < 0 < f(d)$ et $f' > 0$ sur $[c,d]$. On considère la suite récurrente définie par $x_0 \in [c,d]$ et $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ pour $n \in \mathbb{N}$.
Alors en notant a l'unique 0 de f, on a :
(i) il existe $\alpha > 0$ tel que pour tout $x_0 \in [a-\alpha, a+\alpha]$, $(x_n)_{n\in\mathbb{N}}$ converge vers a de manière quadratique : il existe $C > 0$ telle que $\forall n \in \mathbb{N}, |x_{n+1} - a| \leq C |x_n - a|^2$.
(ii) si de plus $f'' > 0$ sur $[a,d]$, alors pour tout $x_0 \in]a,d]$, $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante et $x_{n+1} - a \sim_{n\to+\infty} \frac{f''(a)}{2f'(a)}(x_n - a)^2$.

Application 43. Approximation des zéros d'un polynôme.

III. B. Méthode de descente

[FGN12, §1.21, p39–41]

Théorème 44. [Méthode de gradient à pas optimal]
Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ elliptique, c'est-à-dire f est $\mathcal{C}^1$ et telle qu'il existe $\alpha > 0$ satisfaisant

$$\forall x, y \in \mathbb{R}^n, \langle \nabla f(x) - \nabla f(y) \mid x - y \rangle \geq \alpha \|x - y\|^2$$

On définit $(x_n)_{n\in\mathbb{N}}$ par $x_0 \in \mathbb{R}^n$ et $x_{n+1} = x_n - \rho_n \nabla f(x_n)$ où $\rho_n = \operatorname{argmin}_{\rho>0} f(x_n - \rho \nabla f(x_n))$. Alors $(x_n)_{n\in\mathbb{N}}$ converge vers l'unique minimum global de f.

Application 45. Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$ et $b \in \mathbb{R}^n$. L'application $f : x \longmapsto \frac{1}{2}\langle Ax \mid x \rangle - \langle b \mid x \rangle$ admet un unique minimum $\overline{x}$ caractérisé par $\nabla f(\overline{x}) = A\overline{x} - b = 0$. On converge vers cette solution par l'algorithme de gradient à pas optimal.

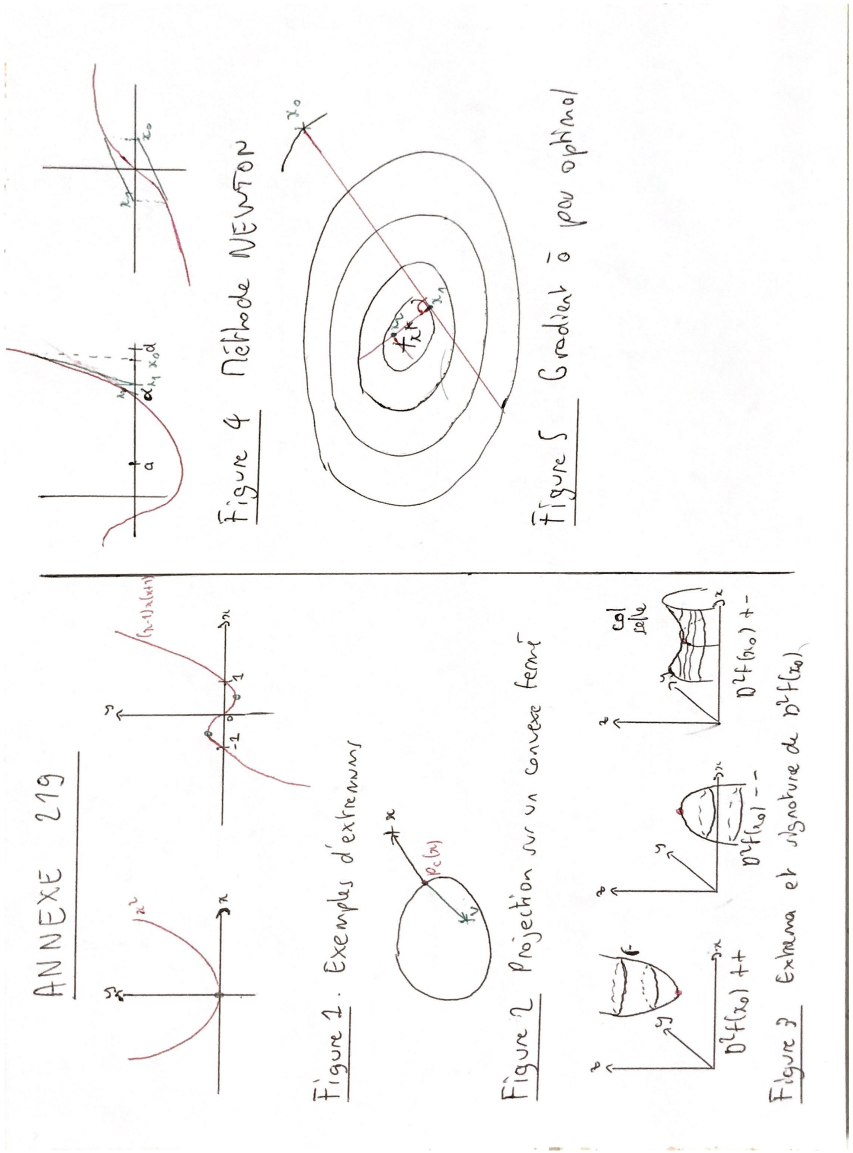
III. C. Problème des moindres carrés

[AK02, Ch7, p135]

Soient $n, p \in \mathbb{N}$ et $A \in \mathcal{M}_{n,p}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On cherche un vecteur $x \in \mathbb{R}^p$ tel que $\|b - Ax\|_2 = \inf_{y\in\mathbb{R}^p} \|b - Ay\|_2$.

Proposition 46.
(i) Il existe toujours une solution au problème,
(ii) x est solution si et seulement si $A^\top Ax = A^\top b$,
(iii) Si $n \geq p$ et $\operatorname{rg}(A) = p$, $A^\top A$ est inversible et il existe une unique matrice réelle B triangulaire inférieure, à diagonale positive, telle que $A^\top A = BB^\top$, et alors $x = (BB^\top)^{-1}A^\top b$ est une solution.

ANNEXE



SPEECH

La recherche d'extremums a de nombreuses applications dans divers domaines (informatique, économie, …). Dans cette leçon on s'intéresse d'abord aux conditions d'existence et d'unicité, selon que l'on soit sur un compact, dans un espace de HILBERT, … puis on fait ensuite le lien avec le calcul différentiel, notamment si f est définie sur $X \subset F$ espace vectoriel normé de dimension finie, les extrema sont à chercher parmi les points critiques, les points intérieurs à X où f n'est pas différentiable et les points non intérieurs à X (faire un schéma).

QUESTIONS

Q Soit $A \in \mathcal{M}_{n,\,p}(\mathbb{R})$ de rang $p \leq n$ et $b \in \mathbb{R}^n$. $x \longmapsto \|Ax-b\|_2$ admet-elle un minimum ?

R Posons $f : x \longmapsto \|Ax-b\|_2^2$. Alors f est différentiable et $\nabla f(X) = A^\top AX - A^\top b$ s'annule si et seulement si $x = (A^\top A)^{-1}A^\top b$ (car $A^\top A \in \mathcal{M}_n(\mathbb{R})$ a même rang que A, donc est inversible [1]). Ainsi $\|Ax-b\|_2 \geq \left\|A(A^\top A)^{-1}A^\top b - b\right\|_2$ et ce minimum est atteint.

Q Minimiser $X^\top Y$ où $Y \in \mathbb{R}^n$ est fixé et $\sum_i x_i^2 \leq 1$.

R On définit $f : X \longmapsto X^\top Y$ et $g : x \longmapsto \|x\|_2^2 - 1$.
Montrons d'abord que si f est convexe sur C convexe, elle atteint son maximum sur ∂C. En effet, f est convexe donc est continue. Si $x^* = \operatorname{argmax}_C f \notin \partial C$, écrivons $x^* = \sum_{i=1}^{\ell} \lambda_i x_i$ où $(x_i)_{1\leq i\leq \ell} \in \partial C$ et $\sum_{i=1}^{\ell}\lambda_i = 1$, les $(\lambda_i)_{1\leq i\leq \ell}$ étant strictement positifs. Par convexité puis définition de x^*, $f(x^*) \leq \sum_i \lambda_i f(x_i) \leq f(x^*)$ et donc $f(x_i) = f(x^*)$ pour $1 \leq i \leq \ell$.
Dans notre problème, f est linéaire donc convexe, donc $\max_{\mathbb{B}(0,1)} -f$ est atteint sur $\mathbb{S}(0,1)$. Sur la sphère, on a $\nabla g(X) = 2X \neq 0$, et $df(X)H = \langle H \mid Y\rangle$. Le théorème des extrema liés donne que si X est un extremum local il existe $\lambda \in \mathbb{R}$ telle que $df(X) = \lambda dg(x)$, ce qui donne $\lambda = \pm 2/\|Y\|_2$, puis $X^\top.Y = \pm\|Y\|_2$.
Remarque : on pouvait utiliser directement l'inégalité de CAUCHY-SCHWARZ.

Q Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ de classe $\mathcal{C}^2$ telle que pour tout x, les valeurs propres de $d^2f(x)$ sont dans $[\alpha,\beta]$ avec $\alpha > 0$. Montrer que f a un unique minimum global.

R On a $d^2f(x)(h,h) \geq \alpha|h|^2$. On en déduit que $f(h) - f(0) - df(0)h \geq \frac{\alpha}{2}\|h\|^2$. Donc f est coercive. Elle atteint son unique mimimum global. Pour le trouver, on peut utiliser l'algorithme de gradient à pas fixe. Quelle condition suffisante sur le pas τ faut-il pour avoir convergence ?
Posons $F(X) = X - \tau\nabla f(X)$. On a $dF(X)(H) = H - \tau H^\top d^2f(X)H$, donc $dF(X) = I - \tau\nabla^2 f(X)$. Comme $\left\|\nabla^2(f(X))\right\|_2 \leq \beta$, on a convergence si $\tau < \frac{1}{\beta}$.
En fait $\mathrm{Sp}(dF(X)) \subset [1-\tau\beta, 1-\tau\alpha]$ donc $\rho(dF(X)) \leq \max(|1-\tau\beta|, 1-\tau\alpha) < 1$ pour $\tau < \frac{2}{\beta}$.

Q Soit $f \in \mathcal{H}(\Omega)$ qui ne s'annule pas. Soit $z = \min_\Omega |f|$. Montrer que $z \in \partial\Omega$.

R $g = \frac{1}{f} \in \mathcal{H}(\Omega)$. On applique le principe du maximum à g, qui atteint ses bornes sur $\partial\Omega$, donc son minimum $z \in \partial\Omega$.

1. il est clair que $\ker(A) \subset \ker(A^\top A)$. Réciproquement si $A^\top Ax = 0, \ldots$

BIBLIOGRAPHIE

[AK02] G. Allaire et S.-M. Kaber : *Algèbre linéaire numérique*. Ellipses, 2002.

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bre99] H. Brezis : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[FGN12] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

220 ÉQUATIONS DIFFÉRENTIELLES $X' = f(t, X)$. EXEMPLES D'ÉTUDE DES SOLUTIONS EN DIMENSION 1 ET 2.

I. Autour du théorème de CAUCHY-LIPSCHITZ
[Ber17] [QZ13, ChX, p353] [Gou08, Ch6, p353]

I. A. Définitions [Ber17, Ch1]

Équation différentielle, ordre, on se ramène à l'ordre 1 matriciellement
Solution maximale, globale (implique maximale, mais pas l'inverse)
Problème de CAUCHY, solution d'un problème de CAUCHY, exemple

I. B. Existence et unicité locale [Ber17, §3.2, p84]

Fonction localement lipschitzienne par rapport à la seconde variable

THÉORÈME 1. [THÉORÈME DE CAUCHY-LIPSCHITZ (CAS GLOBALEMENT LIPSCHITZIEN)]
Soient I un intervalle de $\mathbb{R}$ et $f : I \times \mathbb{K}^n \longrightarrow \mathbb{K}^n$ continue, et globalement lipchitzienne par rapport à la seconde variable pour une norme $\|.\|$. Soit $(t_0, y_0) \in I \times \mathbb{K}^n$.
Alors il existe une unique solution y globale de $y' = f(t, y)$ telle que $y(t_0) = y_0$.

Problème linéaire, exemple, non linéaire, exemple

I. C. Durée de vie des solutions [Ber17, §3.8, p107]

Solution maximale non globale : exemple de $x' = x^2$
Théorème des bouts, cas où $O = \mathbb{K}^n$: solutions non bornées ou en temps infini
Lemme de GRÖNWALL, cas où f est lipschitzienne : solution maximale définie sur I tout entier

II. Résolution des équations différentielles

II. A. Le cas linéaire [Ber17, Ch2, p25]

Équation linéaire, théorème de CAUCHY-LIPSCHITZ avec solutions globales
Structure de l'ensemble des solutions, base de solutions, wronskien, ensemble des solutions
Méthode de la variation de la constante, exemple d'une équation avec des solutions mêlant polynômes et exponentielles

II. B. Équations de BERNOULLI, de RICATTI [Gou08, §6.3, p371] [Ber17, §4.2, p133]

Exemple des équations de BERNOULLI et de RICATTI

II. C. Équations différentielles et séries entières
[QZ13, §X.VI, p408/435] [Gou08, p245]

Il est souvent judicieux de rechercher des solutions particulières d'équations différentielles sous forme de série entière, notamment lorsque les fonctions coefficients sont des polynômes.

THÉORÈME 2. *Soient $p(x) = \sum_{n\geq 0} p_n x^n$ et $q(x) = \sum_{n\geq 0} q_n x^n$ convergeant pour $x \in]-R, R[$ où $R > 0$. Alors pour tout $a_0, a_1 \in \mathbb{C}$, il existe une unique solution y sur $]-R, R[$ de $y'' + py' + qy = 0$ avec $y(0) = a_0$ et $y'(0) = a_1$, y étant développable en série entière.*

APPLICATION 3. Calcul des solutions de $y'' + xy = 0$ avec $y(0) = 1$ et $y'(0) = 0$, de $(1 - x^2)y'' - xfy' = 2$ sur $]-1, 1[$ ou de $2x(1-x)y' + (1-2x)y = 1$ sur $]0, 1[$.

III. Étude qualitative
[Ber17, Ch5/6, p177–262] [QZ13, §X.IV, p380]

III. A. Définitions

Système autonome, les résultats de la première partie restent valables

III. B. Points d'équilibres et isoclines

Point d'équilibre, point stable, instable, asymptotiquement stable
Isocline $\rightarrow$ informations sur les champs de vecteurs tangents
Si $x(t) \underset{t\to+\infty}{\longrightarrow} x_\infty$ et $y(t) \underset{t\to+\infty}{\longrightarrow} y_\infty$, $f(x_\infty, y_\infty) = 0$.
Étude du système de LOKTA-VOLTERRA

III. C. Linéarisation [Ber17, §6.2, p239] [Rou99, §3.3, p127]

Stabilité du système linéaire en fonction des valeurs propres.
Noeuds, foyers, cols, ...

THÉORÈME 4. [STABILITÉ DE LIAPOUNOV]
Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ de classe $\mathcal{C}^1$ telle que $f(0) = 0$. Si les valeurs propres de $A = Df(0)$ sont toutes de partie réelle strictement négative, alors l'origine est un point d'équilibre attractif du système $y' = f(y)$.

Exemples
Contre-exemple lorsque l'on n'a plus les hypothèses : il peut se passer n'importe quoi !

ANNEXE

Diagramme de stabilité des solutions
Portrait de phase du système de LOKTA-VOLTERRA
Schéma d'EULER

QUESTIONS

Q Si $x(t) \underset{t\to+\infty}{\longrightarrow} x_\infty$ et $y(t) \underset{t\to+\infty}{\longrightarrow} y_\infty$, montrer que $f(x_\infty, y_\infty) = 0$.

R Si ce n'est pas le cas, il existe t_1 tel que $|f(x(t), y(t))| \geq \mu > 0$ pour $t \geq t_1$. On a alors $x(t) = x(t_1) + \int_{t_1}^t x'(s)ds > x(t_1) + \mu(t - t_1) \underset{t\to+\infty}{\longrightarrow} +\infty$. Contradiction.

Q Calculer la moyenne de x sur une période du système de LOKTA-VOLTERRA.

R On a $\overline{x} = \frac{1}{T}\int_0^T x(t)dt = \frac{1}{T}\int_0^T \frac{y'}{dy} + \frac{c}{d}dt = \frac{1}{T}\frac{c}{d}(T - 0) = \frac{c}{d}$.

Q Résoudre $x' = f(x)$ avec $f(x) = x\mathbb{1}_{[0,1[}(x) + \mathbb{1}_{[1,+\infty[}(x)$ et une condition initiale (t_0, x_0) quelconque.

R f est lipschitzienne donc admet une unique solution globale. On étudie ensuite selon la valeur de x_0, puis on fait les raccords, …

Q Si $F : \mathbb{R}^n \longrightarrow \mathbb{R}$ de classe $\mathcal{C}^1$ est telle que $\langle f(y) \mid y - v\rangle \leq \alpha - \beta \|y\|^2$ pour un $v \in \mathbb{R}^n$ et $\alpha, \beta > 0$, étudier la durée de vie des solutions de $y' = f(y)$.

R Il existe une unique solution globale à condition initiale fixée par le théorème de CAUCHY-LIPSCHITZ. Si (y, I) est une solution maximale, on a :

$$\langle y'(t) \mid y(t) - v\rangle \leq \alpha - \beta \|y(t)\|^2$$

On en déduit que $\langle y'(t) \mid y(t)\rangle \leq \alpha + \langle y'(t) \mid v\rangle - \beta \|y(t)\|^2$. Ainsi si $g : t \longmapsto \|y(t) - v\|^2$, on a $\frac{g'(t)}{2} \leq \alpha - \beta\frac{\|v\|^2}{2} - \beta\frac{g(t)}{2}$, d'où $\beta g(t) + g'(t) \leq 2\alpha + \beta\|x\|^2$ puis en appliquant le lemme de GRÖNWALL on vérifie que la durée de vie est infinie.
Autre possibilité : on trouver une boule assez grande telle que l'on ne sort pas de la boule.

Q Que dire de $x' = \cos(x + t^2)$?

R Les solutions existent, sont de durée de vie infinie car bornées en temps fini.

BIBLIOGRAPHIE

[Ber17] F. BERTHELIN : *Équations différentielles*. Cassini, 2017.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

221 ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES. SYSTÈMES D'ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES. EXEMPLES ET APPLICATIONS.

I. Théorie des équations différentielles linéaires

[Ber17] [QZ13, ChX, p353] [Gou08, Ch6, p353]

I. A. Définitions et généralités

I. B. Existence et unicité de solutions globales, structure des solutions

Équation linéaire, théorème de CAUCHY-LIPSCHITZ avec solutions globales

THÉORÈME 1. [THÉORÈME DE CAUCHY-LIPSCHITZ (CAS LINÉAIRE)]
Soient I un intervalle de $\mathbb{R}$ et $A, B \in \mathcal{C}(I, \mathcal{M}_n(\mathbb{K}))$. Soit $(t_0, y_0) \in I \times \mathbb{K}^n$.
Alors il existe une unique solution y globale de $y' = Ay + B$ telle que $y(t_0) = y_0$.

I. C. Durée de vie des solutions

II. Résolution explicite

II. A. Équations à coefficients constants

[Ber17, Ch2, p25]

II. B. Méthode de la variation de la constante

Méthode de la variation de la constante, exemple d'une équation avec des solutions mêlant polynômes et exponentielles

II. C. Développements en séries entières

[QZ13, §X.VI, p408/435] [Gou08, p245]

Il est souvent judicieux de rechercher des solutions particulières d'équations différentielles sous forme de série entière, notamment lorsque les fonctions coefficients sont des polynômes.

THÉORÈME 2. *Soient $p(x) = \sum_{n\geq 0} p_n x^n$ et $q(x) = \sum_{n\geq 0} q_n x^n$ convergeant pour $x \in]-R, R[$ où $R > 0$. Alors pour tout $a_0, a_1 \in \mathbb{C}$, il existe une unique solution y sur $]-R, R[$ de $y'' + py' + qy = 0$ avec $y(0) = a_0$ et $y'(0) = a_1$, y étant développable en série entière.*

APPLICATION 3. Calcul des solutions de $y'' + xy = 0$ avec $y(0) = 1$ et $y'(0) = 0$, de $(1 - x^2)y'' - xfy' = 2$ sur $]-1, 1[$ ou de $2x(1-x)y' + (1-2x)y = 1$ sur $]0, 1[$.

II. D. Changements de variables

[Gou08, §6.3, p371] [Ber17, §4.2, p133]

Équations de BERNOULLI, de RICATTI, ramenées à des équations différentielles linéaires

III. Étude qualitative

[Ber17, Ch5/6, p177–262] [QZ13, §X.IV, p380]

III. A. Définitions

Système autonome, les résultats de la première partie restent valables

III. B. Points d'équilibres et isoclines

Point d'équilibre, point stable, instable, asymptotiquement stable
Isocline $\rightarrow$ informations sur les champs de vecteurs tangents
Si $x(t) \underset{t\to+\infty}{\longrightarrow} x_\infty$ et $y(t) \underset{t\to+\infty}{\longrightarrow} y_\infty$, montrer que $f(x_\infty, y_\infty) = 0$.
Étude du système de LOKTA-VOLTERRA

III. C. Vers les équations non linéaires

[Ber17, §6.2, p239] [Rou99, §3.3, p127]

Stabilité du système linéaire en fonction des valeurs propres.
Noeuds, foyers, cols …

THÉORÈME 4. [STABILITÉ DE LIAPOUNOV]
Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ de classe $\mathcal{C}^1$ telle que $f(0) = 0$. Si les valeurs propres de $A = Df(0)$ sont toutes de partie réelle strictement négative, alors l'origine est un point d'équilibre attractif du système $y' = f(y)$.

Exemples
Contre-exemple lorsque l'on n'a plus les hypothèses : il peut se passer n'importe quoi !

ANNEXE

Diagramme de stabilité des solutions
portrait de phase du système de LOKTA-VOLTERRA
Schéma d'EULER

COMMENTAIRES

Voir l'intro historique du [Gou08].
On peut définir les équations différentielles linéaires sur des espaces de BANACH ... mais ce n'est pas du tout une bonne stratégie : il faut faire attention quand on revient en dimension finie et cela engendre des difficultés. Bref rester dans $\mathbb{K}^n$. Il est important de bien travailler les premières questions post-développement : résolution d'une équation différentielle, exemple d'application du théorème de CAUCHY-LIPSCHITZ.

QUESTIONS

Q Résoudre $xy' = y + x$.

R On se place sur $]0, +\infty[$ puis $]-\infty, 0[$ pour se ramener à $y' - \frac{y}{x} = 1$.
Les solutions homogènes sont $y_0 : x \longmapsto C\,|x|$, puis par variation de la constante on obtient une solution particulière, d'où $y(x) = Cx + x\ln(|x|)$ sur $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$.
On regarde ensuite si l'on peut raccorder (penser que la solution doit alors être $\mathcal{C}^1$!)

Q Considérons $y' = Ay$ pour $A \in \mathcal{M}_3(\mathbb{R})$ de rang 2. Montrer que les solutions restent dans un même plan.

R On admet qu'il existe une matrice B de rang 1 telle que $BA = 0$. On remarque alors que $B(\exp(At) - I) = 0$, donc $\mathrm{Im}(\exp(At) - \mathrm{Id}) \subset \ker(B)$ de dimension 2.
Si z est une solution avec $z(0) = z_0$, alors $z(t) = (\mathrm{e}^{At} - I)y_0 + y_0 \in \ker(B) + y_0$.

Q Soit f $\mathcal{C}^1$ et telle que $f' + af \underset{t\to+\infty}{\longrightarrow} 0$ avec $a > 0$. Montrer que $f, f' \underset{t\to+\infty}{\longrightarrow} 0$.

R Si $\lambda = f' + af$, on a $\forall x, f(x) = f(0)\,\mathrm{e}^{-ax} + \mathrm{e}^{-ax}\int_0^x \mathrm{e}^{at}\,\lambda(t)dt$.
D'où $\left|\int_0^x \mathrm{e}^{at}\,\lambda(t)dt\right| \leq \|\lambda\|_\infty \int_0^x \mathrm{e}^{at}\,dt = \|\lambda\|_\infty (\mathrm{e}^{ax} - 1)$, donc f est bornée.
Puis $f'(x) = -af(0)\,\mathrm{e}^{-ax} - a\,\mathrm{e}^{-ax}\int_0^x \mathrm{e}^{at}\,\lambda(t)dt + \lambda(x)$ donc f' est également bornée.

BIBLIOGRAPHIE

[Ber17] F. BERTHELIN : *Équations différentielles*. Cassini, 2017.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

222 EXEMPLES D'ÉQUATIONS AUX DÉRIVÉES PARTIELLES LINÉAIRES.

SPEECH

L'idée de cette leçon est d'étudier quelques exemples illustrants des techniques de résolution d'ÉDP. Dans un premier il y a des méthodes directes, comme l'équation de transport résolue par un changement de variables dans le cas d'une vitesse constante. Dans le cas général on peut se placer sur une courbe sur laquelle l'ÉDP se transforme en une ÉDO. Ensuite pour l'équation des ondes, c'est encore un changement de variables qui permet d'obtenir une équation simple ; on obtient un cône de dépendance et d'influence. La théorie de FOURIER est un outil également utile : dans le cas périodique, les séries de FOURIER permettent sous certaines hypothèses de régularité, d'obtenir des solutions périodiques et plus généralement, on peut utiliser la transformée de FOURIER, par exemple en introduisant une transformée de FOURIER partielle par rapport à la variable d'espace qui va simplifier l'équation dans le domaine de FOURIER, on revient ensuite à la solution via la transformée de FOURIER inverse. Notons également les techniques hilbertiennes : les ÉDP n'ont pas nécessairement besoin d'hypothèses de régularité trop importantes : notion de solution faible. Pour finir on peut parler de l'équation de LAPLACE qui se résout en introduisant les fonctions harmoniques.

QUESTIONS

Q Pourquoi $H^1([0,1])$ est un espace normé ?

Q Pourquoi la convergence forte implique la convergence faible ?

Q Résoudre $\partial_t u + c\partial_x u = u$ avec condition initiale u_0.

R On considère une trajectoire $t \longmapsto (X(t), t)$ avec X de classe $\mathcal{C}^1$. Soit $w : t \longmapsto u(X(t), t)$. On calcule $w'(t) = (X'(t) - c)\partial_t u(X(t), t) + w(t)$. Prenons $X(t) = a + ct$ avec $a \in \mathbb{R}$. On a $w' = w$ donc $w = A\,\mathrm{e}^t$ pour $A \in \mathbb{R}$, et la condition initiale donne $A = u_0(a)$.
On a alors $w(t) = u_0(a)\,\mathrm{e}^t$ puis $u(x,t) = u(x - ct + ct, t) = u_0(x - ct)\,\mathrm{e}^t$.

Q Et en dimension supérieure ? Si $u : \mathbb{R}^n \longrightarrow \mathbb{R}$ est telle que $\sum_{i=1}^n a_i \partial_{x_i} u = 0$?

R On a $\nabla u \in A^\perp$. Fixons une variable comme étant le temps, par exemple $t = x_n$. On prend $a_n = 1$ pour l'instant, de sorte que $\partial_u x + \sum_{i=1}^{n-1} a_i \partial_{x_i} u = 0$. Prenons $X : \mathbb{R} \longrightarrow \mathbb{R}^{n-1}$ de classe $\mathcal{C}^1$ et $w : t \longmapsto u(X(t), t)$. On obtient $w'(t) = \sum_{i=1}^{n-1} (X_i'(t) - a_i)\partial_{x_i} u_i$.
On prend $X_i' = a_i$, de sorte que $X(t) = \zeta + \sum_{i=1}^{n-1} t a_i e_i$. Alors $w = A$ et donc $w(t) = u(X(0), 0) = u_0(\zeta)$.

Q Résoudre $x\partial_x u + y\partial_y u = a\sqrt{x^2 - y^2}$.

R Passons en coordonnées polaires : $u(x,y) = v(r,\theta)$. v vérifie $\partial_r v = a$ donc $v(r,\theta) = ar + c(\theta)$ puis $\lim_{\theta\to\pi} v = \lim_{\theta\to-\pi} v$ donc $\lim_{\theta\to\pi} \partial_\theta v = \lim_{\theta\to-\pi} \partial_\theta v$, et ainsi $c \in \mathcal{C}^1(\mathbb{T})$.

223 SUITES NUMÉRIQUES. CONVERGENCES, VALEURS D'ADHÉRENCE. EXEMPLES ET APPLICATIONS.

Dans cette leçon, on considère des suites à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I. Autour de la convergence de suites

[Gou08, §1.2/Ch4, p19/191]

Définition d'une suite convergente/divergente, exemples de $u_n = (1+1/n)^n \underset{n\to+\infty}{\longrightarrow} \mathrm{e}$ (ou plus simple ...), de $u_n = (-1)^n$
Unicité de la limite, somme, produit de limites ... Une suite convergente est bornée
$\liminf, \limsup$: existence et unicité, la suite converge vers ℓ si et seulement si $\ell = \liminf = \limsup$, exemple d'une suite sous-additive [QZ13]
Valeur d'adhérence, caractérisation, exemples
Convergence si on a une unique valeur d'adhérence
Théorème de Bolzano-Weierstrass
Exemples des suites arithmétiques et géométriques
Suites de Cauchy

II. Comportements de suites réelles

[El 11]

$\mathbb{K} = \mathbb{R}$ dans cette partie, sauf mention explicite (théorème de Cesàro)
Théorème des gendarmes, exemples
Suites adjacentes, exemple [Gou08, p198], segments emboités

II. A. Comparaison asymptotique

[Gou08, §2.2, p85–93]

Définition 1. Soient u et v deux suites. On dit qu'au voisinage de $+\infty$:
- v domine u, et on note $u_n = O(v_n)$, si $\exists C > 0, \exists n_0 \in \mathbb{N} \,|\, \forall n \geq n_0, |u_n| \leq C\,|v_n|$,
- u est négligeable devant v, et on note $u_n = o(v_n)$, si $\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0, |u_n| \leq \varepsilon\,|v_n|$,
- u et v sont équivalentes, et on note $u_n \sim v_n$, si $u_n - v_n = o(v_n)$.

Exemple 2. $n^2 + \sin(n) = O(n^2)$ et $n^2 + \sin(n) \sim n^2$

Proposition 3. *On les propriétés suivantes :*
(i) *o et O sont stables par somme, c'est-à-dire si $u_n = o(w_n)$ et $v_n = o(w_n)$, alors $u_n + v_n = o(w_n)$, et de même avec O,*
(ii) *o, O et $\sim$ sont stables par produit, passage à une puissance. Par exemple si $u_n = O(w_n)$ et $v_n = O(z_n)$, alors $u_n v_n = O(w_n z_n)$, puis si $u_n \sim w_n$ et $v_n \sim z_n$, alors $u_n v_n \sim w_n z_n$.*

Remarque 4. La relation $\sim$ n'est pas compatible avec l'addition : $n+2 \sim n+1$ et $-n \sim -n$ mais $2 \not\sim 1$.

Définition d'un développement asymptotique.

Théorème 5. [Sommation des relations de comparaison]
Soient $u = (u_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{K}$ et $v = (v_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{R}^+$. Notons $S_n(u) = \sum_{k\leq n} u_k$ et $R_n(u) = \sum_{k>n} u_k$ (et de même $S_n(v)$ et $R_n(v)$) les sommes partielles et restes d'ordre $n \in \mathbb{N}$ associés. Alors :

	$u_n = o(v_n)$	$u_n = O(v_n)$	$u_n \sim v_n$
$\sum_{n\in\mathbb{N}} v_n < +\infty$	$R_n(u) = o(R_n(v))$	$R_n(u) = O(R_n(v))$	$R_n(u) \sim R_n(v)$
$\sum_{n\in\mathbb{N}} v_n = +\infty$	$S_n(u) = o(S_n(v))$	$S_n(u) = O(S_n(v))$	$S_n(u) \sim S_n(v)$

II. B. Étude de suites récurrentes

[FGN07, p99–103] [Gou08, Ch4, p191]

Théorème 6. [Théorème de Cesàro]
Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ telle que $a_n \underset{n\to+\infty}{\longrightarrow} \ell$. Alors $\frac{1}{n}\sum_{k=1}^{n} a_k \underset{n\to+\infty}{\longrightarrow} \ell$.

Application 7. Soit f une application continue définie au voisinage de 0^+ admettant un développement asymptotique en 0 de la forme $f(x) = x - ax^\alpha + o(x^\alpha)$, où $a > 0$ et $\alpha > 1$. Alors pour $u_0 > 0$ assez petit, la suite u définie par $u_{n+1} = f(u_n)$ pour $n \in \mathbb{N}$ vérifie $u_n \sim \frac{1}{(na(\alpha-1))^{\frac{1}{\alpha-1}}}$.
Exemples de $f = \sin$ et $f = \log(1+.)$.

Application 8. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 \in \mathbb{R}$ et, pour tout $n \in \mathbb{N}$, $u_{n+1} = u_n + \mathrm{e}^{-u_n}$. Alors on a le DA_2 suivant : $u_n = \ln n + \frac{\ln n}{2n} + o\left(\frac{\ln n}{n}\right)$.

Suites récurrentes linéaires [Gou08]

III. Approximation

[Dem96, ChIV, p93] [Rou99]

Approximation d'un irrationnel par des rationnels [Gou08, Ch4, p196]
Coefficient de convergence, convergence géométrique, quadratique
Suites récurrentes avec point fixe : vitesse de convergence en fonction de la dérivée en le point fixe ...
Méthode de Romberg-Richardson [Dem96, §III.5.2, p85]

Théorème 9.
Soit $f : [c,d] \longrightarrow \mathbb{R}$ une fonction $\mathcal{C}^2$, où $c<d$, et telle que $f(c)<0<f(d)$ et $f'>0$ sur $[c,d]$. On considère la suite récurrente définie par $x_0 \in [c,d]$ et $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ pour $n \in \mathbb{N}$.
Alors en notant a l'unique 0 de f, on a :
(i) il existe $\alpha > 0$ tel que pour tout $x_0 \in [a-\alpha, a+\alpha]$, $(x_n)_{n\in\mathbb{N}}$ converge vers a de manière quadratique et il existe $C>0$ telle que $\forall n \in \mathbb{N}, |x_{n+1}-a| \leq C|x_n-a|^2$.
(ii) si de plus $f'' > 0$ sur $[a,d]$, alors pour tout $x_0 \in]a,d]$, $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante et $x_{n+1} \sim_{n\to+\infty} \frac{f''(a)}{2f'(a)}(x_n-a)^2$.

Autre méthode : descente de gradient

SPEECH

Étude les suites numériques permet de comprendre les nombres réels (constructions, suites des décimaux, …) et offre un cadre fondamental qui amène des applications en analyse, intégration, analyse complexe, probabilités, ….

COMMENTAIRES

Une bonne introduction historique : [FGN07, p57].

QUESTIONS

Q Pour quels $\theta \in \mathbb{R}$ la suite $(u_n = \cos(n\theta))_{n\in\mathbb{N}}$ converge-t-elle ?

R Distinguer selon que θ/π est commensurable ou non : si non la suite ne converge pas car elle est dense dans $[-1,1]$, si oui elle est périodique donc ne converge que si $\theta \in 2\pi\mathbb{Z}$.

Q Même exercice avec $(v_n = \sin(n\theta))_{n\in\mathbb{N}}$.

R On montre qu'une suite converge si et seulement si l'autre converge. Nécessairement la limite est alors 0 … Autre manière de faire : penser que $\cos(n\theta) = \Re(e^{n\theta})$ puis utiliser le théorème de Cesàro.

Q Donner un développement asymptotique de $u_n = \sqrt{n+u_{n-1}}$ où $u_1 = 1$.

R On montrer que $u_n \leq 2\sqrt{n} = o(n)$ par récurrence. Puis :

$$u_{n+1} = \sqrt{n}(\sqrt{1+u_n/n}) = \sqrt{n}(1+1/2u_n/n+o(u_n/n)) = \sqrt{n}+1/2u_n/\sqrt{n}+o(u_n/\sqrt{n})$$

Donc $u_n \sim \sqrt{n}$ puis $u_{n+1} = \sqrt{n} + \frac{1}{2} + o(1)$. En réinjectant on obtient

$$u_{n+1} = \sqrt{n} + \frac{1}{2} - \frac{1}{4n} + o(1/n)$$

BIBLIOGRAPHIE

[Dem96] J.-P. Demailly : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[El 11] M. El Amrani : *Suites et séries numériques, suites et séries de fonctions*. Ellipses, 2011.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[QZ13] H. Queffélec et C. Zuily : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

224 EXEMPLES DE DÉVELOPPEMENTS ASYMPTOTIQUES DE SUITES ET DE FONCTIONS.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et (X, d) un espace métrique.

I. Comparaison de suites et de fonctions [Gou08, §2.2, p85–93]

I. A. Relations de comparaison

Définition 1. Soient f et g deux applications de $D \subset X$ à valeurs dans $\mathbb{K}$ et soit a un point d'accumulation de D. On dit qu'au voisinage de a :
- f est dominée par g, et on note $f(x) \underset{x\to a}{=} O(g(x))$, si $\exists C > 0, \exists V \in \mathcal{V}(a), \forall x \in \mathcal{V} \cap D, \|f(x)\| \leq C \|g(x)\|$,
- f est négligeable devant g, et on note $f(x) \underset{x\to a}{=} o(g(x))$, si $\forall \varepsilon > 0, \exists V \in \mathcal{V}(a), \forall x \in \mathcal{V} \cap D, \|f(x)\| \leq \varepsilon \|g(x)\|$,
- f et g sont équivalentes, et on note $f(x) \underset{x\to a}{\sim} g(x)$, si $f(x) - g(x) \underset{x\to a}{=} o(g(x))$.

Remarque 2. Ces définitions sont valables pour des suites numériques : prendre $X = \mathbb{N}$, $E = \mathbb{R}$ ou $\mathbb{C}$ et $a = +\infty$. Dans ce cas, on omettra le $n \to +\infty$ qui est implicite.

Exemple 3.
- $n^2 + \sin(n) = O(n^2)$ et $n^2 + \sin(n) \sim n^2$,
- Pour $\alpha, \beta > 0$, $x^\alpha \underset{x\to+\infty}{=} o(\mathrm{e}^{\beta x})$ et $x^\alpha \underset{x\to+\infty}{=} o(\beta^x)$,
- Si $f(x) = 3x^5 - x^4 + x^2$ alors $f(x) \underset{x\to0}{=} o(x)$, $f(x) \underset{x\to0}{=} o(x^6)$ et $f(x) \underset{x\to0}{\sim} 3x^5$.

Proposition 4. *On les propriétés suivantes :*
(i) o et O sont stables par somme, c'est-à-dire si $f = o(\varphi)$ et $g = o(\varphi)$, alors $f + g = o(\varphi)$, et de même avec O,
(ii) o, O et $\sim$ sont stables par produit, passage à une puissance. Par exemple si $f = O(\varphi_1)$ et $g = O(\varphi_2)$, alors $fg = O(\varphi_1\varphi_2)$, puis si $f \sim \varphi_1$ et $g \sim \varphi_2$, alors $fg \sim \varphi_1\varphi_2$.

Remarque 5. La relation $\sim$ n'est pas compatible avec l'addition : $n+2 \sim n+1$ et $-n \sim -n$ mais $2 \not\sim 1$.

I. B. Développement limité

Dans cette partie, I désigne un intervalle de $\mathbb{R}$ non trivial. On considère $f : I \longrightarrow \mathbb{K}$.

Définition 6. Soient $n \in \mathbb{N}^*$ et $a \in I$. On dit que f admet un développement limité d'ordre n au voisinage de a (noté $\mathrm{DL}_n(a)$) s'il existe $a_0, \dots, a_n \in \mathbb{K}$ tels que, au voisinage de a, on a $f(x) = a_0 + a_1(x-a) + \cdots + a_n(x-a)^n + o((x-a)^n)$.

Dans la suite quitte translater f, on supposera que $a = 0$ (et donc $0 \in I$).

Théorème 7. [Formule de Taylor-Young]
Si f est n fois dérivable en 0, alors f admet le $\mathrm{DL}_n(0)$ suivant :

$$f(x) = f(a) + f'(a)(x-a) + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + o((x-a)^n)$$

Exemple 8. Développements limités de fonctions usuelles. **[Voir annexe].**

Application 9. [Théorème central limite]
Soit $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires réelles i.i.d. de carré intégrable. Alors :

$$\tfrac{1}{\sqrt{n}} \textstyle\sum_{i=1}^n (X_i - \mathbb{E}[X_1]) \xrightarrow[n\to+\infty]{\mathcal{L}} Z \sim \mathcal{N}(0, \mathrm{Var}(X_1))$$

Proposition 10. *f est continue (resp. dérivable) en 0 si et seulement si f admet un $\mathrm{DL}_0(0)$ (resp. $\mathrm{DL}_1(0)$).*

Remarque 11. On ne peut pas généraliser ce résultat à $n > 1$: par exemple pour f définie par $f(x) = x^3 \sin(\frac{1}{x})$, on a que f admet un $\mathrm{DL}_2(0)$ mais n'est pas deux fois dérivable en 0.

Proposition 12. *Si f admet un $\mathrm{DL}_n(0)$ pour un $n \in \mathbb{N}$, alors il est unique.*

Proposition 13. [Dérivation/intégration de DL]
On a les propriétés suivantes :
(i) Si f et dérivable et si f' admet un $\mathrm{DL}_n(0)$ de la forme $f'(x) = \sum_{k=0}^n a_k x^k + o(x^n)$, alors f admet un $\mathrm{DL}_{n+1}(0)$ de la forme $f(x) = f(0) + \sum_{k=0}^n \frac{a_k}{k+1} x^{k+1} + o(x^{n+1})$,
(ii) Si f est $n \geq 2$ fois dérivables en 0, alors f' admet un $\mathrm{DL}_{n-1}(0)$.

Proposition 14. [Somme et produit de DL]
Soit $g : I \longrightarrow \mathbb{K}$ une autre application. Supposons que f et g admettent un $\mathrm{DL}_n(0)$ et écrivons $f(x) = P_n(x) + o(x^n)$ et $g(x) = Q_n(x) + o(x^n)$ avec $P_n, Q_n \in \mathbb{R}_n[X]$. Alors :
(i) $f + g$ admet un $\mathrm{DL}_n(0)$ et $(f+g)(x) = (P_n + Q_n)(x) + o(x^n)$,
(ii) $f \times g$ admet un $\mathrm{DL}_n(0)$ et $(f \times g)(x) = R_n(x) + o(x^n)$ où R_n est le reste de la division euclidienne de P_nQ_n par X^{n+1}.
(iii) Si $g(0) \neq 0$, alors $\frac{f}{g}$ admet un $\mathrm{DL}_n(0)$ et $(f/g)(x) = R_n(x) + o(x^n)$, où R_n est l'unique polynôme de $\mathbb{K}[X]$ tel que P_n s'écrit $P_n = R_nQ_n + X^{n+1}S_n$, avec $\deg(S_n) \leq n$.

Proposition 15. **[Composition de DL]**
Soit $g : J \longrightarrow \mathbb{K}$ une autre application, où J est un intervalle de $\mathbb{R}$ tel que $x_0 = f(0) \in J$. Supposons que $f(x) = P_n(x) + o(x^n)$ admet un $\mathrm{DL}_n(0)$ et que $g(x_0 + h) = Q_n(h) + o(h^n)$ admet un $\mathrm{DL}_n(x_0)$.
Alors $g \circ f$ admet un $\mathrm{DL}_n(0)$ et $g \circ f(x) = R_n(x) + o(x^n)$ où R_n est le reste de la division euclidienne de $Q_n \circ P_n$ par X^{n+1}.

Application 16. $\mathrm{DL}_3(0)$ de $\arcsin$ à partir du $\mathrm{DL}(0)$ de $\sin$.

I. C. Développement asymptotique

Définition 17. Soit $a \in \overline{X}$. On appelle échelle de comparaison un ensemble $\mathcal{E}$ de fonctions définies au voisinage de a dans X sauf éventuellement en a, et telles que si $f, g \in \mathcal{E}$, alors $f = g$ ou bien $f = o(g)$ ou bien $g = o(f)$.

Exemple 18. $X = \mathbb{R}$, $a = +\infty$: $\mathcal{E}_1 = \{x \longmapsto x^\alpha \,|\, \alpha \in \mathbb{R}\}$ et $\mathcal{E}_2 = \{x \longmapsto x^\alpha (\ln(x))^\beta \,|\, \alpha, \beta \in \mathbb{R}\}$.

Définition 19. Soient $f : D \subset X \longrightarrow \mathbb{K}$ un application et a un point d'accumulation de D dans X. Soit $k \in N^*$. On appelle développement asymptotique à k termes de f par rapport à une échelle de comparaison $\mathcal{E}$ au voisinage de a (noté $\mathrm{DA}_k(a)$) toute expression de la forme $c_1 f_1 + c_2 f_2 + \cdots + c_k f_k$ telle que $(c_i)_{1 \leq i \leq k} \in \mathbb{K}^k$, $(f_i)_{1 \leq i \leq k} \in \mathcal{E}^k$ et :
(i) $f_{i+1} \underset{a}{=} o(f_i)$ pour tout $1 \leq i \leq k-1$,
(ii) $f(x) \underset{x \to a}{=} c_1 f_1(x) + c_2 f_2(x) + \cdots + c_k f_k(x) + o(f_k(x))$.

Proposition 20. *A $\mathcal{E}$ fixé, le DA_k, s'il existe, est unique.*

Remarque 21. Un développement limité est un développement asymptotique par rapport à l'échelle de comparaison constituée des fonctions du type $x^\alpha (\alpha \in \mathbb{N})$. On en déduit l'unicité du développement limité à tout ordre. Notons que l'on peut généraliser le DL à $a = +\infty$ si $+\infty \in \overline{I}$ en considérant $\mathcal{E} = \{x \longmapsto x^{-\alpha} \,|\, \alpha \in \mathbb{N}\}$ et on se ramène en 0 en posant $X = 1/x$.

Application 22. Les DA permettent de préciser la position relative d'une courbe par rapport à une tangente ou une asymptote. Par exemple, considérons $f(x) = x^3 \sin\left(\frac{1}{x}\right)$ pour $x \neq 0$ et $f(0) = 0$. Alors $f(x) \underset{x \to +\infty}{=} x^3 \left(\frac{1}{x} - \frac{1}{6x^3} + \frac{1}{120x^5} + o\left(\frac{1}{x^5}\right)\right)$ lorsque $x \to +\infty$ donc $y = x^2 - \frac{1}{6}$ est une asymptote par valeurs inférieures de f en $+\infty$.

II. Exemples de développements asymptotiques de suites

II. A. Séries numériques

[Gou08, §4.2, p201–206]

Théorème 23. **[Sommation des relations de comparaison]**
Soient $u = (u_n)_{n \in \mathbb{N}}$ à valeurs dans $\mathbb{K}$ et $v = (v_n)_{n \in \mathbb{N}}$ à valeurs dans $\mathbb{R}^+$. Notons $S_n(u) = \sum_{k \leq n} u_k$ et $R_n(u) = \sum_{k > n} u_k$ (et de même $S_n(v)$ et $R_n(v)$) les sommes partielles et restes d'ordre $n \in \mathbb{N}$ associés. Alors :

	$u_n = o(v_n)$	$u_n = O(v_n)$	$u_n \sim v_n$
$\sum_{n \in \mathbb{N}} v_n < +\infty$	$R_n(u) = o(R_n(v))$	$R_n(u) = O(R_n(v))$	$R_n(u) \sim R_n(v)$
$\sum_{n \in \mathbb{N}} v_n = +\infty$	$S_n(u) = o(S_n(v))$	$S_n(u) = O(S_n(v))$	$S_n(u) \sim S_n(v)$

Théorème 24. **[Comparaison série-intégrale]**
Soit $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ une fonction décroissante continue par morceaux.
Alors la série de terme général (positif) $\int_{n-1}^n f(t)dt - f(n)$ converge.
En particulier, $\sum f(k)$ et $(\int_0^n f(t)dt)_{n \in \mathbb{N}}$ ont même nature et on a :
- *si $\sum f(k)$ converge, alors $\int_{n+1}^\infty f(t)dt \leq \sum_{k \geq n} f(k) \leq \int_n^\infty f(t)dt$,*
- *si $\sum f(k)$ diverge, alors $\sum_{k \geq n} f(k) \sim \int_0^n f(t)dt$.*

Application 25. **[Séries de Bertrand]** Soient $\alpha, \beta \in \mathbb{R}$. Alors $\sum_{n \in \mathbb{N}} \frac{1}{n^\alpha \ln(n)^\beta} < +\infty$ si et seulement si $\alpha > 1$ ou $(\alpha = 1, \beta > 1)$.

Exemple 26. [Gou08, p.203] Développement asymptotique de la série harmonique (suite) à l'ordre 3 : $H_n = \ln n + \gamma + \frac{1}{2n} + o\left(\frac{1}{2n}\right)$.

Définition 27. **[Nombres et polynômes de Bernoulli]**
$z \longmapsto \frac{z}{e^z - 1}$ est développable en série entière sur un disque $\mathbb{D}_r(0)$ pour un $r > 0$.
- On note $(b_n)_{n \in \mathbb{N}}$ la suite telle que $\frac{z}{e^z - 1} = \sum_{n \geq 0} \frac{b_n}{n!} z^n$ sur ce disque.
- Il existe une suite de polynômes, notée $(B_n)_{n \in \mathbb{N}}$, telle que $\frac{z e^{xz}}{e^z - 1} = \sum_{n \geq 0} \frac{B_n(x)}{n!} z^n$ par produit de Cauchy.

Proposition 28. *Pour $n \in \mathbb{N}$ et $x \in \mathbb{C}$, on a :*
(i) $B_n(1 - x) = (-1)^n B_n(x)$,
(ii) $B'_{n+1} = (n+1) B_n$,
(iii) $B_n(x+1) - B_n(x) = n x^{n-1}$,
(iv) $B_n(0) = B_n(1) = b_n$ *pour* $n \geq 2$,
(v) $b_{2n+1} = 0$.

Théorème 29. [Formule d'Euler-Maclaurin] *[Gou08, §4.7, p301]*
Soient $m < n \in \mathbb{Z}$, $r \in \mathbb{N}^*$ et $f : [m,n] \longrightarrow \mathbb{C}$ une fonction de classe $\mathcal{C}^r$. Alors :

$$\sum_{k=m}^{n} f(k) = \int_m^n f(t)dt + \frac{1}{2}[f(m)+f(n)] + \sum_{\ell=2}^{r} \frac{b_\ell}{\ell!}[f^{(\ell-1)}(n) - f^{(\ell-1)}(m)] + R_r$$

où $R_r = \frac{(-1)^{r+1}}{r!}\int_m^n \tilde{B}_r(t) f^{(r)}(t)dt$ où $\tilde{B}_r(t) = B_r(t - \lfloor t \rfloor)$.

Application 30. [Série harmonique]
Soit $r \in \mathbb{N}^*$. On a $H_n = \ln n + \gamma + \frac{1}{2n} - \sum_{\ell=1}^{r-1} \frac{b_{2\ell}}{2\ell}\frac{1}{n^{2\ell}} + O\left(\frac{1}{n^{2r}}\right)$.

II. B. Suites récurrentes [FGN07, p99–103]

Théorème 31. [Théorème de Cesàro]
Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ telle que $a_n \underset{n\to+\infty}{\longrightarrow} \ell$. Alors $\frac{1}{n}\sum_{k=1}^{n} a_k \underset{n\to+\infty}{\longrightarrow} \ell$.

Application 32. Soit f une application continue définie au voisinage de 0^+ admettant un développement asymptotique en 0 de la forme $f(x) = x - ax^\alpha + o(x^\alpha)$, où $a > 0$ et $\alpha > 1$. Alors pour $u_0 > 0$ assez petit, la suite u définie par $u_{n+1} = f(u_n)$ pour $n \in \mathbb{N}$ vérifie $u_n \sim \frac{1}{(na(\alpha-1))^{\frac{1}{\alpha-1}}}$.
Exemples de $f = \sin$ et $f = \log(1+.)$.

Application 33. Soit $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 \in \mathbb{R}$ et, pour tout $n \in \mathbb{N}$, $u_{n+1} = u_n + \mathrm{e}^{-u_n}$. Alors on a le DA_2 suivant : $u_n = \ln n + \frac{\ln n}{2n} + o\left(\frac{\ln n}{n}\right)$.

II. C. Suites définies de manière implicite [FGN07, p127]

Les suites définies à partir d'une famille de polynômes sont fréquentes. On se ramène alors à l'étude de ses polynômes, sans forcément qu'il y ait de méthode générale.

Exemple 34. Soit a_n la plus grande racine réelle de $X^{2n} - 2nX + 1$.
Alors on a le DA_2 suivant : $a_n = 1 + \frac{\ln(2n)}{2n} + o\left(\frac{\ln n}{n}\right)$.

Exemple 35. Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels telle que, pour tout $n \in \mathbb{N}$, $u_n^5 + nu_n - 1 = 0$.
Alors on a le DA_2 suivant : $u_n = \frac{1}{n} - \frac{1}{n^6} + o\left(\frac{1}{n^6}\right)$.

III. Exemples de développements asymptotiques de fonctions

III. A. Fonctions définies par une intégrale [Gou08, §3.4, p159]

Théorème 36. [Intégration des relations de comparaison]
Soient $I = [a,b[$ un intervalle semi-ouvert de $\mathbb{R}$, $f : I \longrightarrow \mathbb{R}$ et $g : I \longrightarrow \mathbb{R}_+^*$ des applications continues par morceaux sur I. Alors lorsque $x \to b^-$, on a les mêmes résultats qu'au théorème 23, en remplaçant les sommes partielles par des intégrales entre a et x, et les restes par des intégrales entre x et b, et la condition de sommabilité de v par l'intégrabilité de g.

Exemple 37. [Utilisation de l'intégration par parties] [Gou08, p169]
Pour $x \geq 2$, on définit le logarithme intégral $Li(x) = \int_2^x \frac{dt}{\log t}$. Alors on a le $\mathrm{DA}_k(+\infty)$:

$$Li(x) = \frac{x}{\log x} + \frac{1!x}{\log^2 x} + \cdots + \frac{(k-1)!x}{\log^k x} + o\left(\frac{x}{\log^k x}\right)$$

Proposition 38. [Méthode de Laplace] *[Rou99, p322]*
Soient $[a,b]$ un intervalle de $\mathbb{R}$, $\varphi : [a,b] \longrightarrow \mathbb{R}$ de classe $\mathcal{C}^2$ et $f : [a,b] \longrightarrow \mathbb{C}$ telle que $\mathrm{e}^{-t_0\varphi} f$ soit intégrable pour un certain $t_0 \in \mathbb{R}$. On suppose que f est continue en a et $f(a) \neq 0$, et que $\varphi' > 0$ sur $]a,b[$, $\varphi'(a) = 0$ et $\varphi''(a) > 0$. Alors :

$$\int_a^b e^{-t\varphi(x)} f(x)dx \underset{t\to+\infty}{\sim} \sqrt{\frac{\pi}{2\varphi''(a)}}\frac{e^{-t\varphi(a)}f(a)}{\sqrt{t}}$$

Application 39. [Formule de Stirling] On a $\Gamma(t+1) \underset{t\to+\infty}{\sim} t^t e^{-t}\sqrt{2\pi t}$.

III. B. Fonctions définies par la somme d'une série [Gou08, p154/282]

Exemple 40. Soit $f : [0,+\infty[\longrightarrow \mathbb{R}$ une fonction $\mathcal{C}_{pm}$ et décroissante, telle que $\int_0^{+\infty} f(t)dt$ converge et est non nulle. Alors pour $t > 0$, $\sum_{n=1}^{+\infty} f(nt)$ converge et $\sum_{n=1}^{+\infty} f(nt) \underset{t\to0}{\sim} \frac{1}{t}\int_0^{+\infty} f(x)dx$.

Exemple 41. [Fonction Zeta]
Soit $\zeta : s \longmapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$. Alors $\zeta(s) \underset{s\to1^-}{=} \frac{1}{s-1} + \gamma + o(1)$ où γ est la constante d'Euler.

III. C. Fonctions définies comme solution d'une équation différentielle

ANNEXE

Développements limités usuels en 0

Soit $a \in \mathbb{R}$.

$$(1+x)^a = 1 + ax + \frac{a(a-1)}{2!}x^2 + \cdots + \frac{a(a-1)(a-2)...(a-n+1)}{n!}x^n + o(x^n)$$

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots + x^n + o(x^n)$$

$$\ln(1-x) = x - \frac{x^2}{2} - \frac{x^3}{3} - \cdots - \frac{x^n}{n} + o(x^n)$$

$$\mathrm{e}^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + o(x^n)$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots + (-1)^n \frac{x^{2n}}{(2n)!} + o(x^{2n+1})$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + o(x^{2n+2})$$

$$\cosh x = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots + \frac{x^{2n}}{(2n)!} + o(x^{2n+1})$$

$$\sinh x = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots + \frac{x^{2n+1}}{(2n+1)!} + o(x^{2n+2})$$

SPEECH

Les développements asymptotiques et développements limités sont des outils apparaissant dans presque tous les domaines des mathématiques. Ils permettent en effet de comprendre le comportement typique d'une fonction ou d'une suite en un point ou en l'infini, en les comparant à des fonctions usuelles telles les puissances de x combinées avec des puissances de $\ln$.
Première partie : introduction des notations $o, O, \sim$ qui sont très pratiques de par leur stabilité et la malléabilité de l'écriture. On notera toutefois qu'il faut faire attention avec les équivalents.
On introduit d'abord les développements limités parce que dans un cours de sup, il vaut mieux considérer d'abord ce cas qui est plus simple et évite des notations lourdes que les étudiants auraient du mal à assimiler. On étend ensuite cela aux développements asymptotiques qui la plupart du temps utilisent les familles de l'exemple.
Dans la suite, les développements asymptotiques étant avant tout des outils, on doit surtout les illustrer par une multitude d'exemples, les plus variés possibles. Dans un premier temps, on étudie les exemples de développements asymptotiques de suites. Les suites auxquelles on s'intéresse sont celles que l'on retrouve fréquemment comme les séries, les suites numériques ou encore les suites définies à partir de polynômes.
Enfin les développements asymptotiques de fonctions sont aussi fréquents. Là encore on s'intéresse à des fonctions définies de manières classiques : intégrales à paramètres, séries de fonctions, ou encore solutions d'équations différentielles.

COMMENTAIRES

Il faut s'entrainer pour être à l'aise avec toutes les méthodes ... Leçon avec des outils de niveau prépa mais qui peut être rapidement compliquée.

QUESTIONS

- Q Trouver un DA de la série des $1/k^2$ (en utilisant la formule d'Euler-Maclaurin).
- Q Trouver le $\mathrm{DA}_3(0)$ de $\arcsin$.
- Q On pose $P_n = X^n + X^{n-1} + 2X - 1$. Montrer qu'il existe un unique $x_n > 0$ tel que $P_n(x_n) = 0$. Montrer que $(x_n)_{n\in\mathbb{N}}$ est croissante et converge vers 1. [FGN07, p127]

BIBLIOGRAPHIE

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

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. Généralités sur les suites récurrentes

I. A. Suites récurrentes réelles

[Gou08, Ch4, p191]

Définition à tout ordre, on se place dans le cadre ordre 1 (en fait en utilisant un cadre matriciel on pourra toujours se ramener à ce cas-là)
Exemples des suites arithmétiques, géométriques, homographiques
Propriétés de monotonie lorsque f est croissante/décroissante sur des intervalles stables
Lemme de la grenouille [FGN07, §2.19, p86]

I. B. Suites récurrentes vectorielles

Permet notamment de se ramener à un ordre 1
Équation caractéristique
Application à la résolution d'une suite récurrente linéaire d'ordre p.
Exemple de la suite de FIBONACCI

II. Points fixes et suites récurrentes

II. A. Théorèmes de points fixes

[Dem96, ChIV, p93] [Rou99] [Gou08, §1.2, p21–23]

Définition d'un point fixe, toute suite récurrence convergente converge vers un point fixe de f
Exemples d'existence de points fixes (théorème des valeurs intermédiaires) : $f : [0,1] \longrightarrow [0,1]$ continue, $f : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ telle que $\limsup_{x\to+\infty} f(x)/x < 1$.
Théorème du point fixe de PICARD, corollaire avec une itérée
Exemple/contre-exemple
Vitesses de convergence en fonction de la dérivée, point fixe attractif, répulsif (schémas), exemple du sinus itéré

II. B. Applications en probabilités

[BL07, ChVIII, p193]

Noyau de transition, chaînes de MARKOV, mesure invariante, existence, cas de non unicité ...
Existence dans le cas E fini, convergence sous conditions vers la mesure invariante

PROPOSITION 1. [PROCESSUS DE BRANCHEMENT DE GALTON-WATSON]
Soient $(X_i^j)_{i,j\geq 1}$ des v.a. i.i.d. à valeurs dans $\mathbb{N}$. On note μ leur loi, m leur espérance et 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 $n \in \mathbb{N}$. et enfin $\rho = \mathbb{P}(\exists n \geq 0 \mid Z_n = 0)$. Alors si $\mu \neq \delta_1$, on a :
- *si $m \leq 1$, $\rho = 1$ et on a extinction du processus presque surement,*
- *si $m > 1$, $\rho < 1$ et il y a une probabilité strictement positive de survie.*

III. Application à la résolution d'équations par des méthodes itératives

III. A. Méthode de NEWTON

[Dem96, ChIV, p93] [Rou99]

THÉORÈME 2.
Soit $f : [c,d] \longrightarrow \mathbb{R}$ une fonction $\mathcal{C}^2$, où $c < d$, et telle que $f(c) < 0 < f(d)$ et $f' > 0$ sur $[c,d]$. On considère la suite récurrente définie par $x_0 \in [c,d]$ et $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ pour $n \in \mathbb{N}$.
Alors en notant a l'unique 0 de f, on a :
(i) il existe $\alpha > 0$ tel que pour tout $x_0 \in [a-\alpha, a+\alpha]$, $(x_n)_{n\in\mathbb{N}}$ converge vers a de manière quadratique : il existe $C > 0$ telle que $\forall n \in \mathbb{N}, |x_{n+1} - a| \leq C|x_n - a|^2$.
(ii) si de plus $f'' > 0$ sur $[a,d]$, alors pour tout $x_0 \in]a,d]$, $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante et $x_{n+1} - a \sim_{n\to+\infty} \frac{f''(a)}{2f'(a)}(x_n - a)^2$.

Et en dimension quelconque

III. B. Méthodes de descente de gradient

[FGN12, §, p39]

Méthodes de descente de gradient
Gradient à pas optimal

III. C. Résolution de systèmes linéaires

[AK02, PIV, p153]

Idée : décomposition régulière $A = M - N$ avec M facile à inverser
On définit $x_0 \in \mathbb{K}^n$ et $x_{n+1} = M^{-1}(Nx_n + b)$. Si cette suite converge, la limite est la solution de $Ax = b$
Théorème : la méthode itérative converge pour tout x_0 si et seulement si $\rho(M^{-1}N) < 1$. Dans ce cas, vitesse de convergence est géométrique
Exemple : méthode de RICHARDSON
Pour une matrice A hermitienne définie positive, si M, N est une décomposition satisfaisante, on a $M^* + N$ est hermitienne et si elle est définie positive, alors $\rho(M^{-1}N) < 1$
Méthode de JACOBI : on prend pour D la diagonale de A. On a $M^{-1}N = I_n - D^{-1}A$ (on peut supposer D inversible quitte à permuter les colonnes de A)
Si A est hermitienne, on a convergence si A et $2D - A$ sont définies positives
Méthode de GAUSS-SEIDEL : on prend pour M la matrice triangulaire inférieure issue de A, et pour N l'opposé des coefficients restants. Si A est hermitienne définie positive, on a la conveergence de la méthode car $M^* + N$ l'est aussi
Remarque : les itérations correspondent à un calcul matriciel, on a donc n^2 opérations. Les

inversions de M nécessitent n opérations pour JACOBI, $n^2/2$ pour GAUSS-SEIDEL, donc pour un nombre d'itération $\ll n$, ces méthodes sont plus rapides que les méthodes directes

III. D. Recherche de valeurs propres

[AK02, Ch15, p215]

Méthode de la puissance pour trouver la plus grande valeur propre en module, ainsi qu'un vecteur propre, vitesse géométrique
Matrices de GIVENS, méthode de JACOBI : $A_k \underset{k\to+\infty}{\longrightarrow} \operatorname{diag}(\lambda_{\sigma(i)})$ pour un $\sigma \in \mathfrak{S}_n$

ANNEXE

Suites du sinus itéré
Méthode de NEWTON en dimension 1
Points fixes attractifs/répulsifs, selon la valeur de $|f'|$ et le signe de f'

COMMENTAIRES

Une leçon facile à remplir, il faut sélectionner ce sur quoi on est à l'aise.

QUESTIONS

Q Étudier la suite définie par récurrence par $x_{n+1} = \sin(x_n)$. Donner un équivalent.

R $x_n \in [-1, 1]$ pour $n \geq 1$ et si $f = \sin$, on a que f est croissante sur cet intervalle donc la suite est monotone et converge vers un point fixe de f sur cet intervalle. Cela ne peut être que 0. Donc $x_n \underset{n\to+\infty}{\longrightarrow} 0$.

En utilisant le DL_3 de $\sin$, on a que $x_{n+1} - x_n \sim -\frac{x_n^3}{6}$.
On étudie $x_{n+1}^\beta - x_n^\beta$ qui converge vers la limite finie $\frac{1}{3}$ pour $\beta = -2$.
On a donc par le théorème de CESÀRO que $x_n^{-2} \sim n/3$ et ainsi $x_n \sim \sqrt{\frac{3}{n}}$.

Q Si f est continue de $[0, 1]$ dans $[0, 1]$ et $x_{n+1} = f(x_n)$, montrer que $(x_n)_n$ converge si et seulement si $|x_{n+1} - x_n| \underset{n\to+\infty}{\longrightarrow} 0$ (lemme de la grenouille).

R Le sens direct est évident. Réciproquement, supposons que $(x_n)_n$ possède deux valeurs d'adhérence distinctes ℓ, ℓ', alors on a que $[\ell, \ell']$ est un ensemble de valeurs d'adhérences par hypothèse (faire un dessin). L'ensemble des valeurs d'adhérence est donc connexe. Vérifions qu'une valeur d'adhérence est un point fixe. Si $x_{\varphi(n)} \longrightarrow \ell$, alors $f(x_{\varphi(n)}) \longrightarrow f(\ell)$ et par hypothèse on en déduit que $f(\ell) = \ell$. Comme on a un segment de valeurs d'adhérences, donc de points fixes, on a que dès qu'un des termes est dans le segment, la suite est constante. Ce qui contredit le fait que l'on ait deux valeurs d'adhérence. Donc il y a une unique valeur d'adhérence et la suite converge.

Q Considérons $\varphi : (a, b) \longmapsto (\frac{a+b}{2}, \sqrt{ab})$. Montrer $(a_n)_n$ et $(b_n)_n$ ont même limite. Montrer que la convergence de $(a_n - b_n)_n$ vers 0 est géométrique.

R On a que $a_n, b_n \in [\min(a_0, b_0), \max(a_0, b_0)]$ pour tout n. On vérifie par récurrence que $(a_n)_n$ est décroissante et $(b_n)_n$ est croissante et de plus $a_n \geq b_n$. Les deux suites sont donc convergentes. Si elles convergent vers ℓ_1, ℓ_2, alors on a $(\ell_1, \ell_2) = (\frac{\ell_1+\ell_2}{2}, \sqrt{\ell_1\ell_2})$, ce qui n'est possible que si $\ell_1 = \ell_2$.

Q Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ de classe $\mathcal{C}^2$ telle que $\beta \|h\|^2 \geq \nabla^2 f(x)(h, h) \geq \alpha \|h\|^2$. Montrer que f a un unique minimiseur et donner un algorithme convergeant vers ce minimiseur.

R Utiliser la formule de TAYLOR avec reste intégral. Une méthode à descente de gradient convient.

BIBLIOGRAPHIE

[AK02] G. ALLAIRE et S.-M. KABER : *Algèbre linéaire numérique*. Ellipses, 2002.

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[Dem96] J.-P. DEMAILLY : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[FGN12] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

228 CONTINUITÉ ET DÉRIVABILITÉ DES FONCTIONS RÉELLES D'UNE VARIABLE RÉELLE. EXEMPLES ET APPLICATIONS.

Soit I un intervalle de $\mathbb{R}$ et $f : I \longrightarrow \mathbb{R}$ une application.

I. Généralités autour de la continuité et de la dérivabilité
[Gou08, §2.1, p69]

I. A. Définitions et exemples
[Gou08, §1.1/2.3, p12/94]

Continuité, dérivabilité, exemple de fonctions continue, dérivable, continue non dérivable (valeur absolue), de dérivée non continue ($x \longmapsto x^2 \sin(1/x)$)
Dérivabilité implique continuité
Lien avec les développements limités
Fonctions lipschitziennes, notion d'uniforme continuité
Fonctions convexes

I. B. Propriétés de stabilité et dérivations successives

Stabilité par composition, somme, produit, formules de la dérivée associée ...
Dérivée de la fonction réciproque lorsque f' ne s'annule pas ...
Formule de Leibniz

II. Résultats autour de la continuité et de la dérivabilité
[Gou08, §2.1, p69]

II. A. Théorème des valeurs intermédiaires
[Gou08, §1.3/1.4, p31/41]

TVI, applications basiques : il existe un zéros entre a et b si $f(a)f(b) < 0$, un polynôme de degré impair admet une racine
Une fonction continue sur un intervalle compact $[a, b]$ est bornée et atteint ses bornes
Cas d'une fonction continue coercive sur $\mathbb{R}$

II. B. Théorème de Heine
[Gou08, §1.3, p31]

Théorème de Heine.
Exemples : fonctions continues périodiques, ou continues avec une limite finie en $\pm\infty$, deuxième théorème de Dini

II. C. Théorème de Rolle et accroissement finis

Théorème de Rolle, inégalité des accroissements finis, règle de l'Hospital

II. D. Densité des polynômes
[QZ13, §XIII.II.1, p518–519]

Théorème 1. [Théorème de Weierstrass]
$\mathbb{R}[X]$ est dense dans $\mathcal{C}([a, b], \mathbb{C}, \|.\|_\infty)$ pour $a < b \in \mathbb{R}$.

Cas où $I = \mathbb{R}$: cela ne fonctionne plus
Si $\int_a^b f(x)x^n dx = 0$ pour tout n alors $f = 0$ si f est continue
Plus généralement théorème de Stone-Weierstrass $\rightarrow$ densité des polynômes trigonométriques

II. E. Formules de Taylor
[Rou99, Ch6, p278]

Formule de Taylor avec reste intégral, formule de Taylor-Young
Formule de Taylor pour un polynôme ...
Application : méthode de Newton

III. Théorèmes de passage à la limite

III. A. Suites de fonctions
[AF91, El 11]

Soient $(f_n)_{n\in\mathbb{N}}$ et f des fonctions de I dans $\mathbb{R}$.
Prolongement par continuité de f.

Exemple 2. [Hau07, p235] Pour $f_n : x \in [0, 1] \longmapsto x^n$, on a $\lim_{n\to+\infty} \lim_{x\to1^-} f_n(x) = 1 \neq 0 = \lim_{x\to1^-} \lim_{n\to+\infty} f_n(x)$.

Théorème 3. *Soit $a \in \overline{I}$ tel que $f_n(x) \underset{x\to a}{\longrightarrow} \ell_n \in \mathbb{R}$ et $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ sur un voisinage de a. Alors $\lim_{n\to+\infty} \ell_n$ et $\lim_{x\to a} f(x)$ existent et sont égales. Autrement dit :*

$$\lim_{n\to+\infty} \lim_{x\to a} f_n(x) = \lim_{x\to a} \lim_{n\to+\infty} f_n(x)$$

Théorème 4. *Dans le même contexte, si les $(f_n)_{n\in\mathbb{N}}$ sont continues en a et si $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ sur un voisinage de a, alors f est continue en a.*

Exemple 5. $\zeta : x > 1 \longrightarrow \sum_{n\geq1} \frac{1}{n^x}$ est continue et $\zeta(x) \underset{x\to+\infty}{\longrightarrow} 1$.

Application 6. Une série entière de rayon de convergence $R > 0$ est continue sur $\mathbb{D}_R(O)$.

REMARQUE 7. On ne peut rien dire sur le cercle de convergence : par exemple avec $\sum_{n\geq 0}(-1)^n z^n = \frac{1}{1+z}$ définie pour $|z|<1$, on a $\frac{1}{1+z} \underset{z\to 1}{\longrightarrow} 1/2$ mais $\sum(-1)^n$ diverge.

PROPOSITION 8. *Soit I un intervalle de $\mathbb{R}$, on suppose les $(f_n)_{n\in\mathbb{N}}$ dans $\mathcal{C}^1(I,\mathbb{R})$ telles que $f_n' \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g$ et $f_n \underset{n\to+\infty}{\overset{s}{\longrightarrow}} f$. Alors $f\in\mathcal{C}^1(I,\mathbb{R})$, $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ et $f'=g$.*

COROLLAIRE 9. *Si les $(f_n)_{n\in\mathbb{N}}$ sont $\mathcal{C}^k([a,b],\mathbb{R})$ et telles que $f_n^{(p)} \underset{n\to+\infty}{\overset{s}{\longrightarrow}} g_p$ pour $p\leq k$ avec $f_n^{(k)} \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g_k$, alors $g_0\in\mathcal{C}^k([a,b],\mathbb{R})$, $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g_0$ et $g_0^{(p)}=g_p$ pour $p\leq k$.*

EXEMPLE 10. Soit $f_u : t\longmapsto \exp(tu)$ $(u\in\mathbb{R})$. Alors f_u est $\mathcal{C}^\infty$ et $f_u^{(p)} : t\longmapsto \sum_{n\in\mathbb{N}} \frac{t^{n-p}}{(n-p)!}u^n$.

EXEMPLE 11. [Hau07, p241] Importance de la convergence uniforme de $(f_n')_{n\in\mathbb{N}}$: considérer $f_n(x)=\sqrt{x^2+1/n}$.

III. B. Intégrales dépendant d'un paramètre

[BP15, §8.3, p140–147] [Far00, §VII.2, p98]

Soit $(E,\mathcal{A},\mu)$ un espace mesuré.

THÉORÈME 12. [CONTINUITÉ SOUS LE SIGNE INTÉGRALE]
Soient I un intervalle de $\mathbb{R}$ et $f : I\times E\longrightarrow\mathbb{K}$ telles que :
- *pour tout $t\in I$, $x\longmapsto f(t,x)$ est mesurable,*
- *pour μ-presque tout x, $t\longmapsto f(t,x)$ est continue en $t_0\in I$,*
- *il existe g intégrable telle que pour tout $t\in I$, $|f(t,x)|\leq g(x)$ μ- p.p..*

Alors $t\longmapsto\int_E f(t,x)d\mu(x)$ est bien définie sur I et est continue en t_0.

APPLICATION 13. La fonction Γ est continue sur $\mathbb{R}_+^*$.

THÉORÈME 14. [DÉRIVATION SOUS LE SIGNE INTÉGRALE]
Soient I un intervalle de $\mathbb{R}$ et $f : I\times E\longrightarrow\mathbb{K}$ telles que :
- *pour tout $t\in I$, $x\longmapsto f(t,x)$ est intégrable sur E,*
- *pour μ-presque tout x, $t\longmapsto f(t,x)$ est dérivable sur I,*
- *il existe g intégrable telle que pour tout $t\in I$, $\left|\frac{\partial f}{\partial t}(t,x)\right|\leq g(x)$ μ- p.p..*

Alors $F : t\longmapsto\int_E f(t,x)d\mu(x)$ est définie, dérivable sur I et $F' : t\longmapsto\int_E \frac{\partial f}{\partial t}(t,x)d\mu(x)$.

APPLICATION 15. Prenant $f : (t,x)\longmapsto \frac{\sin(x)}{x}\,\mathrm{e}^{-tx}$, on montre que $\int_0^{+\infty}\frac{\sin(x)}{x}dx=\frac{\pi}{2}$.

COMMENTAIRES

Faire un dessin de la continuité et de la dérivabilité lors du speech.
La difficulté de la leçon est d'aller plus loin que le programme du lycée voire de sup. C'est une leçon vague qui peut aller jusqu'aux distributions si on est à l'aise dessus. Le plan continuité puis dérivabilité n'est pas forcément le plus palpitant : plutôt essayer de trouver des liens, faire un plan par thèmes.
Il est important de mettre beaucoup d'exemples et de contre-exemples.
On peut également parler du théorème de DINI, du théorème fondamental de l'analyse (avec la formule de TAYLOR avec reste intégral !) ou du théorème d'ASCOLI.

QUESTIONS

Q Continuité au sens de CESÀRO : que peut-on dire de f telle que pour toute suite $(x_n)_n$ telle que $x_n \underset{n\to+\infty}{\longrightarrow} x$ au sens de CESÀRO, alors $f(x_n) \underset{n\to+\infty}{\longrightarrow} f(x)$ au sens de CESÀRO ?

R On montre qu'une telle application conserve les barycentres …

BIBLIOGRAPHIE

[AF91] J.M. ARNAUDIÈS et H. FRAYSSE : *Cours de mathématiques, Tome 2, Analyse*. Dunod, 1991.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[El 11] M. EL AMRANI : *Suites et séries numériques, suites et séries de fonctions*. Ellipses, 2011.

[Far00] J. FARAUT : *Calcul intégral*. Belin, 2000.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Hau07] D. HAUCHECORNE : *Les contre-exemples en Mathématiques*. Ellipses, 2ème édition, 2007.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

229 FONCTIONS MONOTONES. FONCTIONS CONVEXES. EXEMPLES ET APPLICATIONS.

I. Fonctions monotones

I. A. Généralités

[RDO98, §4.3, p118] [Gou08, §4.3, p228]

Fonction monotone, exemples et contre-exemples
Caractérisation avec la dérivée
Exemples : fonction de répartition d'une variable aléatoire réelle, monotonie d'une homographie
Stabilités par somme, produit
Existence d'une limite à gauche, à droite
Ensemble des points de discontinuité est au plus dénombrable
Théorème de Dini

I. B. Fonctions à variation bornées

[RDO98, §4.3, p114] [Gou08, §2.4, p114]

II. Fonctions convexes

[Gou08, §1.5/2.3, p51/94] [BMP05, §1.5.1, p26]

II. A. Généralités

Définition 1. $A \subset E$ est convexe si $\forall a, b \in A, \forall t \in [0,1], (1-t)a + tb \in A$.

Exemple 2. Un intervalle de $\mathbb{R}$ est convexe, une boule de E est convexe.

Définition 3. $f : E \longrightarrow \mathbb{R}$ est dite
- convexe si $\forall a, b \in E, \forall t \in]0,1[, f((1-t)a+tb) \leq (1-t)f(a) + tf(b)$,
- strictement convexe si $\forall a, b \in E, \forall t \in]0,1[, f((1-t)a+tb) < (1-t)f(a) + tf(b)$,
- concave si $-f$ est convexe.

Exemple 4. Une application affine est convexe et concave.

Exemple 5. Toute norme $\|.\|$ de E est convexe, non strictement convexe dès que $E \neq \{0\}$.

Proposition 6. *$f : E \longrightarrow \mathbb{R}$ est convexe si et seulement si*
- *$E_f = \{(x,y) \in \mathbb{R}^2 \mid f(x) \leq y\}$ est convexe,*
- *$\forall n \in \mathbb{N}^*, \forall (a_1, \dots, a_n) \in E^n, \forall (t_1, \dots, t_n) \in (\mathbb{R}_+)^n \setminus \{0_{\mathbb{R}^n}\}, f(\mathrm{Bar}((a_i, t_i)_i)) \leq \mathrm{Bar}((f(a_i), t_i)_i))$.*

II. B. Liens entre convexité et monotonie

Proposition 7. *Soit $f : I \longrightarrow \mathbb{R}$ où I est un intervalle de $\mathbb{R}$. f est convexe si et seulement si :*
- *pour tout $a \in I$, $x \longmapsto \frac{f(x)-f(a)}{x-a}$ est croissante sur $I \setminus \{a\}$,*
- *pour tout $a, x \in I$, $f'(a)(x-a) + f(a) \leq f(x)$,*
- *f' est croissante,*
- *$f'' \geq 0$.*

les trois dernières équivalences ayant lieu lorsque f est assez régulière ($\mathcal{C}^1$ ou $\mathcal{C}^2$).
On déduit de la première équivalence qu'une fonction convexe sur I est continue sur I° et admet une dérivée à droite et à gauche en tout point de I°.

Exemple 8. $\exp$ est convexe, $\log$ est concave. Fonction convexe non continue : voir annexe.

III. Applications

III. A. Inégalités de convexité

[Gou08, §1.5/2.3, p51/94] [BMP05, §1.5.1, p26]

Exemple 9. On a des inégalités provenant de la convexité/concavité de certaines fonctions :

$$\forall x \in \mathbb{R}, \mathrm{e}^x \geq 1 + x \qquad \forall y \in]-1, +\infty[, \ln(1+y) \leq y \qquad \forall \theta \in \left[0, \frac{\pi}{2}\right], \frac{2}{\pi}\theta \leq \sin(\theta) \leq \theta$$

Proposition 10. **[Inégalité arithmético-géométrique]** *Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{R}_+$. Alors $\sqrt[n]{a_1 \dots a_n} \leq \frac{1}{n}\sum_{i=1}^n a_i$.*

Exemple 11. On peut généraliser pour toute famille $a_1, \dots, a_n \in \mathbb{R}_+$ et $b_1, \dots, b_n \in \mathbb{R}_+^*$, on a

$$(a_1^{b_1} \dots a_n^{b_n})^{1/b} \leq \frac{1}{b}\sum_{i=1}^n b_i a_i \qquad \text{où} \quad b = \sum_{i=1}^n b_i$$

Proposition 12. **[Inégalité de Young]** *Soient $p, q > 0$ tels que $\frac{1}{p} + \frac{1}{q} = 1$. Alors pour tout $a, b \in \mathbb{R}_+$, on a $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$ avec égalité si et seulement si $a^p = b^q$.*

Application 13. **[Inégalités de Hölder et de Minkowski]**
Soit $(E, \mathcal{A}, \mu)$ un espace mesuré. Soit $p \in [1, +\infty]$ et q sont exposant conjugué. Pour toutes fonctions $f, g : E \longrightarrow \mathbb{K}$ mesurables, on a $\|fg\|_1 \leq \|f\|_p \|g\|_q$, puis $\|f+g\|_p \leq \|f\|_p + \|g\|_p$.

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé. Soit X une variable aléatoire.

Proposition 14. [Inégalité de Jensen]
Si $X \in L^1$ et ϕ est convexe, alors $\phi(\mathbb{E}[X]) \leq \mathbb{E}[\phi(X)]$. De plus, si ϕ est strictement convexe, on a égalité si et seulement si X est constante presque sûrement.

Application 15. Soit $X_1, \dots, X_n$ des v.a. i.i.d. de loi $\mathcal{E}(\theta)$ pour un paramètre $\theta > 0$ inconnu. Alors $\overline{X}_n = \frac{1}{n}\sum_{i=1}^n X_i$ est un estimateur sans biais fortement convergeant de $\mathbb{E}[\mathcal{E}(\theta)] = \frac{1}{\theta}$. Alors $\frac{1}{\overline{X}_n}$ est un estimateur fortement convergeant avec biais de θ.

Proposition 16. [Inégalité de Hoeffding]
Soient $(X_i)_{1\leq i\leq n}$ des variables aléatoires indépendantes telles que pour tout i, $X_i \in [a_i, b_i]$ p.s. pour des réels $a_i \leq b_i$. Alors pour tout $t \geq 0$:

$$\mathbb{P}(|\sum_{i=1}^n X_i - \mathbb{E}[X_i]| \geq t) \leq 2\exp(-2t^2/\sum_{i=1}^n (b_i - a_i)^2)$$

Application 17. Soient $(X_i)_{1\leq i\leq n}$ des variables aléatoires indépendantes et identiquement distribuées de Rademacher centrées, c'est-à-dire $\mathbb{P}(X_1 = 1) = \mathbb{P}(X_1 = -1) = 1/2$. Alors :

$$\forall t > 0, \mathbb{P}(|\sum_{i=1}^n X_i| \geq t) \leq 2\exp(-\tfrac{t^2}{2n})\mathbb{1}_{t\leq n}$$

III. B. Étude de suites récurrentes

[El 11, §1.5/2.2, p38/91] [Ouv09, p162/508]

Suite récurrente : selon la monotonie, le signe de $u_{n+1}u_n$ est soit constant soit alterné
Comparaison série-intégrale. Application : série harmonique

Définition 18. [Fonction génératrice, fonction caractéristique]
Soit X une variable aléatoire à valeurs dans $\mathbb{N}$ presque sûrement. On définit g_X la fonction génératrice de X par $g_X(s) = \mathbb{E}[s^X] = \sum_{k\geq 0}\mathbb{P}(X = k)s^k$ (lorsque la série converge).

Proposition 19. *g_X est bien définie, croissante et convexe sur $[0, 1]$. Si de plus $P(X = k) > 0$ pour au moins un $k \geq 2$, alors g_X est strictement convexe sur $[0, 1]$.*

Proposition 20. [Processus de branchement de Galton-Watson]
Soient $(X_i^j)_{i,j\geq 1}$ des v.a. i.i.d. à valeurs dans $\mathbb{N}$. On note μ leur loi, m leur espérance et 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 $n \in \mathbb{N}$. et enfin $\rho = \mathbb{P}(\exists n \geq 0 \mid Z_n = 0)$. Alors si $\mu \neq \delta_1$, on a :
- *si $m \leq 1$, $\rho = 1$ et on a extinction du processus presque surement,*
- *si $m > 1$, $\rho < 1$ et il y a une probabilité strictement positive de survie.*

IV. Convexité et optimisation

[Rou99, Ch4, p140] [FGN07, §4.51, p287] [FGN12, §4.51, p39–41]

On a la même définition de la convexité pour une fonction f définie sur un convexe de $\mathbb{R}^p$.

Proposition 21. *Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$.*
- *Si f est différentiable, f est convexe (resp. strictement convexe) si et seulement si pour tout $x \neq y \in \mathbb{R}^p$, $f(y) - f(x) \geq \langle \nabla f(x) \mid y - x\rangle$ (resp. $f(y) - f(x) > \langle \nabla f(x) \mid y - x\rangle$,*
- *Si f est $\mathcal{C}^2$, f est convexe (resp. strictement convexe) si et seulement si $\nabla^2 f(x)$ est positive (resp. définie positive) pour tout $x \in \mathbb{R}^p$.*

Exemple 22. Soit $A \in \mathcal{S}_n(\mathbb{R})$, $b \in \mathbb{R}^n$, $c \in \mathbb{R}$ et $f : x \longmapsto \frac{1}{2}\langle Ax \mid x\rangle - \langle b \mid x\rangle + c$.
Si A est positive (resp. définie positive), f est convexe (resp. strictement convexe). Ainsi par exemple si $(E, \langle . \mid . \rangle)$ est euclidien, l'application $x \longmapsto \|x\|^2$ est strictement convexe.

Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$ une fonction convexe.

Proposition 23. *Soit C un convexe de $\mathbb{R}^p$ et $M = \{x \in C \mid f(x) = \inf_C f\}$ l'ensemble des minimums globaux de f sur C.*
On suppose qu'il existe un minimum local $x_\star$ de f sur C. Alors :
- *M est un ensemble convexe et $x_\star \in M$ est un minimum global,*
- *si de plus f est strictement convexe, alors $M = \{x_\star\}$.*

Théorème 24. [Méthode de Newton]
Soit $f : [c, d] \longrightarrow \mathbb{R}$ une fonction $\mathcal{C}^2$, où $c < d$, et telle que $f(c) < 0 < f(d)$ et $f' > 0$ sur $[c, d]$. On considère la suite récurrente définie par $x_0 \in [c, d]$ et $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ pour $n \in \mathbb{N}$.
Alors en notant a l'unique 0 de f, on a :
(i) il existe $\alpha > 0$ tel que pour tout $x_0 \in [a - \alpha, a + \alpha]$, $(x_n)_{n\in\mathbb{N}}$ converge vers a de manière quadratique et il existe $C > 0$ telle que $\forall n \in \mathbb{N}, |x_{n+1} - a| \leq C|x_n - a|^2$.
(ii) si de plus $f'' > 0$ (f est strictement convexe) sur $[a, d]$, alors pour tout $x_0 \in]a, d]$, $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante et $x_{n+1} - a \sim_{n\to+\infty} \frac{f''(a)}{2f'(a)}(x_n - a)^2$.

Application 25. Approximation des zéros d'un polynôme.

Théorème 26. [Méthode de gradient à pas optimal]
Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$ elliptique, c'est-à-dire f est $\mathcal{C}^1$ et telle qu'il existe $\alpha > 0$ satisfaisant

$$\forall x, y \in \mathbb{R}^p, \langle \nabla f(x) - \nabla f(y) \mid x - y \rangle \geq \alpha \|x - y\|^2$$

On définit $(x_n)_{n\in\mathbb{N}}$ par $x_0 \in \mathbb{R}^p$ et $x_{n+1} = x_n - \rho_n \nabla f(x_n)$ où $\rho_n = \operatorname{argmin}_{\rho>0} f(x_n - \rho \nabla f(x_n))$. Alors $(x_n)_{n\in\mathbb{N}}$ converge vers l'unique minimum global de f.

Application 27. Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. L'application $f : x \longmapsto \frac{1}{2}\langle Ax \mid x\rangle - \langle b \mid x\rangle$ admet un unique minimum $\overline{x}$ caractérisé par $\nabla f(\overline{x}) = A\overline{x} - b = 0$. On converge vers cette solution par l'algorithme de gradient à pas optimal.

COMMENTAIRES

Le plan est un peu facile ici, il serait mieux d'essayer de mettre en parallèle les deux notions. Le théorème de Dini est important car en utilisant la monotonie, il permet de remplacer une hypothèse pas toujours facile à montrer dans le cas général.

QUESTIONS

Q Soit $g : \mathbb{R} \longrightarrow \mathbb{R}$ continue telle que $g^2 = 2g - \mathrm{id}$. Montrer que g est bijective.

R Si $g(x) = g(y)$, l'égalité fonctionnelle donne $x = y$, donc g est injective.
g est injective donc strictement monotone, donc bijective ...

Q Que dire d'une fonction convexe sur $\mathbb{R}$ (resp. sur $\mathbb{R}^+$) et majorée ?

R Elle est constante (resp. converge vers une limite $\ell \in]-\infty, +\infty]$).

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[El 11] M. El Amrani : *Suites et séries numériques, suites et séries de fonctions*. Ellipses, 2011.

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[FGN12] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Ouv09] J.-Y. Ouvrard : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[RDO98] E. Ramis, C. Deschamps et J. Odoux : *Cours de mathématiques 3, Topologie et éléments d'analyse*. Dunod, 1998.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

230 SÉRIES DE NOMBRES RÉELS OU COMPLEXES. COMPORTEMENT DES RESTES OU DES SOMMES PARTIELLES DES SÉRIES NUMÉRIQUES. EXEMPLES.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $u = (u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$ et $v = (v_n)_{n\in\mathbb{N}} \in (\mathbb{R}_+)^{\mathbb{N}}$.

I. Généralités sur les séries

[Gou08, §4.2, p200–202/219]

Définition 1. [Série, reste, convergence]
- On appelle série de terme général u_n la suite $(S_n)_{n\in\mathbb{N}}$ définie par $S_n = \sum_{k=0}^{n} u_k$.
  On note $\sum u_k$ la série $(S_n)_{n\in\mathbb{N}}$ de sorte que $(\sum u_k)_n = \sum_{k=0}^{n} u_k$.
  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.
- On dit que $\sum u_k$ converge lorsque $(S_n)_{n\in\mathbb{N}}$ converge. Dans ce cas, sa limite est appelée somme de la série et notée $\sum_{n=0}^{\infty} u_n$ ou $\sum_{n\in\mathbb{N}} u_n$ ou $\sum_{n\geq 0} u_n \dots$
- Une série non convergente est dite divergente.

Exemple 2. [Séries arithmétique et géométrique]
- Si $u_n = na$, la série converge si et seulement si $a = 0$.
- Si $u_n = b^n$, la série converge si et seulement si $|b| < 1$ et dans ce cas, $\sum_{n\in\mathbb{N}} b^n = \frac{1}{1-b}$.

Proposition 3. [Critère de Cauchy]
$\sum u_k$ converge si et seulement si $\forall \varepsilon > 0, \exists N \in \mathbb{N} \,|\, \forall m > n \geq N, |\sum_{k=n}^{m} u_k| \leq \varepsilon$.

Exemple 4. Étude des séries de termes généraux $\frac{1}{n\sigma(n)}$ et $\frac{\sigma(n)}{n}$ pour σ permutation de $\mathbb{N}^*$.

Remarque 5. $\sum u_k$ converge $\iff R_n \underset{n\to+\infty}{\longrightarrow} 0$ et $\sum u_k$ converge $\implies |u_n| \underset{n\to+\infty}{\longrightarrow} 0$

II. Séries de termes réels positifs

[Gou08, §4.2, p201–206]

On suppose $(u_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{R}_+$ dans cette partie.

II. A. Critères de convergence et divergence

Proposition 6. *La convergence de la série $\sum u_k$ équivaut au fait que $(S_n)_{n\in\mathbb{N}}$ soit majorée.*

On notera donc $\sum_{n\in\mathbb{N}} u_n < +\infty$ pour dire que $\sum u_k$ converge, et $\sum_{n\in\mathbb{N}} u_n = +\infty$ sinon.

Lemme 7. *Si u_n est le terme général d'une série convergente, alors $\sum u_k + v_k$ et $\sum v_k$ ont même nature et si elles convergent, on a $\sum_{n\in\mathbb{N}} u_n + v_n = \sum_{n\in\mathbb{N}} u_n + \sum_{n\in\mathbb{N}} v_n$.*

Théorème 8. [Comparaison série-intégrale]
Soit $f : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ une fonction décroissante continue par morceaux.
Alors la série de terme général (positif) $\int_{n-1}^{n} f(t)dt - f(n)$ converge.
En particulier, $\sum f(k)$ et $(\int_0^n f(t)dt)_{n\in\mathbb{N}}$ ont même nature et on a :
- *si $\sum f(k)$ converge, alors $\int_{n+1}^{\infty} f(t)dt \leq \sum_{k\geq n} f(k) \leq \int_n^{\infty} f(t)dt$,*
- *si $\sum f(k)$ diverge, alors $\sum_{k\geq n} f(k) \sim \int_0^n f(t)dt$.*

Application 9. [Séries de Bertrand] Soient $\alpha, \beta \in \mathbb{R}$. Alors $\sum_{n\in\mathbb{N}} \frac{1}{n^\alpha \ln(n)^\beta} < +\infty$ si et seulement si $\alpha > 1$ ou $(\alpha = 1, \beta > 1)$.

Théorème 10. [Comparaisons de séries]
i) Si $u_n = O(v_n)$ et $\sum v_k$ converge, alors $\sum u_k$ converge,
ii) Si $u_n \sim v_n$, alors $\sum u_k$ et $\sum v_k$ ont même nature.

Exemple 11. La série de terme général $1/n$ est divergente. En notant $(H_n)_{n\in\mathbb{N}}$ les sommes partielles associées, il existe une constante $\gamma > 0$ (appelée constante d'Euler) telle que $H_n = \ln(n) + \gamma + \frac{1}{2n} + o(\frac{1}{n})$.

Théorème 12. [Sommation des relations de comparaison]
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 :

	$\sum_{n\in\mathbb{N}} v_n < +\infty$	$\sum_{n\in\mathbb{N}} v_n = +\infty$
$u_n = o(v_n)$	$R_n(u) = o(R_n(v))$	$S_n(u) = o(S_n(v))$
$u_n = O(v_n)$	$R_n(u) = O(R_n(v))$	$S_n(u) = O(S_n(v))$
$u_n \sim v_n$	$R_n(u) \sim R_n(v)$	$S_n(u) \sim S_n(v)$

Théorème 13. [Règles de d'Alembert, de Cauchy et de Raab-Duhamel]
Supposons $(u_n)_{n\in\mathbb{N}}$ à termes strictement positifs.
i) Supposons que $u_{n+1}/u_n \underset{n\to+\infty}{\longrightarrow} \lambda \in [0, +\infty]$, alors :
- *Si $\lambda < 1$, $\sum u_k$ converge,*
- *Si $\lambda > 1$ (ou si $\lambda = 1$ et $\forall n, u_{n+1}/u_n \geq 1$), $\sum u_k$ diverge.*

ii) Supposons que $\sqrt[n]{u_n} \underset{n\to+\infty}{\longrightarrow} \lambda \in [0, +\infty]$, alors :
- *Si $\lambda < 1$, $\sum u_k$ converge,*
- *Si $\lambda > 1$ (ou si $\lambda = 1$ et $\forall n, \sqrt[n]{u_n} \geq 1$), $\sum u_k$ diverge.*

iii) Supposons que $u_{n+1}/u_n = \frac{1}{1+a/n+O(1/n^2)}$. Alors il existe $\lambda > 0$ tel que $u_n \sim \lambda/n^a$.

Exemple 14. Étude des séries de terme général $1/n!$ et $1/(\lambda^n+1)$ pour $\lambda \in \mathbb{R}_+$.

III. Séries de termes généraux quelconques [Gou08, §4.2, p206–209]

On suppose $(u_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{K}$.

III. A. Importance de l'absolue convergence

Définition 15. [absolument convergente, semi-convergence]
- On dit que $\sum u_k$ est absolument convergente si $\sum |u_k|$ est convergente.
- On dit que $\sum u_k$ est semi-convergente si $\sum u_k$ est convergente et non absolument convergente.

Théorème 16. [réarrangement de Riemann] *[FGN07, §3.48, p217]*
Soit $\sum u_k$ une série semi-convergente réelle. Alors pour tout $\ell \in \mathbb{R}$, il existe une permutation σ de $\mathbb{N}$ telle que $\sum_{n\in\mathbb{N}} u_{\sigma(n)} \underset{n\to+\infty}{\longrightarrow} \ell$.

Proposition 17. *Si $\sum u_k$ est absolument convergente, alors pour toute permutation σ de $\mathbb{N}$, on a $\sum_{n\in\mathbb{N}} u_n = \sum_{n\in\mathbb{N}} u_{\sigma(n)}$.*

Remarque 18. On peut en fait choisir ℓ dans $\mathbb{R}\cup\{\pm\infty\}$!

Exemple 19. Dans le cas complexe, le théorème de réarrangement ne s'applique pas ! Considérer par exemple $u_n = \frac{(-1)^n}{n} + \frac{(-1)^n}{n} i$.

III. B. Étude de l'absolue convergence

Proposition 20. [lien entre convergence et absolue convergence]
Si $\sum u_k$ est absolument convergente, alors elle est convergente et on a

$$\left|\sum_{n\in\mathbb{N}} u_n\right| \leq \sum_{n\in\mathbb{N}} |u_n|$$

Remarque 21. Lorsque $\sum u_k$ converge ou lorsque $|S_n| \underset{n\to+\infty}{\longrightarrow} +\infty$, l'inégalité $\left|\sum_{n\in\mathbb{N}} u_n\right| \leq \sum_{n\in\mathbb{N}} |u_n|$ est en fait valable dans $\mathbb{R}_+\cup\{+\infty\}$ que la série soit absolument convergente ou non.

Corollaire 22. *Si $(u_n)_{n\in\mathbb{N}}$ est absolument convergente, les résultats du Théorème 10 et du Théorème 12 restent vrais (en supposant toujours $(v_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{R}_+$!).*

Exemple 23. [moyenne de Cesàro]
Si $u_n \underset{n\to+\infty}{\longrightarrow} \ell \in \mathbb{C}$, alors $\frac{1}{n}\sum_{k=0}^n u_k \underset{n\to+\infty}{\longrightarrow} \ell$.

Exemple 24. Contre-exemple du point ii) du Théorème 10 dans le cas ou les deux suites ne sont pas de signe constant : on verra que les séries de termes généraux $u_n = \frac{(-1)^n}{n^\alpha}$ et $v_n = \frac{(-1)^n}{n^\alpha+(-1)^n}$ n'ont pas même nature lorsque $0 \leq \alpha \leq 1/2$.

III. C. Étude de la semi-convergence

Définition 25. [série alternée]
On dit que $\sum u_k$ est alternée si $u_n u_{n+1} \leq 0$ pour tout $n \in \mathbb{N}$.

Proposition 26. [critère des séries alternées]
Soit $(a_n)_{n\in\mathbb{N}}$ une suite de réels positifs. Si $(a_n)_{n\in\mathbb{N}}$ est décroissante et tend vers 0, alors la série de terme général $(-1)^n a_n$ converge et on a pour $n \in \mathbb{N}$, $|R_n| \leq a_{n+1}$.

Proposition 27. [transformation d'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 $(\sum_{k=0}^n v_k)_{n\in\mathbb{N}}$ est bornée). Alors $\sum u_k$ est convergente.

Exemple 28. La série de terme général $\mathrm{e}^{in\theta}/n^\alpha$ où $\theta \in \mathbb{R}\setminus 2\pi\mathbb{Z}$ est convergente pour $\alpha > 0$.

Proposition 29. [produit de Cauchy]
Soient $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$. Si $\sum a_k$ et $\sum b_k$ sont absolument convergentes, alors la série de terme général $c_n = \sum_{k=0}^n a_k b_{n-k}$ (appelée produit de Cauchy) est absolument convergente et on a

$$\sum_{n\in\mathbb{N}} c_n = \sum_{p\in\mathbb{N}} a_p \sum_{q\in\mathbb{N}} b_q$$

Exemple 30. Pour $a, b \in \mathbb{C}$, on a $\exp(a+b) = \exp(a)\exp(b)$.

IV. Applications

IV. A. Séries entières

[Gou08, §4.4, p236]

Définition 31. [Série entière]
On appelle série entière toute série de fonctions de la forme $z \longmapsto \sum_{n\geq 0} a_n z^n$ où $(a_n)_{n\in\mathbb{N}}$ est à valeurs dans $\mathbb{C}$.

Définition 32. [Rayon de convergence]
On définit le rayon de convergence de la série entière par le réel $R = \sup(\{r \geq 0 \,|\, (|a_n r^n|)_{n\in\mathbb{N}} \text{ est bornée}\})$.

Proposition 33.
- *Si $|z| < R$, la série $\sum a_k z^k$ converge,*
- *Si $|z| > R$, la série $\sum a_k z^k$ diverge (grossièrement).*

Corollaire 34. *On a $R^{-1} = \limsup_{n\to+\infty} \sqrt[n]{a_n}$.*

Application 35. Si $\sum a_k z^k$ et $\sum b_k z^k$ sont des séries entières de rayons de convergence R_a et R_b, alors leur produit de Cauchy a un rayon de convergence supérieur à $\min(R_a, R_b)$.

Exemple 36. [Différents comportements possibles en R]
- si $a_n = 1$, on a convergence sur $\mathbb{D}_1(0)$.
- si $a_n = 1/n$, on a convergence sur $\overline{\mathbb{D}}_1(0,1) \setminus \{1\}$.
- si $a_n = 1/n^2$, on a convergence sur $\overline{\mathbb{D}}_1(0,1)$.

Théorème 37. [Théorème d'Abel]
Soit $f : z \longrightarrow \sum_{n\geq 0} a_n z^n$ de rayon de convergence 1. On suppose que $\sum_{n\geq 0} a_n$ converge. Alors pour tout $\alpha \in [0, \pi/2[$, on a

$$\lim_{z\to 1, z\in\Delta_\alpha} f(z) = \sum_{n\geq 0} a_n \quad \text{où } \Delta_\alpha = \left\{z = 1 - \rho\, e^{i\theta} \in \mathbb{C} \,|\, |z| < 1, \rho > 0, \theta \in [-\alpha, \alpha]\right\}$$

Théorème 38. [Théorème taubérien faible]
Soit $f : z \longrightarrow \sum_{n\geq 0} a_n z^n$ de rayon de convergence 1. On suppose que $a_n = o(1/n)$ et qu'il existe $S \in \mathbb{C}$ tel que $f(x) \underset{x\to 1^-}{\longrightarrow} S$. Alors $\sum_{n\geq 0} a_n$ converge et $\sum_{n\geq 0} a_n = S$.

Proposition 39. *Soit $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence $R > 0$. La convergence de $\sum_{n\geq 0} a_n z^n$ est normale sur tout disque $\overline{\mathbb{D}}_r(O)$ de rayon $r < R$. En particulier, la série entière est continue sur $\mathbb{D}_R(O)$.*

IV. B. Vers la formule d'Euler-Maclaurin

[Gou08, §4.7, p301]

Définition 40. [Nombres et polynômes de Bernoulli]
$z \longmapsto \frac{z}{e^z - 1}$ est développable en série entière sur un disque $\mathbb{D}_r(0)$ pour un $r > 0$.
- On note $(b_n)_{n\in\mathbb{N}}$ la suite telle que $\frac{z}{e^z-1} = \sum_{n\geq 0} \frac{b_n}{n!} z^n$ sur ce disque.
- Il existe une suite de polynômes, notée $(B_n)_{n\in\mathbb{N}}$, telle que $\frac{z\,e^{xz}}{e^z-1} = \sum_{n\geq 0} \frac{B_n(x)}{n!} z^n$ par produit de Cauchy.

Proposition 41. *Pour $n \in \mathbb{N}$ et $x \in \mathbb{C}$, on a :*

(i) $B_n(1-x) = (-1)^n B_n(x)$,
(ii) $B'_{n+1} = (n+1)B_n$,
(iii) $B_n(x+1) - B_n(x) = nx^{n-1}$,
(iv) $B_n(0) = B_n(1) = b_n$ *pour* $n \geq 2$,
(v) $b_{2n+1} = 0$.

Théorème 42. [Formule d'Euler-Maclaurin]
Soient $m < n \in \mathbb{Z}$, $r \in \mathbb{N}^*$ et $f : [m, n] \longrightarrow \mathbb{C}$ une fonction de classe $\mathcal{C}^r$. Alors :

$$\sum_{k=m}^{n} f(k) = \int_m^n f(t)dt + \frac{1}{2}[f(m) + f(n)] + \sum_{\ell=2}^{r} \frac{b_\ell}{\ell!}[f^{(\ell-1)}(n) - f^{(\ell-1)}(m)] + R_r$$

où $R_r = \frac{(-1)^{r+1}}{r!} \int_m^n \tilde{B}_r(t) f^{(r)}(t)dt$ où $\tilde{B}_r(t) = B_r(t - \lfloor t \rfloor)$.

Application 43. [Série harmonique]
Soit $r \in \mathbb{N}^*$. On a $H_n = \ln n + \gamma + \frac{1}{2n} - \sum_{\ell=1}^{r-1} \frac{b_{2\ell}}{2\ell} \frac{1}{n^{2\ell}} + O\left(\frac{1}{n^{2r}}\right)$.

COMMENTAIRES

Speech : une bonne manière de faire consiste à se poser des questions (teaser) puis d'introduire les outils qui y répondent.

QUESTIONS

Q Montrer que la convergence d'une série entière de rayon de convergence R est uniforme sur un disque $\overline{\mathbb{D}}_r(O)$ avec $r < R$.

Q Déterminer la nature de la série de terme général $u_n = \cos(\pi\sqrt{n^2+n+1})$.

R Écrire $u_n = \cos(n\pi\sqrt{1+1/n+1/n^2})$ et faire un développement limité.

Q Supposons $u_n S_n \underset{n\to+\infty}{\longrightarrow} 1$ et que $u_n > 0$ pour tout $n \in \mathbb{N}^*$. Donner un équivalent de u_n.

R On vérifie que la série diverge et que le terme général tend vers 0. On écrit

$$S_n^2 - S_{n-1}^2 = u_n(2S_n - u_n) = 2S_n u_n - u_n^2 \underset{n\to+\infty}{\longrightarrow} 2$$

d'où $S_N^2 = \sum_{n=1}^N S_n^2 - S_{n-1}^2 \sim 2N$ et donc $u_N^2 \sim 1/S_N^2 \sim \frac{1}{2N}$. Finalement $u_N \sim \frac{1}{\sqrt{2N}}$.

BIBLIOGRAPHIE

[FGN07] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

233 ANALYSE NUMÉRIQUE MATRICIELLE : RÉSOLUTION APPROCHÉE DE SYSTÈMES LINÉAIRES, RECHERCHE DE VECTEURS PROPRES, EXEMPLES.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $n \in \mathbb{N}$. Pour $A \in \mathcal{M}_n(\mathbb{K})$, on désigne par A^* la matrice $\overline{A^\top}$.

I. Préliminaires théoriques

I. A. Normes matricielles

[AK02, ChI.3, p51]

Définition norme matricielle : norme sous-multiplicative sur $\mathcal{M}_n(\mathbb{K})$
Contre-exemple : $\|A\| = \max_{i,j} |a_{i\,j}|$
Définition norme subordonnée : dérive d'une autre norme
Une norme subordonnée est une norme matricielle
Exemples des normes p subordonnées : $|||A|||_1 = \sup_{1\leq j\leq n} \sum_{1\leq i\leq n} |a_{i\,j}|$ et $|||A|||_\infty = \sup_{1\leq i\leq n} \sum_{1\leq j\leq n} |a_{i\,j}|$
Exemple de norme matricielle non subordonnée : la norme de Frobenius : $\|A\|_F = \sqrt{\mathrm{Tr}(A^\top A)}$

I. B. Rayon spectral

[AK02, ChI.3, p51]

Définition du rayon spectral. Lien avec la norme 2 subordonnée : $|||A|||_2 = |||A^*|||_2 = \sqrt{\rho(AA^*)}$
Proposition : toute norme matricielle vérifie $\rho(.) \leq \|.\|$. Réciproquement pour toute matrice A, on a $\rho(A) = \inf\{\|A\| \mid \|.\| \text{ est une norme subordonnée}\}$ (Householder)
Remarque : c'est faux pour une norme quelconque (considérer $\|A\| = \max_{i,j} |a_{i\,j}|$)
Équivalence entre $A^n \longrightarrow 0$, $A^n x \longrightarrow 0 \quad \forall x$, $\rho(A) < 1$ et il existe une norme subordonnée telle que $\|A\| < 1$
Application : lorsque $\rho(A) < 1$, $I_n - A$ est inversible, d'inverse $\sum_{i\geq 0} A^i$

I. C. Conditionnement

[All05, §II.5.5, p89]

Soit A une matrice inversible.
Exemple de matrice A et vecteur b pour laquelle les résolution de $Ax = b$ et $Ax = b + \delta b$ donnent des solutions très différentes. (petite erreur sur les données implique grosse erreur sur la solution.
Contrôle de cette erreur par la notion de conditionnement
Définition du conditionnement par rapport à une norme subordonnée
Exemples de cond_p
Proposition : si $Ax = b$ et $A(x + \delta x) = b + \delta b$, alors $\frac{\|\delta x\|}{\|x\|} \leq \mathrm{cond}(A)\frac{\|\delta b\|}{\|b\|}$ et l'égalité est atteinte pour certains choix de x et δb. Si de plus $(A + \delta A)(x + \delta x) = b$, alors on a $\frac{\|\delta x\|}{\|x+\delta x\|} \leq \mathrm{cond}(A)\frac{\|\delta A\|}{\|A\|}$ et l'égalité est atteinte pour certains choix de δa et b
Propriétés du conditionnement : $\mathrm{cond}(A) = \mathrm{cond}(A^{-1}) = \mathrm{cond}(\alpha A)$ $(\alpha \neq 0)$
Pour la norme 2 : si U est unitaire, $\mathrm{cond}_2(AU) = \mathrm{cond}_2(UA) = \mathrm{cond}_2(A)$, et si A, B sont symétriques définies positives, on a $\mathrm{cond}_2(A + B) \leq \max(\mathrm{cond}_2(A), \mathrm{cond}_2(B))$. Liens avec les valeurs singulières ou même les valeurs propres dans le cas particulier où A est normale
Exemple : problème du laplacien

II. Résolutions de systèmes linéaires $Ax = b$

Soit A inversible.

II. A. Méthodes directes

[AK02, PIII, p105]

Formules de Cramer. Dans la pratique le coût en $O(n!)$ est très mauvais ! On ne l'utilise donc jamais (sauf en dimensions 2 ou 3)
Remarque : pour une matrice triangulaire, le coût est en $n^2/2$ (voir algorithme en annexe), on se ramène donc à l'étude de systèmes linéaires !
Théorème d'élimination de Gauss : il existe T triangulaire supérieure telle que $T = M_1 \dots M_r A$ où les M_i sont des matrices de transvection ou de permutation.
Méthode : en pratique on ne calcule pas $M_1 \dots M_r$: on met à jour le second membre $b' = M_1 \dots M_r b$ à chaque étape puis on résout $Tx = b'$. On a une complexité en $n^3/3$ mais on peut récupérer $\det(A)$.

Théorème 1. [Factorisation LU]
Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice dont tous les mineurs principaux sont non nuls. Alors il existe un unique couple (L, U) de matrices tel que L est triangulaire inférieure avec diagonale de 1, U est triangulaire supérieure et $A = LU$.

Théorème 2. [Factorisation de Cholesky]
Soit A une matrice symétrique réelle définie positive. Alors il existe une unique matrice B triangulaire inférieure telle que tous ses éléments diagonaux soient positifs et $A = BB^*$.

Théorème : factorisation LU, lorsque les mineurs principaux de A sont tous non nuls
Méthode : on résout $Ly = b$ puis $Ux = y$
Théorème : méthode de Cholesky : si A est symétrique réelle définie positive, il existe B triangulaire inférieure réelle à diagonale positive telle que $A = BB^\top$
Complexité en $n^3/6$, exemple

II. B. Méthodes itératives

[AK02, PIV, p153]

Idée : décomposition régulière $A = M - N$ avec M facile à inverser
On définit $x_0 \in \mathbb{K}^n$ et $x_{n+1} = M^{-1}(Nx_n + b)$. Si cette suite converge, la limite est la solution de $Ax = b$
Théorème : la méthode itérative converge pour tout x_0 si et seulement si $\rho(M^{-1}N) < 1$. Dans

ce cas, la vitesse de convergence est géométrique.
Exemple : méthode de RICHARDSON
Pour une matrice A hermitienne définie positive, si M, N est une décomposition satisfaisante, on a $M^* + N$ est hermitienne et si elle est définie positive, alors $\rho(M^{-1}N) < 1$
Méthode de JACOBI : on prend pour D la diagonale de A. On a $M^{-1}N = I_n - D^{-1}A$ (on peut supposer D inversible quitte à permuter les colonnes de A
Si A est hermitienne, on a convergence si A et $2D - A$ sont définies positives
Méthode de GAUSS-SEIDEL : on prend pour M la matrice triangulaire inférieure issue de A, et pour N l'opposé des coefficients restants. Si A est hermitienne définie positive, on a la convergence de la méthode car $M^* + N$ l'est aussi
Remarque : les itérations correspondent à un calcul matriciel, on a donc n^2 opérations. Les inversions de M nécessitent n opérations pour JACOBI, $n^2/2$ pour GAUSS-SEIDEL, donc pour un nombre d'itérations $\ll n$, ces méthodes sont plus rapides que les méthodes directes

II. C. Minimisation de fonctionnelle

[FGN12, §1.21, p39–41]

Minimisation de $x \longmapsto \frac{1}{2}\langle Ax \mid x\rangle - \langle b \mid x\rangle$

THÉORÈME 3. [MÉTHODE DE GRADIENT À PAS OPTIMAL]
Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$ elliptique, c'est-à-dire f est $\mathcal{C}^1$ et telle qu'il existe $\alpha > 0$ satisfaisant

$$\forall x, y \in \mathbb{R}^p, \langle \nabla f(x) - \nabla f(y) \mid x - y\rangle \geq \alpha \|x - y\|^2$$

Alors la suite $(x_n)_{n\in\mathbb{N}}$ définie par $x_0 \in \mathbb{R}^p$ et $x_{n+1} = x_n - \rho_n \nabla f(x_n)$ où $\rho_n = \operatorname{argmin}_{\rho>0} f(x_n - \rho\nabla f(x_n))$ converge vers l'unique minimum global de f.

III. Recherche de valeurs propres

III. A. Localisation

[FGN07, §2.8, p80]

Proposition : matrice à diagonale dominante
Disques de GERSHGÖRIN.

III. B. Méthode de la puissance

[AK02, Ch15, p215]

Méthode de la puissance pour trouver la plus grande valeur propre en module, ainsi qu'un vecteur propre, vitesse géométrique

III. C. Méthode de JACOBI

[AK02, Ch15, p215]

Matrices de GIVENS
Méthode de JACOBI : $A_k \underset{k\to+\infty}{\longrightarrow} \operatorname{diag}(\lambda_{\sigma(i)})$ pour un $\sigma \in \mathfrak{S}_n$

ANNEXE

Quelques algorithmes vus dans la leçon

SPEECH

On s'intéresse à deux problèmes : résoudre l'équation $Ax = b$ et rechercher des valeurs propres de matrices données.

COMMENTAIRES

Si [AK02] n'est pas disponible, la dernière annexe de [All05] peut permettre de s'en sortir quand même, mais reste beaucoup moins détaillée.

QUESTIONS

Q Montrer que $\operatorname{cond}_2(A+B) \leq \max(\operatorname{cond}_2(A), \operatorname{cond}_2(B))$ pour $A, B \in S_n^{++}(\mathbb{R})$.

R Comme $A + B \in S_n^{++}(\mathbb{R})$, écrivons $\operatorname{Sp}(A) = \{\lambda_1 \leq \cdots \leq \lambda_n\}$, $\operatorname{Sp}(B) = \{\mu_1 \leq \cdots \leq \mu_n\}$ et $\operatorname{Sp}(A+B) = \{\gamma_1 \leq \cdots \leq \gamma_n\}$. Alors $\|A\|_2 = \lambda_n$ et $\left\|A^{-1}\right\|_2 = 1/\lambda_1$. Donc

$$\operatorname{cond}_2(A) = \lambda_n/\lambda_1 \qquad \operatorname{cond}_2(B) = \mu_n/\mu_1 \qquad \operatorname{cond}_2(A+B) = \gamma_n/\gamma_1$$

Or il est clair que $\gamma_n \leq \lambda_n + \mu_n$ puisque si x est un vecteur propre associé à γ_n, on a $\|(A+B)x\| \leq (\lambda_n + \mu_n)\|x\|$.
De plus $\gamma_1 \geq \lambda_1 + \mu_1$ puisque l'on a :

$$\gamma_1 = \inf_{\|x\|=1} \langle x \mid (A+B)x\rangle \geq \inf_{\|x\|=1} \langle x \mid Ax\rangle + \inf_{\|x\|=1} \langle x \mid Bx\rangle = \lambda_1 + \mu_1$$

On en déduit le résultat.

Q Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A_{ij} = 0$ lorsque $|i-j| \geq p$ (A est une matrice bande). Soit L, U sa décomposition. Montrer que L, U sont des matrices bandes. [AK02, p119]

BIBLIOGRAPHIE

[AK02] G. ALLAIRE et S.-M. KABER : *Algèbre linéaire numérique*. Ellipses, 2002.

[All05] G. ALLAIRE : *Analyse numérique et optimisation*. Les éditions de l'École Polytechnique, 2005.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 2*. Cassini, 2007.

[FGN12] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

234 FONCTIONS ET ESPACES DE FONCTIONS LEBESGUE-INTÉGRABLES.

Soit $(E, \mathcal{A}, \mu)$ un espace mesuré. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Soit Ω un ouvert de $\mathbb{R}^d$, muni de sa tribu borélienne et de la restriction à Ω de la mesure de LEBESGUE, dont on suppose la construction connue.
Soit $p \in [1, +\infty]$ et q son exposant conjugué ($\frac{1}{p} + \frac{1}{q} = 1$).

I. Construction de l'intégrale et théorèmes d'intégration

[BP15, Ch7, p115]

I. A. Intégrale de fonctions étagées

Définitions, exemple avec la mesure de DIRAC, la mesure de comptage
Résultats d'additivité, de croissance, de positive homogénéité

I. B. Intégrales de fonctions mesurables positives

Définition de l'intégrale de f à partir des fonctions étagées
Convergence uniforme d'une suite de fonctions étagées vers f (fondamental)
Convergence monotone (contre exemple dans le cas décroissant)
Transfert des propriétés des intégrales de fonctions étagées
Lemme de FATOU, exemples

I. C. Fonctions intégrables

Fonction intégrable (cas $\mathbb{R}$ puis $\mathbb{C}$), exemples, contre-exemples
Théorème de convergence dominée
Importance de l'hypothèse de domination
Théorème de continuité sous le signe intégral, application à la transformée de FOURIER

II. Espaces L^p

[BP15, Ch9, p157–194] [Bre99, ChIV, p54]

II. A. Définition

DÉFINITION 1. [APPLICATION $\|.\|_p$, ESPACE $\mathcal{L}^p$]
Pour $f : E \longrightarrow \mathbb{K}$ mesurable, on définit $\|f\|_p = \left(\int_E |f|^p \, d\mu\right)^{\frac{1}{p}}$ lorsque p est fini, et $\|f\|_\infty = \inf\{M > 0 \mid |f| \leq M \ \mu\text{-p.p.}\}$. On définit l'espace vectoriel :

$$\mathcal{L}^p(E, \mathcal{A}, \mu) = \{f : E \longrightarrow \mathbb{K} \text{ mesurable} \mid \|f\|_p < +\infty\}$$

THÉORÈME 2. [INÉGALITÉ DE HÖLDER]
Pour toutes fonctions $f, g : E \longrightarrow \mathbb{K}$ mesurables, on a $\|fg\|_1 \leq \|f\|_p \|g\|_q$.

COROLLAIRE 3. [INÉGALITÉ DE MINKOWSKI]
Pour toutes fonctions $f, g : E \longrightarrow \mathbb{K}$ mesurables, on a $\|f + g\|_p \leq \|f\|_p + \|g\|_p$.

On vérifie que deux fonctions f, g mesurables égales μ-p.p. vérifient $\|f\|_p = \|g\|_p$. Ainsi :

DÉFINITION 4. [ESPACE L^p]
On note $L^p(E, \mathcal{A}, \mu) = \mathcal{L}^p(E, \mathcal{A}, \mu)/\{\|.\|_p = 0\}$ (ou $L^p(E)$, ou L^p) l'ensemble des fonctions de $\mathcal{L}^p(E, \mathcal{A}, \mu)$ quotienté par la relation d'égalité μ-p.p.. L'application $\|.\|_p$ passe au quotient et définit ainsi une application sur $L^p(E, \mathcal{A}, \mu)$ notée également $\|.\|_p$ par abus.

COROLLAIRE 5. *$\|.\|_p$ est une norme et l'espace $(L^p(E), \|.\|_p)$ est un espace vectoriel normé.*

EXEMPLE 6. [ESPACE ℓ^p]
Cas où $E = \mathbb{N}$ et μ est la mesure de comptage.
Si p est fini, on note ℓ^p l'espace $\mathcal{L}^p = L^p = \{(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}} \mid \sum_{n=0}^{+\infty} |a_n|^p < +\infty\}$.
$\ell^\infty = \mathcal{L}^\infty = L^\infty$ est l'espace des suites bornées.

APPLICATION 7. [INCLUSION ENTRE ESPACES L^p] Soient $p, p' \in [1, +\infty]$.
- lorsque $\mu(E) < +\infty$, on a $p < p' \Longrightarrow L^{p'} \subset L^p$,
- contre-exemple dans le cas où $\mu(E) = +\infty$: $f : x \longrightarrow (1+x)^{-1} \mathbb{1}_{\mathbb{R}_+^*}(x) \in L^2 \setminus L^1$.
- on a $p' < p \Longrightarrow \ell^{p'} \subset \ell^p$.

II. B. Premières propriétés des espaces L^p

THÉORÈME 8. [CONVERGENCE DOMINÉE DANS LES L^p]
Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions de L^p convergeant μ-p.p. vers une fonction f. On suppose qu'il existe une fonction $g \in \mathbb{L}^p$ telle que $|f_n| \leq g$ μ-p.p. pour tout $n \in \mathbb{N}$. Alors $f \in L^p$ et on a $\|f_n - f\|_p \underset{n\to+\infty}{\longrightarrow} 0$.

THÉORÈME 9. [THÉORÈME DE RIESZ-FICHER]
L'espace $(L^p(E, \mathcal{A}, \mu), \|.\|_p)$ est un espace de BANACH.

COROLLAIRE 10. *Toute suite convergente dans L^p admet une sous-suite qui converge μ-p.p..*

EXEMPLE 11. Contre-exemple de non-convergence de la suite μ-p.p.. : les bosses roulantes.

THÉORÈME 12. *Lorsque $p < \infty$:*
(i) l'ensemble des fonctions en escalier à support compact est dense dans L^p,
(ii) l'ensemble des fonctions continues à support compact est dense dans L^p.

APPLICATION 13. Uniforme continuité de l'opérateur par translation : pour tout $f \in L^p$, $a \longmapsto \tau_a f$ est uniformément continue sur $\mathbb{R}$.

COROLLAIRE 14. *L^p est séparable lorsque $p < +\infty$.*

III. Convolution et régularisation [BP15, Ch14, p291–314]

III. A. Convolution

On se place sur $E = \mathbb{R}^d$ où d est un entier quelconque. Soit $p \in [1, +\infty]$ et q son exposant conjugué.

DÉFINITION 15. [CONVOLUTION]
On appelle convolution de f et g la fonction $f \star g : x \longmapsto \int_{\mathbb{R}^d} f(y)g(x-y)dy$, lorsque celle-ci est bien définie.

THÉORÈME 16.
(i) Si $f \in L^1$ et $g \in L^p$, alors $f \star g$ existe μ-p.p. et $\|f \star g\|_p \leq \|f\|_1 \|g\|_p$.
(ii) Si $f \in L^p$ et $g \in L^q$, alors $f \star g$ existe pour tout x et $\|f \star g\|_\infty \leq \|f\|_p \|g\|_q$.
De plus, si $1 < p, q < +\infty$, alors $\lim_{|x|\to+\infty} f \star g(x) = 0$.

PROPOSITION 17. *La convolution est commutative, associative et bilinéaire sur $L^1(\mathbb{R}^d)$. Autrement dit, $(L^1(\mathbb{R}^d), +, \star)$ est une algèbre de* BANACH. *Elle est cependant sans unité.*

APPLICATION 18. La somme de deux variables aléatoires indépendantes définies sur $\mathbb{R}^d$ et de densités respectives f, g par rapport à la mesure de LEBESGUE a pour densité $f \star g$.

EXEMPLE 19. Si $G_\sigma : t \longmapsto \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{-\frac{x^2}{2\sigma^2}}$, alors $G_\sigma \star G_{\sigma'} = G_{\sigma+\sigma'}$

III. B. Approximation de l'unité et régularisation par convolution

DÉFINITION 20. [APPROXIMATION DE L'UNITÉ ET SUITE RÉGULARISANTE]
Une suite $(\alpha_n)_{n\geq 1}$ de fonctions positives de L^1 est une approximation de l'unité si :
- pour tout $n \in \mathbb{N}$, on a $\int_{\mathbb{R}^d} \alpha_n d\lambda_d = 1$,
- pour tout $\varepsilon > 0$, on a $\lim_{n\to+\infty} \int_{\{x\geq\varepsilon\}} \alpha_n d\lambda_d = 0$.

Si de plus les $(\alpha_n)_{n\geq 1}$ sont de classe $\mathcal{C}_c^\infty$, alors on dit que c'est une suite régularisante.

PROPOSITION 21. *Soient $p < +\infty$, $f \in L^p$ et $(\alpha_n)_{n\in\mathbb{N}}$ une approximation de l'unité. Alors $f * \alpha_n \xrightarrow[n\to+\infty]{L^p} f$.*

EXEMPLE 22. [EXISTENCE D'UNE SUITE RÉGULARISANTE]
On considère $\phi : x \longmapsto \exp(\frac{1}{\|x\|^2-1})\mathbb{1}_{]0,1]}(\|x\|)$ puis $\alpha : x \longmapsto \frac{\phi(x)}{\int_{\mathbb{R}^d}\phi d\lambda_d}$.
Alors la suite $\alpha_n : x \longmapsto n^d\alpha(nx)$ est une suite régularisante.

PROPOSITION 23. *Si $f \in \mathcal{C}_c^k(\mathbb{R}^d)$ et $f \in L^1(\mathbb{R}^d)$, alors $f \star g \in \mathcal{C}^k(\mathbb{R}^d)$ et*

$$\forall |\alpha| \leq k, \partial^\alpha(f \star g) = (\partial^\alpha f) \star g$$

APPLICATION 24. [CONSTRUCTION DE FONCTIONS PLATEAUX] [QZ13, ChIX.III, p318]
Soit K un compact de $\mathbb{R}^d$ et Ω un ouvert contenant K. Alors il existe $\theta \in \mathcal{C}^\infty(\mathbb{R}^d)$ telle que $\theta = 1$ sur K, $\theta = 0$ sur $\mathbb{R}^d \setminus \Omega$ et $0 \leq \theta \leq 1$.

THÉORÈME 25. *$\mathcal{C}_c^\infty(\mathbb{R}^d)$ est dense dans L^p pour $1 \leq p < +\infty$.*

APPLICATION 26. Si $f \in L^p$ et $g \in L^q$, $f \star g$ est uniformément continue.

IV. Le cas de L^2

COROLLAIRE 27. [DU THÉORÈME 9]
$L^2(E, \mathcal{A}, \mu)$ est un espace de HILBERT *pour le produit scalaire : $\langle f \mid g\rangle = \int_E f\bar{g}d\mu$.*

IV. A. Application en probabilités [BL07, ChVI, p149]

PROPOSITION 28. [ESPÉRANCE CONDITIONNELLE]
Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé, et soit $\mathcal{B}$ une sous-tribu de $\mathcal{A}$. Soit de plus X une variable aléatoire réelle sur $(\Omega, \mathcal{A}, \mathbb{P})$, intégrable ($X \in L^1(\Omega, \mathcal{A}, \mathbb{P})$). Alors il existe une unique (presque sûrement) variable aléatoire Z telle que :
(i) Z est $\mathcal{B}$-mesurable,
(ii) pour tout $B \in \mathcal{B}$, $\mathbb{E}[X\mathbb{1}_B] = \mathbb{E}[Z\mathbb{1}_B]$.
De plus, Z est intégrable. On l'appelle espérance conditionnelle de X sachant $\mathcal{B}$, notée $\mathbb{E}[X \mid \mathcal{B}]$.

APPLICATION 29. Soit $\mathcal{B}$ une tribu. Soient X une variable aléatoire indépendante de $\mathcal{B}$ et Y une variable aléatoire $\mathcal{B}$-mesurable. Alors pour toute fonction ψ telle que $\psi(X,Y)$ est intégrable :

$$\mathbb{E}[\psi(X,Y)\,|\,\mathcal{B}] = \int \psi(x,Y)\,d\mu_X(x) = h(Y)$$

où $h(y) = \mathbb{E}[\psi(X,y)]$.

EXEMPLE 30. Soit $(S_n)_{n\in\mathbb{N}}$ la marche aléatoire centrée réduite sur $\mathbb{Z}^d$. Alors $\mathbb{E}[S_{n+1}\,|\,S_n] = S_n$.

IV. B. Polynômes orthogonaux

[BMP05, §3.1.5, p110] [Dem96, §II.5, p51]

Soit I un intervalle de $\mathbb{R}$.

DÉFINITION 31. Soit $\rho : I \longrightarrow \mathbb{R}$ une fonction mesurable, strictement positive et telle que pour tout $n \in \mathbb{N}$, $\int_I |x|^n \rho(x)dx < +\infty$. On dit alors que ρ est une fonction de poids.

DÉFINITION 32. On définit $L^2(I,\rho) = \left\{ f : I \longrightarrow \mathbb{C} \text{ mesurable} \,|\, \int_I |f(x)|^2 \rho(x)dx < +\infty \right\}$.

PROPOSITION 33. *$L^2(I,\rho)$ est un espace de* HILBERT *pour le produit du scalaire $\langle f \mid g\rangle_\rho = \int_I f(x)\overline{g(x)}\rho(x)dx$.*

PROPOSITION 34. *Il existe une unique famille $(P_n)_{n\in\mathbb{N}}$ de polynômes unitaires deux à deux orthogonaux pour $\langle . \mid . \rangle_\rho$ et tels que $\deg(P_n) = n$ pour tout n.*

EXEMPLE 35. Voir les dessins en annexe :
- Pour $I = \mathbb{R}$ et $\rho : x \longmapsto \mathrm{e}^{-x^2}$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de HERMITE,
- Pour $I = [-1,1]$ et $\rho : x \longmapsto 1$, les $(P_n)_{n\in\mathbb{N}}$ sont les polynômes de LEGENDRE.

THÉORÈME 36. [BASE HILBERTIENNE DE POLYNÔMES ORTHOGONAUX]
Soit ρ une fonction de poids. S'il existe $\alpha > 0$ tel que $\int_I \mathrm{e}^{\alpha|x|}\rho(x)dx < +\infty$, alors la famille $(P_n)_{n\in\mathbb{N}}$ est une base hilbertienne de $L^2(I,\rho)$.

APPLICATION 37. Si I est borné, on a donc nécessairement une base hilbertienne.
La famille $(P_n \exp(-.^2/2))_n$, pour $(P_n)_{n\in\mathbb{N}}$ les polynômes de HERMITE, est une base hilbertienne de $L^2(\mathbb{R})$.

EXEMPLE 38. Sans l'hypothèse on a le contre-exemple suivant : soit la fonction de poids w : $x \longmapsto x^{-\ln(x)}$ sur $I = \mathbb{R}_+$. Alors $(P_n)_{n\in\mathbb{N}}$ ne forme pas une base de $L^2(I,w)$.

SPEECH

La théorie de LEBESGUE a permis de s'abstenir de nombreuses conditions jusqu'alors nécessaires pour définir l'intégrale d'une fonction. Si CAUCHY puis RIEMANN ont défini les intégrales de fonctions continues et d'autres classes de fonctions régulières, c'est bien LEBESGUE qui avec la notion de mesure a permis une nouvelle approche de l'intégrale, avec une intégration en tranches horizontales et non plus verticales. Cette nouvelle théorie s'étend a des espaces de fonctions extrêmement riches, qui sont des espaces de BANACH. De plus, les théorèmes d'interversion de symboles ne nécessitent que peu d'hypothèses.

QUESTIONS

Q Soit $p_0 > 1$ et $f > 0 \in L^{p_0}(\mu)$ où μ est une mesure de probabilité. On suppose que $\ln(f)$ est intégrable, d'intégrale m. Mq la suite $\|f\|_p \underset{p\to 0}{\longrightarrow} \exp(m)$. [BP15]

R

$$\ln(\|f\|_p) = \frac{1}{p}\ln(1-(1-\int|f|^p)) = -\frac{1-\int|f|^p}{p} + o(1) = -\frac{\int 1-|f|^p}{p} + o(1)$$
$$= -\int_\Omega \frac{1-\exp(p\ln(f))}{p}d\mu$$

On sépare selon si $f > 1$ ou non.

Q Montrer que $\Psi : L^q \longrightarrow (L^p)*, g \longmapsto (f \longmapsto \int fg)$ est une isométrie.

Q Montrer que $\|f\|_p \underset{p\to+\infty}{\longrightarrow} \|f\|_\infty$ si $\|f\|_p < +\infty$ pour tout p.

BIBLIOGRAPHIE

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Bre99] H. BREZIS : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[Dem96] J.-P. DEMAILLY : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

235 PROBLÈMES D'INTERVERSION DE LIMITES ET D'INTÉGRALES.

On considère une suite $(f_n)_{n\in\mathbb{N}}$ de fonctions et f une fonction, toutes définies sur un même ensemble E et à valeurs dans $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$.

Définition 1. [convergences simple, uniforme]
On dit que $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f si pour tout $x\in E$, on a $f_n(x) \underset{n\to+\infty}{\longrightarrow} f(x)$.
On dit que $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f si $\sup_E |f_n - f| \underset{n\to+\infty}{\longrightarrow} 0$.

I. Suites et séries de fonctions : propriétés de la limite et de la somme

I. A. Interversion limite-limite [AF91, El 11]

Exemple 2. [Hau07, p235] Pour $f_n : x\in[0,1]\longmapsto x^n$, on a $\lim_{n\to+\infty}\lim_{x\to1^-} f_n(x) = 1 \neq 0 = \lim_{x\to1^-}\lim_{n\to+\infty} f_n(x)$.

Théorème 3. *Supposons E métrique. Soit $a\in\overline{E}$ tel que $f_n(x) \underset{x\to a}{\longrightarrow} \ell_n\in\mathbb{K}$ et $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ sur un voisinage de a.*
Alors $\lim_{n\to+\infty}\ell_n$ et $\lim_{x\to a} f(x)$ existent et sont égales. Autrement dit :

$$\lim_{n\to+\infty}\lim_{x\to a} f_n(x) = \lim_{x\to a}\lim_{n\to+\infty} f_n(x)$$

Théorème 4. *Dans le même contexte, si les $(f_n)_{n\in\mathbb{N}}$ sont continues en a et si $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ sur un voisinage de a, alors f est continue en a.*

Corollaire 5. [séries de fonctions]
Supposons E métrique et soit $a\in\overline{E}$. Si $\lim_{x\to a} f_n(x)$ existe pour tout $n\in\mathbb{N}$ et $\sum f_k$ converge uniformément au voisinage de a, alors :

$$\lim_{x\to a}\sum_{n\geq0} f_n(x) = \sum_{n\geq0}\lim_{x\to a} f_n(x)$$

Remarque 6. Dans les deux théorèmes on aurait pu plus généralement considérer les fonctions à valeurs dans un espace complet. Dans le corollaire on aurait pu les supposer à valeurs dans un espace de Banach.

Exemple 7. $\zeta : x>1 \longrightarrow \sum_{n\geq1}\frac{1}{n^x}$ est continue et $\zeta(x) \underset{x\to+\infty}{\longrightarrow} 1$.

Application 8. Une série entière de rayon de convergence $R>0$ est continue sur $\mathbb{D}_R(O)$.

Remarque 9. On ne peut rien dire sur le cercle de convergence : par exemple avec $\sum_{n\geq0}(-1)^n z^n = \frac{1}{1+z}$ définie pour $|z|<1$, on a $\frac{1}{1+z} \underset{z\to1}{\longrightarrow} 1/2$ mais $\sum(-1)^n$ diverge.

Proposition 10. *Soit I un intervalle de $\mathbb{R}$, on suppose les $(f_n)_{n\in\mathbb{N}}$ dans $\mathcal{C}^1(I,\mathbb{R})$ telles que $f_n' \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g$ et $f_n \underset{n\to+\infty}{\overset{s}{\longrightarrow}} f$.*
Alors $f\in\mathcal{C}^1(I,\mathbb{R})$, $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ et $f'=g$.

Remarque 11. La preuve de ce théorème utilise le Théorème 16.

Corollaire 12. *Si les $(f_n)_{n\in\mathbb{N}}$ sont $\mathcal{C}^k([a,b],\mathbb{R})$ et telles que $f_n^{(p)} \underset{n\to+\infty}{\overset{s}{\longrightarrow}} g_p$ pour $p\leq k$ avec $f_n^{(k)} \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g_k$, alors $g_0\in\mathcal{C}^k([a,b],\mathbb{R})$, $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g_0$ et $g_0^{(p)}=g_p$ pour $p\leq k$.*

Exemple 13. Soit $f_u : t\longmapsto\exp(tu)$ $(u\in\mathbb{R})$. Alors f_u est $\mathcal{C}^\infty$ et $f_u^{(p)} : t\longmapsto\sum_{n\in\mathbb{N}}\frac{t^{n-p}}{(n-p)!}u^n$.

Exemple 14. [Hau07, p241] Importance de la convergence uniforme de $(f_n')_{n\in\mathbb{N}}$: considérer $f_n(x)=\sqrt{x^2+1/n}$.

I. B. Interversion limite-intégrale sur un segment [Gou08, §4.3, p222–223]

Exemple 15. On considère la suite de fonctions $(f_n)_{n\in\mathbb{N}}$ définie sur $[0,1]$ par $f_n(0)=0$, $f_n(1/n)=n^2$, $f_n([2/n,1])=0$ et f_n est affine sur $[0,1/n]$ puis $[1/n,2/n]$.
Alors f_n est continue, converge simplement vers 0 mais $\lim_{n\to+\infty}\int_0^1 f_n = \lim_{n\to+\infty}\int_0^1 n = +\infty \neq 0 = \int_0^1\lim_{n\to+\infty} f_n$.

Théorème 16. *Soit $[a,b]$ un segment de $\mathbb{R}$ et $(f_n)_{n\in\mathbb{N}}$ définies, continues et convergeant uniformément sur $[a,b]$ vers f. Alors f est continue et :*

$$\lim_{n\to+\infty}\int_a^b f_n = \int_a^b f$$

Exemple 17. $f_n : x\in[0,1]\longmapsto x^n(1-x)^n$.
On a $\sup_{[0,1]} f_n = 1/4^n \underset{n\to+\infty}{\longrightarrow} 0$ donc $\int_0^1 f_n \underset{n\to+\infty}{\longrightarrow} 0$.

Exemple 18. Importance de l'hypothèse de compacité : considérer f_n définie par $f_n(0)=0$, $f_n(n)=1/\sqrt{n}$, $f_n([2n,+\infty[)=0$ et f_n affine sur $[0,n]$ et $[n,2n]$.
Alors $\sup_{\mathbb{R}^+}|f_n| = 1/\sqrt{n} \underset{n\to+\infty}{\longrightarrow} 0$ et $\int_0^\infty f_n = \sqrt{n} \underset{n\to+\infty}{\longrightarrow} +\infty$.

Corollaire 19. [Séries de fonctions]
Dans le même contexte, soit $(f_n)_{n\in\mathbb{N}}$ telle que $\sum f_k$ converge uniformément sur $[a,b]$, alors :

$$\int_a^b \sum_{n\geq 0} f_n(t)dt = \sum_{n\geq 0}\int_a^b f_n(t)dt$$

Application 20. Si $f(x)=\sum_{n\geq 0}a_n x^n$ est une série entière de rayon de convergence $R>0$, alors pour $[a,b]\subset]-R,R[$, on a $\int_a^b f(x)dx = \sum_{n\geq 0} a_n \int_a^b x^n dx$.

Exemple 21. Pour $x\in]-1,1[$, on a $\frac{1}{1+x^2} = \sum_{n\geq 0}(-1)^n x^{2n}$, d'où $\arctan(x) = \sum_{n\geq 0}\frac{(-1)^n}{2n+1}x^{2n+1}$.

II. Théorèmes d'interversion en théorie de l'intégration

Dans toute la suite $(E,\mathcal{A},\mu)$ désigne un espace mesuré.

II. A. Les théorèmes fondamentaux

[BP15, Ch7/8, p115–157]

Théorème 22. [Convergence monotone]
Soit $(f_n)_{n\in\mathbb{N}}$ une suite croissante μ- p.p. de fonctions mesurables positives μ- p.p.. Alors :

$$\lim_{n\to+\infty}\uparrow \int_E f_n d\mu = \int_E \lim_{n\to+\infty}\uparrow f_n d\mu \quad (\in[0,+\infty])$$

Exemple 23. Le résultat est faux pour des fonctions décroissantes : $f_n = 1/n$ ou $f_n = \mathbb{1}_{[n,+\infty[}$.

Corollaire 24. *Soit $(f_n)_{n\in\mathbb{N}}$ des fonctions mesurables positives μ- p.p.. Alors :*

$$\sum_{n\geq 0}\int_E f_n d\mu = \int_E \lim_{n\to+\infty}\sum_{n\geq 0} f_n d\mu \quad (\in[0,+\infty])$$

Théorème 25. [Lemme de Fatou]
Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions mesurables positives μ- p.p..

$$\int_E \liminf_{n\to+\infty} f_n d\mu \leq \liminf_{n\to+\infty}\int_E f_n d\mu \leq +\infty$$

Application 26. Si $(f_n)_{n\in\mathbb{N}}$ est une suite de fonctions positives p.p. telles que $f_n \underset{n\to+\infty}{\longrightarrow} +\infty$ p.p., alors $\int_E f_n d\mu \underset{n\to+\infty}{\longrightarrow} +\infty$.

Théorème 27. [Convergence dominée]
Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions mesurables telles que :
- *$\lim_{n\to+\infty} f_n$ existe μ- p.p.,*
- *il existe g intégrable sur E telle que $|f_n(x)|\leq g(x)$ μ- p.p.pour tout $n\geq 0$.*

Alors f est intégrable et $\lim_{n\to+\infty}\int_E |f_n - f|\,d\mu = 0$ (et donc $\int_E f_n d\mu \underset{n\to+\infty}{\longrightarrow} \int_E f d\mu$).

Exemple 28. L'hypothèse de domination est cruciale : considérer $f_n = n\mathbb{1}_{[0,1/n]}$.

Corollaire 29. *Si les $(f_n)_{n\in\mathbb{N}}$ sont mesurables et telles que $\sum_{n\geq 0}\int_E |f_n|\,d\mu < +\infty$, alors les $(f_n)_{n\in\mathbb{N}}$ et $\sum_{n\geq 0} f_n$ sont intégrables et on a :*

$$\int_E \sum_{n\geq 0} f_n d\mu = \sum_{n\geq 0}\int_E f_n d\mu$$

Application 30. $\int_0^n (1+x/n)^n \,\mathrm{e}^{-\alpha x}\,dx \underset{n\to+\infty}{\longrightarrow} \begin{cases} \infty & \text{si } \alpha\leq 1 \\ 1/(\alpha-1) & \text{sinon} \end{cases}$.

Théorème 31. [Équation de la chaleur périodique]
Soit $u_0:\mathbb{R}\longrightarrow\mathbb{R}$ non identiquement nulle, 2π-périodique, $\mathcal{C}^1$ par morceaux et continue. Alors il existe une unique solution $u\in\mathcal{C}^0(\mathbb{R}_+\times\mathbb{R})\cap\mathcal{C}^\infty(\mathbb{R}_+^*\times\mathbb{R})$ telle que :

$$\begin{cases} \partial_t u(t,x) = \partial^2_{xx}u(t,x) & \forall t>0, x\in\mathbb{R} \\ u(0,x) = u_0(x) & \forall x\in\mathbb{R} \end{cases}$$

II. B. Conséquences sur les intégrales à paramètres [BP15, §8.3, p140–147]

Théorème 32. [Continuité sous le signe intégrale]
Soient U un espace métrique, $u_0 \in U$ et $f : U \times E \longrightarrow \mathbb{K}$ telles que :
- *pour tout $u \in U$, $x \longmapsto f(u,x)$ est mesurable,*
- *pour μ-presque tout x, $u \longmapsto f(u,x)$ est continue en u_0,*
- *il existe g intégrable telle que pour tout $u \in U$, $|f(u,x)| \leq g(x)$ μ- p.p..*

Alors $u \longmapsto \int_E f(u,x)d\mu(x)$ est bien définie sur U et est continue en u_0.

Application 33. Continuité de la transformée de Fourier d'une fonction $L^1(\mathbb{R}^d)$.

Théorème 34. [Dérivation sous le signe intégrale]
Soient I un intervalle de $\mathbb{R}$ et $f : I \times E \longrightarrow \mathbb{K}$ telles que :
- *pour tout $u \in I$, $x \longmapsto f(u,x)$ est intégrable sur E,*
- *pour μ-presque tout x, $u \longmapsto f(u,x)$ est dérivable sur I,*
- *il existe g intégrable telle que pour tout $u \in I$, $\left|\frac{\partial f}{\partial u}(u,x)\right| \leq g(x)$ μ- p.p..*

Alors $F : u \longmapsto \int_E f(u,x)d\mu(x)$ est définie, dérivable sur I et $F' : u \longmapsto \int_E \frac{\partial f}{\partial u}(u,x)d\mu(x)$.

Application 35. $\int_0^{+\infty} \frac{\sin(x)}{x}dx = \frac{\pi}{2}$.

Application 36. La transformée de Fourier d'une gaussienne est une gaussienne. Si $G_\sigma : x \longmapsto \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{-\frac{x^2}{2\sigma^2}}$ pour un $\sigma > 0$, alors $\hat{G}_\sigma : \zeta \longmapsto \mathrm{e}^{-\frac{\sigma^2\zeta^2}{2}}$.

Proposition 37. [Formule sommatoire de Poisson] *[Gou08, §6.4, p273]*
Soit $f : \mathbb{R} \longrightarrow \mathbb{C}$ une fonction $\mathcal{C}^1$ telle que $f(x) = O(1/x^2)$ et $f'(x) = O(1/x^2)$ en $\pm\infty$. Alors les sommes suivantes sont bien définies et on a :

$$\forall x \in \mathbb{R}, \sum_{n\in\mathbb{Z}} f(x+2n\pi) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \hat{f}(n)\,\mathrm{e}^{inx}$$

où $\hat{f}(n) = \int_{\mathbb{R}} f(t)\,\mathrm{e}^{-int}\,dt$.

Application 38. [Équation fonctionnelle de la fonction de Jacobi]
Pour $x > 0$, $\Theta(x) = \sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n^2 x}$ vérifie $\Theta(x) = \frac{1}{\sqrt{x}}\Theta(\frac{1}{x})$.

Théorème 39. [Holomorphie sous le signe intégrale]
Soient Ω un ouvert de $\mathbb{C}$ et $f : \Omega \times E \longrightarrow \mathbb{C}$ tels que :
- *pour tout $z \in \Omega$, $x \longmapsto f(z,x)$ est mesurable sur E,*
- *pour μ-presque tout x, $u \longmapsto f(z,x)$ est holomorphe sur Ω,*
- *il existe g intégrable telle que pour tout $z \in \Omega$, $|f(z,x)| \leq g(x)$ μ- p.p..*

Alors $F : z \longmapsto \int_E f(z,x)d\mu(x)$ est holomorphe sur Ω et

$$\forall k \geq 0, F^{(k)} : z \longmapsto \int_E \frac{\partial^k f}{\partial z^k}(z,x)d\mu(x)$$

Exemple 40. La fonction $\Gamma : z \longmapsto \int_0^\infty \mathrm{e}^{-t}\,t^{z-1}dt$ est définie et holomorphe sur $\{\Re(z) > 0\}$.

II. C. Interversion intégrale-intégrale [BP15, §11.3, p235–241]

Soit $(F, \mathcal{B}, \nu)$ un autre espace mesuré. On suppose que μ et ν sont σ-finies.

Théorème 41. [Théorème de Fubini-Tonelli]
Soit $f : (E \times F, \mathcal{A}\otimes\mathcal{B}, \mu\otimes\nu) \longrightarrow \mathbb{R}^+$ mesurable positive. Alors $x \longmapsto \int_F f(x,y)d\nu(y)$ et $y \longmapsto \int_E f(x,y)d\mu(x)$ sont mesurables et on a :

$$\int_{E\times F} f(x,y)d(\mu\otimes\nu)(x,y) = \int_E\int_F f(x,y)d\nu(y)d\mu(x) = \int_F\int_E f(x,y)d\mu(x)d\nu(y) \quad \in [0,+\infty]$$

Application 42. Considérons μ et ν les mesures de comptages sur $\mathbb{N}$. Alors pour tout famille de réels positifs $(u_{i,j})_{i,j\in\mathbb{N}}$, on a $\sum_{i\geq0}\sum_{j\geq0} u_{i,j} = \sum_{j\geq0}\sum_{i\geq0} u_{i,j}$.

Théorème 43. [Théorème de Fubini-Lebesgue]
Soit $f : (E \times F, \mathcal{A}\otimes\mathcal{B}, \mu\otimes\nu) \longrightarrow \mathbb{K}$ intégrable. Alors
- *$x \longmapsto \int_F f(x,y)d\nu(y)$ est définie μ- p.p. et est intégrable sur E,*
- *$y \longmapsto \int_E f(x,y)d\mu(x)$ est définie ν- p.p. et est intégrable sur F,*
- *$\int_{E\times F} f(x,y)d(\mu\otimes\nu)(x,y) = \int_E\int_F f(x,y)d\nu(y)d\mu(x) = \int_F\int_E f(x,y)d\mu(x)d\nu(y)$*

Exemple 44. Considérons $f : [0,+\infty[\times[0,1] \longrightarrow \mathbb{R}, (x,y) \longmapsto 2\,\mathrm{e}^{-2xy} - \mathrm{e}^{xy}$.
Elle est continue mais $\int_0^1\int_0^\infty f(x,y)dxdy = 0 < \int_0^\infty\int_0^1 f(x,y)dydx$.

Application 45. Calcul du volume de la boule unité euclidienne de $\mathbb{R}^n$:

$$V_n = \mathrm{Leb}_n(\overline{\mathbb{B}}(0,1)) = \frac{\pi^{n/2}}{\Gamma(n/2+1)}$$

SPEECH

On s'intéresse à plusieurs situations dans lesquelles on veut intervertir limites et intégrales :
- $\lim_{n\to+\infty} \int f_n = \int \lim_{n\to+\infty} f_n$,
- intégrales à paramètres $u \longmapsto \int_E f(x,u)d\mu(x)$,
- $\int_E \int_Y f = \int_Y \int_E f$.

Nous allons voir dans une première partie l'importance de la convergence uniforme, qui permet l'interversion limite limite, puis même limite intégrale dans le cas de segments.
Ensuite nous verrons comment la théorie de l'intégration apporte beaucoup de souplesse. Les outils des espaces L^p comme la convergence monotone, le lemme de FATOU ou le théorème de convergence dominée permettent des inversions faciles et ont des conséquences notables sur les intégrales à paramètres
Enfin l'inversion entre intégrales va être également possible dans le cadre de cette théorie : c'est l'objet des théorèmes de FUBINI.

COMMENTAIRES

Autres références possibles : [Bre99, Far00, QZ13, Rud98].
Dans le speech, ne pas trop parler de la différence des deux théories d'intégration RIEMANN/LEBESGUE pour éviter des questions piège.

QUESTIONS

Q Pourquoi le théorème de continuité sous le signe intégral est-il une conséquence des théorèmes précédents ?

R On se ramène à des suites car l'espace est métrique. On fait le lien entre les hypothèses qui vont permettre d'appliquer les théorèmes précédents.

Q Soit $T > 0$ et $f : [0,T] \longrightarrow \mathbb{C}$ continue. Pour $n \in \mathbb{N}$ et $t \in [0,T]$, on pose $g_n(t) = \sum_{k\geq 1} \frac{(-1)^k}{k!} \int_0^T f(u)\,\mathrm{e}^{-kn(t-u)}\,du$. Déterminer la limite simple de $(g_n)_{n\in\mathbb{N}}$.

Q Étudier l'existence et la continuité de la fonction $x \longmapsto \int_{\mathbb{R}} \frac{\sin(t)}{1+(x-t)^4} dt$.

Q On considère la série de fonctions $\sum f_k$ avec $f_k : x \longmapsto \mathrm{e}^{-nx} - 2\,\mathrm{e}^{-2nx}$ pour $x \geq 0$. Comparer l'intégrale sur $(\mathbb{R}^+)^*$ de la limite avec la limite de l'intégrale. Que peut-on dire de la convergence simple ? normale ?

BIBLIOGRAPHIE

[AF91] J.M. ARNAUDIÈS et H. FRAYSSE : *Cours de mathématiques, Tome 2, Analyse*. Dunod, 1991.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Bre99] H. BREZIS : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[El 11] M. EL AMRANI : *Suites et séries numériques, suites et séries de fonctions*. Ellipses, 2011.

[Far00] J. FARAUT : *Calcul intégral*. Belin, 2000.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Hau07] D. HAUCHECORNE : *Les contre-exemples en Mathématiques*. Ellipses, 2ème édition, 2007.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Rud98] W. RUDIN : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

236 ILLUSTRER PAR DES EXEMPLES QUELQUES MÉTHODES DE CALCUL D'INTÉGRALES DE FONCTIONS D'UNE OU PLUSIEURS VARIABLES.

I. Méthodes de calcul directes

I. A. Calculs de primitives

[Gou09, §2.3, p70] [Gou09, §3.2, p132]

Théorème 1. *Si F est une primitive de f sur $[a,b]$, alors on a $\int_a^b f(t)dt = F(b) - F(a)$.*

Exemple 2. Pour $\alpha > 1$, $\int_1^{+\infty} \frac{1}{t^\alpha} dt = \frac{1}{\alpha+1}$. Pour $x \in \mathbb{R}$, $\int_0^x \frac{1}{1+x^2} dx = \arctan(x)$.

Théorème 3. [Décomposition en éléments simples]
Soit $f \in \mathbb{K}(X)$ non nulle ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), écrivons $f = N/D$ avec $N, D \in \mathbb{K}[X]$ premiers entre eux et D unitaire. Ecrivons $D = \prod_{i=1}^n D_i^{\alpha_i}$ 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 4. Pour calculer une intégrale d'une fraction rationnelle réelle, on la décompose en éléments simples. Il suffit alors de connaître les intégrales :

- de $x \longmapsto \frac{1}{(x-a)^h}$ pour $a \in \mathbb{R}$ et $h \in \mathbb{N}^*$. On calcule facilement une primitive :

$$x \longmapsto \frac{1}{(1-h)(x-a)^{h-1}} \quad \text{si } h \neq 1 \qquad x \longrightarrow \ln(|x-a|) \quad \text{si } h = 1$$

- de $x \longmapsto \frac{ax+b}{(x^2+cx+d)^h}$ pour $c^2 - 4d < 0$ et $h \in \mathbb{N}^*$. Ecrivons $\frac{ax+b}{(x^2+cx+d)^h} = \frac{2\alpha(x-p)}{[(x-p)^2+q^2]^h} + \frac{\beta}{[(x-p)^2+q^2]^h}$. On calcule facilement la première primitive, et on procède par récurrence sur h pour la seconde.

Exemple 5. En décomposant en éléments simples $\frac{1}{x(x^2+1)} = \frac{1}{x} - \frac{x}{x^2+1} - \frac{x}{(x^2+1)^2}$, on obtient que $x \longmapsto \ln(|x|) - \frac{1}{2}\ln(x^2+1) + \frac{1}{2}\frac{1}{1+x^2}$ est une primitive de $x \longmapsto \frac{1}{x(x^2+1)}$.

I. B. Intégration par parties

[Gou08, §3.1, p123]

Théorème 6. [Intégration par parties]
Soient $u, v : [a,b] \longrightarrow \mathbb{C}$ deux fonctions de classe $\mathcal{C}^1$. Alors

$$\int_a^b u(x)v'(x)dx = [uv]_a^b - \int_a^b u'(x)v(x)dx$$

Application 7. L'intégrale $\int_0^{+\infty} \frac{\sin(x)}{x} dx$ est semi-convergente.

Exemple 8. [Intégrales de Wallis]
Posons $I_n = \int_0^{\pi/2} \sin^n(x)dx$ pour $n \in \mathbb{N}$. Alors $I_n = \frac{n-1}{n} I_{n-2}$ pour $n \geq 2$.

Exemple 9. Soit $\Gamma : x \longmapsto \int_0^{+\infty} \mathrm{e}^{-t} t^{x-1} dt$ pour $x \in \mathbb{R}_+^*$. Alors $\Gamma(x+1) = x\Gamma(x)$ pour $x > 0$. On en déduit $\Gamma(n+1) = n!$ pour $n \in \mathbb{N}$.

I. C. Changement de variables

[Gou08, §3.1, p123] [BP15, §12.2, p255]

Théorème 10. [Changement de variables en dimension 1]
Soit $\varphi : [a,b] \longrightarrow \mathbb{R}$ de classe $\mathcal{C}^1$ dont la dérivée ne s'annule pas de $f : I \longrightarrow \mathbb{R}$ continue par morceaux telle que $\varphi([a,b]) \subset I$. Alors

$$\int_a^b f(\varphi(t))\varphi'(t)dt = \int_{\varphi(a)}^{\varphi(b)} f(u)du$$

Application 11. [Règle de Bioche]
On cherche à calculer une primitive de fraction rationnelle en $\cos(x), \sin(x)$. Notons-là $R(\cos(x), \sin(x))$.

- Si $R(\cos(x), \sin(x))dx$ est inchangé par $x \longmapsto \pi - x$, on pose $t = \sin(x)$,
- Si $R(\cos(x), \sin(x))dx$ est inchangé par $x \longmapsto -x$, on pose $t = \cos(x)$,
- Si $R(\cos(x), \sin(x))dx$ est inchangé par $x \longmapsto \pi + x$, on pose $t = \tan(x)$,
- Sinon, on peut toujours essayer $t = \tan(x/2)$

Exemple 12. $\int_0^\pi \frac{\sin^3(x)}{1+\cos^2(x)} = \int_{-1}^1 \frac{1-t^2}{1+t^2} dt = \pi - 2$ via le changement de variables $t = \cos(x)$.

Théorème 13. [Changement de variables en dimension quelconque]
Soit U, V deux ouverts de $\mathbb{R}^n$ et ϕ un $\mathcal{C}^1$-difféomorphisme de U sur V. Alors pour toute fonction borélienne $f : V \longrightarrow \mathbb{R}_+$, on a :

$$\int_V f(v)dv = \int_U f(\phi(u)) \, |J_\phi(u)| \, du \quad \text{où} \quad J_\phi(u) = \det(d\,\phi_u)$$

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 14. [Passage en coordonnées polaires]
Pour $f : \mathbb{R}^2 \longrightarrow \mathbb{R}_+$ borélienne, on a $\int_{\mathbb{R}^2} f(x,y)dxdy = \int_{\mathbb{R}_+^* \times]-\pi,\pi[} f(r\cos(\theta), r\sin(\theta))rdrd\theta$.

Exemple 15. $\int_{\mathbb{R}} \mathrm{e}^{-x^2} dx = \sqrt{\pi}$.

I. D. Théorèmes de Fubini [BP15, §11.3, p235–241]

Soient $(E, \mathcal{A}, \mu)$ et $(F, \mathcal{B}, \nu)$ des espaces mesurés. On suppose que μ et ν sont σ-finies.

Théorème 16. [Théorème de Fubini-Tonelli]
Soit $f : (E \times F, \mathcal{A} \otimes \mathcal{B}, \mu \otimes \nu) \longrightarrow \mathbb{R}^+$ mesurable positive. Alors $x \longmapsto \int_F f(x,y)d\nu(y)$ et $y \longmapsto \int_E f(x,y)d\mu(x)$ sont mesurables et on a :

$$\int_{E\times F} f(x,y)d(\mu\otimes\nu)(x,y) = \int_E \int_F f(x,y)d\nu(y)d\mu(x) = \int_F \int_E f(x,y)d\mu(x)d\nu(y) \quad \in [0,+\infty]$$

Exemple 17. Soit $D = \left\{(x,y) \in \mathbb{R}_+^2 \mid x+y \leq 1\right\}$. Alors $\int_D xydxxy = \frac{1}{24}$.

Théorème 18. [Théorème de Fubini-Lebesgue]
Soit $f : (E \times F, \mathcal{A} \otimes \mathcal{B}, \mu \otimes \nu) \longrightarrow \mathbb{K}$ intégrable. Alors
- *$x \longmapsto \int_F f(x,y)d\nu(y)$ est définie μ- p.p. et est intégrable sur E,*
- *$y \longmapsto \int_E f(x,y)d\mu(x)$ est définie ν- p.p. et est intégrable sur F,*
- *$\int_{E\times F} f(x,y)d(\mu\otimes\nu)(x,y) = \int_E \int_F f(x,y)d\nu(y)d\mu(x) = \int_F \int_E f(x,y)d\mu(x)d\nu(y)$*

Exemple 19. Considérons $\begin{array}{rccc} f : & [0,+\infty[\times[0,1] & \longrightarrow & \mathbb{R} \\ & (x,y) & \longmapsto & 2\,\mathrm{e}^{-2xy} - \mathrm{e}^{xy} \end{array}$.
Elle est continue mais $\int_0^1 \int_0^\infty f(x,y)dxdy = 0 < \int_0^\infty \int_0^1 f(x,y)dydx$.

Application 20. Calcul du volume de la boule unité euclidienne de $\mathbb{R}^n$:

$$V_n = \mathrm{Leb}_n(\overline{\mathbb{B}}(0,1)) = \frac{\pi^{n/2}}{\Gamma(n/2+1)}$$

II. Techniques indirectes

II. A. Paramétrisation, interversions somme-intégrale [BP15, Ch7/8, p115–157]

Soit $(E, \mathcal{A}, \mu)$ un espace mesuré.

Théorème 21. [Convergence dominée]
Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions mesurables telles que :
- *$\lim_{n\to+\infty} f_n$ existe μ- p.p.,*
- *il existe g intégrable sur E telle que $|f_n(x)| \leq g(x)$ μ- p.p.pour tout $n \geq 0$.*

Alors f est intégrable et $\lim_{n\to+\infty} \int_E |f_n - f|\, d\mu = 0$ (et donc $\int_E f_n d\mu \underset{n\to+\infty}{\longrightarrow} \int_E f d\mu$).

Exemple 22. L'hypothèse de domination est cruciale : considérer $f_n = n\mathbb{1}_{[0,1/n]}$.

Application 23. Pour $x > 0$, $\Gamma(x) = \lim_{n\to+\infty} \int_0^n (1-t/n)^n t^{x-1} = \lim \frac{n!n^x}{x(x+1)\ldots(x+n)}$.

Application 24. Lorsque l'on peut écrire f comme série de fonctions, on peut souvent appliquer le théorème de convergence dominée.

$$\int_0^1 \frac{\ln(x)}{x-1}dx = \sum_{n\in\mathbb{N}^*} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Théorème 25. [Dérivation sous le signe intégrale]
Soient I un intervalle de $\mathbb{R}$ et $f : I \times E \longrightarrow \mathbb{K}$ telles que :
- *pour tout $u \in I$, $x \longmapsto f(u,x)$ est intégrable sur E,*
- *pour μ-presque tout x, $u \longmapsto f(u,x)$ est dérivable sur I,*
- *il existe g intégrable telle que pour tout $u \in I$, $\left|\frac{\partial f}{\partial u}(u,x)\right| \leq g(x)$ μ- p.p..*

Alors $F : u \longmapsto \int_E f(u,x)d\mu(x)$ est définie, dérivable sur I et $F' : u \longmapsto \int_E \frac{\partial f}{\partial u}(u,x)d\mu(x)$.

Application 26. La transformée de Fourier d'une gaussienne est une gaussienne. Si $G_\sigma : x \longmapsto \frac{1}{\sqrt{2\pi\sigma^2}}\,\mathrm{e}^{-\frac{x^2}{2\sigma^2}}$ pour un $\sigma > 0$, alors $\hat{G}_\sigma : \zeta \longmapsto \mathrm{e}^{-\frac{\sigma^2\zeta^2}{2}}$.

Application 27. Prenant $f : (t,x) \longmapsto \frac{\sin(x)}{x}\,\mathrm{e}^{-tx}$, on montre que $\int_0^{+\infty} \frac{\sin(x)}{x}dx = \frac{\pi}{2}$.

II. B. Analyse complexe [Tau06, §15.2.5, p192]

Théorème 28. [Théorème des résidus]
Soit U un ouvert convexe ou étoilé (ou simplement convexe). Soit f méromorphe sur U. On note P l'ensemble de pôles de f. Alors pour $\gamma : [0,1] \longrightarrow U \setminus P$ chemin fermé, on a :

$$\frac{1}{2i\pi}\int_\gamma f(z)dz = \sum_{a\in P} \mathrm{Res}(f,a)\ \mathrm{Ind}(\gamma,a)$$

Application 29. Pour $\alpha \in \mathbb{R}_+^*$, on a $\int_{\mathbb{R}_+} \exp(-x^2)\cos(\alpha x)dx = \frac{\sqrt{\pi}}{2}\exp(-\alpha^2/4)$.

Application 30. On retrouve $\int_{\mathbb{R}} \frac{1}{1+x^2}dx = \pi$ ou $\int_0^{2\pi} \frac{\sin(x)}{x}dx = \frac{\pi}{2}$.

Exemple 31. Soit $-1 < \alpha < 1$. Alors $I_\alpha = \displaystyle\int_0^{+\infty} \frac{x^\alpha \ln(x)}{x^2-1} dx = \frac{\pi^2}{4\cos^2(\frac{\pi}{2}\alpha)}$.

III. Méthodes d'approximation numérique

III. A. Méthodes de quadrature

[Dem96, ChIII, p59]

Soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction continue. On cherche des formules pour approcher $I(f) = \int_a^b f(t)dt$. 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 32. [Méthode de quadrature]
Une méthode de quadrature consiste, pour $0 \leq i \leq n-1$ à approcher $I_i = \int_{x_i}^{x_{i+1}} f$ par $A_i(f) = h_i \sum_{j=0}^{\ell_j} \omega_{i\,j} f(\zeta_{i\,j})$ où les $(\zeta_{i\,j})_j$ sont dans $[x_i, x_{i+1}]$ et les $(\omega_{i\,j})_{0\leq j\leq n}$ sont des réels fixés tels que $\sum_j \omega_{i\,j} = 1$.
On note alors $E(f) = I(f) - \sum_{i=0}^{n-1} A_i(f)$ l'erreur de la méthode.

Définition 33. [Méthode de quadrature]
On dit qu'une méthode de quadrature est d'ordre N si elle est exacte ($E(f) = 0$) pour tout $f \in \mathbb{R}_N[X]$ et s'il existe $f \in \mathbb{R}_{N+1}[X]$ telle qu'elle soit inexacte.

Définition 34. [Méthode par interpolation de Lagrange]
Fixons i et $(\zeta_j)_j$. La méthode d'interpolation de Lagrange associée consiste à prendre $\omega_j = \frac{1}{h_i}\int_{[x_i,x_{i+1}]} \ell_j$ où $\ell_j = \prod_{k\neq j} \frac{X-\zeta_k}{\zeta_j-\zeta_k}$.

Application 35. Comme $\sum_j \ell_j = 1$, on utilise souvent comme fonction de poids les $(\ell_j)_j$ associés à une subdivision de $[x_i, x_{i+1}]$: ce sont les méthodes par interpolation de Lagrange.

(i) **[Méthode des rectangles]**
On approxime $I(f)$ par $\sum_{i=0}^{n-1} h_i f(z_i)$ où $(z_i)_i = (x_i)_i$ ou $(x_{i+1})_i$. Méthode d'ordre 0.

(ii) **[Méthode des points milieux]**
De même avec $(z_i)_i = (\frac{x_{i+1}-x_i}{2})_i$. Méthode d'ordre 1 et $E(f) \leq \frac{1}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iii) **[Méthode des trapèzes]**
On approxime $I(f)$ par $\sum_{i=0}^{n-1} h_i \frac{f(x_{i+1})+f(x_i)}{2}$. Méthode d'ordre 1 et $E(f) \leq \frac{2}{3}\|f''\|_\infty$ si f est $\mathcal{C}^2$.

(iv) **[Méthode de Simpson]**
On approxime $I(f)$ par $\sum_{i=0}^{n-1} h_i \frac{f(x_{i+1})+4f(\frac{x_{i+1}-x_i}{2})+f(x_i)}{6}$. Méthode d'ordre 3 et $E(f) = O(\|f^{(4)}\|_\infty)$ si f est $\mathcal{C}^4$.

Exemple 36. Approximation de $\int_0^\pi \cos^2(x)dx = \frac{\pi}{4}$:
(i) méthode des rectangles (à gauche ou à droite) : π,
(ii) méthode des points milieux : 0,
(iii) méthode des trapèzes : π,
(iv) méthode de Simpson : $\frac{\pi}{3}$.

III. B. Méthode de Monte-Carlo

[BL07, §V.5, p132] et [Mé11, §5.3/6.5, p147/178]

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé.

Théorème 37. [Loi des grands nombres]
Soit $(X_i)_{i\in\mathbb{N}^*}$ des variables aléatoires i.i.d. intégrables. Alors :

$$\frac{1}{n}\sum_{i=1}^n X_i \underset{n\to+\infty}{\longrightarrow} \mathbb{E}[X_1] \quad \text{p.s.}$$

Application 38. [Méthode de Monte-Carlo]
Soit $f : [0,1]^d \longrightarrow \mathbb{R}$ intégrable par rapport à la mesure de Lebesgue. Soit $(X_i)_{n\in\mathbb{N}^*}$ une suite de variables aléatoires i.i.d. de loi $\mathcal{U}([0,1]^d)$. Alors

$$I_n = \frac{1}{n}\sum_{i=1}^n f(X_i) \underset{n\to+\infty}{\longrightarrow} I = \int_{[0,1]^d} f(x)dx \text{ p.s.}$$

Théorème 39. [Théorème central limite]
Soit $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires réelles i.i.d. de carré intégrable. Alors :

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n (X_i - \mathbb{E}[X_1]) \underset{n\to+\infty}{\overset{\mathcal{L}}{\longrightarrow}} Z \sim \mathcal{N}(0, \mathrm{Var}(X_1))$$

Application 40. Supposons f telle que $\mathrm{Var}(f) = \int_{[0,1]^d} f(x)^2dx - \left(\int_{[0,1]^d} f(x)dx\right)^2$ soit majorée par M. Alors $IC_\alpha^\infty = \left[I_n \pm q_{1-\alpha/2}\sqrt{\frac{M}{n}}\right]$ est un intervalle de confiance asymptotique de niveau α pour $I(f)$, où $q_{1-\alpha/2}$ est le quantile de niveau $1-\alpha/2$ de $\mathcal{N}(0,1)$.

ANNEXE

Contours utilisés en analyse complexe.
Illustration des différentes méthodes numériques.

SPEECH

Calculer la valeur d'une intégrale est une question fréquente pour laquelle nous n'avons pas de procédure automatique donnant la solution : on a donc besoin de nombreux outils de calculs.
Dans la première partie, on regarde ce qu'il se passe en dimension 1.
En dimension supérieure, on doit parfois se ramener en dimension 1, ou encore utiliser le théorème de changement de variables multidimensionnel, par exemple pour passer en coordonnées polaires.
Ensuite on donne des résultats issus de la théorie de l'intégration, qui permettent par exemple dans le cas d'intégrales à paramètres ou d'intégrales d'une série de fonctions d'obtenir des résultats sur les intégrales aux limites.
Enfin, d'autres méthodes comme l'analyse complexe et la transformée de FOURIER permettent d'étoffer les outils à notre disposition.

QUESTIONS

Q Calculer $\int_0^{+\infty} \frac{x}{1+\mathrm{e}^x} dx$.

R C'est l'intégrale d'une fonction continue sur $\mathbb{R}_+$, intégrable en $+\infty$ car $o(1/x^2)$. On a $\frac{1}{1+t} = \sum_{n\geq 0}(-1)^n t^n$ pour $t \in]-1,1[$, donc :

$$\frac{x}{1+\mathrm{e}^x} = \frac{x}{\mathrm{e}^x}\frac{1}{1+\mathrm{e}^{-x}} = \frac{x}{\mathrm{e}^x}\sum_{n\geq 0}(-1)^n \mathrm{e}^{-nx}$$

On a $\int_0^{+\infty} x\,\mathrm{e}^{-(n+1)x}\,dx = \frac{1}{(n+1)^2}$, donc on peut appliquer le théorème de FUBINI-LEBESGUE :

$$\int_0^{+\infty} \frac{x}{1+\mathrm{e}^x} dx = \sum_{n\in\mathbb{N}}(-1)^n \frac{1}{(n+1)^2}$$

et :

$$\sum_{n\in\mathbb{N}}(-1)^n \frac{1}{(n+1)^2} = \sum_{p\in\mathbb{N}} \frac{1}{(2p+1)^2} - \sum_{p\in\mathbb{N}^*} \frac{1}{(2p)^2} = \sum_{p\in\mathbb{N}} \frac{1}{(2p+1)^2} - \frac{\pi^2}{24}$$
$$= \frac{\pi^2}{6} - \sum_{p\in\mathbb{N}^*} \frac{1}{(2p)^2} - \frac{\pi^2}{24} = \frac{\pi^2}{12}$$

Q Quel avantage/inconvénient voyez vous à la méthode de MONTE-CARLO ?

R Avantage : valable même pour f très irrégulière, et temps de calcul linéaire en la dimension.
Inconvénient : approximation aléatoire, donc pas de contrôle déterministe de l'erreur.

BIBLIOGRAPHIE

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Dem96] J.-P. DEMAILLY : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Mé11] S. MÉLÉARD : *Aléatoire : introduction à la théorie et au calcul des probabilités*. Les éditions de l'École Polytechnique, 2011.

[Tau06] P. TAUVEL : *Analyse complexe pour la Licence 3*. Dunod, 2006.

239 FONCTIONS DÉFINIES PAR UNE INTÉGRALE DÉPENDANT D'UN PARAMÈTRE. EXEMPLES ET APPLICATIONS.

I. Généralités sur les intégrales à paramètre

I. A. Régularité

[BP15, §8.3, p140–147] [BMP05, §2.7, p82]

Soit $(E, \mathcal{A}, \mu)$ un espace mesuré et U un espace métrique. On considère $f : U \times E \longrightarrow \mathbb{C}$ et on pose lorsque cela à un sens $F(t) = \int_E f(t,x)d\mu(x)$ pour $t \in U$.

Théorème 1. [Continuité sous le signe intégrale]
Supposons que :
- *pour tout $t \in U$, $x \longmapsto f(t,x)$ est mesurable,*
- *pour μ-presque tout x, $u \longmapsto f(t,x)$ est continue en t_0,*
- *il existe g intégrable telle que pour tout $t \in U$, $|f(t,x)| \leq g(x)$ μ- p.p..*

Alors F est bien définie sur U et est continue en t_0.

Application 2. Continuité de la transformée de Fourier d'une fonction $L^1(\mathbb{R}^d)$.

Théorème 3. [Dérivation sous le signe intégrale]
Si U est un intervalle I de $\mathbb{R}$, supposons que :
- *pour tout $t \in I$, $x \longmapsto f(t,x)$ est intégrable sur E,*
- *pour μ-presque tout x, $u \longmapsto f(t,x)$ est dérivable sur I,*
- *il existe g intégrable telle que pour tout $t \in I$, $\left|\frac{\partial f}{\partial t}(t,x)\right| \leq g(x)$ μ- p.p..*

Alors F est définie, dérivable sur I et $F' : t \longmapsto \int_E \frac{\partial f}{\partial t}(t,x)d\mu(x)$.

Application 4. Prenant $f : (t,x) \longmapsto \frac{\sin(x)}{x}\mathrm{e}^{-tx}$, on montre que $\int_0^{+\infty} \frac{\sin(x)}{x}dx = \frac{\pi}{2}$.

Corollaire 5. [Dérivation multiple sous le signe intégrale]
Si U est un intervalle I de $\mathbb{R}$, supposons que pour un $k \in \mathbb{N}^*$:
- *pour tout $t \in I$, $x \longmapsto f(t,x)$ est intégrable sur E,*
- *pour μ-presque tout x, $t \longmapsto f(t,x)$ est $\mathcal{C}^k$ sur I,*
- *pour $1 \leq i \leq k$, il existe g_i intégrable telle que pour tout $u \in I$, $\left|\frac{\partial^i f}{\partial u^i}(t,x)\right| \leq g_i(x)$ μ- p.p..*

Alors F est $\mathcal{C}^k$ sur I et $F^i : t \longmapsto \int_E \frac{\partial^i f}{\partial t^i}(t,x)d\mu(x)$ pour tout $1 \leq i \leq k$.

Exemple 6. La fonction $\Gamma : z \longmapsto \int_0^\infty \mathrm{e}^{-t}\, t^{z-1}dt$ est $\mathcal{C}^\infty$ sur $\mathbb{R}_+^*$.

Théorème 7. [Holomorphie sous le signe intégrale]
Supposons que U est un ouvert Ω de $\mathbb{C}$ et $f : \Omega \times E \longrightarrow \mathbb{C}$ tels que :
- *pour tout $z \in \Omega$, $x \longmapsto f(z,x)$ est mesurable sur E,*
- *pour μ-presque tout x, $u \longmapsto f(z,x)$ est holomorphe sur Ω,*
- *il existe g intégrable telle que pour tout $z \in \Omega$, $|f(z,x)| \leq g(x)$ μ- p.p..*

Alors F est holomorphe sur Ω et pour tout $k \geq 0$, $F^{(k)} : z \longmapsto \int_E \frac{\partial^k f}{\partial z^k}(z,x)d\mu(x)$.

Exemple 8. Γ est holomorphe sur $\{\Re(z) > 0\}$.

Application 9. Γ admet un unique prolongement méromorphe sur $\mathbb{C}$, holomorphe sur $\mathbb{C} \setminus -\mathbb{N}$. Celui-ci ne s'annule pas et de plus $1/\Gamma$ est une fonction entière.

I. B. Comportement asymptotique

[Gou08, §3.4, p159]

Théorème 10. [Intégration des relations de comparaison]
Soient $I = [a,b[$ un intervalle semi-ouvert de $\mathbb{R}$, $f : I \longrightarrow \mathbb{R}$ et $g : I \longrightarrow \mathbb{R}_+^*$ des applications continues par morceaux sur I. Alors lorsque $x \to b^-$:

	$f = o(g)$	$f = O(g)$	$f \sim g$
$\int_a^b g < +\infty$	$\int_x^b f = o(\int_x^b g)$	$\int_x^b f = O(\int_x^b g)$	$\int_x^b f \sim \int_x^b g$
$\int_a^b g = +\infty$	$\int_a^x f = o(\int_a^x g)$	$\int_a^x f = O(\int_a^x g)$	$\int_a^x f \sim \int_a^x g$

Application 11.
- $\ln(x) = \int_1^x \frac{1}{t}dt =_{x\to+\infty} o(x^\alpha)$ pour tout $\alpha > 0$.
- $\int_1^x \mathrm{e}^{-t}\ln(t)dt =_{x\to 1^+} o(\mathrm{e}^{1-x}) = o(x-1)$.

Proposition 12. [Méthode de Laplace] *[Rou99, p322]*
Soient $[a,b[$ un intervalle de $\mathbb{R}$, $\varphi : [a,b[\longrightarrow \mathbb{R}$ de classe $\mathcal{C}^2$ et $f : [a,b[\longrightarrow \mathbb{C}$ telle que $\mathrm{e}^{-t_0\varphi} f$ soit intégrable pour un certain $t_0 \in \mathbb{R}$. On suppose que f est continue en a et $f(a) \neq 0$, et que $\varphi' > 0$ sur $]a,b[$, $\varphi'(a) = 0$ et $\varphi''(a) > 0$. Alors :

$$\int_a^b e^{-t\varphi(x)} f(x)dx \underset{t\to+\infty}{\sim} \sqrt{\frac{\pi}{2\varphi''(a)}}\frac{e^{-t\varphi(a)}f(a)}{\sqrt{t}}$$

Application 13.
- **[Formule de Stirling]** $\Gamma(t+1) \sim_{t\to+\infty} \sqrt{2\pi t}\left(\frac{t}{\mathrm{e}}\right)^t$
- Pour $\alpha > 0$, $\int_{\mathbb{R}_+} x^{-\alpha x} t^x dx \sim \sqrt{\frac{2\pi}{\mathrm{e}\,\alpha}} t^{1/(2\alpha)} \exp\left(\frac{\alpha t^{1/\alpha}}{\mathrm{e}}\right)$.

II. Produit de convolution

[BP15, Ch14, p291–314] [QZ13, ChIX.III, p318]

On se place sur $E = \mathbb{R}^d$ où d est un entier quelconque. Soit $p \in [1, +\infty]$ et q son exposant conjugué.

Définition 14. [convolution]
On appelle convolution de f et g la fonction $f \star g : x \longmapsto \int_{\mathbb{R}^d} f(y)g(x-y)dy$, lorsque celle-ci est bien définie.

Théorème 15.
(i) Si $f \in L^1$ et $g \in L^p$, alors $f \star g$ existe μ-p.p. et $\|f \star g\|_p \leq \|f\|_1 \|g\|_p$.
(ii) Si $f \in L^p$ et $g \in L^q$, alors $f \star g$ existe pour tout x et $\|f \star g\|_\infty \leq \|f\|_p \|g\|_q$. De plus, si $1 < p, q < +\infty$, alors $\lim_{|x|\to+\infty} f \star g(x) = 0$.

Proposition 16. *La convolution est commutative, associative et bilinéaire sur $L^1(\mathbb{R}^d)$. Autrement dit, $(L^1(\mathbb{R}^d), +, \star)$ est une algèbre de Banach. Elle est cependant sans unité.*

Application 17. La somme de deux variables aléatoires indépendantes définies sur $\mathbb{R}^d$ et de densités respectives f, g par rapport à la mesure de Lebesgue a pour densité $f \star g$.

Exemple 18. Si $G_\sigma : t \longmapsto \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{-\frac{x^2}{2\sigma^2}}$, alors $G_\sigma \star G_{\sigma'} = G_{\sigma+\sigma'}$

Proposition 19. *Si $f \in \mathcal{C}_c^k(\mathbb{R}^d)$ et $f \in L^1(\mathbb{R}^d)$, alors $f \star g \in \mathcal{C}^k(\mathbb{R}^d)$ et*

$$\forall |\alpha| \leq k, \partial^\alpha(f \star g) = (\partial^\alpha f) \star g$$

Définition 20. [approximation de l'unité et suite régularisante]
Une suite $(\alpha_n)_{n\geq 1}$ de fonctions positives de L^1 est une approximation de l'unité si :
- pour tout $n \in \mathbb{N}$, on a $\int_{\mathbb{R}^d} \alpha_n d\lambda_d = 1$,
- pour tout $\varepsilon > 0$, on a $\lim_{n\to+\infty} \int_{\{x\geq\varepsilon\}} \alpha_n d\lambda_d = 0$.

Si de plus les $(\alpha_n)_{n\geq 1}$ sont de classe $\mathcal{C}_c^\infty$, alors on dit que c'est une suite régularisante.

Exemple 21. [existence d'une suite régularisante]
On considère $\phi : x \longmapsto \exp(\frac{1}{\|x\|^2-1})\mathbb{1}_{]0,1]}(\|x\|)$ puis $\alpha : x \longmapsto \frac{\phi(x)}{\int_{\mathbb{R}^d}\phi d\lambda_d}$.
Alors la suite $\alpha_n : x \longmapsto n^d\alpha(nx)$ est une suite régularisante.

Proposition 22. *Soient $p < +\infty$, $f \in L^p(\mathbb{R}^d)$ et $(\alpha_n)_{n\in\mathbb{N}}$ une approximation de l'unité. Alors $f * \alpha_n \xrightarrow[n\to+\infty]{L^p} f$.*

Application 23. [construction de fonctions plateaux]
Soit K un compact de $\mathbb{R}^d$ et Ω un ouvert contenant K. Alors il existe $\theta \in \mathcal{C}^\infty(\mathbb{R}^d)$ telle que $\theta = 1$ sur K, $\theta = 0$ sur $\mathbb{R}^d \setminus \Omega$ et $0 \leq \theta \leq 1$.

Théorème 24. *$\mathcal{C}_c^\infty(\mathbb{R}^d)$ est dense dans L^p pour $1 \leq p < +\infty$.*

Application 25. Si $f \in L^p$ et $g \in L^q$, $f \star g$ est uniformément continue.

III. Transformée de Fourier

[BP15, Ch15, p315] [Rud98, Ch9, p219]

Définition 26. Pour $f \in L^1(\mathbb{R}^d)$, on définit sa transformée de Fourier par :

$$\mathcal{F}(f) : \zeta \longmapsto \hat{f}(\zeta) = \int_{\mathbb{R}^d} f(x)\,\mathrm{e}^{-i\langle x|\zeta\rangle dx}$$

Définition 27. Pour $f \in L^1(\mathbb{R}^d)$, on note $\check{f}$ l'application $x \longmapsto f(-x)$.

Proposition 28. *$\mathcal{F}$ est linéaire et pour $f \in L^1(\mathbb{R}^d)$, $\hat{f}$ est uniformément continue et bornée.*

Théorème 29. [lemme de Riemann-Lebesgue]
Si $f \in L^1(\mathbb{R}^d)$ alors $\hat{f} \in \mathcal{C}_0(\mathbb{R}^d)$.

Proposition 30. *Soient $f, g \in L^1(\mathbb{R}^d)$.*
(i) $\hat{\check{f}} = \overline{\hat{f}} = \check{\hat{f}}$,
(ii) $\mathcal{F}(f \star g) = \mathcal{F}(f)\mathcal{F}(g)$,
(iii) Si τ_h est l'opérateur de translation par $h \in \mathbb{R}^d$ alors $\mathcal{F}(\tau_h f)(\zeta) = \mathrm{e}^{-i\langle h|\zeta\rangle}\,\mathcal{F}(f)(\zeta)$.
(iv) Pour $\lambda > 0$, $\mathcal{F}(f(./\lambda)) = \lambda\hat{f}(\lambda.)$

Application 31. La transformée de Fourier d'une gaussienne est une gaussienne. On a $\hat{G}_\sigma : \zeta \longmapsto \mathrm{e}^{-\frac{\sigma^2\zeta^2}{2}}$.

Proposition 32. *$\mathcal{F} : L^1(\mathbb{R}^d) \longrightarrow \mathcal{C}_0(\mathbb{R}^d)$ est injective et continue.*

Application 33. En probabilité, la fonction caractéristique caractérise la loi d'une variable aléatoire.

Définition 34. [Classe de Schwartz]
On définit la classe de Schwartz sur $\mathbb{R}^d$, notée $\mathcal{S}(\mathbb{R}^d)$, comme l'ensemble des fonctions $f \in \mathcal{C}^\infty(\mathbb{R}^d)$ telles que :

$$\forall p \in \mathbb{N}, N_p(f) = \sup_{|\alpha|\leq p, |\beta|\leq p} \sup_{x\in\mathbb{R}^d} \left|x^\beta \partial^\alpha f(x)\right| < +\infty$$

On munit cet espace de la famille dénombrable de semi-normes $(N_p)_{p\in\mathbb{N}}$, il est donc métrisable (espace de Fréchet).

Exemple 35. $\mathcal{C}_c^\infty(\mathbb{R}^d) \subset \mathcal{S}(\mathbb{R}^d)$ et $G_\sigma \in \mathcal{S}(\mathbb{R}^d)$.

Proposition 36. *Pour $f \in \mathcal{S}(\mathbb{R}^d)$, on a $\hat{f} \in \mathcal{S}(\mathbb{R}^d)$.*

Proposition 37. *$\mathcal{S}(\mathbb{R}^d)$ est complet et s'injecte continument dans les $L^p(\mathbb{R}^d)$, dans lesquels il est dense pour $p < +\infty$.*

Proposition 38. *$\mathcal{S}(\mathbb{R}^d)$ est stable par dérivation, multiplication interne, multiplication par un polynôme (ces opérations étant continues).*

Proposition 39. *Pour $\alpha, \beta \in \mathbb{N}^n$ et $f \in \mathcal{S}(\mathbb{R}^d)$, on a :*

$$\forall \zeta \in \mathbb{R}^d, \quad \mathcal{F}(\partial^\alpha f)(\zeta) = i^{|\alpha|}\zeta^\alpha \mathcal{F}(f)(\zeta) \quad \text{et} \quad \mathcal{F}(.^\beta f)(\zeta) = i^{|\beta|}\partial^\beta \mathcal{F}(f)(\zeta)$$

Corollaire 40. *Si $f \in L^1(\mathbb{R}^d)$ est telle que $\hat{f} \in L^1(\mathbb{R}^d)$, alors*

$$\forall x \in \mathbb{R}^d, f(x) = \frac{1}{(2\pi)^d}\hat{\hat{f}}(-x) \quad p.p.$$

En particulier f est égale p.p. à une fonction $\mathcal{C}_0(\mathbb{R}^d)$.

Exemple 41. On a $\mathcal{F}(\mathrm{e}^{-|x|}) : \zeta \longmapsto \frac{2}{1+\zeta^2}$. On en déduit que $\mathcal{F}(\frac{1}{1+x^2}) : \zeta \longmapsto \pi\,\mathrm{e}^{-|\zeta|}$.

Corollaire 42. [Inversion de Fourier dans $\mathcal{S}(\mathbb{R}^d)$]
$\mathcal{F} : \mathcal{S}(\mathbb{R}^d) \longrightarrow \mathcal{S}(\mathbb{R}^d)$ est un automorphisme continu et on a $\mathcal{F}^{-1} : f \longmapsto \frac{1}{(2\pi)^d}\mathcal{F}(\check{f})$.

Application 43. [Résolution d'EDP] [Bon01, §9.6, p184]

- On considère l'équation de la chaleur $\partial_t u = \partial_x^2 u$ avec condition initiale $f \in \mathcal{S}(\mathbb{R}^d)$. Alors il existe une unique solution $u \in \mathcal{C}^2(\mathbb{R}\times\mathbb{R}^d)$ telle que $u(t,.) \in \mathcal{S}(\mathbb{R}^d)$ uniformément en t sur tout compact et $u(t,.) \underset{t\to 0}{\longrightarrow} f$ dans L^1. Cette solution est donnée par :

$$\forall t>0, \forall x\in\mathbb{R}^d, u(t,x) = \frac{1}{(4\pi t)^{d/2}}\int_{\mathbb{R}^d} f(y)\,\mathrm{e}^{-\frac{|x-y|^2}{4t}}\,dy = f\star k_t(x) \quad \text{où } k_t = \frac{1}{(4\pi t)^{d/2}}\,\mathrm{e}^{-\frac{|.|^2}{4t}}$$

- On considère l'équation de Schrödinger $\partial_t u = i\partial_x^2 u$ avec condition initiale $f \in \mathcal{S}(\mathbb{R})$. Cette équation possède une unique solution $u \in \mathcal{C}^2(\mathbb{R}\times\mathbb{R})$ telle que pour tout t, $u(t,.) \in \mathcal{S}(\mathbb{R})$ uniformément en t sur tout compact. On a :

$$\forall t>0, \forall x\in\mathbb{R}^d, u(t,x) = \frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(\zeta)\,\mathrm{e}^{-i\zeta^2 t}\,\mathrm{e}^{ix\zeta}\,d\zeta$$

Proposition 44. *Si $f, g \in \mathcal{S}(\mathbb{R}^d)$ alors*

$$\int_{\mathbb{R}^d} f(x)\hat{g}(x)dx = \int_{\mathbb{R}^d} \hat{f}(x)g(x)dx$$

Théorème 45. [Théorème de Fourier-Plancherel]
$\mathcal{F}$ se prolonge en un unique opérateur linéaire (toujours noté $\mathcal{F}$) de $L^2(\mathbb{R}^d)$ dans lui-même vérifiant :

- *$\mathcal{F}\circ\mathcal{F} = (2\pi)^d\check{\mathrm{Id}}$,*
- *Pour $f \in L^2(\mathbb{R})^d$, $\|f\|_{L^2}^2 = \frac{1}{(2\pi)^d}\left\|\hat{f}\right\|_{L^2}^2$,*
- *Pour $f, g \in L^2(\mathbb{R}^d)$, $\int_{\mathbb{R}^d} f(x)\overline{g}(x)dx = \frac{1}{(2\pi)^d}\int_{\mathbb{R}^d}\hat{f}(x)\overline{\hat{g}}(x)dx$.*

Remarque 46. La définition de $\mathcal{F}$ ci-dessus coïncide avec celle sur L^1, il n'y a donc pas d'ambiguïté.

Exemple 47. On calcule $\widehat{\mathbb{1}_{[-1,1]}} : \zeta \longmapsto 2\,\mathrm{sinc}(\zeta)$. Les deux fonctions étant $L^2(\mathbb{R})$, on en déduit que $\widehat{\mathrm{sinc}} = \pi\mathbb{1}_{[-1,1]}$.

SPEECH

Les intégrales à paramètres sont l'analogue des séries de fonctions si on voit l'intégrale comme une généralisation de la somme. On voudrait donc voir les propriétés de la régularité de ces intégrales, c'est l'objet de la première partie. Notons également des propriétés de comportement asymptotique (méthode de LAPLACE).
Le cas particulier du produit de convolution qui est une intégrale à paramètres : bonne structure cependant sans unité, mais on peut essayer d'approcher ces unités via une approximation de l'unité. On peut alors par exemple construire des fonctions plateaux et avoir des résultats de densité.
Ensuite les transformées de FOURIER, qui sont l'analogue continu des séries de FOURIER. On a envie d'étendre la transformée de FOURIER via l'espace de SCHWARTZ qui est un espace dans lequel tout se passe bien. Cela permet notamment d'obtenir le théorème d'inversion de FOURIER et d'étendre la transformée de FOURIER à de nouvelles fonctions. Cela offre de nombreuses applications en ÉDP : l'esprit des méthodes de résolution est de passer en FOURIER pour obtenir des ÉDO, plus simples, puis repasser en temporel.
Notons aussi des applications en probabilités via la fonction caractéristique qui va caractériser la loi d'une variable aléatoire.

QUESTIONS

Q Quelle est l'idée derrière la méthode de LAPLACE ?

R On cherche l'endroit « qui va le plus compter dans l'intégrale », c'est-à-dire l'endroit où l'exponentielle est la plus importante. Voir l'explication heuristique du [Rou99].

Q Et pour la phase stationnaire ?

R En un point stationnaire, la fonction φ est à peu près constante, on perd en quelque sorte le caractère oscillant autour de ce point. C'est donc cette partie de l'intégrale qui va compter, alors que le reste va plus ou moins s'annuler par oscillations.

Q Soit $F : x \longmapsto \int_0^{+\infty} \frac{1}{t^x(1+t)} dt$. Trouver son domaine de définition, montrer que la fonction est continue. Donner le comportement de F en 0.

R Soit $f : (t,x) \longmapsto \frac{1}{t^x(1+t)}$. $f(.,x) \in \mathcal{C}^0(\mathbb{R}_+^*)$ est mesurable, $f(t,x) \sim \frac{1}{t^x}$ en 0 donc est intégrable si et seulement si $x < 1$, puis $f(t,x) \sim \frac{1}{t^{x+1}}$ en $+\infty$ est intégrable si et seulement si $x+1 > 1$. Ainsi F est définie sur $]0,1[$.
Comportement en 0 : si jamais on avait du $t^{1/x}$ on aurait pour $t < 1$, $t^{1/x} \longrightarrow 0$ et si $t > 1$, $t^{1/x} \longrightarrow +\infty$.
Pour s'y ramener, procédons au changement de variables $u = t^x$, qui donne $du = \frac{x}{t}\exp(\mathrm{e}\ln(t))dt = \frac{x}{t}udt$, ou encore $du/u = xdt/t$, et finalement $dt = x\ln t = u^{1/x}$. Ainsi :

$$F(x) = \int_0^{+\infty} \frac{u^{1/x}}{xu^2(1+u^{1/x})} du = \frac{1}{x}\int_0^{+\infty} \frac{u^{1/x}}{u^2(1+u^{1/x})} du$$

Pour $u < 1$, $\frac{u^{1/x}}{u^2(1+u^{1/x})} \longrightarrow 0$. Pour $u > 1$, $\frac{u^{1/x}}{u^2(1+u^{1/x})} \longrightarrow 1/u^2$.

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bon01] J.-M. BONY : *Théorie des distributions et analyse de* FOURIER. Les éditions de l'École Polytechnique, 2001.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

[Rud98] W. RUDIN : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

241 SUITES ET SÉRIES DE FONCTIONS. EXEMPLES ET CONTRE-EXEMPLES.

I. Convergences

On considère une suite $(f_n)_{n\in\mathbb{N}}$ de fonctions et f une fonction, toutes définies sur un même ensemble E et à valeurs dans $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$.

I. A. Autour de la convergence uniforme

[Gou08, §4.3, p220-222] [QZ13, §V.III, p149]

Définition 1. [Convergences simple, uniforme]
On dit que $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f si pour tout $x\in E$, on a $f_n(x) \underset{n\to+\infty}{\longrightarrow} f(x)$.
On dit que $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f si $\sup_E |f_n - f| \underset{n\to+\infty}{\longrightarrow} 0$.

Exemple 2. $(x\longmapsto x^n)_{n\in\mathbb{N}}$ converge simplement mais pas uniformément vers 0 sur $[0,1[$.

Théorème 3. *Soient E un espaces métrique. Soit $a\in E$. On suppose que $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ sur un voisinage de a et que les $(f_n)_{n\in\mathbb{N}}$ sont continues en a. Alors f est continue en a.*

Proposition 4. [Critère de Cauchy uniforme]
Il existe une fonction g telle que $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g$ si et seulement si :

$$\forall\varepsilon>0, \exists N\in\mathbb{N}\,|\,\forall p,q\geq N, \forall x\in E, |f_p-f_q|(x)\leq\varepsilon$$

Remarque 5. $\mathcal{C}_b(X,\|.\|_\infty)$ est complet (où X est un espace métrique complet).

Théorème 6. [Théorème d'Arzela-Ascoli]
Supposons E compact. Alors on peut extraire de $(f_n)_{n\in\mathbb{N}}$ une sous-suite uniformément convergente si et seulement si pour tout $x\in E$:
(i) $\forall\varepsilon>0, \exists\eta>0\,|\,\forall n\in\mathbb{N}, \forall y\in E, d(x,y)\leq\eta\Longrightarrow d(f_n(x),f_n(y))\leq\varepsilon$,
(ii) $F_x=\{f_n(x)\,|\,n\in\mathbb{N}\}$ est relativement compact.

Théorème 7. [Théorème de Weierstrass] *[QZ13, §XIII.II.1, p518–519]*
$\mathbb{R}[X]$ est dense dans $\mathcal{C}([a,b],\mathbb{R},\|.\|_\infty)$ pour $a<b\in\mathbb{R}$.

Définition 8. [Convergences de séries de fonctions]
On définit de même les convergences simple et uniforme d'une série de fonctions. On dit que $\sum f_k$ converge normalement si $\sum_{n\in} \|f_n\|_\infty<+\infty$.

Exemple 9. La série de terme général $f_n : x\longmapsto \frac{1}{x+n^2}$ converge normalement pour $x\in[a,A]$ où $0<a<A$.

Théorème 10. *La convergence normale implique la convergence uniforme.*

Exemple 11. La réciproque est fausse. Considérer $f_n=\frac{1}{n+1}\mathbb{1}_{[n,n+1[}$.

Proposition 12. *Soit I un intervalle de $\mathbb{R}$, on suppose les $(f_n)_{n\in\mathbb{N}}$ dans $\mathcal{C}^1(I,\mathbb{R})$ telles que $f_n' \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g$ et $f_n \underset{n\to+\infty}{\overset{s}{\longrightarrow}} f$.*
Alors $f\in\mathcal{C}^1([a,b],\mathbb{R})$, $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} f$ et $f'=g$.

Remarque 13. La preuve de ce théorème utilise le Théorème 21.

Corollaire 14. *Si les $(f_n)_{n\in\mathbb{N}}$ sont $\mathcal{C}^k([a,b],\mathbb{R})$ et telles que $f_n^{(p)} \underset{n\to+\infty}{\overset{s}{\longrightarrow}} g_p$ pour $p\leq k$ avec $f_n^{(k)} \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g_k$, alors $g_0\in\mathcal{C}^k([a,b],\mathbb{R})$, $f_n \underset{n\to+\infty}{\overset{u}{\longrightarrow}} g$ et $g_0^{(p)}=g_p$ pour $p\leq k$.*

Exemple 15. Soit $f_u : t\longmapsto\exp(tu)$ $(u\in\mathbb{R})$. Alors f_u est $\mathcal{C}^\infty$ et $f_u^{(p)} : t\longmapsto\sum_{n\in\mathbb{N}}\frac{t^{n-p}}{(n-p)!}u^n$.

Exemple 16. [Hau07, p241] Importance de la convergence uniforme de $(f_n')_{n\in\mathbb{N}}$: considérer $f_n(x)=\sqrt{x^2+1/n}$.

I. B. Convergence en théorie de l'intégration

[Gou08, §4.3, p222] [BP15, Ch7/8, p115–157]

Soit $(E,\mathcal{A},\mu)$ un espace mesuré.

Théorème 17. [Convergence dominée]
Si $(f_n)_{n\in\mathbb{N}}$ est une suite de fonctions mesurables telles que :
- *$\lim_{n\to+\infty} f_n$ existe et vaut f μ- p.p.,*
- *il existe g intégrable sur E telle que $|f_n(x)|\leq g(x)$ μ- p.p.pour tout $n\geq 0$.*

Alors f est intégrable et $\lim_{n\to+\infty}\int_E|f_n-f|\,d\mu=0$ (et donc $\int_E f_n d\mu \underset{n\to+\infty}{\longrightarrow}\int_X f d\mu$).

Exemple 18.
- L'hypothèse d'intégrabilité est nécessaire : considérer $f_n=1/n$ sur $\mathbb{R}_+$.
- L'hypothèse de domination est cruciale : considérer $f_n=n\mathbb{1}_{[0,1/n]}$.

Application 19. $\int_0^n (1+x/n)^n \mathrm{e}^{-\alpha x}\,dx \underset{n\to+\infty}{\longrightarrow} \begin{cases} \infty & \text{si } \alpha \leq 1 \\ 1/(\alpha-1) & \text{sinon} \end{cases}$.

Corollaire 20. *Si $(f_n)_{n\in\mathbb{N}}$ est une suite de fonctions mesurables telles que $\sum_{n\geq 0}\int_X |f_n|\,d\mu < +\infty$, alors les $(f_n)_{n\in\mathbb{N}}$ et $\sum_{n\geq 0} f_n$ sont intégrables et on a :*

$$\int_E \sum_{n\geq 0} f_n d\mu = \sum_{n\geq 0}\int_E f_n d\mu$$

Corollaire 21. *Si $(f_n)_{n\in\mathbb{N}}$ converge uniformément vers f sur $[a,b]$ un segment de $\mathbb{R}$ alors f est continue et $\int_a^b f_n(t)dt \underset{n\to+\infty}{\longrightarrow} \int_a^b f(t)dt$.*

Définition 22. [convergence L^p]
On dit que $(f_n)_{n\in\mathbb{N}}$ tend vers f dans L^p si ce sont des éléments de L^p et si $\|f_n - f\|_p \underset{n\to+\infty}{\longrightarrow} 0$.

Proposition 23. *La convergence L^p implique la convergence μ- p.p.d'une sous-suite.*

Exemple 24. Stroboscope (bosses roulantes) : on n'a pas convergence simple de la suite.

Définition 25. [approximation de l'unité et suite régularisante]
Une suite $(\alpha_n)_{n\geq 1}$ de fonctions positives de L^1 est une approximation de l'unité si :
- pour tout $n\in\mathbb{N}$, on a $\int_{\mathbb{R}^d}\alpha_n d\lambda_d = 1$,
- pour tout $\varepsilon > 0$, on a $\lim_{n\to+\infty}\int_{\{x\geq\varepsilon\}}\alpha_n d\lambda_d = 0$.

Si de plus les $(\alpha_n)_{n\geq 1}$ sont de classe $\mathcal{C}_c^\infty$, alors on dit que c'est une suite régularisante.

Exemple 26. [existence d'une suite régularisante]
On considère $\phi : x \longmapsto \exp(\frac{1}{\|x\|^2-1})\mathbb{1}_{[0,1]}(\|x\|)$ puis $\alpha : x \longmapsto \frac{\phi(x)}{\int_{\mathbb{R}^d}\phi d\lambda_d}$.
Alors la suite $\alpha_n : x \longrightarrow n^d\alpha(nx)$ est une suite régularisante.

Proposition 27. *Soit $(\rho_n)_{n\in\mathbb{N}}$ une suite régularisante et $f\in L^p$. Alors $(\rho_n * f)_{n\in\mathbb{N}}$ est une suite de fonctions $\mathcal{C}_c^\infty$ qui converge vers f dans L^p.*

Corollaire 28. *$\mathcal{C}_c^\infty$ est dense dans L^p.*

II. Séries entières

[Gou08, §4.4, p236–256]

Définition 29. [série entière]
On appelle série entière toute fonction de la forme $z \longmapsto \sum_{n\geq 0} a_n z^n$ où $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$.

Définition 30. [rayon de convergence]
On définit le rayon de convergence de la série entière par le réel $R = \sup(\{r\geq 0 \,|\, (|a_n r^n|)_{n\in\mathbb{N}} \text{ est bornée}\})$.

Exemple 31. La série entière $\sum_{n\geq 0}\frac{z^n}{n!}$ a un rayon de convergence infini.

Soit désormais $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence R.

Proposition 32. [lemme d'Abel]
- *Si $|z| < R$, la série $\sum_{n\geq 0} a_n z^n$ converge absolument,*
- *La série entière $\sum_{n\geq 0} a_n z^n$ convergence normalement sur $\mathbb{D}_r(0)$ pour tout $r < R$. En particulier, la série entière est continue sur $\mathbb{D}_R(O)$,*

Exemple 33. On n'a pas forcément convergence ou continuité sur $\overline{\mathbb{D}}_R(0)$! Par exemple $\sum_{n\geq 0}(-1)^n z^n = \frac{1}{1-z}$ sur $\mathbb{D}_1(0)$, prolongeable en 1 par $1/2$ mais dont la série en 1 diverge.

Proposition 34.
- *Si $|z| > R$, la série $\sum a_k z^k$ diverge (grossièrement),*
- *La série entière $\sum a_k z^k$ convergence normalement sur tout compact $K \subset \mathbb{D}_R(0)$.*

Exemple 35. [différents comportements possibles sur le cercle $\mathscr{C}_R(0)$]
- $\sum_{n\geq 1} z^n$ diverge en tout point de $\mathscr{C}_1(0)$,
- $\sum_{n\geq 1} z^n/n$ converge en tout point de $\mathscr{C}_1(0)$ sauf en 1,
- $\sum_{n\geq 1} z^n/n^2$ converge en tout point de $\mathscr{C}_1(0)$.

Théorème 36. [règles de d'Alembert et de Cauchy]
i) Si $a_{n+1}/a_n \underset{n\to+\infty}{\longrightarrow} \lambda \in [0,+\infty]$, alors $R = 1/\lambda$.
ii) Si $\sqrt[n]{|a_n|} \underset{n\to+\infty}{\longrightarrow} \lambda \in [0,+\infty]$, alors $R = 1/\lambda$.

Exemple 37. Pour $a_n = \begin{cases} 1/3^n & \text{si } n \text{ est pair} \\ 4/3^n & \text{si } n \text{ est impair} \end{cases}$, on peut appliquer la règle de Cauchy mais pas la règle de Hadamard.

Théorème 38. *$f : \mathbb{D}_R(0) \longrightarrow \mathbb{C}, z \longmapsto \sum_{n\geq 0} a_n z^n$ est de classe $\mathcal{C}^\infty$ et ses dérivées sont des séries entières de rayon de convergence R.*

Application 39. Si $\sum a_k z^k$ et $\sum b_k z^k$ sont des séries entières de rayons de convergence R_a et R_b, alors leur produit de Cauchy a un rayon de convergence supérieur à $\min(R_a, R_b)$.

III. Séries de Fourier

[Gou08, Ch4.5, p256–270] [QZ13, Ch4, p68–135] [BMP05, §3.3.3/3.3.4, p127]

On note $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$, $e_n = \mathrm{e}^{in\cdot}$ pour $n \in \mathbb{Z}$. On définit lorsque cela a un sens $\langle f \mid g\rangle = \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{g(t)}dt$ et $\|f\|_1 = \sqrt{\langle f \mid f\rangle}$.

Définition 40. [Coefficient de Fourier]
Pour $f \in L^1(\mathbb{T})$, on définit $c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{-int}\,dt = \langle f \mid e_n\rangle$ le n-ième coefficient de Fourier de f, où $n \in \mathbb{Z}$.

Exemple 41.

- Pour $f = \mathbb{1}_{]-a,a[}$ où $0 < a < \pi$, on a $c_n(f) = \begin{cases} a/\pi & \text{si } n = 0 \\ \sin(na)/n\pi & \text{sinon} \end{cases}$.
- Pour $f : x \longmapsto 1 - \frac{x^2}{\pi^2}$, on a $c_n(f) = \begin{cases} 1 & \text{si } n = 0 \\ \frac{2(-1)^n}{\pi^2 n^2} & \text{sinon} \end{cases}$.

Proposition 42. *Pour $f \in L^1(\mathbb{T})$, on a :*
(i) $c_n(\overline{f}) = \overline{c_{-n}(f)}$,
(ii) $c_n(\tau_a f) = \mathrm{e}^{ina}\,c_n(f)$,
(iii) $f * e_n = c_n(f)e_n$,
(iv) si $f \in \mathcal{C}(\mathbb{T}) \cap \mathcal{C}^1_{pm}(\mathbb{T})$, on a $c_n(f') = inc_n(f)$.

Lemme 43. [Lemme de Riemann-Lebesgue]
Si $f \in L^1(\mathbb{T})$, alors $c_n(f) \underset{n\to+\infty}{\longrightarrow} 0$.

Définition 44. [Somme partielles de Fourier, de Fejér]
On appelle somme partielle de Fourier d'ordre $N \in \mathbb{N}$ la quantité $S_N(f) = \sum_{n=-N}^{N} c_n(f)e_n$.
On appelle somme partielle de Fejér d'ordre $N \in \mathbb{N}$ la quantité $\sigma_N(f) = \frac{1}{N}\sum_{n=0}^{N-1} S_N(f)$.

Remarque 45. On peut voir $S_N(f)$ comme la projection sur $\mathcal{P}_N = \mathrm{Vect}((e_n)_{-N\leq n\leq N})$.

Définition 46. [Noyaux de Dirichlet, de Fejér]
On appelle noyau de Dirichlet à l'ordre $N \in \mathbb{N}$ la fonction $D_N = \sum_{n=-N}^{N} e_n$.
On appelle noyau de Fejér à l'ordre $N \in \mathbb{N}$ la fonction $K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n = \sum_{n=-N}^{N}(1 - |n|/N)e_n$.

Proposition 47. *On a les propriétés suivantes :*

D1) $S_N(f) = f * D_N$,
D2) D_N *est pair et* $\|D_N\|_1 = 1$,
D3) $\forall x \in \mathbb{T}, D_N(x) = \frac{\sin\left(\frac{2N+1}{2}x\right)}{\sin(x/2)}$,

F1) $\sigma_N(f) = f * K_N$,
F2) $\|K_N\|_1 = 1$,
F3) $\forall x \in \mathbb{T}, K_N(x) = \frac{1}{N}\frac{\sin^2(Nx/2)}{\sin^2(x/2)} \geq 0$,
F4) $\forall \delta \in]0,\pi], \int_{\delta\leq|t|\leq\pi} K_N(t)dt \underset{N\to+\infty}{\longrightarrow} 0$.

Théorème 48. [Théorème de Fejér]

- *Soit $f \in \mathcal{C}(\mathbb{T})$. Alors $\|\sigma_N(f)\|_\infty \leq \|f\|_\infty$ pour tout $N \geq 1$ et $\sigma_N(f) = f * K_N \underset{N\to+\infty}{\overset{u}{\longrightarrow}} f$.*
- *Soit $f \in L^p(\mathbb{T})$ pour un $p \in [1,+\infty[$. Alors $\|\sigma_N(f)\|_p \leq \|f\|_p$ pour tout $N \geq 1$ et $\lim_{N\to+\infty}\|\sigma_N(f) - f\|_p = 0$.*

Remarque 49. On peut retrouver le théorème de Weierstrass à partir du premier résultat.

Application 50. $\mathcal{F} : \mathcal{C}(\mathbb{T}) \longrightarrow c_0(\mathbb{Z}), f \longmapsto (c_n(f))_{n\in\mathbb{Z}}$ est injective.

Théorème 51. *$(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L^2(\mathbb{T})$. En particulier, pour $f \in L^2(\mathbb{T})$:*

$$f = \sum_{n\in\mathbb{Z}} c_n(f)e_n \qquad \text{et} \qquad \|f\|_{L^2}^2 = \sum_{n\in\mathbb{Z}} |c_n(f)|^2$$

Application 52. [Calculs de séries]
On peut reprendre l'Exemple 41 pour calculer les normes des applications dans L^2 : pour $a \in [\![0, 2\pi]\!]$: $\sum_{n\in\mathbb{N}^*} \frac{\sin(na)}{n} = \frac{\pi - a}{2}$ (première fonction) et $\sum_{n\in\mathbb{N}^*} \frac{1}{n^4} = \frac{\pi^4}{90}$ (deuxième fonction).
On peut aussi calculer classiquement $\sum_{n\in\mathbb{N}^*} \frac{1}{n^2} = \frac{\pi^2}{6}$ et $\sum_{n\in\mathbb{N}^*} \frac{1}{(2n-1)^2} = \frac{\pi^2}{8}$.

Théorème 53. *Si $f \in \mathcal{C}(\mathbb{T}) \cap \mathcal{C}^1_{pm}(\mathbb{T})$, alors $(S_N(f))_{N\in\mathbb{N}}$ converge normalement vers f.*

Exemple 54. Contre-exemple sans l'hypothèse $\mathcal{C}^1_{pm}$: il existe une fonction $f \in \mathcal{C}(\mathbb{T})$ telle que $(S_N(f)(0))_{N\in\mathbb{N}}$ ne converge pas (c'est un corollaire du théorème de Banach-Steinhaus).

COMMENTAIRES

Références pour la théorie de FOURIER : [SS03, QZ13].

QUESTIONS

Q Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ telle que f est limite uniforme de polynômes sur $\mathbb{R}$. Que dire de f ?

Q Soient $(X_n)_{n\in\mathbb{N}}$ des variables aléatoires (pas forcément indépendantes) de lois respectives $\mathcal{E}(n^2)$. Montrer que $\sum X_k$ converge dans L^2 et presque surement.

Q On pose $f : x \longrightarrow \sum_{n\geq 1} \frac{\mathrm{e}^{-nx}}{n^2+1}$ sur $\mathbb{R}_+$.

1) Montrer que f est bien définie et continue sur $\mathbb{R}_+$.
2) Montrer que f est $\mathcal{C}^\infty$ sur $\mathbb{R}_+^*$ et qu'elle est solution d'une ÉDO linéaire d'ordre 2 à coefficients constants.
3) Quelle est la limite de f en $+\infty$?
4) f est-elle dérivable en 0 ?

Q On prend une suite $(u_n)_{n\in\mathbb{N}}$ croissante qui tend vers $+\infty$ avec $u_n > 0$ pour tout n. On s'intéresse à la somme de la série de fonctions $\sum_{n\geq 1}(-1)^n \exp(-u_n.)$. Cette application est-elle bien définie ? La somme de la série est-elle continue ? Peut-on calculer la valeur de l'intégrale entre 0 et $+\infty$ de cette fonction ?

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Hau07] D. HAUCHECORNE : *Les contre-exemples en Mathématiques*. Ellipses, 2ème édition, 2007.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[SS03] E. STEIN et R. SHAKARCHI : *Complex Analysis*. Princeton University Press, 2003.

243 CONVERGENCE DES SÉRIES ENTIÈRES, PROPRIÉTÉS DE LA SOMME. EXEMPLES ET APPLICATIONS.

I. Généralités

[Gou08, §4.4, p236–256] [BMP05, §2.1/2.2, p47–56]

I. A. Série entière et rayon de convergence

Définition 1. [Série entière]
On appelle série entière toute fonction de la forme $z \longmapsto \sum_{n\geq 0} a_n z^n$ où $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$.

Définition 2. [Rayon de convergence]
On définit le rayon de convergence de la série entière par le réel $R = \sup(\{r \geq 0 \,|\, (|a_n r^n|)_{n\in\mathbb{N}} \text{ est bornée}\})$.

Exemple 3. La série entière $\sum_{n\geq 0} \frac{z^n}{n!}$ a un rayon de convergence infini.

Soit désormais $\sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence R.

Proposition 4. [Lemme d'Abel]
- *Si $|z| < R$, la série $\sum_{n\geq 0} a_n z^n$ converge absolument,*
- *La série entière $\sum_{n\geq 0} a_n z^n$ convergence normalement sur $\mathbb{D}_r(0)$ pour tout $r < R$. En particulier, la série entière est continue sur $\mathbb{D}_R(O)$,*

Exemple 5. On n'a pas forcément continuité sur $\overline{\mathbb{D}}_R(0)$! Considérer par exemple $\sum_{n\geq 0}(-1)^n z^n = \frac{1}{1-z}$ sur $\mathbb{D}_1(0)$, prolongeable en 1 par $1/2$ mais dont la série en 1 diverge.

Proposition 6.
- *Si $|z| > R$, la série $\sum a_k z^k$ diverge (grossièrement),*
- *La série entière $\sum a_k z^k$ convergence normalement sur tout compact $K \subset \mathbb{D}_R(0)$.*

Exemple 7. [Différents comportements possibles sur le cercle $\mathscr{C}_R(0)$]
- $\sum_{n\geq 0} z^n$ diverge en tout point de $\mathscr{C}_1(0)$,
- $\sum_{n\geq 0} z^n/n$ converge en tout point de $\mathscr{C}_1(0)$ sauf en 1,
- $\sum_{n\geq 0} z^n/n^2$ converge en tout point de $\mathscr{C}_1(0)$.

Théorème 8. [Règles de d'Alembert et de Cauchy]
i) Si $a_{n+1}/a_n \underset{n\to+\infty}{\longrightarrow} \lambda \in [0,+\infty]$, alors $R = 1/\lambda$.
ii) Si $\sqrt[n]{|a_n|} \underset{n\to+\infty}{\longrightarrow} \lambda \in [0,+\infty]$, alors $R = 1/\lambda$.

Exemple 9. Pour $a_n = \begin{cases} 1/3^n & \text{si } n \text{ est pair} \\ 4/3^n & \text{si } n \text{ est impair} \end{cases}$, on peut appliquer la règle de Cauchy mais pas la règle de Hadamard.

Corollaire 10. [Formule de Cauchy-Hadamard]
On a $R^{-1} = \limsup_{n\to+\infty} \sqrt[n]{a_n}$.

Exemple 11. $\sum_{n\geq 0} n^a z^n$, où $a \in \mathbb{R}$, a un rayon de convergence égal à 1.
$\sum_{n\geq 0} \frac{n^n}{n!} z^n$ a un rayon de convergence égal à $1/e$.

I. B. Opérations sur les séries entières

Soient $\sum_{n\geq 0} a_n z^n$ et $\sum_{n\geq 0} b_n z^n$ des séries entières de rayons de convergence R_a et R_b.

Proposition 12. *Si $a_n \underset{n\to+\infty}{=} O(|b_n|)$ alors $R_a \geq R_b$.*

Proposition 13. [Somme de séries entières]
$\sum_{n\geq 0}(a_n + b_n)z^n$ a un rayon de convergence R supérieur à $\min(R_a, R_b)$ et on a :

$$\forall z \in D(0, \min(R_a, R_b)), \sum_{n\geq 0}(a_n + b_n)z^n = \sum_{n\geq 0} a_n z^n + \sum_{n\geq 0} b_n z^n$$

Définition 14. [Produit de Cauchy]
On définit la série entière $\sum_{n\geq 0} c_n z^n$, où $c_n = \sum_{k=0}^n a_k b_{n-k}$, appelée produit de Cauchy de $\sum_{n\geq 0} a_n z^n$ et $\sum_{n\geq 0} b_n z^n$. On note R_c sont rayon de convergence.

Proposition 15. [Produit de Cauchy]
On a $R_c \geq \min(R_a, R_b)$ et :

$$\forall z \in D(0, \min(R_a, R_b)), \sum_{n\geq 0} c_n z^n = \left(\sum_{n\geq 0} a_n z^n\right)\left(\sum_{n\geq 0} b_n z^n\right)$$

Exemple 16. Les rayons des sommes/produits peuvent être distincts de $\min(R_a, R_b)$:
- $\sum_{n\geq 0}(1+2^n)z^n + \sum_{n\geq 0}(1-2^n)z^n = \sum_{n\geq 0} z^n$ $\quad (R_a, R_b, R) = (1/2, 1/2, 1)$.
- $(1-z)\sum_{n\geq 0} z^n = 1$ $\quad (R_a, R_b, R_c) = (+\infty, 1, +\infty)$.
- $\begin{cases} a_n = 2\mathbb{1}_{n=0} + 2^n \mathbb{1}_{n\geq 1} \\ b_n = -\mathbb{1}_{n=0} + \mathbb{1}_{n\geq 1} \end{cases} \implies c_n = -2\mathbb{1}_{n=0}$ $\quad (R_a, R_b, R_c) = (1/2, 1, +\infty)$.

II. Régularité de la somme [Gou08, §4.4, p236–256] [BMP05, §2.1/2.2, p47–56]

II. A. Régularité sur le disque de convergence, restriction à $\mathbb{R}$

Soit $f : z \longrightarrow \sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence $R > 0$. On a vu que f est continue sur $\mathbb{D}_R(0)$, normalement sur tout compact.

Théorème 17. *f est holomorphe sur $\mathbb{C}$ (dérivable au sens complexe) sur $\mathbb{D}_R(0)$, de dérivée $f' : z \longrightarrow \sum_{n\geq 1} n a_n z^{n-1}$, qui a pour rayon de convergence R.*

Corollaire 18. *On a pour tout $n \in \mathbb{N}$, $a_n = \frac{f^{(n)}(0)}{n!}$.*

Remarque 19. Ainsi f coïncide sur $\mathbb{D}_R(0)$ avec sa série de Taylor en 0.

Soit désormais $f : x \longrightarrow \sum_{n\geq 0} a_n x^n$ définie sur $]-R, R[$ où $R > 0$.

Corollaire 20. [Régularité]
f est $\mathcal{C}^\infty$ sur $]-R, R[$ et pour tout $k \in \mathbb{N}$ et $x \in]-R, R[$, on a $f^{(k)}(x) = \sum_{n\geq k} \frac{n!}{k!} a_n x^{n-k}$.

Corollaire 21. *La série $F : x \longrightarrow \sum_{n\geq 0} \frac{a_n}{n+1} x^{n+1}$ est une primitive de f sur $]-R, R[$.*

Exemple 22. Développements de $\log(1+.)$, $\arctan$, $\arcsin$, argth, argsh.

II. B. Convergence sur le cercle

Théorème 23. [Théorème d'Abel] *[Gou08, p252-253]*
Soit $f : z \longmapsto \sum_{n\geq 0} a_n z^n$ de rayon de convergence 1. On suppose que $\sum_{n\geq 0} a_n$ converge. Alors pour tout $\alpha \in [0, \pi/2[$, on a $\lim_{z\to 1, z\in\Delta_\alpha} f(z) = \sum_{n\geq 0} a_n$, où

$$\Delta_\alpha = \left\{1 - \rho\, \mathrm{e}^{i\theta} \in \mathbb{D}(0,1) \,|\, |z| < 1, \rho > 0, \theta \in [-\alpha, \alpha]\right\}$$

Théorème 24. [Théorème taubérien faible] *[Gou08, p253-254]*
Soit $f : z \longmapsto \sum_{n\geq 0} a_n z^n$ de rayon de convergence 1. On suppose que $a_n = o(1/n)$ et qu'il existe $S \in \mathbb{C}$ tel que $f(x) \underset{x\to 1^-}{\longrightarrow} S$. Alors $\sum_{n\geq 0} a_n$ converge et $\sum_{n\geq 0} a_n = S$.

Théorème 25. [Théorème taubérien fort]
Le résultat précédent est toujours vrai si l'on suppose $a_n = O(1/n)$.

III. Fonctions développables en série entière

[Gou08, §4.4, p236–256] [BMP05, §2.1/2.2, p47–56]

III. A. Sur $\mathbb{C}$

Soit Ω un ouvert de $\mathbb{C}$ et $f : \Omega \longrightarrow \mathbb{C}$. On suppose $0 \in \Omega$ (sinon on translate la fonction).

Définition 26. [Fonction développable en série entière, analytique, entière]
- On dit que f est développable en série entière au voisinage de $z_0 \in \Omega$ s'il existe $r > 0$ et $(a_n)_{n\in\mathbb{N}}$ tels que $\mathbb{D}_r(a) \subset \Omega$ et $f(z) = \sum_{n\geq 0} a_n (z - z_0)^n$ sur $\mathbb{D}_r(a)$,
- On dit que f est analytique sur Ω si elle est développable en série entière au voisinage de tout point de Ω,
- Si $\Omega = \mathbb{C}$, f est dite entière si elle est analytique.

Exemple 27. $\frac{1}{1-z} = \sum_{n\geq 0} z^n$ est développable en série entière en 0.

On supposera dans la suite f analytique.

Proposition 28. *Si f admet un développement en série entière sur $\mathbb{D}_R(0)$ autour de 0, alors pour tout $z_0 \in \mathbb{D}_R(0)$, le développement en série entière de f en z_0 a un rayon de convergence au moins égal à $R - |z_0|$ et coïncide avec f sur $\mathbb{D}_{R-|z_0|}(z_0)$.*

Théorème 29. [Formule de Cauchy]
Pour tout $r \in]0, R[$ et $n \in \mathbb{N}$, on a $2\pi r^n a_n = \int_0^{2\pi} f(r\,\mathrm{e}^{i\theta})\,\mathrm{e}^{-ni\theta}\, d\theta$.

Théorème 30. [Théorème des zéros isolés]
Si $f : \Omega \longrightarrow \mathbb{C}$ est non nulle, l'ensemble des zéros de f n'admet pas de point d'accumulation.

Corollaire 31. [Unicité du développement en série entière]
Deux séries entières sont égales si et seulement si leurs coefficients sont égaux.

Corollaire 32. [Théorème de Liouville]
Une fonction entière est bornée si et seulement si elle est constante.

Application 33. Une fonction entière telle que $\forall z \in \mathbb{C}, |f(z)| \leq P(|z|)$ où $P \in \mathbb{R}_+[X]$ est un polynôme de degré inférieur à $\deg(m)$.
Une fonction entière qui évite deux valeurs est constante **[Petit théorème de Picard]**.

Proposition 34. [Holomorphie]
$g : \Omega \longrightarrow \mathbb{C}$ est holomorphe si et seulement si elle est analytique.
Dans ce cas, on a pour tout $z_0 \in \Omega$, $g(z) = \sum_{n\geq 0} \frac{g^{(n)}(z_0)}{n!}(z - z_0)^n$ au voisinage de z_0.

III. B. Sur $\mathbb{R}$

Dans le cas réel, le développement en série entière est beaucoup moins puissant. En effet :

Exemple 35. Une fonction $\mathcal{C}^\infty$ peut ne pas être développable en série entière en un point. Considérer par exemple en 0 la fonction $f : x \longrightarrow \mathrm{e}^{-1/x^2}\mathbb{1}_{x>0}$.

Théorème 36. *[RDO98] Si f est $\mathcal{C}^\infty$ sur un voisinage de 0, alors f est développement en série entière en 0 si et seulement si il existe $\alpha > 0$ tel que $]-\alpha,\alpha[\subset I$ et $\forall x \in]-\alpha,\alpha[, R_n(x) = f(x) - \sum_{k=0}^n \frac{f^{(k)}(x)}{k!}x^k \underset{n\to+\infty}{\longrightarrow} 0$.*

Théorème 37. [Théorème de Bernstein]
Soit $a > 0$ et $f :]-a,a[\longrightarrow \mathbb{R}$ une fonction $\mathcal{C}^\infty$ telle que pour tout entier k, $f^{(2k)} \geq 0$ sur $]-a,a[$. Alors f admet un développement en série entière sur $]-a,a[$.

IV. Applications

IV. A. Exponentielle complexe

[Rud98, Prologue, p1–4] [AF93, §VI.7, p226]

Définition 38. [Exponentielle, cosinus et sinus]
On définit les séries entières suivantes :

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

Proposition 39.
(i) $\exp, \sin, \cos$ 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,
(ii) Pour tout $z \in \mathbb{C}$, on $\exp(iz) = \cos(z) + i\sin(z)$,
(iii) Pour $\theta \in \mathbb{R}$, $\cos(\theta)$ et $\sin(\theta)$ sont réels et $\left|\mathrm{e}^{i\theta}\right| = 1$.
(iv) $\exp$ est un morphisme surjectif de $(\mathbb{C},+)$ dans $(\mathbb{C}^*,\times)$ de noyau $2i\pi\mathbb{Z}$.
(v) Pour $z_1, z_2 \in \mathbb{C}$, $\exp(z_1+z_2) = \exp(z_1)\exp(z_2)$,

Corollaire 40. [Formule de Moivre et d'Euler]
- *Pour $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$, on a $(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$.*
- *Pour $\theta \in \mathbb{R}$, on a $\cos(\theta) = \frac{\mathrm{e}^{i\theta}+\mathrm{e}^{-i\theta}}{2}$ et $\sin(\theta) = \frac{\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta}}{2i}$.*

Application 41. Développement de $\cos(n\theta)$ et $\sin(n\theta)$ par la formule de Moivre. Linéarisation de $\cos^n(\theta)$ et $\sin^n(\theta)$ par les formules d'Euler. Exemples de $\cos^5(\theta)$ et $\sin(5\theta)$. Polynômes de Tchebychev.

IV. B. Équations différentielles

[QZ13, §X.VI, p408/435] [Gou08, p245]

Il est souvent judicieux de rechercher des solutions particulières d'équations différentielles sous forme de série entière, notamment lorsque les fonctions coefficients sont des polynômes.

Théorème 42. *Soient $p(x) = \sum_{n\geq 0} p_n x^n$ et $q(x) = \sum_{n\geq 0} q_n x^n$ convergeant pour $x \in]-R,R[$ où $R > 0$. Alors pour tout $a_0, a_1 \in \mathbb{C}$, il existe une unique solution y sur $]-R,R[$ de $y'' + py' + qy = 0$ avec $y(0) = a_0$ et $y'(0) = a_1$, y étant développable en série entière.*

Application 43. Calcul des solutions de $y'' + xy = 0$ avec $y(0) = 1$ et $y'(0) = 0$, de $(1-x^2)y'' - xfy' = 2$ sur $]-1,1[$ ou de $2x(1-x)y' + (1-2x)y = 1$ sur $]0,1[$.

IV. C. Combinatoire : dérangements de n

[Rom17, Ch2, p53/73] [FGN07, §I.2–6, p6]

Définition 44. Pour $n \in \mathbb{N}^*$, on appelle dérangement de n une permutation de $[\![1,n]\!]$ sans point fixe. On note d_n le nombre de dérangements de n.

Proposition 45. *On a $\sum_{k=0}^n \binom{n}{k} d_k = n!$.*

Proposition 46. *Soit $f : z \longrightarrow \sum_{n\geq 0} \frac{d_n}{n!} z^n$.*
- *Le rayon de convergence de f est supérieur à 1,*
- *$x \longmapsto f(x)\exp(x)$ est développable en série entière sur $]-1,1[$ et on a $f(x) = \frac{\mathrm{e}^{-x}}{1-x}$,*
- *$d_n = n!\sum_{k=0}^n \frac{(-1)^k}{k!}$.*

IV. D. La fonction génératrice en probabilités

[Mé11, p62/188]

Définition 47. Soit X une variable aléatoire à valeurs dans $\mathbb{N}$. On définit sa fonction génératrice g_X par $g_X(s) = \mathbb{E}[s^X] = \sum_{n\in\mathbb{N}} \mathbb{P}(X=n)s^n$.

C'est une série entière de rayon de convergence supérieur ou égal à 1 et $g_X(1) = 1$.

Exemple 48. Fonctions génératrices de $\mathcal{B}(p), \mathcal{B}(n,p), \mathcal{P}(\lambda), \mathcal{G}(p)$.

Proposition 49. *X admet un moment d'ordre $p \in \mathbb{N}^*$ si et seulement si g_X est p fois dérivable en 1, et dans ce cas $G_X^{(p)}(1) = \mathbb{E}[X(X-1)\dots(X-p)]$.*

Proposition 50. *Si X et Y ont même fonction génératrice, elles ont même loi.*

Application 51. [Processus de branchement de Galton-Watson]
Soit $(Z_n)_{n\in\mathbb{N}}$ un processus de branchement de Galton-Watson de loi μ. Alors $g_{Z_n} = g_\mu^{\otimes n}$ pour tout $n \in \mathbb{N}$ et si $\mu \neq \delta_0$, on a $\mathbb{P}(\text{survie du processus}) > 0 \iff \mathbb{E}[\mu] > 1$.

ANNEXE

Schéma des différents types de convergences [BMP05, p48]
Schéma de Δ_α.
Principaux développements en série entière.

QUESTIONS

Q Quel critère est le plus fort : CAUCHY ou HADAMARD ?

Q Qu'en est-il de la composition de séries entières ?

Q Développement en série entière de $\arctan(x+a)$.

BIBLIOGRAPHIE

[AF93] J.M. ARNAUDIÈS et H. FRAYSSE : *Cours de mathématiques, Tome 1, Algèbre*. Dunod, 1993.

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Mé11] S. MÉLÉARD : *Aléatoire : introduction à la théorie et au calcul des probabilités*. Les éditions de l'École Polytechnique, 2011.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[RDO98] E. RAMIS, C. DESCHAMPS et J. ODOUX : *Cours de mathématiques 4, Séries et équations différentielles*. Dunod, 1998.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rud98] W. RUDIN : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

245 FONCTIONS HOLOMORPHES SUR UN OUVERT DE $\mathbb{C}$. EXEMPLES ET APPLICATIONS.

Soit Ω un ouvert de $\mathbb{C}$, et $f : \Omega \longrightarrow \mathbb{C}$.

I. Fonctions holomorphes

[Tau06, §3.4/Ch5, p39/58]

I. A. Holomorphie, différentiabilité, analycité

Fonction holomorphe

Exemple 1. Soit $f : z \longmapsto \frac{1}{z}$. Alors pour $z \in \mathbb{C}^*$, on a si $|h| < |z|$:

$$\frac{f(z+h)-f(z)}{h} = -\frac{1}{(z+h)z} \underset{|h|\to 0}{\longrightarrow} -\frac{1}{z^2}$$

Donc $f \in \mathcal{H}(\mathbb{C}^*)$.

Stabilité par somme, produit, composition, inverse, selon les hypothèses ...
Équations de Cauchy-Riemann, application : $f' = 0$ implique f contante sur U sur un connexe, puis f contante sur U correspond à $\Re(f)$ constante correspond à $|f|$ constante, etc
Fonction analytique (c'est-à-dire développable en série entière en tout point)

Définition 2. [Fonction développable en série entière, analytique, entière]
- On dit que f est développable en série entière au voisinage de $z_0 \in \Omega$ s'il existe $r > 0$ et $(a_n)_{n\in\mathbb{N}}$ tels que $\mathbb{D}_r(a) \subset \Omega$ et $f(z) = \sum_{n\geq 0} a_n (z-z_0)^n$ sur $\mathbb{D}_r(a)$,
- On dit que f est analytique sur Ω si elle est développable en série entière au voisinage de tout point de Ω,
- Si $\Omega = \mathbb{C}$, f est dite entière si elle est analytique.

Exemple 3. $\frac{1}{1-z} = \sum_{n\geq 0} z^n$ est développable en série entière en 0.

On supposera dans la suite f analytique.

Proposition 4. *Si f admet un développement en série entière sur $\mathbb{D}_R(0)$ autour de 0, alors pour tout $z_0 \in \mathbb{D}_R(0)$, le développement en série entière de f en z_0 a un rayon de convergence au moins égal à $R - |z_0|$ et coïncide avec f sur $\mathbb{D}_{R-|z_0|}(z_0)$.*

DSE implique holomorphe, relation entre les dérivées et les coefficients du DSE, exemple de l'exponentielle

I. B. Application : détermination continue du logarithme

Définition 5.
- Un argument continu sur Ω est une application continue $\Theta : \Omega \longrightarrow \mathbb{R}$ telle que pour tout $z \in \Omega$, $\frac{z}{|z|} = \varepsilon \circ \Theta(z)$.
- Un logarithme continu sur Ω est une application continue $\ell : \Omega \longrightarrow \mathbb{C}$ telle que pour tout $z \in \Omega$, $z = \exp \circ \ell(z)$.

Proposition 6. *Soit $\Omega = \mathbb{C} \setminus \mathbb{R}_-$.*
- *Il existe un argument continu Θ sur Ω. Si on suppose de plus Θ à valeurs dans $]-\pi, \pi[$, on a alors unicité et on appelle Θ la détermination principale de l'argument,*
- *Il existe un logarithme continu sur Ω.*

Application : détermination continue de z^α

II. Intégrales sur des chemins

[Tau06, Ch6, p67]

II. A. Définitions

Arcs, chemins, intégrales le long d'un chemin, exemples de $z \longmapsto z$, $z \longmapsto \overline{z}$, $z \longmapsto z^{-1}$
L'intégrale est invariante par chemins équivalents, opposée par chemin opposé

II. B. Théorie de Cauchy

f continue admet une primitive sur Ω si et seulement si pour tout chemin fermé, $\int_\gamma f(z)dz = 0$
Sur un convexe, f admet une primitive dès que $\int_T f(z)dz = 0$ pour tout triangle
Théorème de Goursat, formule de Cauchy 1 : $\int_\gamma f(z)dz = 0$
Lemme de l'indice, exemple (en annexe)
Formule de Cauchy 2, exemples

Corollaire 7. *Une fonction holomorphe est analytique. Plus précisément si $\mathbb{D}(z_0, R) \subset U$ et f est holomorphe sur U alors f est développable en série entière sur $\mathbb{D}(z_0, R)$ et on a pour tout chemin γ d'indice 1 en z_0 :*

$$\forall n \in \mathbb{N}, \frac{f^{(n)}(z_0)}{n!} = \frac{1}{2i\pi}\int_\gamma \frac{f(s)}{(s-z_0)^{n+1}} ds$$

En particulier f est $\mathcal{C}^\infty$
Dans le cas réel, le développement en série entière est beaucoup moins puissant. En effet :

Exemple 8. Une fonction $\mathcal{C}^\infty$ peut ne pas être développable en série entière en un point. Considérer par exemple en 0 la fonction $f : x \longrightarrow \mathrm{e}^{-1/x^2}\mathbb{1}_{x>0}$.

Inégalité de Cauchy

III. Propriétés des fonctions holomorphes [Tau06, Ch7, p84]

III. A. Propriétés liées à l'analycité et/ou l'holomorphie

Formule de la moyenne, principe du maximum
Lemme de Schwarz, automorphismes du disque

Théorème 9. [théorème des zéros isolés]
Si $f : \Omega \longrightarrow \mathbb{C}$ est non nulle, l'ensemble des zéros de f n'admet pas de point d'accumulation.

Théorème de Liouville

III. B. Convergence de suites de fonctions holomorphes [BMP05, §2.7, p82]

Convergence uniforme sur tout compact implique fonction limite holomorphe

Théorème 10. [holomorphie sous le signe intégrale]
Supposons que U est un ouvert Ω de $\mathbb{C}$ et $f : \Omega \times E \longrightarrow \mathbb{C}$ tels que :
- *pour tout $z \in \Omega$, $x \longmapsto f(z,x)$ est mesurable sur E,*
- *pour μ-presque tout x, $u \longmapsto f(z,x)$ est holomorphe sur Ω,*
- *il existe g intégrable telle que pour tout $z \in \Omega$, $|f(z,x)| \leq g(x)$ μ- p.p..*

Alors F est holomorphe sur Ω et pour tout $k \geq 0$, $F^{(k)} : z \longmapsto \int_E \frac{\partial^k f}{\partial z^k}(z,x)d\mu(x)$.

Prolongement des fonctions holomorphes (par le théorème des zéros isolés)

Exemple 11. Γ est holomorphe sur $\{\Re(z) > 0\}$.

Application 12. Γ admet un unique prolongement méromorphe sur $\mathbb{C}$, holomorphe sur $\mathbb{C} \setminus -\mathbb{N}$. Celui-ci ne s'annule pas et de plus $1/\Gamma$ est une fonction entière.

IV. Fonctions méromorphes [Tau06, Ch8, p98]

IV. A. Singularités isolées

Singularité isolée, 3 cas possibles, tous distincts
Pôle simple, pôle multiple, résidu, exemples
Fonction méromorphe

IV. B. Calculs d'intégrales

Théorème 13. [théorème des résidus]
Soit U un ouvert convexe ou étoilé (ou simplement convexe). Soit f méromorphe sur U. On note P l'ensemble de pôles de f. Alors pour $\gamma : [0,1] \longrightarrow U \setminus P$ chemin fermé, on a :

$$\frac{1}{2i\pi}\int_\gamma f(z)dz = \sum_{a\in P} \mathrm{Res}(f,a)\ \mathrm{Ind}(\gamma,a)$$

Application 14. Pour $\alpha \in \mathbb{R}_+^*$, on a $\int_{\mathbb{R}_+} \exp(-x^2)\cos(\alpha x)dx = \frac{\sqrt{\pi}}{2}\exp(-\alpha^2/4)$.

Application 15. On retrouve $\int_{\mathbb{R}} \frac{1}{1+x^2}dx = \pi$ ou $\int_0^{2\pi} \frac{\sin(x)}{x}dx = \frac{\pi}{2}$.

Exemple 16. Soit $-1 < \alpha < 1$. Alors $I_\alpha = \displaystyle\int_0^{+\infty} \frac{x^\alpha \ln(x)}{x^2-1}dx = \frac{\pi^2}{4\cos^2(\frac{\pi}{2}\alpha)}$.

Autres exemples

ANNEXE

Exemples de contours, dessins d'indices

SPEECH

On étend la notion de dérivée pour des fonctions de variables complexes. En fait cette nouvelle notion va donner une structure extrêmement forte qui va découler sur toute une théorie.

COMMENTAIRES

C'est une leçon vaste, rester sur ce que l'on maitrise.

QUESTIONS

Q Soit $f : t \longmapsto 1/(1+t^2)$. f est la restriction d'une fonction holomorphe sur un voisinage de $\mathbb{R}$. Pourquoi le rayon de convergence n'est pas infini ?

R $\pm i$ sont pôles.

Q Quelle est la caractérisation géométrique d'une fonction holomorphe ?

R La différentielle d'une fonction holomorphe préserve les angles.

Q Interprétation géométrique de l'indice ?

Q Soit $(f_n)_n$ une suite de fonctions holomorphes convergeant vers f holomorphe, telle que les $(f_n)_n$ ne s'annulent pas. Que dire de f ?

R f est soit nulle, soit ne s'annule pas. Supposons f non nulle.
En admettant la formule $N = \frac{1}{2i\pi}\int \frac{f'(z)}{f(z)}dz$ le nombre de 0 dans l'ouvert délimité par γ tel que f ne s'annule pas sur γ.
Si a est un zéros de f, on prend un chemin autour de γ et $N_n = 0$ pour tout n puisque les $(f_n)_n$ ne s'annulent pas. Par convergence uniforme, $N_n \longrightarrow N$ donc $N = 0$. Absurde.
Il faut vérifier la convergence uniforme sur tout compact de $\frac{f_n'}{f_n}$ vers $\frac{f'(z)}{f(z)}$, on utilise les convergences uniformes de f_n' vers f' et de f_n vers f.

Q On rappelle le théorème de Baire : si (X,d) est métrique et les $(F_n)_n$ sont des fermés tels que $\mathbb{F}_n^\circ = \varnothing$, alors $(\cup_n F_n)^\circ = \varnothing$. Soit $f \in \mathcal{H}(\mathbb{C})$ telle que $\forall z \in \mathbb{C}, \exists n_0 \mid f^{(n)}(z) = 0$. Montrer que f est un polynôme.

R On a $\mathbb{C} = \cup_{n\geq 0} Z(f^{(n)})$. $Z(f^{(n)})$ est un fermé. Si $f^{(n)} \neq 0$ alors par le théorème des zéros isolés $Z(f^{(n)})$ est d'intérieur vide. Si c'est le cas pour tout n, par Baire on aurait $\mathbb{C} = \varnothing$. Donc $f^{(n_0)} = 0$ pour un n_0. Donc f est un polynôme.

BIBLIOGRAPHIE

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Tau06] P. Tauvel : *Analyse complexe pour la Licence 3*. Dunod, 2006.

246 SÉRIES DE FOURIER. EXEMPLES ET APPLICATIONS.

On note $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$, $e_n = \mathrm{e}^{in\cdot}$ pour $n \in \mathbb{Z}$. On définit lorsque cela a un sens $\langle f \mid g \rangle = \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{g(t)}dt$ et $\|f\|_1 = \sqrt{\langle f \mid f\rangle}$.

I. Coefficients et séries de FOURIER

[Gou08, §4.5, p256–270] [QZ13, ChIV, p68]

I. A. Séries trigonométriques et coefficients de FOURIER

Polynôme trigonométrique : polynôme en les $(e_n)_n$, coefficients c_n, a_n, b_n, liens entre les deux série trigonométrique, convergence normale dans certains cas

DÉFINITION 1. [COEFFICIENT DE FOURIER]
Pour $f \in L^1(\mathbb{T})$, on définit $c_n(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{-int}\,dt = \langle f \mid e_n\rangle$ le n-ième coefficient de FOURIER de f, où $n \in \mathbb{Z}$.

Coefficients $a_n(f), b_n(f)$, nuls quand f est paire ou impaire
Par inclusion des L^p, le coefficient de FOURIER est défini sur tout L^p, lien avec le produit scalaire sur L^2

EXEMPLE 2.

- $c_k(e_n) = \delta_{k,n}$
- Pour $f = \mathbb{1}_{]-a,a[}$ où $0 < a < \pi$, on a $c_n(f) = \begin{cases} a/\pi & \text{si } n = 0 \\ \sin(na)/n\pi & \text{sinon} \end{cases}$.
- Pour $f : x \longmapsto 1 - \frac{x^2}{\pi^2}$, on a $c_n(f) = \begin{cases} 1 & \text{si } n = 0 \\ \frac{2(-1)^n}{\pi^2 n^2} & \text{sinon} \end{cases}$.

PROPOSITION 3. *Pour $f, g \in L^1(\mathbb{T})$, on a :*
(i) $c_n(\overline{f}) = \overline{c_{-n}(f)}$,
(ii) $c_n(\tau_a f) = \mathrm{e}^{ina}\,c_n(f)$,
(iii) $f * e_n = c_n(f)e_n$,
(iv) si $f \in \mathcal{C}(\mathbb{T}) \cap \mathcal{C}^1_{pm}(\mathbb{T})$, *on a* $c_n(f') = inc_n(f)$.
(v) $c_n(f * g) = c_n(f)c_n(g)$,

LEMME 4. [LEMME DE RIEMANN-LEBESGUE]
Si $f \in L^1(\mathbb{T})$, *alors* $c_n(f) \underset{n\to+\infty}{\longrightarrow} 0$.

$\mathcal{F} : \mathcal{C}(\mathbb{T}) \longrightarrow c_0(\mathbb{Z}), f \longmapsto (c_n(f))_{n\in\mathbb{Z}}$ est linéaire, de norme 1

I. B. Séries de FOURIER et noyaux trigonométriques

Série de FOURIER associée à f

DÉFINITION 5. [SOMME PARTIELLES DE FOURIER, DE FEJÉR]
On appelle somme partielle de FOURIER d'ordre $N \in \mathbb{N}$ la quantité $S_N(f) = \sum_{n=-N}^{N} c_n(f)e_n$.
On appelle somme partielle de FEJÉR d'ordre $N \in \mathbb{N}$ la quantité $\sigma_N(f) = \frac{1}{N}\sum_{n=0}^{N-1} S_N(f)$.

REMARQUE 6. Dans l'espace de HILBERT L^2, $S_N(f)$ est la projection sur $\mathcal{P}_N = \mathrm{Vect}((e_n)_{-N\le n\le N})$.

Exemple : si f est un polynôme trigonométrique

DÉFINITION 7. [NOYAUX DE DIRICHLET, DE FEJÉR]
On appelle noyau de DIRICHLET à l'ordre $N \in \mathbb{N}$ la fonction $D_N = \sum_{n=-N}^{N} e_n$.
On appelle noyau de FEJÉR à l'ordre $N \in \mathbb{N}$ la fonction $K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n = \sum_{n=-N}^{N}(1 - |n|/N)e_n$.

PROPOSITION 8. *On a les propriétés suivantes :*

D1) $S_N(f) = f * D_N$,
D2) D_N *est pair et* $\|D_N\|_1 = 1$,
D3) $\forall x \in \mathbb{T}, D_N(x) = \frac{\sin\left(\frac{2N+1}{2}x\right)}{\sin(x/2)}$,

F1) $\sigma_N(f) = f * K_N$,
F2) $\|K_N\|_1 = 1$,
F3) $\forall x \in \mathbb{T}, K_N(x) = \frac{1}{N}\frac{\sin^2(Nx/2)}{\sin^2(x/2)} \ge 0$,
F4) $\forall \delta \in]0,\pi], \int_{\delta\le|t|\le\pi} K_N(t)dt \underset{N\to+\infty}{\longrightarrow} 0$.

II. Convergences des séries de FOURIER

[QZ13, ChIV, p68] [Gou08, ChIV.5] [BMP05, Ch3.3, p122]

II. A. Convergence au sens de CESÀRO

THÉORÈME 9. [THÉORÈME DE FEJÉR]

- *Soit* $f \in \mathcal{C}(\mathbb{T})$. *Alors* $\|\sigma_N(f)\|_\infty \le \|f\|_\infty$ *pour tout* $N \ge 1$ *et* $\sigma_N(f) = f * K_N \underset{N\to+\infty}{\overset{u}{\longrightarrow}} f$.
- *Soit* $f \in L^p(\mathbb{T})$ *pour un* $p \in [1, +\infty[$. *Alors* $\|\sigma_N(f)\|_p \le \|f\|_p$ *pour tout* $N \ge 1$ *et* $\lim_{N\to+\infty}\|\sigma_N(f) - f\|_p = 0$.

Applications :

- si f est continue et $S_N(f)(x_0) \longrightarrow \ell$, alors $\ell = f(x_0)$,
- si f est continue et si $S_N(f)$ converge uniformément alors elle converge vers f,

- théorème de Weierstrass
- injectivité de $\mathcal{F} : \mathcal{C}(\mathbb{T}) \longrightarrow c_0(\mathbb{Z}), f \longmapsto (c_n(f))_{n\in\mathbb{Z}}$.

Exemple : fonction triangle

II. B. Convergence en moyenne quadratique

Inégalité de Bessel

Théorème 10. *$(e_n)_{n\in\mathbb{Z}}$ est une base hilbertienne de $L^2(\mathbb{T})$. En particulier, pour $f \in L^2(\mathbb{T})$:*

$$f = \sum_{n\in\mathbb{Z}} c_n(f)e_n \qquad \text{et} \qquad \|f\|_{L^2}^2 = \sum_{n\in\mathbb{Z}} |c_n(f)|^2$$

Applications :

- deux fonctions L^1 ayant mêmes coefficients de Fourier sont égales p.p.
- convolution : si $f \in L^2$, alors $f * f = \sum_n c_n(f)^2\, \mathrm{e}_n$
- $\mathcal{F}$ est une isométrie bijective

Exemple : fonction signal : valeur au point limite $1/2$

II. C. Convergence ponctuelle et uniforme

[Bre99, II.1, p16–17] [Gou08, An. A, p404–405]

Contre-exemple si f n'est pas continue

Théorème 11. [Théorème de Banach-Steinhaus]
Soit E un espace de Banach et F un espace vectoriel normé. Soit $(u_i)_{i\in I}$ une famille d'applications de $\mathcal{L}_c(E,F)$ simplement bornée (c'est-à-dire $\forall x \in E, \sup_{i\in I} \|u_i(x)\| \leq +\infty$). Alors $\sup_{i\in I} |||u_i||| < +\infty$.

Application 12. Existence d'une fonction continue 2π-périodique telle que sa série de Fourier diverge en 0.

Théorème 13. [Théorème de Jordan-Dirichlet]
Si f est $L^1(\mathbb{T})$ et telle qu'en x_0 elle admet limite à droite et à gauche, et si $h = \ldots$ est bornée au voisinage de 0, alors $S_N(f)(x_0) \longrightarrow \frac{1}{2}(f(x_0^+) + f(x_0^-))$

Corollaire 14. [Théorème de Dirichlet]
Si $f \in \mathcal{C}(\mathbb{T}) \cap \mathcal{C}^1_{pm}(\mathbb{T})$, alors $(S_N(f))_{N\in\mathbb{N}}$ converge normalement vers f.

III. Applications

III. A. Calcul de séries

[Gou08, §IV.5, p256] [QZ13, ChIV, p68]

Application 15. [Calculs de séries]
On peut reprendre l'Exemple 2 pour calculer les normes des applications dans L^2 : pour $a \in [\![0, 2\pi]\!]$: $\sum_{n\in\mathbb{N}^*} \frac{\sin(na)}{n} = \frac{\pi-a}{2}$ (première fonction) et $\sum_{n\in\mathbb{N}^*} \frac{1}{n^4} = \frac{\pi^4}{90}$ (deuxième fonction).
On peut aussi calculer classiquement $\sum_{n\in\mathbb{N}^*} \frac{1}{n^2} = \frac{\pi^2}{6}$ et $\sum_{n\in\mathbb{N}^*} \frac{1}{(2n-1)^2} = \frac{\pi^2}{8}$.

III. B. Formule de Poisson

[Gou08, §IV.5/IV.6, p256/273] [FGN07, §4.16/17, p304–308]

Proposition 16. [Formule sommatoire de Poisson]
Soit $f : \mathbb{R} \longrightarrow \mathbb{C}$ une fonction $\mathcal{C}^1$ telle que $f(x) = O(1/x^2)$ et $f'(x) = O(1/x^2)$ en $\pm\infty$. Alors les sommes suivantes sont bien définies et on a :

$$\forall x \in \mathbb{R}, \sum_{n\in\mathbb{Z}} f(x+2n\pi) = \frac{1}{2\pi} \sum_{n\in\mathbb{Z}} \hat{f}(n)\, \mathrm{e}^{inx} \qquad \text{où } \hat{f}(n) = \int_{\mathbb{R}} f(t)\, \mathrm{e}^{-int}\, dt$$

Application 17. [Équation fonctionnelle de la fonction de Jacobi]
Pour $s > 0$, $\Theta(x) = \sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n^2 s}$ vérifie $\Theta(s) = \frac{1}{\sqrt{s}}\Theta(\frac{1}{s})$.

III. C. Equation de la chaleur périodique [FGN12, §1.28, p49] [QZ13, §IV.VI.3, p105]

Théorème 18. [Équation de la chaleur périodique]
Soit $u_0 : \mathbb{R} \longrightarrow \mathbb{R}$ non identiquement nulle, 2π-périodique continue et $\mathcal{C}^1_{pm}$. Alors il existe une unique solution $u \in \mathcal{C}^0(\mathbb{R}_+ \times \mathbb{R}) \cap \mathcal{C}^\infty(\mathbb{R}_+^* \times \mathbb{R})$ telle que :

$$\begin{cases} \partial_t u = \partial_{xx}^2 u & \text{sur } \mathbb{R}_+^* \times \mathbb{R} \\ u(0,.) = u_0 & \text{sur } \mathbb{R} \end{cases}$$

ANNEXE

Fonction signal, triangle

SPEECH

Historiquement introduction pour l'étude des fonctions périodiques. Mais pas de réelle justification de la convergence des séries, ce que l'on voudrait étudier ici.

COMMENTAIRES

Attention à bien préparer les exemples, et à ne pas trop se disperser dans plusieurs livres avec plusieurs notations.
Ne pas justifier l'intérêt des séries de FOURIER par le calcul de sommes (juste le signaler rapidement).

QUESTIONS

Q À quoi correspond $S_N(f)$?

R C'est une projection sur l'espace vectoriel engendré par $\mathrm{e}_{-N}, \dots, \mathrm{e}_N$.

Q Pourquoi le noyau de FEJÉR fonctionne-t-il mieux que celui de DIRICHLET ?

Q Si f est $\mathcal{C}^0_{2\pi} \cap \mathcal{C}^1_{pm}$, a-t-on convergence normale de la série de FOURIER ?

R On a puisque $f' \in L^2$:

$$\sum_{n\in\mathbb{Z}} |c_n(f)| = \sum_{n\in\mathbb{Z}} \frac{|c_n(f')|}{n} \leq \left(\sum_n |c_n(f')|^2\right)^{1/2} (\sum_n \frac{1}{n^2})^{1/2} \leq \left(\sum_n |c_n(f')|^2\right)^{1/2} \|f\|_2^2$$

On en déduit $\sum_{|n|\geq N} |c_n(f)| \leq \frac{2C\|f'\|_2}{\sqrt{N}}$. On a même $\sum_{|n|\geq N} |c_n(f)| = o(1/\sqrt{N})$.

Q Si l'on remplace $\mathcal{C}^1$ par $\mathcal{C}^k$, qu'obtient-on ?

R On va trouver $o(1/\sqrt{N^{2k-1}})$.

Q Soit $f \in \mathcal{C}^0_{2\pi}$ avec $c_n(f) \in \mathbb{R}_+$ pour tout $n \in \mathbb{Z}$. A-t-on convergence de $S_N(f)$?

R Si $S_N(f)(0) \underset{N\to+\infty}{\longrightarrow} +\infty$, alors $\sigma_N(f)(0) \underset{N\to+\infty}{\longrightarrow} +\infty$: c'est absurde.

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bre99] H. BREZIS : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 2*. Cassini, 2007.

[FGN12] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[QZ13] H. QUEFFÉLEC et C. ZUILY : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

250 TRANSFORMATION DE FOURIER. APPLICATIONS.

I. Transformée de FOURIER sur $L^1(\mathbb{R}^d)$ [BP15, Ch15, p315] [Rud98, Ch9, p219]

DÉFINITION 1. Pour $f \in L^1(\mathbb{R}^d)$, on définit sa transformée de FOURIER par :

$$\mathcal{F}(f) : \zeta \longmapsto \hat{f}(\zeta) = \int_{\mathbb{R}^d} f(x)\, \mathrm{e}^{-i\langle x|\zeta\rangle dx}$$

DÉFINITION 2. Pour $f \in L^1(\mathbb{R}^d)$, on note $\check{f}$ l'application $x \longmapsto f(-x)$.

PROPOSITION 3. *$\mathcal{F}$ est linéaire et pour $f \in L^1(\mathbb{R}^d)$, $\hat{f}$ est uniformément continue et bornée.*

THÉORÈME 4. [LEMME DE RIEMANN-LEBESGUE]
Si $f \in L^1(\mathbb{R}^d)$ alors $\hat{f} \in \mathcal{C}_0(\mathbb{R}^d)$.

PROPOSITION 5. *Soient $f, g \in L^1(\mathbb{R}^d)$.*
(i) $\hat{\check{f}} = \check{\hat{f}} = \check{f}$,
(ii) $\mathcal{F}(f \star g) = \mathcal{F}(f)\mathcal{F}(g)$,
(iii) Si τ_h est l'opérateur de translation par $h \in \mathbb{R}^d$ alors $\mathcal{F}(\tau_h f)(\zeta) = \mathrm{e}^{-i\langle h|\zeta\rangle}\, \mathcal{F}(f)(\zeta)$.
(iv) Pour $\lambda > 0$, $\mathcal{F}(f(./\lambda)) = \lambda \hat{f}(\lambda.)$

Exemple de convolution : $f = \mathbb{1}_{[-1,1]} \star \mathbb{1}_{[-1,1]}$ donne $\hat{f} = 4\,\mathrm{sinc}^2$

APPLICATION 6. La transformée de FOURIER d'une gaussienne est une gaussienne. On a $\hat{G}_\sigma : \zeta \longmapsto \mathrm{e}^{-\frac{\sigma^2\zeta^2}{2}}$.

Convolution, approximation de l'unité

PROPOSITION 7. *$\mathcal{F} : L^1(\mathbb{R}^d) \longrightarrow \mathcal{C}_0(\mathbb{R}^d)$ est injective et continue.*

Inversion de FOURIER L^1

EXEMPLE 8. On a $\mathcal{F}(\mathrm{e}^{-|x|}) : \zeta \longmapsto \frac{2}{1+\zeta^2}$. On en déduit que $\mathcal{F}(\frac{1}{1+x^2}) : \zeta \longmapsto \pi\, \mathrm{e}^{-|\zeta|}$.

Inversion ponctuelle

II. Régularité de la transformée de FOURIER, prolongement à $L^2(\mathbb{R}^d)$ [BP15, Ch15, p315] [Rud98, Ch9, p219]

DÉFINITION 9. [CLASSE DE SCHWARTZ]
On définit la classe de SCHWARTZ sur $\mathbb{R}^d$, notée $\mathcal{S}(\mathbb{R}^d)$, comme l'ensemble des fonctions $f \in \mathcal{C}^\infty(\mathbb{R}^d)$ telles que :

$$\forall p \in \mathbb{N}, N_p(f) = \sup_{|\alpha|\leq p, |\beta|\leq p} \sup_{x\in\mathbb{R}^d} \left|x^\beta \partial^\alpha f(x)\right| < +\infty$$

On munit cet espace de la famille dénombrable de semi-normes $(N_p)_{p\in\mathbb{N}}$, il est donc métrisable (espace de FRÉCHET).

EXEMPLE 10. $\mathcal{C}_c^\infty(\mathbb{R}^d) \subset \mathcal{S}(\mathbb{R}^d)$ et $G_\sigma \in \mathcal{S}(\mathbb{R}^d)$.

PROPOSITION 11. *Pour $f \in \mathcal{S}(\mathbb{R}^d)$, on a $\hat{f} \in \mathcal{S}(\mathbb{R}^d)$.*

PROPOSITION 12. *$\mathcal{S}(\mathbb{R}^d)$ est complet et s'injecte continument dans les $L^p(\mathbb{R}^d)$, dans lesquels il est dense pour $p < +\infty$.*

PROPOSITION 13. *$\mathcal{S}(\mathbb{R}^d)$ est stable par dérivation, multiplication interne, multiplication par un polynôme (ces opérations étant continues).*

PROPOSITION 14. *Pour $\alpha, \beta \in \mathbb{N}^n$ et $f \in \mathcal{S}(\mathbb{R}^d)$, on a :*

$$\forall \zeta \in \mathbb{R}^d, \quad \mathcal{F}(\partial^\alpha f)(\zeta) = i^{|\alpha|}\zeta^\alpha \mathcal{F}(f)(\zeta) \quad \text{et} \quad \mathcal{F}(.^\beta f)(\zeta) = i^{|\beta|}\partial^\beta \mathcal{F}(f)(\zeta)$$

COROLLAIRE 15. [INVERSION DE FOURIER DANS $\mathcal{S}(\mathbb{R}^d)$]
$\mathcal{F} : \mathcal{S}(\mathbb{R}^d) \longrightarrow \mathcal{S}(\mathbb{R}^d)$ est un automorphisme continu et on a $\mathcal{F}^{-1} : f \longmapsto \frac{1}{(2\pi)^d}\mathcal{F}(\check{f})$.

PROPOSITION 16. *Si $f, g \in \mathcal{S}(\mathbb{R}^d)$ alors*

$$\int_{\mathbb{R}^d} f(x)\hat{g}(x)dx = \int_{\mathbb{R}^d} \hat{f}(x)g(x)dx$$

Théorème 17. [Théorème de Fourier-Plancherel]
$\mathcal{F}$ se prolonge en un unique opérateur linéaire (toujours noté $\mathcal{F}$) de $L^2(\mathbb{R}^d)$ dans lui-même vérifiant :
- $\mathcal{F} \circ \mathcal{F} = (2\pi)^d \check{\mathrm{Id}}$,
- *Pour* $f \in L^2(\mathbb{R})^d$, $\|f\|_{L^2}^2 = \frac{1}{(2\pi)^d} \left\|\hat{f}\right\|_{L^2}^2$,
- *Pour* $f, g \in L^2(\mathbb{R}^d)$, $\int_{\mathbb{R}^d} f(x)\overline{g}(x)dx = \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} \hat{f}(x)\overline{\hat{g}}(x)dx$.

Remarque 18. La définition de $\mathcal{F}$ ci-dessus coïncide avec celle sur L^1, il n'y a donc pas d'ambiguïté.

Exemple 19. On calcule $\widehat{\mathbb{1}_{[-1,1]}} : \zeta \longmapsto 2\,\mathrm{sinc}(\zeta)$. Les deux fonctions étant $L^2(\mathbb{R})$, on en déduit que $\widehat{\mathrm{sinc}} = \pi \mathbb{1}_{[-1,1]}$.

III. Applications

III. A. Fonction caractéristique en probabilités

[Ouv09, §12.2, p197] [BL07, §III.5, p61]

Soit X une variable aléatoire à valeurs dans $\mathbb{R}^d$.

Définition 20. [Fonction caractéristique]
On définit ϕ_X la fonction caractéristique de X par $\phi_X(\lambda) = \mathbb{E}\left[\mathrm{e}^{i\langle\lambda|X\rangle}\right]$ pour $\lambda \in \mathbb{R}^d$.

Exemple 21. Fonctions caractéristiques de $\mathcal{B}(n,p), \mathcal{E}(\lambda)\ldots$ **[voir annexe]**

Exemple 22. $\phi_{\mathcal{N}(0,\sigma^2)} : \zeta \longmapsto \mathrm{e}^{-\frac{\sigma^2\zeta^2}{2}}$.

Proposition 23. *ϕ_X caractérise $\mathbb{P}_X$.*

Application 24. [Loi multinomiale poissonnifiée]
Soient $(p_j)_{1\le j\le d}$ des réels positifs tels que $\sum_{1\le j\le d} p_j = 1$. Soient $(Y^k)_{k\ge1}$ des variables aléatoires indépendantes et identiquement distribuées telles que $\mathbb{P}(Y^k = j) = p_j$. Soit N indépendante des $(Y^k)_{k\ge1}$ de loi $\mathcal{P}(\lambda)$ pour un $\lambda > 0$.
En posant $X^k = (\mathbb{1}_{Y^k=1}, \ldots, \mathbb{1}_{Y^k=d})$, la loi de $S = \sum_{k=1}^N X^k$ est $\mathcal{P}(\lambda p_1) \otimes \cdots \otimes \mathcal{P}(\lambda p_d)$.

Proposition 25. *Si X est réelle et admet un moment d'ordre p, alors ϕ_X est p fois dérivable et on a $\phi_X^{(p)}(\lambda) = i^p\mathbb{E}[X^p\,\mathrm{e}^{i\lambda X}]$. En particulier, $\phi^{(p)}(0) = i^p\mathbb{E}[X^p]$.*

Remarque 26. Réciproquement, si p est pair est ϕ_X est p fois dérivable en 0, alors X admet un moment d'ordre p. On peut construire X n'admettant pas d'espérance mais telle que ϕ_X soit dérivable en 0 (admis).

Caractérisation de l'indépendance de variables aléatoires, exemple
Théorème de Lévy

Théorème 27. [Théorème central limite]
Si les $(X_i)_{i\in\mathbb{N}^*}$ sont i.i.d. de carré intégrable, alors :

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n (X_i - \mathbb{E}[X_1]) \xrightarrow[n\to+\infty]{\mathcal{L}} Z \sim \mathcal{N}(0, \mathrm{Var}(X_1))$$

Application 28. [Intervalle de confiance asymptotique] [RS12, §3.4, p25]
Soient $(X_i)_{i\in\mathbb{N}^*}$ des réalisations i.i.d. de $\mathcal{B}(p)$ pour un $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\hat{p}_n = \frac{1}{n}\sum_{k=1}^n X_i : \mathrm{IC}_\alpha(p) = \left[\hat{p}_n \pm \frac{q_{1-\alpha/2}}{2}\frac{1}{\sqrt{n}}\right]$, où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Théorème central limite poissonien

III. B. Vers la résolution d'EDP

[Bon01, §9.6, p184]

Transformée de Fourier partielle.

Application 29. [Résolution d'EDP]
- On considère l'équation de la chaleur $\partial_t u = \partial_x^2 u$ avec condition initiale $f \in \mathcal{S}(\mathbb{R}^d)$. Alors il existe une unique solution $u \in \mathcal{C}^2(\mathbb{R}\times\mathbb{R}^d)$ telle que $u(t,.) \in \mathcal{S}(\mathbb{R}^d)$ uniformément en t sur tout compact et $u(t,.) \xrightarrow[t\to0]{} f$ dans L^1. Cette solution est donnée par :

$$\forall t>0, \forall x\in\mathbb{R}^d, u(t,x) = \frac{1}{(4\pi t)^{d/2}}\int_{\mathbb{R}^d} f(y)\,\mathrm{e}^{-\frac{|x-y|^2}{4t}}\,dy = f\star k_t(x) \quad \text{où } k_t = \frac{1}{(4\pi t)^{d/2}}\,\mathrm{e}^{-\frac{|.|^2}{4t}}$$

- On considère l'équation de Schrödinger $\partial_t u = i\partial_x^2 u$ avec condition initiale $f \in \mathcal{S}(\mathbb{R})$. Cette équation possède une unique solution $u \in \mathcal{C}^2(\mathbb{R}\times\mathbb{R})$ telle que pour tout t, $u(t,.) \in \mathcal{S}(\mathbb{R})$ uniformément en t sur tout compact. On a :

$$\forall t>0, \forall x\in\mathbb{R}^d, u(t,x) = \frac{1}{2\pi}\int_{\mathbb{R}} \hat{f}(\zeta)\,\mathrm{e}^{-i\zeta^2 t}\,\mathrm{e}^{ix\zeta}\,d\zeta$$

III. C. Polynômes orthogonaux

[BMP05, §3.4, p140]

THÉORÈME 30. [BASE HILBERTIENNE DE POLYNÔMES ORTHOGONAUX]
Soit ρ une fonction de poids. S'il existe $\alpha > 0$ tel que $\int_I \mathrm{e}^{\alpha|x|}\,\rho(x)dx < +\infty$, alors la famille $(P_n)_{n\in\mathbb{N}}$ est une base hilbertienne de $L^2(I,\rho)$.

EXEMPLE 31. Sans l'hypothèse on a le contre-exemple suivant : soit la fonction de poids $w : x \longmapsto x^{-\ln(x)}$ sur $I = \mathbb{R}_+$. Alors $(P_n)_{n\in\mathbb{N}}$ ne forme pas une base de $L^2(I,w)$.

ANNEXE

Quelques fonctions et leur transformée de FOURIER
Fonctions caractéristiques usuelles

COMMENTAIRES

Les points forts de la transformée de FOURIER :
- son injectivité sur les espaces sur lesquels elle est définie,
- la formule d'inversion sous certaines hypothèses,
- la simplification des calculs dans le domaine de FOURIER (typiquement, permutations des propriétés de convolution et de produit, équations dérivées partielles deviennent des équations différentielles ordinaires, …).

L'intérêt de la transformée de FOURIER est donc de simplifier des calculs, via le troisième point, mais pour que cela soit un minimum intéressant, les deux premiers points sont nécessaires, on ne pourrait pas faire grand chose d'autre sinon !
Le théorème d'échantillonnage de SHANNON utilise a priori plutôt la transformée de FOURIER mais on peut le voir comme une utilisation des séries de FOURIER. On montre que la suite des translatées du sinus cardinal est une base hilbertienne de l'espace considéré. Les calculs faits reviennent à développer en série de FOURIER la fonction $x \longmapsto \mathrm{e}^{-2i\pi ax}$, où $a \in \mathbb{R}$.

QUESTIONS

Q Théorème d'inversion ponctuelle, exemple ?

R Voir [BP15, Far00]. L'intérêt du théorème est surtout de faire l'analogie avec les séries de FOURIER.

Q Donner une fonction dans la classe de SCHWARTZ ? Pourquoi a-t-on densité de $\mathcal{S}(\mathbb{R}^d)$ dans L^2 ?

R Une gaussienne. $\mathcal{S}(\mathbb{R}^d)$ contient les fonctions $\mathcal{C}_K^\infty$, donc est dense dans L^2.

Q Avez-vous un exemple de fonctions $\mathcal{C}_K^\infty$?

R Voir l'exemple de suite régularisante.

Q Expliquer le principe de la marche aléatoire.

Q Soit $\mathbb{P}$ une probabilité sur $\mathbb{R}$. On considère $T : \mathcal{S} \longrightarrow \mathbb{R}, \varphi \longmapsto \int \varphi d\mathbb{P}$. Cette application est-elle une distribution ? Peut-on calculer sa transformée de FOURIER ? Quelle est le lien avec la fonction caractéristique ?

R L'application est linéaire et continue puisque $|\langle T \mid \varphi\rangle| \leq \|\varphi\|_\infty \leq N_0(\varphi)$.
On calcule $\hat{T} = T_{-\phi_X}$.

Q Soit $f_q : t \longmapsto \mathrm{e}^{-|t|^q}$ pour un entier $q \in \mathbb{N}$. Est-ce la transformée de FOURIER d'une certaine fonction ?

R La transformée de FOURIER de $1 \longmapsto 1 + x^2$ est f_1 (à une constante près).
Si $q \geq 3$, montrons que ce n'est pas une transformée de FOURIER. On a que f_q est $q-1$ fois dérivable en 0, elle a donc un moment d'ordre 2 égal à $f_q''(0) = 0$, par ailleurs $f_q'(0) = 0$, donc si X est une variable aléatoire de fonction caractéristique f_q, alors X est constante presque sûrement, égale à 0, et on vérifie que $\varphi_X = 1$, ce qui est absurde.

BIBLIOGRAPHIE

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bon01] J.-M. BONY : *Théorie des distributions et analyse de* FOURIER. Les éditions de l'École Polytechnique, 2001.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Far00] J. FARAUT : *Calcul intégral*. Belin, 2000.

[Ouv09] J.-Y. OUVRARD : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[RS12] V. RIVOIRARD et G. STOLTZ : *Statistique mathématique en action*. Vuibert, 2 ème édition, 2012.

[Rud98] W. RUDIN : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

253 UTILISATION DE LA NOTION DE CONVEXITÉ EN ANALYSE.

Soit E un $\mathbb{R}$-espace vectoriel normé.

I. Généralités autour de la convexité

[Gou08, §1.5/2.3, p51/94] [BMP05, §1.5.1, p26]

I. A. Ensembles et fonctions convexes

Définition 1. $A \subset E$ est convexe si $\forall a, b \in A, \forall t \in [0,1], (1-t)a + tb \in A$.

Exemple 2. Un intervalle de $\mathbb{R}$ est convexe, une boule de E est convexe.

Définition 3. $f : E \longrightarrow \mathbb{R}$ est dite
- convexe si $\forall a, b \in E, \forall t \in]0,1[, f((1-t)a+tb) \leq (1-t)f(a) + tf(b)$,
- strictement convexe si $\forall a, b \in E, \forall t \in]0,1[, f((1-t)a+tb) < (1-t)f(a) + tf(b)$,
- concave si $-f$ est convexe.

Exemple 4. Une application affine est convexe et concave.

Exemple 5. Toute norme $\|.\|$ de E est convexe, non strictement convexe dès que $E \neq \{0\}$.

Proposition 6. *$f : E \longrightarrow \mathbb{R}$ est convexe si et seulement si*
- *$E_f = \{(x,y) \in \mathbb{R}^2 \mid f(x) \leq y\}$ est convexe,*
- *$\forall n \in \mathbb{N}^*, \forall (a_1, \dots, a_n) \in E^n, \forall (t_1, \dots, t_n) \in (\mathbb{R}_+)^n \setminus \{0_{\mathbb{R}^n}\}, f(\mathrm{Bar}((a_i, t_i)_i)) \leq \mathrm{Bar}((f(a_i), t_i)_i))$.*

Proposition 7. *Soit $f : I \longrightarrow \mathbb{R}$ où I est un intervalle de $\mathbb{R}$. f est convexe si et seulement si :*
- *pour tout $a \in I$, $x \longmapsto \frac{f(x)-f(a)}{x-a}$ est croissante sur $I \setminus \{a\}$,*
- *pour tout $a, x \in I$, $f'(a)(x-a) + f(a) \leq f(x)$,*
- *f' est croissante,*
- *$f'' \geq 0$.*

les trois dernières équivalences ayant lieu lorsque f est assez régulière ($\mathcal{C}^1$ ou $\mathcal{C}^2$).

On déduit de la première équivalence qu'une fonction convexe sur I est continue sur $\mathring{I}$ et admet une dérivée à droite et à gauche en tout point de $\mathring{I}$.

Exemple 8. $\exp$ est convexe, $\log$ est concave.

Exemple 9. Fonction convexe non continue sur le bord : voir annexe.

I. B. Inégalités de convexité

Exemple 10. On a des inégalités provenant de la convexité/concavité de certaines fonctions :

$$\forall x \in \mathbb{R}, \mathrm{e}^x \geq 1 + x \qquad \forall y \in]-1, +\infty[, \ln(1+y) \leq y \qquad \forall \theta \in \left[0, \frac{\pi}{2}\right], \frac{2}{\pi}\theta \leq \sin(\theta) \leq \theta$$

Proposition 11. [Inégalité arithmético-géométrique]
Soient $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{R}_+$. Alors $\sqrt[n]{a_1 \dots a_n} \leq \frac{1}{n}\sum_{i=1}^n a_i$.

Exemple 12. On peut généraliser pour toute famille $a_1, \dots, a_n \in \mathbb{R}_+$ et $b_1, \dots, b_n \in \mathbb{R}_+^*$, on a

$$(a_1^{b_1} \dots a_n^{b_n})^{1/b} \leq \frac{1}{b}\sum_{i=1}^n b_i a_i \qquad \text{où} \quad b = \sum_{i=1}^n b_i$$

Proposition 13. [Inégalité de Young]
Soient $p, q > 0$ tels que $\frac{1}{p} + \frac{1}{q} = 1$. Alors pour tout $a, b \in \mathbb{R}_+$, on a $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$ avec égalité si et seulement si $a^p = b^q$.

II. Exemples d'applications dans certains espaces

II. A. Espaces de Hilbert

[BMP05, §3.1.2, p95] [Bre99, ChV/VIII, p79–82/136]

Soit $(H, \langle . \mid . \rangle)$ un espace de Hilbert.

Théorème 14. [Projection sur un convexe fermé]
Soit C un convexe fermé de Hilbert H. Alors :

$$\forall x \in H, \exists! p \in C \mid \|x - p\| = d(x, C)$$

De plus, p est l'unique élément de C satisfaisant $\forall c \in C, \Re(\langle x - p \mid c - p \rangle) \leq 0$.

Remarque 15. On a en fait juste besoin de C complet et H préhilbertien.

Exemple 16. Si C n'est pas convexe : soit $H = \mathbb{R}$ et $C = \mathbb{R} \setminus]-1, 1[$. Alors 1 et -1 minimisent la distance de 0 à C.

Corollaire 17. *Soit F un sous-espace vectoriel fermé de H. Alors $H = F \oplus F^\perp$.*

Application 18. Existence de l'espérance conditionnelle d'une variable aléatoire L^2.

Théorème 19. [Théorème de Riesz-Fréchet]
Pour toute application $\phi \in H'$, il existe un unique $f \in H$ tel que $\forall v \in H, \phi(v) = \langle f \mid v \rangle$.
De plus $\phi \longmapsto f$ est une isométrie ($\|f\|_H = \|\phi\|_{H'}$).

Application 20. Existence et unicité de l'adjoint d'un opérateur $T \in \mathcal{L}(H)$.

Théorème 21. [Théorème de Lax-Milgram]
Soit $a : H^2 \longrightarrow \mathbb{R}$ une forme bilinéaire continue et coercive. Alors pour tout $\ell \in H'$, il existe un unique $u \in H$ tel que $\forall v \in H, a(u,v) = \ell(v)$.
Si de plus a est symétrique alors u est l'unique élément de H minimisant $v \longmapsto \frac{1}{2}a(v,v) - \ell(v)$.

Application 22. [Problème de Dirichlet faible]
Soit $I =]0,1[$ et $f \in L^2(I)$. Alors

$$\exists! u \in H_0^1(I) \mid \forall v \in H_0^1(I), \int_I u'.v' + \int_I uv = \int_I fv$$

De plus u minimise la fonction $v \longmapsto \frac{1}{2}\int_I |v'|^2 + v^2 - \int_I fv$.

II. B. Espaces L^p

[BP15, Ch9, p157–194] [Bre99, ChIV, p54]

Soit $(E, \mathcal{A}, \mu)$ un espace mesuré. Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Soit $p \in [1, +\infty]$ et q son exposant conjugué ($\frac{1}{p} + \frac{1}{q} = 1$).

Définition 23. Pour $f : E \longrightarrow \mathbb{K}$ mesurable, on définit $\|f\|_p = \left(\int_E |f|^p \, d\mu\right)^{\frac{1}{p}}$ lorsque p est fini, et $\|f\|_\infty = \inf\{M > 0 \mid |f| \leq M \ \mu\text{-p.p.}\}$. On définit l'espace vectoriel :

$$\mathcal{L}^p(E, \mathcal{A}, \mu) = \{f : E \longrightarrow \mathbb{K} \text{ mesurable} \mid \|f\|_p < +\infty\}$$

Théorème 24. [Inégalité de Hölder]
Pour toutes fonctions $f, g : E \longrightarrow \mathbb{K}$ mesurables, on a $\|fg\|_1 \leq \|f\|_p \|g\|_q$.

Corollaire 25. [Inégalité de Minkowski]
Pour toutes fonctions $f, g : E \longrightarrow \mathbb{K}$ mesurables, on a $\|f+g\|_p \leq \|f\|_p + \|g\|_p$.

Définition 26. On note $L^p(E, \mathcal{A}, \mu) = \mathcal{L}^p(E, \mathcal{A}, \mu)/\{\|.\|_p = 0\}$ (ou $L^p(E)$, ou L^p) l'ensemble des fonctions de $\mathcal{L}^p(E, \mathcal{A}, \mu)$ quotienté par la relation d'égalité μ-p.p.. L'application $\|.\|_p$ passe au quotient et définit ainsi une application sur $L^p(E, \mathcal{A}, \mu)$ notée également $\|.\|_p$.

Corollaire 27. *$\|.\|_p$ est une norme et l'espace $(L^p(E), \|.\|_p)$ est un espace vectoriel normé.*

Application 28. [Inclusion entre espaces L^p]
Soient $p, p' \in [1, +\infty]$.
- lorsque $\mu(E) < +\infty$, on a $p < p' \Longrightarrow L^{p'} \subset L^p$,
- contre-exemple dans le cas où $\mu(E) = +\infty$: $f : x \longrightarrow (1+x)^{-1}\mathbb{1}_{\mathbb{R}_+^*}(x) \in L^2 \setminus L^1$.
- on a $p' < p \Longrightarrow \ell^{p'} \subset \ell^p$.

Proposition 29. [Inégalité de Jensen]
Si μ est une mesure de probabilité, alors pour toute fonction $f \in L^1$ à valeurs réelles et $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction convexe, on a $\varphi(\int_E f d\mu) \leq \int_E \varphi(f) d\mu$.

Application 30. On retrouve que $f(\sum_i \lambda_i x_i) \leq \sum_i \lambda_i f(x_i)$ dans le cas d'une fonction convexe avec des $(\lambda_i)_{1 \leq i \leq n}$ positifs de somme 1.

Application 31. [Théorème de Young]
Soient $p, q, r \in [1, +\infty]$ tels que $\frac{1}{p} + \frac{1}{q} = 1 + \frac{1}{r}$.
Alors si $f \in L^p$ et $g \in L^q$, on a $f * g \in L^r$ et $\|f * g\|_r \leq \|f\|_p \|g\|_q$.
Lorsque $q = 1$ et $p = r$, c'est une application de l'inégalité de Jensen.
Plus généralement, hormis le cas $p = q = 1$, c'est une application de l'inégalité de Hölder.

II. C. Inégalités en probabilités

[Ouv09, p162/508]

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé. Soit X une variable aléatoire.

Proposition 32. [Inégalité de Jensen]
Si $X \in L^1$ et ϕ est convexe, alors $\phi(\mathbb{E}[X]) \leq \mathbb{E}[\phi(X)]$. De plus, si ϕ est strictement converxe, on a égalité si et seulement si X est constante presque sûrement.

Remarque 33. En particulier on retrouve $|\mathbb{E}[X]| \leq \mathbb{E}[|X|]$ et $\mathbb{E}[X]^2 \leq \mathbb{E}[X^2]$.

Application 34. Soit $X_1, \ldots, X_n$ des v.a. i.i.d. de loi $\mathcal{E}(\theta)$ pour un paramètre $\theta > 0$ inconnu.
Alors $\overline{X}_n = \frac{1}{n}\sum_{i=1}^n X_i$ est un estimateur sans biais fortement convergeant de $\mathbb{E}[\mathcal{E}(\theta)] = \frac{1}{\theta}$.
Alors $\frac{1}{\overline{X}_n}$ est un estimateur fortement convergeant avec biais de θ.

Application 35. L'inégalité de Jensen reste valable si l'on remplace l'espérance par une espérance conditionnelle.
Ainsi pour φ convexe, si $(X_n)_{n \in \mathbb{N}}$ est une martingale, alors $(\varphi(X_n))_{n \in \mathbb{N}}$ est une sur-martingale.
On a aussi $\|\mathbb{E}[Y \mid \mathcal{B}]\|_p \leq \|Y\|_p$ pour toute v.a. $Y \in L^p$ et $\mathcal{B}$ une sous-tribu de $\mathcal{A}$.

Proposition 36. [Inégalité de Hoeffding]
Soient $(X_i)_{1\leq i\leq n}$ des variables aléatoires indépendantes telles que pour tout i, $X_i \in [a_i, b_i]$ p.s. pour des réels $a_i \leq b_i$. Alors pour tout $t \geq 0$:

$$\mathbb{P}(|\sum_{i=1}^n X_i - \mathbb{E}[X_i]| \geq t) \leq 2\exp(-2t^2/\sum_{i=1}^n (b_i - a_i)^2)$$

Remarque 37. Par un argument de convexité on montre que chaque X_i est $(b_i-a_i)/2$-sous-gaussienne (vérifie $\mathbb{E}[e^{\lambda X_i}] \leq \exp(\lambda^2(b_i-a_i)^2/8)$ pour tout $\lambda \in \mathbb{R}$). L'inégalité de Hoeffding est alors une application d'une inégalité similaire sur les variables sous-gaussiennes.

Application 38. Soient $(X_i)_{1\leq i\leq n}$ des variables aléatoires indépendantes et identiquement distribuéesde Rademacher centrées, c'est-à-dire $\mathbb{P}(X_1 = 1) = \mathbb{P}(X_1 = -1) = 1/2$. Alors :

$$\forall t > 0, \mathbb{P}(|\sum_{i=1}^n X_i| \geq t) \leq 2\exp(-\tfrac{t^2}{2n})\mathbb{1}_{t\leq n}$$

Définition 39. [Fonction génératrice, fonction caractéristique]
Soit X une variable aléatoire à valeurs dans $\mathbb{N}$ presque sûrement. On définit g_X la fonction génératrice de X par $g_X(s) = \mathbb{E}[s^X] = \sum_{k\geq 0} \mathbb{P}(X = k)s^k$ (lorsque la série converge).

Proposition 40. *g_X est bien définie, croissante et convexe sur $[0, 1]$. Si de plus $P(X = k) > 0$ pour au moins un $k \geq 2$, alors g_X est strictement convexe sur $[0, 1]$.*

Proposition 41. [Processus de branchement de Galton-Watson]
Soient $(X_i^j)_{i,j\geq 1}$ des v.a. i.i.d. à valeurs dans $\mathbb{N}$. On note μ leur loi, m leur espérance et 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 $n \in \mathbb{N}$. et enfin $\rho = \mathbb{P}(\exists n \geq 0 \mid Z_n = 0)$. Alors si $\mu \neq \delta_1$, on a :
- *si $m \leq 1$, $\rho = 1$ et on a extinction du processus presque surement,*
- *si $m > 1$, $\rho < 1$ et il y a une probabilité strictement positive de survie.*

III. Recherche d'extrema et de points fixes

[Rou99, Ch4, p140] [FGN07, §4.51, p287] [FGN12, §4.51, p39–41] [BMP05, §1.3.2, p19]

Proposition 42. *Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$.*
- *Si f est différentiable, f est convexe (resp. strictement convexe) si et seulement si pour tout $x \neq y \in \mathbb{R}^p$, $f(y) - f(x) \geq \langle \nabla f(x) \mid y - x\rangle$ (resp. $f(y) - f(x) > \langle \nabla f(x) \mid y - x\rangle$,*
- *Si f est $\mathcal{C}^2$, f est convexe (resp. strictement convexe) si et seulement si $\nabla^2 f(x)$ est positive (resp. définie positive) pour tout $x \in \mathbb{R}^p$.*

Exemple 43. Soit $A \in \mathcal{S}_n(\mathbb{R})$, $b \in \mathbb{R}^n$, $c \in \mathbb{R}$ et $f : x \longmapsto \frac{1}{2}\langle Ax \mid x\rangle - \langle b \mid x\rangle + c$.
Si A est positive (resp. définie positive), f est convexe (resp. strictement convexe). Ainsi par exemple si $(E, \langle . \mid . \rangle)$ est euclidien, l'application $x \longmapsto \|x\|^2$ est strictement convexe.

Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$ une fonction convexe.

Proposition 44. *Soit C un convexe de $\mathbb{R}^p$ et $M = \{x \in C \mid f(x) = \inf_C f\}$ l'ensemble des minimums globaux de f sur C.*
On suppose qu'il existe un minimum local $x_\star$ de f sur C. Alors :
- *M est un ensemble convexe et $x_\star \in M$ est un minimum global,*
- *si de plus f est strictement convexe, alors $M = \{x_\star\}$.*

Proposition 45. [Inégalité d'Euler]
Soit C un convexe de $\mathbb{R}^p$. Si f admet un minimum local sur C en $x_\star$ et si f est différentiable en $x_\star$ alors $df(x_\star)(y - x_\star) \geq 0$ pour tout $y \in C$.

Théorème 46. [Méthode de Newton]
Soit $f : [c, d] \longrightarrow \mathbb{R}$ une fonction $\mathcal{C}^2$, où $c < d$, et telle que $f(c) < 0 < f(d)$ et $f' > 0$ sur $[c, d]$. On considère la suite récurrente définie par $x_0 \in [c, d]$ et $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ pour $n \in \mathbb{N}$.
Alors en notant a l'unique 0 de f, on a :
(i) il existe $\alpha > 0$ tel que pour tout $x_0 \in [a - \alpha, a + \alpha]$, $(x_n)_{n\in\mathbb{N}}$ converge vers a de manière quadratique et il existe $C > 0$ telle que $\forall n \in \mathbb{N}, |x_{n+1} - a| \leq C|x_n - a|^2$.
(ii) si de plus $f'' > 0$ (f est strictement convexe) sur $[a, d]$, alors pour tout $x_0 \in]a, d]$, $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante et $x_{n+1} - a \sim_{n\to+\infty} \frac{f''(a)}{2f'(a)}(x_n - a)^2$.

Application 47. Approximation des zéros d'un polynôme.

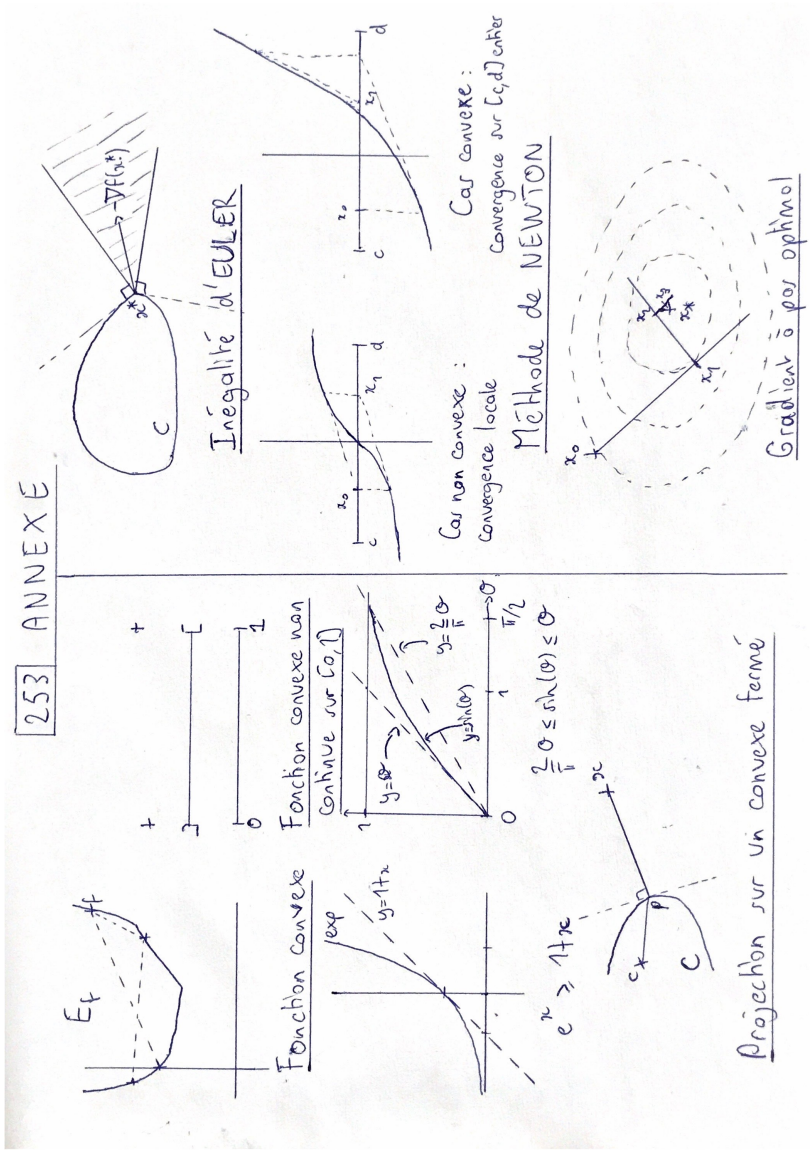
Théorème 48. [Méthode de gradient à pas optimal]
Soit $f : \mathbb{R}^p \longrightarrow \mathbb{R}$ elliptique, c'est-à-dire f est $\mathcal{C}^1$ et telle qu'il existe $\alpha > 0$ satisfaisant

$$\forall x, y \in \mathbb{R}^p, \langle \nabla f(x) - \nabla f(y) \mid x - y\rangle \geq \alpha \|x - y\|^2$$

On définit $(x_n)_{n\in\mathbb{N}}$ par $x_0 \in \mathbb{R}^p$ et $x_{n+1} = x_n - \rho_n \nabla f(x_n)$ où $\rho_n = \operatorname{argmin}_{\rho>0} f(x_n - \rho\nabla f(x_n))$. Alors $(x_n)_{n\in\mathbb{N}}$ converge vers l'unique minimum global de f.

Application 49. Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$, $b \in \mathbb{R}^n$ et $c \in \mathbb{R}$. L'application $f : x \longmapsto \frac{1}{2}\langle Ax \mid x\rangle - \langle b \mid x\rangle$ admet un unique minimum $\overline{x}$ caractérisé par $\nabla f(\overline{x}) = A\overline{x} - b = 0$. On converge vers cette solution par l'algorithme de gradient à pas optimal.

ANNEXE



SPEECH

La convexité est une propriété forte sur des ensembles ou des fonctions, qui va se traduire par tout un tas de propriétés, caractérisations, rappelées au début du plan, et qui va offrir un cadre très adéquat pour les problèmes d'optimisation. La définition de la convexité est une propriété de dimension finie (nombre fini de points), donc on va pouvoir avoir des raisonnements géométriques, notamment dans les espaces de Hilbert.
La convexité fournit de nombreuses inégalités pratiques provenant de certaines fonctions, fréquemment utilisés notamment lorsque l'on travaille au voisinage du point d'égalité.
L'inégalité arithmético-géométrique va avoir pour application l'inégalité de Young, qui elle même sera très utile dans la construction des espaces L^p, avec l'inégalité de Hölder.
La convexité est un véritable outil dans de nombreux cadres, c'est ce que l'on voit dans la partie 2. Déjà dans les Hilbert, un théorème fondamental est le théorème de projection sur un convexe fermé qui va avoir de nombreuses conséquences : avec notamment le théorème de Riesz-Fréchet puis de Lax-Milgram et ses applications aux EDP, mais aussi l'existence de l'espérance conditionnelle en probabilités.
Ensuite la construction des espaces L^p repose sur les inégalités de Hölder et de Minkowski, qui vont permettre d'assurer que l'on a une norme sur cet espace, et qui reposent sur l'inégalité de Young vue précédemment. La convexité va aussi servir lorsque l'on s'intéresse aux convolutions de fonctions, par exemple avec le théorème de Young.
Enfin en probabilités, la convexité intervient avec l'inégalité de Jensen, mais elle permet aussi d'avoir des inégalités de concentration, comme par exemple l'inégalité de Hoeffding : le fait d'additionner des variables indépendantes va augmenter leur régularité. Enfin la fonction génératrice de variables aléatoires à valeurs dans $\mathbb{N}$ est convexe sur $[0,1]$, et on pourra appliquer cela dans le premier développement sur le processus de branchement de Galton-Watson, où l'on fait une distinction de cas dont chacun utilise différentes propriétés de convexité.
Enfin dans une dernière partie, je parle d'optimisation puisque la convexité fournit un cadre intéressant : tout minimum local va être global, et unique si on a stricte convexité. La convexité d'une fonction va permettre à la méthode de Newton de passer d'un comportement local à un comportement global. Enfin en deuxième développement on montrera la convergence de l'algorithme de gradient à pas optimal dans le cas d'une fonction elliptique, c'est-à-dire fortement convexe dans un certain sens (convexe + coercive etc).

QUESTIONS

Q Soit $f : U \longrightarrow \mathbb{R}$ une fonction convexe définie sur un convexe U de $\mathbb{R}^n$, supposé borné. On suppose qu'il existe C convexe de U et $\varepsilon > 0$ tel que $\forall x \in C, \overline{B}(x, 2\varepsilon) \subset U$. Montrer que f est lispchitzienne sur C.

R On prend deux points x, y distincts et on regarde sur la droite (xy) les points x_ε et y_ε à distance ε de x et y en dehors de $[x, y]$. Ces points sont dans U par hypothèse, et on peut écrire x comme barycentre de x_ε et y, puis y comme barycentre de x et y_ε. En utilisant alors la convexité de f, on peut majorer $|f(x) - f(y)|$ par $\frac{d}{d+\varepsilon} \max(|f(x) - f(y_\varepsilon)|, |f(y) - f(x_\varepsilon)|)$ où $d = d(x, y)$.

Reste alors à utiliser que f est continue sur U (propriété un peu compliqué qui est admise pour l'exercice), en on obtient que $|f(x)-f(y)| \leq \frac{d}{\varepsilon} 2 \|f\|_{\infty,\overline{C_\varepsilon}}$ où $C_\varepsilon = C + B(0,\varepsilon)$ est un ensemble borné de U, et f est continue sur le compact $\overline{C_\varepsilon}$.

R Soit Z une variable aléatoire réelle et $r \geq s > 0$. Montrer que $\mathbb{E}[|Z|^r]^{1/r} \geq \mathbb{E}[|Z|^s]^{1/s}$.

Q Il s'agit d'appliquer l'inégalité de HÖLDER :

$$\mathbb{E}[|Z|^s] \leq \mathbb{E}[|Z|^r]^{s/r}$$

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[BP15] M. BRIANE et G. PAGÈS : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Bre99] H. BREZIS : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[FGN12] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

[Gou08] X. GOURDON : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Ouv09] J.-Y. OUVRARD : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[Rou99] F. ROUVIÈRE : *Petit guide de calcul différentiel*. Cassini, 1999.

260 ESPÉRANCE, VARIANCE ET MOMENTS D'UNE VARIABLE ALÉATOIRE.

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé, et $(E, \mathcal{E})$ un espace probabilisable.

I. Autour de l'espérance et de la variance [BL07, §III.4/5, p52–71]

I. A. Espérance

Définition 1. [variable aléatoire]
Une variable aléatoire X est une fonction mesurable $X : (\Omega, \mathcal{A}) \longrightarrow (E, \mathcal{E})$.
On note $\mathbb{P}_X$ la mesure image de $\mathbb{P}$ par X et on l'appelle loi de X.
Si on a $(E, \mathcal{E}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$, on dit que X est une variable aléatoire réelle.

Soit X une variable aléatoire à valeurs dans $E = \mathbb{R}^d$ où $d \in \mathbb{N}^*$.

Définition 2. [espérance]
- Si $E = \mathbb{R}_+$, on définit l'espérance de X par $\mathbb{E}[X] = \int_\Omega X(\omega)\, d\mathbb{P}(\omega) \in [0, +\infty]$,
- Si $E = \mathbb{R}$ et $\mathbb{E}[|X|] < +\infty$, on définit l'espérance de X par la même formule,
- Si $E = \mathbb{R}^d$, on définit l'espérance de $X = (X_1, \dots, X_d)$ lorsque $\mathbb{E}[\|X\|] < +\infty$ par $\mathbb{E}[X] = (\mathbb{E}[X_1], \dots, \mathbb{E}[X_d])$.

Exemple 3. Espérance d'une loi binomiale et d'une loi normale, … **[voir annexe]**
Les lois de Cauchy n'admettent pas d'espérance.

Remarque 4. L'espérance est une forme linéaire positive et les résultats classiques d'intégration sont valables pour l'espérance : lemme de Fatou, théorèmes de convergence dominée et convergence monotone, inégalité de Cauchy-Schwarz.

Proposition 5. [lemme de transfert]
Si X est à valeurs dans $\mathbb{R}^d$, soit $f : \mathbb{R}^d \longrightarrow \mathbb{R}$ une fonction borélienne.
Alors $f(X) \in L^1(\Omega, \mathcal{A}, \mathbb{P}) \iff f \in L^1(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d), \mathbb{P}_X)$ et dans ce cas :

$$\mathbb{E}[f(X)] = \int_\Omega f(X(\omega)) d\mathbb{P}(\omega) = \int_{\mathbb{R}^d} f(x) d\mathbb{P}_X(x)$$

Application 6. Si $X \sim \mathcal{E}(\lambda)$ avec $\lambda > 0$ et $\theta > 0$, alors $\theta X \sim \mathcal{E}(\lambda/\theta)$.
Si $X \sim \mathcal{G}(p)$ et $f : n \longmapsto \mathbb{1}_{n \text{ est pair}}$, alors $\mathbb{E}[f(X)] = 1/3$.

Remarque 7. Si X est réelle positive, on a $\mathbb{E}[X] = \int_0^\infty \mathbb{P}(X > t) dt$. Dans le cas où X est à valeurs dans $\mathbb{N}$, on a $\mathbb{E}[X] = \sum_{n \geq 1} \mathbb{P}(X \geq n)$.

Proposition 8. [espérance conditionnelle]
Soit $\mathcal{B}$ une sous-tribu de $\mathcal{A}$. Soit X une variable aléatoire réelle sur $(\Omega, \mathcal{A}, \mathbb{P})$, intégrable.
Alors il existe une unique (presque sûrement) variable aléatoire Z telle que :
(i) Z est $\mathcal{B}$-mesurable,
(ii) pour tout $B \in \mathcal{B}$, $\mathbb{E}[X \mathbb{1}_B] = \mathbb{E}[Z \mathbb{1}_B]$.
De plus, Z est intégrable.

Définition 9. [espérance conditionnelle]
Z est appelée espérance conditionnelle de X sachant $\mathcal{B}$, et est notée $\mathbb{E}[X \mid \mathcal{B}]$.

Application 10. Soient X une variable aléatoire indépendante de $\mathcal{B}$ et Y une variable aléatoire $\mathcal{B}$-mesurable. Alors pour toute fonction ψ telle que $\psi(X, Y)$ est intégrable :

$$\mathbb{E}[\psi(X, Y) \mid \mathcal{B}] = \int \psi(x, Y)\, d\mu_X(x) = h(Y) \qquad \text{où} \qquad h(y) = \mathbb{E}[\psi(X, y)]$$

Exemple 11. Soit $(X_i)_{i \in \mathbb{N}^*}$ des v.a. i.i.d. intégrables. Alors si $S_n = \sum_{k=1}^n X_i$, on a pour $p < q$, $\mathbb{E}[S_q \mid S_p] = S_p + (q - p)\mathbb{E}[X_1]$.

I. B. Variance

Soient X et Y deux variables aléatoires à valeurs dans $E = \mathbb{R}^d$ de carré intégrable.

Définition 12. [covariance, variance]
Si $d = 1$, on définit la covariance de X et Y par $\mathrm{Cov}(X, Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])]$, la variance de X par $\mathrm{Var}(X) = \mathrm{Cov}(X, X) = \mathbb{E}[(X - \mathbb{E}[X])^2]$.
Sinon, on définit $\Sigma = (\mathrm{Cov}(X_i, X_j))_{1 \leq i,j \leq d}$ la matrice de covariance de $X = (X_1, \dots, X_d)$.

Application 13. Si $A \in \mathcal{M}_d(\mathbb{R})$ et $b \in \mathbb{R}^d$ alors $\Sigma_{AX+b} = A \Sigma_X A^\top$.

Proposition 14. *Cov est une forme bilinéaire symétrique positive sur L^2 et on a $\mathrm{Cov}(X, Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$ et $\mathrm{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2$.*

Remarque 15. $\mathrm{Var}(X)$ s'interprète comme la projection de X sur l'espace des fonctions constantes presque sûrement.

Exemple 16. Variance d'une loi de poisson et d'une loi exponentielle, … **[voir annexe]**

Proposition 17. *Si $X \perp\!\!\!\perp Y$ alors $\mathrm{Cov}(X,Y)=0$ et $\mathrm{Var}(X+Y)=\mathrm{Var}(X)+\mathrm{Var}(Y)$.*

Exemple 18. La réciproque est fausse : prendre $X\sim\mathcal{N}(0,1)$ ou $X\sim\mathcal{U}([-1,1])$ et $Y=X^2$.

I. C. Inégalités importantes en probabilités

Soit X une variable aléatoire réelle.

Proposition 19. [Inégalité de Markov]
Si $X\geq 0$ p.s., alors $\forall t>0, \mathbb{P}(X\geq t)\leq \frac{\mathbb{E}[X]}{t}$.

Proposition 20. [Inégalité de Bienaymé-Tchebychev]
On a $\forall t>0, \mathbb{P}(|X-\mathbb{E}[X]|\geq t)\leq \frac{\mathrm{Var}(X)}{t^2}$.

Proposition 21. [Inégalité de Jensen]
Si $X\in L^1$ et ϕ est convexe, alors $\phi(\mathbb{E}[X])\leq\mathbb{E}[\phi(X)]$. De plus, si ϕ est strictement converxe, on a égalité si et seulement si X est constante presque sûrement.

Remarque 22. En particulier $|\mathbb{E}[X]|\leq\mathbb{E}[|X|]$ et $\mathbb{E}[X]^2\leq\mathbb{E}[X^2]$. L'inégalité de Jensen s'applique en dehors du cadre des probabilités, par exemple pour montrer que $f*g$ est bien défini et $\|f*g\|_p\leq\|f\|_1\|g\|_p$ lorsque $f\in L^1, g\in L^p$.

Application 23. Si $(X_i)_{1\leq i\leq n}$ sont des v.a. i.i.d. d'espérance m et de variance σ^2 finies, alors

$$\forall t>0, \mathbb{P}\Big(\frac{1}{n}\Big|\sum_{k=1}^n X_i - m\Big|\geq t\Big)\leq\frac{\sigma^2}{nt^2}$$

Application 24. [Théorème de Weierstrass]
$\mathbb{R}[X]$ est dense dans $\mathcal{C}([a,b],\mathbb{C},\|.\|_\infty)$ pour $a<b\in\mathbb{R}$.

II. Moments d'une variable aléatoire

[BL07, §III.4/5, p52–71]

Soit X une variable aléatoire réelle. Soit $p\in\mathbb{N}^*$.

II. A. Généralités

Définition 25. [Moment et moment centré d'ordre p]
Si $\mathbb{E}[|X|^p]<+\infty$, on dit que X admet un moment d'ordre p (ou $X\in L^p$) et alors on appelle $\mathbb{E}[X^p]$ le moment d'ordre p et $\mathbb{E}[(X-\mathbb{E}[X])^p]$ le moment centré d'ordre p de X.

Remarque 26. Si X admet un moment d'ordre p, l'inégalité de Markov assure que $\mathbb{P}(|X-\mathbb{E}[X]|\geq x)=\mathbb{P}(|X-\mathbb{E}[X]|^p\geq x^p)\leq\frac{\mathbb{E}[|X-\mathbb{E}[X]|^p]}{x^p}$. Plus X admet de moments d'ordre élevé, plus on a un contrôle sur la queue de distribution de X.

Proposition 27. *Si $X\in L^p$ alors $X\in L^q$ pour tout $1\leq q\leq p$.*

Définition 28. [Fonction génératrice des moments]
On définit M_X la fonction génératrice des moments de X par $M_X(\lambda)=\mathbb{E}[\mathrm{e}^{\lambda X}]$ pour $\lambda\in\mathbb{R}$ tel que cette quantité soit définie.

Proposition 29. *Si M_X est définie sur un voisinage de 0, alors M_X caractérise la loi de X et alors on a $M_X(\lambda)=\sum_{k\geq 0}\frac{t^k}{k!}\mathbb{E}[X^k]$ au voisinage de 0, en particulier X admet des moments de tout ordre et $\mathbb{E}[X^p]=M_X^{(p)}(0)$ pour tout p.*

Exemple 30. $M_{\mathcal{N}(0,1)}:\lambda\longmapsto\exp(\lambda^2/2)$ et $M_{\mathcal{R}(1/2)}:\lambda\longmapsto\mathrm{ch}(\lambda)$.

Proposition 31. $\forall t\in\mathbb{R}, \mathbb{P}(X\geq t)\leq\inf_{\lambda\geq 0}\{\mathrm{e}^{-\lambda t}M_X(\lambda)\}$ **[Borne de Chernoff]**

Application 32. [Variables aléatoires sous-gaussiennes]
On dit que X est K-sous-gaussienne si $M_X(\lambda)\leq\exp(\lambda^2K^2/2)$ pour un $K>0$.
On a alors X centrée, $\mathbb{V}(X)\leq\mathbb{E}(X^2)\leq K^2$ et pour $t\geq 0, \mathbb{P}(|X|\geq t)\leq 2\exp(-t^2/2K^2)$.
Si $X\sim\mathcal{N}(0,1)$, X est 1-sous-gaussienne.
Si $X\in[a,b]$ p.s., $X-\mathbb{E}[X]$ est $(b-a)/2$-sous-gaussienne (lemme de Hoeffding, admis).
Si $(X_i)_{1\leq i\leq n}$ est une famille de variables aléatoires indépendantes et si pour tout i, X_i est K_i-sous gaussienne, alors $\sum_{i=1}^n X_i$ est $\sqrt{\sum_{i=1}^n K_i^2}$ sous-gaussienne.
En particulier, on obtient l'inégalité de Hoeffding : si pour tout i, $X_i\in[a_i,b_i]$ p.s., alors :

$$\forall t\geq 0, \mathbb{P}\left(|\textstyle\sum_{i=1}^n(X_i-\mathbb{E}[X_i])|\geq t\right)\leq 2\exp(-2t^2/\sum_{i=1}^n(b_i-a_i)^2)$$

Théorème 33. [Théorème des moments] *(admis)*
Si X et Y sont bornées p.s. et si leurs moments sont égaux à tout ordre, alors $X\sim Y$.

Remarque 34. C'est faux si X et Y ne sont pas bornées : les considérer de densités $f_X: x\longmapsto\frac{1}{\sqrt{2\pi}x}\mathrm{e}^{-\ln(x)^2/2}\mathbb{1}_{\mathbb{R}_+}(x)$ et $f_Y: x\longmapsto f_X(x)(1+a\sin(2\pi\ln(x)))$ pour un $a\in[-1,1]$.

II. B. Liens avec les fonctions génératrices et caractéristiques

[BL07, §III.5, p61]

Soient X,Y des variables aléatoires à valeurs dans $\mathbb{R}^d$ ou $\mathbb{N}$ selon le contexte.

Définition 35. [Fonction génératrice, fonction caractéristique]
Si X est à valeurs dans $\mathbb{N}$ presque sûrement, on définit g_X la fonction génératrice de X par $g_X(s) = \mathbb{E}[s^X] = \sum_{k\geq 0} \mathbb{P}(X=k)s^k$ (lorsque la série converge).
On définit ϕ_X la fonction caractéristique de X par $\phi_X(\lambda) = \mathbb{E}\left[e^{i\langle\lambda|X\rangle}\right]$ pour $\lambda \in \mathbb{R}^d$.

Remarque 36. Le rayon de convergence de cette série est au moins égal à 1 et $G_X(1) = 1$.

Exemple 37. Fonctions génératrices de $\mathcal{B}(p), \mathcal{B}(n,p), \mathcal{P}(\lambda), \mathcal{G}(p)$ … Fonctions caractéristiques de $\mathcal{B}(n,p), \mathcal{E}(\lambda)$ …**[voir annexe]**

Proposition 38. *ϕ_X et G_X caractérisent la loi de X. En particulier, $\forall k \in \mathbb{N}, \mathbb{P}(X=k) = \frac{G^{(k)}(0)}{k!}$.*

Proposition 39.
- *X admet un moment d'ordre $p \in \mathbb{N}^*$ si et seulement si g_X est p fois dérivable en 1, et dans ce cas $G_X^{(p)}(1) = \mathbb{E}[X(X-1)\dots(X-p)]$,*
- *Si X est réelle et admet un moment d'ordre p, alors ϕ_X est p fois dérivable et on a $\phi_X^{(p)}(\lambda) = i^p\mathbb{E}[X^p e^{i\lambda X}]$. En particulier, $\phi^{(p)}(0) = i^p\mathbb{E}[X^p]$.*

Application 40. Expression de l'espérance, la variance, ou plus généralement d'un moment en fonction des dérivées en 0 de G_X.

Proposition 41. *Si $X \perp\!\!\!\perp Y$ alors $G_{X+Y} = G_X G_Y$ ou selon le contexte $\forall(\lambda_1,\lambda_2) \in \mathbb{R}^d \times \mathbb{R}^\ell, \phi_{(X+Y)}(\lambda_1,\lambda_2) = \phi_X(\lambda_1)\phi_Y(\lambda_2)$.*

Application 42. [Processus de branchement de Galton-Watson]
Soit $(Z_n)_{n\in\mathbb{N}}$ un processus de branchement de Galton-Watson de loi μ. Alors $g_{Z_n} = g_\mu^{\otimes n}$ pour tout $n \in \mathbb{N}$ et si $\mu \neq \delta_0$, on a $\mathbb{P}(\text{survie du processus}) > 0 \iff \mathbb{E}[\mu] > 1$.

Application 43. Les composantes d'un vecteur gaussien sont indépendantes si et seulement si sa matrice de covariance est diagonale.

Application 44. Calcul de la loi d'une variable aléatoire multinomiale dont le paramètre n n'est pas déterministe mais suit une loi $\mathcal{P}(\lambda)$.

III. Théorèmes limites

[BL07, §V.5, p131–147]

Des conditions sur les moments d'une loi apparaissent naturellement dans plusieurs énoncés fondamentaux de convergence de variables aléatoires.

III. A. Loi des grands nombres

Théorème 45. [Loi des grands nombres]
Soit $(X_i)_{i\in\mathbb{N}^*}$ des variables aléatoires réelles i.i.d. intégrables. Alors :

$$\frac{1}{n}\sum_{i=1}^n X_i \underset{n\to+\infty}{\longrightarrow} \mathbb{E}[X_1] \quad \text{p.s.}$$

L'hypothèse d'intégrabilité est cruciale :

Proposition 46. *Soient $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires i.i.d. telle que $\mathbb{E}[|X_1|] = +\infty$. Alors la probabilité que la limite de $\frac{1}{n}\sum_{i=1}^n X_i$ existe dans $\mathbb{R}$ est nulle.*

Application 47. [Méthode de Monte-Carlo] [Mé11]
Soit $f : [0,1] \longrightarrow \mathbb{R}$ intégrable par rapport à la mesure de Lebesgue et $(X_i)_{n\in\mathbb{N}^*}$ une suite de variables aléatoiresi.i.d. de loi $\mathcal{U}([0,1])$. Alors $I_n = \frac{1}{n}\sum_{i=1}^n f(X_i) \underset{n\to+\infty}{\longrightarrow} \int_0^1 f(x)dx$ p.s..

III. B. Théorème central limite

Théorème 48. [Théorème de Lévy (faible)]
Soient $(X_n)_{n\in\mathbb{N}}$ et X des variables aléatoires à valeurs dans $(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d))$. Alors $X_n \underset{n\to+\infty}{\xrightarrow{\mathcal{L}}} X$ si et seulement si $\phi_{X_n} \underset{n\to+\infty}{\xrightarrow{s}} \phi_X$.

Théorème 49. [Théorème central limite]
Soit $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires réelles i.i.d. de carré intégrable. Alors :

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n (X_i - \mathbb{E}[X_1]) \underset{n\to+\infty}{\xrightarrow{\mathcal{L}}} Z \sim \mathcal{N}(0, \mathrm{Var}(X_1))$$

Application 50. [Intervalle de confiance asymptotique] [RS12, §3.4, p25]
Soient $(X_i)_{i\in\mathbb{N}^*}$ des réalisations i.i.d. de $\mathcal{B}(p)$ pour un $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\hat{p}_n = \frac{1}{n}\sum_{k=1}^n X_i : \mathrm{IC}_\alpha(p) = \left[\hat{p}_n \pm \frac{q_{1-\alpha/2}}{2}\frac{1}{\sqrt{n}}\right]$, où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

ANNEXE

[BL07, Appendice, p229]

Tableau des principales lois discrètes

Soit X une loi discrète et $p \in [0,1], q \in]0,1[, n \in \mathbb{N}, \lambda > 0$.

$\mathcal{L}(X)$	$\mathbb{P}_X$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$\phi_X(t)$	$G_X(t)$
$\mathcal{U}(\llbracket 1,n \rrbracket)$	$\sum_{k=1}^{n} \frac{1}{n}\delta_k$	$\frac{n+1}{2}$	$\frac{n^2-1}{12}$	$\frac{1}{n}\sum_{k=1}^{n} \mathrm{e}^{ikt}$	$\frac{1}{n}\frac{t-t^{n+1}}{1-t}$ $(t \neq 1)$
$\mathcal{B}(p)$	$p\delta_1 + (1-p)\delta_0$	p	$p(1-p)$	$p\,\mathrm{e}^{it}+(1-p)$	$1-p+pt$
$\mathcal{B}(n,p)$	$\sum_{k=0}^{n} \binom{n}{k} p^k(1-p)^{n-k}\delta_k$	np	$np(1-p)$	$p\,\mathrm{e}^{it}+(1-p)^n$	$(1-p+pt)^n$
$\mathcal{P}(\lambda)$	$\sum_{k=0}^{\infty} \frac{\lambda^k \mathrm{e}^{-\lambda}}{k!}\delta_k$	λ	λ	$\mathrm{e}^{\lambda(\mathrm{e}^{it}-1)}$	$\mathrm{e}^{(\lambda-1)t}$
$\mathcal{G}(q)$	$\sum_{k=1}^{\infty} q(1-q)^{k-1}\delta_k$	$\frac{1}{q}$	$\frac{1-q}{q^2}$	$\frac{q\,\mathrm{e}^{it}}{1-(1-q)\,\mathrm{e}^{it}}$	$\frac{pt}{1-(1-p)t}$

Tableau des principales lois à densité

Soit X une loi admettant une densité f par rapport à la mesure de LEBESGUE. Soit $a < b \in \mathbb{R}, m \in \mathbb{R}, \sigma > 0, \lambda > 0, \alpha, \beta > 0$.

$\mathcal{L}(X)$	$f(t)$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$\phi_X(t)$
$\mathcal{U}([a,b])$	$\frac{\mathbb{1}_{[a,b]}(t)}{b-a}$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$	$\frac{\mathrm{e}^{itb}-\mathrm{e}^{ita}}{it(b-a)}$
$\mathcal{N}(m,\sigma^2)$	$\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(t-m)^2}{2\sigma^2}\right)$	m	σ^2	$\mathrm{e}^{imt-\frac{t^2\sigma^2}{2}}$
$\mathcal{C}(m,\sigma^2)$	$\frac{1}{\pi\sigma}\frac{1}{1+(\frac{t-m}{\sigma})^2}$	/	/	$\mathrm{e}^{-\lvert t\rvert}$
$\mathcal{E}(\lambda)$	$\lambda\exp(-\lambda t)\mathbb{1}_{[0,+\infty[}(t)$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	$\frac{1}{1-\frac{it}{\lambda}}$
$\Gamma(\alpha,\beta)$	$\frac{\beta^\alpha}{\Gamma(\alpha)}\mathrm{e}^{-\beta t}t^{\alpha-1}\mathbb{1}_{[0,+\infty[}(t)$	$\frac{\alpha}{\beta}$	$\frac{\alpha}{\beta^2}$	$\left(1-\frac{it}{\beta}\right)^{-\alpha}$

QUESTIONS

Q Donner une variable aléatoire sans moment.

R Une variable aléatoire de loi de CAUCHY.

Q Quelles sont les applications de l'inégalité de MARKOV ?

R De nombreuses autres inégalités classiques, le fait que la convergence L^1 implique la convergence en probabilité. Aussi, si X centrée admet un moment d'ordre p, alors $\mathbb{P}(X \geq x) = \mathbb{P}(X^p \geq x) \leq \mathbb{E}[X^p]/x^p$, et donc plus X admets des moments d'ordres élevés, plus on a une décroissance rapide de la queue de distribution.

Q Quel est l'intérêt de regarder la matrice de covariance d'un vecteur gaussien ?

R Les coordonnées du vecteur sont indépendantes si et seulement si la matrice de covariance est diagonale (le sens réciproque n'est vrai que pour des vecteurs gaussiens).

Q Démontrer le théorème central limite en dimension d ?

R On se ramène au cas réel à partir du théorème de LÉVY.

Q Soit $\theta > 0$ et $(X_k)_{k\geq 1}$ i.i.d. de loi $\mathcal{U}([0,\theta])$. On pose $\hat{\theta}_n = \max_{1\leq i\leq n} X_k$. Calculer la fonction de répartition, la densité, l'espérance et la variance de $\hat{\theta}_n$.

Q Soit $X \in L^2$ d'espérance m, de variance σ^2. Montrer que $\mathbb{P}(X - m \geq \alpha) \leq \frac{\sigma^2+\lambda^2}{(\alpha+\lambda)^2}$ pour tout $\alpha, \lambda > 0$.

R $\mathbb{P}(X - m + \lambda \geq \alpha + \lambda) \leq \mathbb{P}((X-m+\lambda)^2 \geq (\alpha+\lambda)^2)$ puis on applique l'inégalité de MARKOV et on développe l'espérance.

Q Dans le même contexte, montrer que $\mathbb{P}(X - m \geq \alpha) \leq \frac{\sigma^2}{\alpha^2+\sigma^2}$ pour tout $\alpha > 0$.

R On minimise la fonction précédemment obtenue en $\lambda = \sigma^2/\alpha$.

Q Montrer que $\mathbb{P}(\lvert X - m\rvert \geq \alpha) \leq 2\frac{\sigma^2}{\alpha^2+\sigma^2}$. Comparer ce résultat avec l'inégalité de BIENAYMÉ-TCHEBYCHEV.

R Pour $\sigma \geq \alpha$, cette inégalité est meilleure que l'inégalité de BIENAYMÉ-TCHEBYCHEV.

BIBLIOGRAPHIE

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[Mé11] S. MÉLÉARD : *Aléatoire : introduction à la théorie et au calcul des probabilités*. Les éditions de l'École Polytechnique, 2011.

[RS12] V. RIVOIRARD et G. STOLTZ : *Statistique mathématique en action*. Vuibert, 2 ème édition, 2012.

261 LOI D'UNE VARIABLE ALÉATOIRE : CARACTÉRISATIONS, EXEMPLES, APPLICATIONS.

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé, et $(E, \mathcal{E})$ un espace probabilisable. Soit $d \in \mathbb{N}^*$.

I. Loi d'une variable aléatoire et premières caractérisations

I. A. Définitions et caractérisation des variables aléatoires discrètes [Ouv08, Ch1, p14–20] [BL07, §III.4/5, p52–71]

Définition 1. [Variable aléatoire, loi d'une variable aléatoire]
- Une variable aléatoire X est une fonction mesurable $X : (\Omega, \mathcal{A}) \longrightarrow (E, \mathcal{E})$.
- On note $\mathbb{P}_X$ la mesure image de $\mathbb{P}$ par X et on l'appelle loi de X.
- Si $(E, \mathcal{E}) = (\mathbb{R}, \mathcal{B}(\mathbb{R}))$, on dit que X est une variable aléatoire réelle.
- Si $X(\Omega)$ est dénombrable presque sûrement, on dit que X est discrète.
- Si $\mathbb{P}_X$ est absolument continue par rapport à la mesure de Lebesgue, on dit que X est à densité, de densité $d\mathbb{P}_X / d\,\mathrm{Leb}$.

Exemple 2. Variable aléatoire qui associe le résultat du lancer d'une pièce : $E = \{\mathrm{P}, \mathrm{F}\}$, le résultat de la couleur d'une boule tirée dans une urne : $E = \{\text{couleurs}\}$.
$\mathcal{B}(p)$ est discrète, $\mathcal{E}(\lambda)$ est continue.

Soit X une variable aléatoire discrète à valeurs dans E.

Proposition 3. *Enumérons $E' = (e_i)_{i\in I} \subset E$ où I est au plus dénombrable de sorte que $X(\Omega) \subset E'$ p.s.. Alors $\mathbb{P}_X$ est caractérisée par la famille $(p_i)_{i\in I}$ où $p_i = \mathbb{P}(X = e_i)$ et $\sum_{i\in I} p_i = 1$. De plus, on a $\mathbb{P}_X = \sum_{i\in I} p_i \delta_{e_i}$.*

Remarque 4. Réciproquement, si $f : E' \longrightarrow [0,1]$ est telle que $\sum_{i\in I} f(e_i) = 1$, alors il existe une unique probabilité $\mathbb{Q}$ sur $(E, \mathcal{E})$ telle que $\forall i \in I, \mathbb{Q}(e_i) = f(e_i)$. Une variable aléatoire de loi Q est alors discrète.

Exemple 5. $\mathcal{B}(p), \mathcal{B}(n,p), \mathcal{G}(p), \mathcal{P}(\lambda), \ldots$ et leur loi $\mathbb{P}_X$ associée **[voir annexe]**

I. B. Caractérisation par l'espérance de classes de fonctions [BL07, ChIII, p41]

Soit X une variable aléatoire à valeurs dans $E = \mathbb{R}^d$.

Remarque 6. Il est clair que $\mathbb{P}_X$ est entièrement déterminée par la donnée de $\mathbb{P}_X(A)$ pour $A \in \mathcal{B}(\mathbb{R}^d)$, ou pour $A \in \Lambda$ où Λ est un π-système générateur de $\mathcal{B}(\mathbb{R}^d)$.

Définition 7. [Espérance] Si X est réelle, on définit lorsque $\int_\Omega |X(\omega)| \, d\mathbb{P}(\omega) < +\infty$ l'espérance de X par $\mathbb{E}[X] = \int_\Omega X(\omega) \, d\mathbb{P}(\omega)$. Sinon, on définit l'espérance de $X = (X_1, \ldots, X_d)$ lorsque $\mathbb{E}[\|X\|] < +\infty$ par $\mathbb{E}[X] = (\mathbb{E}[X_1], \ldots, \mathbb{E}[X_d])$.

Exemple 8. Espérance de $\mathcal{B}(n,p), \mathcal{N}(0,1), \ldots$ **[voir annexe]**
Les lois de Cauchy n'admettent pas d'espérance.

Remarque 9. L'espérance ne dépend que de la loi de la variable aléatoire.

Proposition 10. [Lemme de transfert]
Soit $f : \mathbb{R}^d \longrightarrow \mathbb{R}$ une fonction borélienne.
Alors $f(X) \in L^1(\Omega, \mathcal{A}, \mathbb{P}) \iff f \in L^1(\mathbb{R}^d, \mathcal{B}(\mathbb{R}^d), \mathbb{P}_X)$ et dans ce cas :

$$\mathbb{E}[f(X)] = \int_\Omega f(X(\omega)) d\mathbb{P}(\omega) = \int_{\mathbb{R}^d} f(x) d\mathbb{P}_X(x)$$

Application 11. Si $X \sim \mathcal{E}(\lambda)$ avec $\lambda > 0$ et $\theta > 0$, alors $\theta X \sim \mathcal{E}(\lambda/\theta)$.

Application 12. [Théorème de Weierstrass]
$\mathbb{R}[X]$ est dense dans $\mathcal{C}([a,b], \mathbb{C}, \|.\|_\infty)$ pour $a < b \in \mathbb{R}$.

Proposition 13. *La donnée de $\mathbb{E}[f(X)]$ pour $f \in \mathcal{C}_c^+(\mathbb{R}^d)$ l'ensemble des fonctions continues positives à support compact caractérise la loi de X. [Ouv09, p10]*

Remarque 14. On peut aussi prendre pour famille de fonctions $\mathcal{C}_b(\mathbb{R}^d), \mathcal{C}_0(\mathbb{R}^d), \mathcal{C}_c^\infty(\mathbb{R}^d) \ldots$

Application 15. Si $U_1, U_2 \sim \mathcal{N}(0,1)$ et sont indépendantes, alors $U_1/U_2 \sim \mathcal{C}(0,1)$.

II. Caractérisations par des fonctions

II. A. Fonction de répartition [BL07, §III.2, p45]

Soit X une variable aléatoire réelle.

Définition 16. On définit F_X la fonction de répartition de X par $F_X(x) = \mathbb{P}_X(]-\infty, x]) = \mathbb{P}(X \leq x)$ pour $x \in \mathbb{R}$.

Exemple 17. Fonction de répartition de $\mathcal{B}(p), \mathcal{E}(\lambda)$.

Proposition 18.
(i) F_X est croissante, continue à droite et $\lim_{-\infty} F_X = 0, \lim_{+\infty} F_X = 1$.
(ii) Réciproquement, toute fonction F satisfaisant ces hypothèses est la fonction de répartition d'une variable aléatoire.
(iii) Si f est une densité de probabilité, alors $F : x \longmapsto \int_{-\infty}^{x} f(t)dt$ est la fonction de répartition d'une variable aléatoire Y telle que $\mathbb{P}_Y$ admette pour densité f.

Application 19. On définit l'inverse généralisée de F_X par $F^{\leftarrow}(u) = \inf\{t \mid F_X(t) \geq u\}$ pour $u \in [0,1]$. Alors si $U \sim \mathcal{U}([0,1])$, on a que $F^{\leftarrow}(U) \sim \mathbb{P}_X$. Par exemple $-\ln(1-U) \sim \mathcal{E}(1)$.

Proposition 20. *F_X caractérise $\mathbb{P}_X$.*

Remarque 21. On peut généraliser la notion de fonction de répartition pour une variable aléatoire à valeurs dans $\mathbb{R}^d$. Le résultat reste alors valable.

II. B. Fonction caractéristique

[BL07, §III.5, p61]

Soit X une variable aléatoire à valeurs dans $\mathbb{R}^d$.

Définition 22. [Fonction caractéristique]
On définit ϕ_X la fonction caractéristique de X par $\phi_X(\lambda) = \mathbb{E}\left[e^{i\langle\lambda|X\rangle}\right]$ pour $\lambda \in \mathbb{R}^d$.

Exemple 23. Fonctions caractéristiques de $\mathcal{B}(n,p), \mathcal{E}(\lambda)\ldots$ **[voir annexe]**

Proposition 24. *ϕ_X caractérise $\mathbb{P}_X$.*

Proposition 25. *Si X est réelle et admet un moment d'ordre p, alors ϕ_X est p fois dérivable et on a $\phi_X^{(p)}(\lambda) = i^p\mathbb{E}[X^p e^{i\lambda X}]$. En particulier, $\phi^{(p)}(0) = i^p\mathbb{E}[X^p]$.*

Remarque 26. [Ouv09, p205] Réciproquement, si p est pair est ϕ_X est p fois dérivable en 0, alors X admet un moment d'ordre p. On peut construire X n'admettant pas d'espérance mais telle que ϕ_X soit dérivable en 0 (admis).

II. C. Fonction génératrice

[Ouv08, §5.3, p138]

Soit X une variable aléatoire à valeurs dans $\mathbb{N}$ presque sûrement.

Définition 27. [Fonction génératrice]
On définit g_X la fonction génératrice de X par $g_X(s) = \mathbb{E}[s^X] = \sum_{k\geq 0}\mathbb{P}(X = k)s^k$ (lorsque la série converge).

Remarque 28. Le rayon de convergence de cette série est au moins égal à 1 et $G_X(1) = 1$.

Exemple 29. Fonctions génératrices de $\mathcal{B}(p), \mathcal{B}(n,p), \mathcal{P}(\lambda), \mathcal{G}(p)\ldots$ **[voir annexe]**

Proposition 30. *G_X caractérise $\mathbb{P}_X$. En particulier, $\forall k \in \mathbb{N}, \mathbb{P}(X = k) = \frac{G^{(k)}(0)}{k!}$.*

Proposition 31. *X admet un moment d'ordre $p \in \mathbb{N}^*$ si et seulement si g_X est p fois dérivable en 1, et dans ce cas $G_X^{(p)}(1) = \mathbb{E}[X(X-1)\ldots(X-p)]$.*

Application 32. Expression de l'espérance, la variance, ou plus généralement d'un moment en fonction des dérivées en 0 de G_X.

Application 33. Calcul de la loi d'une variable aléatoire multinomiale dont le paramètre n n'est pas déterministe mais suit une loi $\mathcal{P}(\lambda)$.

II. D. Moments et fonction génératrice des moments

[BL07, §III.5, p66]

Soit X une variable aléatoire réelle.

Définition 34. [Moment et moment centré d'ordre p]
Si $\mathbb{E}[|X|^p] < +\infty$, on dit que X admet un moment d'ordre p (ou $X \in L^p$) et alors on appelle $\mathbb{E}[X^p]$ le moment d'ordre p et $\mathbb{E}[(X - \mathbb{E}[X])^p]$ le moment centré d'ordre p de X.

Proposition 35. *Si $X \in L^p$ alors $X \in L^q$ pour tout $1 \leq q \leq p$.*

Définition 36. [Fonction génératrice des moments]
On définit M_X la fonction génératrice des moments de X par $M_X(\lambda) = \mathbb{E}[e^{\lambda X}]$ pour $\lambda \in \mathbb{R}$ tel que cette quantité soit définie.

Exemple 37. $M_{\mathcal{N}(0,1)} : \lambda \longmapsto \exp(\lambda^2/2)$ et $M_{\mathcal{R}(1/2)} : \lambda \longmapsto \mathrm{ch}(\lambda)$.

Proposition 38. *Si M_X est définie sur un voisinage de 0, alors M_X caractérise $\mathbb{P}_X$ et alors on a $M_X(\lambda) = \sum_{k\geq 0}\frac{t^k}{k!}\mathbb{E}[X^k]$ au voisinage de 0, en particulier X admet des moments de tout ordre et $\mathbb{E}[X^p] = M_X^{(p)}(0)$ pour tout p.*

Théorème 39. **[Théorème des moments]** *(admis)*
Si X et Y sont bornées p.s. et si leurs moments sont égaux à tout ordre, alors $X \sim Y$.

Remarque 40. C'est faux si X et Y ne sont pas bornées : les considérer de densités $f_X : x \longmapsto \frac{1}{\sqrt{2\pi}x} \mathrm{e}^{-\ln(x)^2/2} \mathbb{1}_{\mathbb{R}^+}(x)$ et $f_Y : x \longmapsto f_X(x)(1+a\sin(2\pi\ln(x)))$ pour un $a \in [-1,1]$.

III. Vecteurs aléatoires et indépendance

[BL07, ChIV, p73]

Soient X, Y deux variables aléatoires à valeurs dans E, F des espaces probabilisables.

Définition 41. **[Lois conjointes, lois marginales]**
La loi du couple (X,Y) est appelée loi conjointe.
Les lois de X et de Y sont appelées lois marginales.

Remarque 42. La donnée de la loi conjointe permet de retrouver les lois marginales. La réciproque est fausse : si $X \perp\!\!\!\perp Y \sim \mathcal{B}(1/2)$, alors (X,X) et (X,Y) ont même lois marginales mais pas même loi conjointe.

Proposition 43. *X et Y sont indépendantes si et seulement si :*
(i) $\mathbb{P}_{(X,Y)} = \mathbb{P}_X \otimes \mathbb{P}_Y$,
et lorsque $E = \mathbb{R}^d$ et $F = \mathbb{R}^\ell$:
(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, f_2 définies sur $\mathbb{R}^d$ et $\mathbb{R}^\ell$ respectivement,*
(iii) $\forall(\lambda_1,\lambda_2) \in \mathbb{R}^d \times \mathbb{R}^\ell, \phi_{(X,Y)}(\lambda_1,\lambda_2) = \phi_X(\lambda_1)\phi_Y(\lambda_2)$.
Si X et Y sont indépendantes, alors $\mathrm{Cov}(X,Y) = 0$, $\mathbb{P}_{X+Y} = \mathbb{P}_X * \mathbb{P}_Y$ et $G_{X+Y} = G_X G_Y$ lorsque ces quantités sont définies.

Remarque 44. On peut généraliser ces propositions à des familles quelconques de v.a..

Application 45. Un vecteur gaussien est une variable aléatoire à valeurs dans $\mathbb{R}^d$ telle que toute combinaison linéaire de ses composantes suit une loi normale. Les composantes d'un vecteur gaussien sont indépendantes si et seulement si sa matrice de covariance est diagonale.

IV. Convergence en loi

[BL07, §V.4, p121]

Soient $(X_n)_{n\in\mathbb{N}}$ et X des variables aléatoires à valeurs dans $\mathbb{R}^d$.

Définition 46. **[Convergence en loi]**
On dit que $(X_n)_{n\in\mathbb{N}}$ converge en loi vers X si pour tout fonction $f \in \mathcal{C}_b(\mathbb{R}^d)$, on a $\mathbb{E}[f(X_n)] \underset{n\to+\infty}{\longrightarrow} \mathbb{E}[f(X)]$.

Exemple 47. $X_n \sim \mathcal{N}(0,\sigma_n^2)$ converge en loi vers $X \sim \mathcal{N}(0,\sigma^2)$ si $\sigma_n \to \sigma$.

Théorème 48. **[Théorème de Lévy (faible)]**
$X_n \underset{n\to+\infty}{\overset{\mathcal{L}}{\longrightarrow}} X$ si et seulement si $\phi_{X_n} \underset{n\to+\infty}{\overset{s}{\longrightarrow}} \phi_X$.

Supposons maintenant $d = 1$ et les variables aléatoires réelles.

Proposition 49. *Si les variables sont à valeurs dans $\mathbb{N}$, $X_n \underset{n\to+\infty}{\overset{\mathcal{L}}{\longrightarrow}} X$ si et seulement si $\forall k \in \mathbb{N}, \mathbb{P}(X_n = k) \underset{n\to+\infty}{\longrightarrow} \mathbb{P}(X = k)$.*

Proposition 50. *$X_n \underset{n\to+\infty}{\overset{\mathcal{L}}{\longrightarrow}} X$ si et seulement si $F_{X_n} \underset{n\to+\infty}{\longrightarrow} F_X$ en tout point de continuité de F_X.*

Théorème 51. **[Théorème central limite]**
Si les $(X_i)_{i\in\mathbb{N}^*}$ sont i.i.d. de carré intégrable, alors :

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n (X_i - \mathbb{E}[X_1]) \underset{n\to+\infty}{\overset{\mathcal{L}}{\longrightarrow}} Z \sim \mathcal{N}(0, \mathrm{Var}(X_1))$$

Application 52. **[Intervalle de confiance asymptotique]** [RS12, §3.4, p25]
Soient $(X_i)_{i\in\mathbb{N}^*}$ des réalisations i.i.d. de $\mathcal{B}(p)$ pour un $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\hat{p}_n = \frac{1}{n}\sum_{k=1}^n X_i : \mathrm{IC}_\alpha(p) = \left[\hat{p}_n \pm \frac{q_{1-\alpha/2}}{2}\frac{1}{\sqrt{n}}\right]$, où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Application 53. **[Méthode de Monte-Carlo]** [Mé11]
Soit $f : [0,1] \longrightarrow \mathbb{R}$ intégrable par rapport à la mesure de Lebesgue et $(X_i)_{n\in\mathbb{N}^*}$ une suite de variables aléatoires i.i.d. de loi $\mathcal{U}([0,1])$. Alors $I_n = \frac{1}{n}\sum_{i=1}^n f(X_i) \underset{n\to+\infty}{\longrightarrow} \int_0^1 f(x)dx$ p.s..

Théorème 54. [Théorème de Slutsky]
Reprenons les $(X_n)_n$ et X dans $\mathbb{R}^d$ et soient $(Y_n)_{n\in\mathbb{N}}$ des variables aléatoires de $\mathbb{R}^\ell$ ($\ell \in \mathbb{N}^*$) convergeant en probabilité vers une constante c. Alors $(X_n, Y_n) \xrightarrow[n\to+\infty]{\mathcal{L}} (X, c)$.

Application 55. [Intervalle de confiance asymptotique 2]
Dans le même cadre on a l'intervalle de confiance asymptotique : $\widetilde{\mathrm{IC}}_\alpha(p) = \left[\hat{p}_n \pm q_{1-\alpha/2}\frac{\sqrt{\hat{p}_n(1-\hat{p}_n)}}{\sqrt{n}}\right]$.

ANNEXE

[BL07, Appendice, p229]
Tableau des principales lois discrètes
Soit X une loi discrète et $p \in [0,1], q \in]0,1[, n \in \mathbb{N}, \lambda > 0$.

$\mathcal{L}(X)$	$\mathbb{P}_X$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$\phi_X(t)$	$G_X(t)$
$\mathcal{U}(\llbracket 1,n \rrbracket)$	$\sum_{k=1}^{n} \frac{1}{n}\delta_k$	$\frac{n+1}{2}$	$\frac{n^2-1}{12}$	$\frac{1}{n}\sum_{k=1}^{n} \mathrm{e}^{ikt}$	$\frac{1}{n}\frac{t-t^{n+1}}{1-t}$ $(t\neq 1)$
$\mathcal{B}(p)$	$p\delta_1 + (1-p)\delta_0$	p	$p(1-p)$	$p\,\mathrm{e}^{it}+(1-p)$	$1-p+pt$
$\mathcal{B}(n,p)$	$\sum_{k=0}^{n}\binom{n}{k}p^k(1-p)^{n-k}\delta_k$	np	$np(1-p)$	$p\,\mathrm{e}^{it}+(1-p)^n$	$(1-p+pt)^n$
$\mathcal{P}(\lambda)$	$\sum_{k=0}^{\infty}\frac{\lambda^k \mathrm{e}^{-\lambda}}{k!}\delta_k$	λ	λ	$\mathrm{e}^{\lambda(\mathrm{e}^{it}-1)}$	$\mathrm{e}^{(\lambda-1)t}$
$\mathcal{G}(q)$	$\sum_{k=1}^{\infty} q(1-q)^{k-1}\delta_k$	$\frac{1}{q}$	$\frac{1-q}{q^2}$	$\frac{q\,\mathrm{e}^{it}}{1-(1-q)\,\mathrm{e}^{it}}$	$\frac{pt}{1-(1-p)t}$

Tableau des principales lois à densité
Soit X une loi admettant une densité f par rapport à la mesure de Lebesgue. Soit $a < b \in \mathbb{R}, m \in \mathbb{R}, \sigma > 0, \lambda > 0, \alpha, \beta > 0$.

$\mathcal{L}(X)$	$f(t)$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$\phi_X(t)$
$\mathcal{U}([a,b])$	$\frac{\mathbb{1}_{[a,b]}(t)}{b-a}$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$	$\frac{\mathrm{e}^{itb}-\mathrm{e}^{ita}}{it(b-a)}$
$\mathcal{N}(m,\sigma^2)$	$\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(t-m)^2}{2\sigma^2}\right)$	m	σ^2	$\mathrm{e}^{imt-\frac{t^2\sigma^2}{2}}$
$\mathcal{C}(m,\sigma^2)$	$\frac{1}{\pi\sigma}\frac{1}{1+(\frac{t-m}{\sigma})^2}$	/	/	$\mathrm{e}^{-\lvert t\rvert}$
$\mathcal{E}(\lambda)$	$\lambda\exp(-\lambda t)\mathbb{1}_{[0,+\infty[}(t)$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	$\frac{1}{1-\frac{it}{\lambda}}$
$\Gamma(\alpha,\beta)$	$\frac{\beta^\alpha}{\Gamma(\alpha)}\mathrm{e}^{-\beta t}t^{\alpha-1}\mathbb{1}_{[0,+\infty[}(t)$	$\frac{\alpha}{\beta}$	$\frac{\alpha}{\beta^2}$	$\left(1-\frac{it}{\beta}\right)^{-\alpha}$

COMMENTAIRES

Point de vue historique : la théorie des probabilités a été formalisée dans les années 30 par KOLMOGOROV. Théorème de DE MOIVRE-LAPLACE $\rightarrow$ TCL dans le cadre d'une loi binomiale.
Aujourd'hui point de vue fonctionnel : les variables aléatoires ... il est plus intéressant d'étudier la loi d'une variable aléatoire plutôt que la variable aléatoire en elle-même.

QUESTIONS

Q Une variable aléatoire sans atomes admet-elle nécessairement une densité ?

R Non ! Penser par exemple à l'escalier de CANTOR ... C'est la fonction de répartition d'une certaine variable aléatoire X ! On a alors $\mathbb{P}(X \in K) = 1$ où K est l'ensemble de CANTOR. La loi est sans atome et n'admet pas de densité car $\mathrm{Leb}(K) = 0$.

BIBLIOGRAPHIE

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[Mé11] S. MÉLÉARD : *Aléatoire : introduction à la théorie et au calcul des probabilités*. Les éditions de l'École Polytechnique, 2011.

[Ouv08] J.-Y. OUVRARD : *Probabilités : Tome 1*. Cassini, 2ème édition, 2008.

[Ouv09] J.-Y. OUVRARD : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[RS12] V. RIVOIRARD et G. STOLTZ : *Statistique mathématique en action*. Vuibert, 2 ème édition, 2012.

262 CONVERGENCES D'UNE SUITE DE VARIABLES ALÉATOIRES. THÉORÈMES LIMITE. EXEMPLES ET APPLICATIONS.

$(\Omega, \mathcal{A}, \mathbb{P})$ espace probabilisé. On considère des variables aléatoires à valeurs dans $\mathbb{R}^d$.

I. Modes de convergence

[BL07, ChV, p109] [Ouv09, Ch10, p89]

Soit $(X_n)_n$ et X des variables aléatoires définies sur un même espace probabilisé.

I. A. Convergence presque sure

Définition
Lemme de Borel-Cantelli, application à la convergence de $\frac{\max \mathcal{E}(1)}{\ln(n)}$ vers 1 presque sûrement.

Proposition 1. [Inégalité de Hoeffding]
Soient $(X_i)_{1\leq i\leq n}$ des variables aléatoires réelles indépendantes, centrées et telles que pour tout $i \in [\![1, n]\!]$, $|X_i| \leq c_i$ p.s. pour un réel c_i. Alors pour tout $t \geq 0$:

$$\mathbb{P}(|S_n| \geq t) \leq 2\,\mathrm{e}^{-t^2/2\sum_{i=1}^n c_i^2} \qquad \text{où } S_n = \sum_{i=1}^n X_i$$

Corollaire 2. *Supposons maintenant la suite $(X_i)_{i\in\mathbb{N}}$ infinie, avec les mêmes hypothèses.*
S'il existe $\alpha, \beta > 0$ tels que $\sum_{i=1}^n c_i^2 \leq n^{2\alpha-\beta}$, alors $\frac{S_n}{n^\alpha} \underset{n\to+\infty}{\longrightarrow} 0$ p.s..

Stabilité de la convergence presque sure par somme, produit

I. B. Convergence en probabilité

Définition, indépendance avec la norme choisie, compatibilité avec le couple, et par passage à une fonction continue
Exemple
Inégalités de concentration : Bienaymé-Tchebychev, Hoeffding, donnent des convergences en probabilité

I. C. Convergence L^p

Définition, exemple

I. D. Convergence en loi

Variables plus nécessairement définies sur le même espace probabilisé

Définition 3. [convergence en loi]
On dit que $(X_n)_{n\in\mathbb{N}}$ converge en loi vers X si pour tout fonction $f \in \mathcal{C}_b(\mathbb{R}^d)$, on a $\mathbb{E}[f(X_n)] \underset{n\to+\infty}{\longrightarrow} \mathbb{E}[f(X)]$.

Définition, convergence ne dépendant que de la loi des variables aléatoires

Exemple 4. $X_n \sim \mathcal{N}(0, \sigma_n^2)$ converge en loi vers $X \sim \mathcal{N}(0, \sigma^2)$ si $\sigma_n \to \sigma$.

Théorème de Portmanteau
En dimension 1 :

Proposition 5. *$X_n \underset{n\to+\infty}{\xrightarrow{\mathcal{L}}} X$ si et seulement si $F_{X_n} \underset{n\to+\infty}{\longrightarrow} F_X$ en tout point de continuité de F_X.*

Proposition 6. *Si les variables sont à valeurs dans $\mathbb{N}$, $X_n \underset{n\to+\infty}{\xrightarrow{\mathcal{L}}} X$ si et seulement si $\forall k \in \mathbb{N}, \mathbb{P}(X_n = k) \underset{n\to+\infty}{\longrightarrow} \mathbb{P}(X = k)$.*

Incompatibilité avec l'addition

II. Liens entre les modes de convergence

[BL07, ChV, p109] [Ouv09, §Ch10, p89]

II. A. Implications

Convergence L^p implique convergence L^q pour $p > q$, contre-exemple sinon
Convergence p.s. implique en convergence probabilité : contre-exemple de $X_n \sim \mathcal{B}(1/n)$
Convergence L^p implique convergence en probabilité
Convergence L^p n'implique pas convergence p.s., mais on peut extraire une sous-suite convergeant p.s. Contre-exemple de $X_n \sim \mathcal{B}(1/n)$ (idem avec convergence en probabilité verscon-vergence p.s.)
Convergence p.s. implique convergence L^p si domination. Contre-exemple de $X_n \sim n^2\mathcal{B}(1/n^2)$
Convergence en probabilités implique convergence en loi, la réciproque est vraie si la variable limite est constante p.s., fausse dans le cas général : si $X \sim \mathcal{B}(1/2)$, alors $1 - X \underset{n\to+\infty}{\longrightarrow} X$ en loi mais pas en probabilités.

II. B. Notion d'uniforme continuité

Variables uniformément intégrables
Exemple avec des familles finies/iid/dominées L^1

Formulation équivalente
UI de variables aléatoires définies comme espérances conditionnelles d'une variable aléatoire L^1
Convergence en proba et UI équivaut à convergence L^1
Application à la convergence L^1 de martingales

III. Théorèmes limites

[BL07, ChV, p109]

III. A. Loi des grands nombres et théorème central limite

Théorème 7. [Loi des grands nombres]
Soit $(X_i)_{i\in\mathbb{N}^*}$ des variables aléatoires réelles i.i.d. intégrables. Alors :

$$\frac{1}{n}\sum_{i=1}^n X_i \underset{n\to+\infty}{\longrightarrow} \mathbb{E}[X_1] \quad p.s.$$

L'hypothèse d'intégrabilité est cruciale :

Proposition 8. *Soient $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires i.i.d. telle que $\mathbb{E}[|X_1|] = +\infty$. Alors la probabilité que la limite de $\frac{1}{n}\sum_{i=1}^n X_i$ existe dans $\mathbb{R}$ est nulle.*

Application 9. [Méthode de Monte-Carlo] [Mé11]
Soit $f : [0,1] \longrightarrow \mathbb{R}$ intégrable par rapport à la mesure de Lebesgue et $(X_i)_{n\in\mathbb{N}^*}$ une suite de variables aléatoiresi.i.d. de loi $\mathcal{U}([0,1])$. Alors $I_n = \frac{1}{n}\sum_{i=1}^n f(X_i) \underset{n\to+\infty}{\longrightarrow} \int_0^1 f(x)dx$ p.s..

Théorème 10. [Théorème central limite]
Si les $(X_i)_{i\in\mathbb{N}^*}$ sont i.i.d. de carré intégrable, alors :

$$\frac{1}{\sqrt{n}}\sum_{i=1}^n (X_i - \mathbb{E}[X_1]) \underset{n\to+\infty}{\overset{\mathcal{L}}{\longrightarrow}} Z \sim \mathcal{N}(0, \mathrm{Var}(X_1))$$

Application 11. [Intervalle de confiance asymptotique] [RS12, §3.4, p25]
Soient $(X_i)_{i\in\mathbb{N}^*}$ des réalisations i.i.d. de $\mathcal{B}(p)$ pour un $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\hat{p}_n = \frac{1}{n}\sum_{k=1}^n X_i$: $\mathrm{IC}_\alpha(p) = \left[\hat{p}_n \pm \frac{q_{1-\alpha/2}}{2}\frac{1}{\sqrt{n}}\right]$, où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

Application 12. Dans la méthode de Monte-Carlo, on obtient un intervalle de confiance de probabilité asymptotique $1-\alpha$ de longueur proportionnelle à $1/\sqrt{n}$.

Théorème 13. [Théorème de Slutsky]
Reprenons les $(X_n)_n$ et X dans $\mathbb{R}^d$ et soient $(Y_n)_{n\in\mathbb{N}}$ des variables aléatoires de $\mathbb{R}^\ell$ ($\ell \in \mathbb{N}^*$) convergeant en probabilité vers une constante c. Alors $(X_n, Y_n) \underset{n\to+\infty}{\overset{\mathcal{L}}{\longrightarrow}} (X, c)$.

Application 14. [Intervalle de confiance asymptotique 2]
Dans le même cadre on a l'intervalle de confiance asymptotique : $\widetilde{\mathrm{IC}}_\alpha(p) = \left[\hat{p}_n \pm q_{1-\alpha/2}\frac{\sqrt{\hat{p}_n(1-\hat{p}_n)}}{\sqrt{n}}\right]$.

TCL multidimensionnel, application aux marches aléatoires $\to$ nombre de visites dans $\mathbb{B}(0,R)$.

III. B. Convergence de chaines de Markov

[BL07, ChVIII]

Chaînes de Markov, mesures invariantes
Irréductibilité, apériodicité
Propriétés de Markov
Conditions d'existence/unicité de mesures invariantes
Théorème ergodique, cas d'un espace d'état fini
Exemples ...

ANNEXE

Liens entre les modes de convergence

COMMENTAIRES

Intérêt de la méthode de MONTE-CARLO : ça converge toujours à vitesse $\sqrt{n}$ quelque soit la dimension (application du TCL multidimensionnel) : en dimension 1 on a des méthodes plus rapides, mais pas en multidimentionnel.

QUESTIONS

Q Soit $(X_n)_n$ telles que $X_n \sim \mathcal{N}(m_n, \sigma_n^2)$. Si $m_n \longrightarrow m$ et $\sigma_n \longrightarrow \sigma$, que dire de $(X_n)_n$?

R X_n a même loi que $m_n + \sigma_n Z$ où $Z \sim \mathcal{N}(0,1)$, Or $m_n + \sigma_n Z \longrightarrow m + \sigma Z$ presque sûrement, ce qui implique la convergence en loi.
Donc $X_n \longrightarrow \mathcal{N}(m, \sigma^2)$ en loi (si $\sigma = 0$, c'est δ_m).

Q Soit $X_n \in [\![0, N]\!]$ telle que $\forall k \in \mathbb{N}, \mathbb{E}[X_n^k] \longrightarrow \mathbb{E}[X^k]$. A-t-on $X_n \longrightarrow X$ en loi ? X reste-t-elle dans $[\![0, N]\!]$?

R On vérifie que X est positive, et si $X > N$ avec probabilité positive, on vérifie aussi que ce n'est pas possible ... Par convergence dominée (trois fois !) :

$$\phi_{X_n}(t) = \mathbb{E}\Big[\sum_{k\geq 0} \frac{i^k X_n^k t^k}{k!}\Big] = \sum_{k\geq 0} \mathbb{E}\Big[\frac{i^k X_n^k t^k}{k!}\Big] = \sum_{k\geq 0} \frac{i^k \mathbb{E}[X_n^k] t^k}{k!}$$
$$\underset{n\to+\infty}{\longrightarrow} \sum_{k\geq 0} \frac{i^k \mathbb{E}[X^k] t^k}{k!} = \phi_X(t)$$

Puis $\mathbb{P}(X \in]0, N[) \leq \liminf_n \mathbb{P}(X_n \in]0, N[) = 0$ donc $X \in [\![0, N]\!]$ p.s..

Q Soit une particule évoluant entre trois points : on passe de 1 à 2 ou de 1 à 3 avec proba $1/2$. Si elle est en 2, elle reste avec proba $1/2$ et va en 1 ou 3 avec proba $1/4$. Si elle est en 3 elle va avec proba $1/2$ en 1 ou 2. On part de $X_0 = 1$ et X_n est la position au temps n. Quelle est la loi limite ? Que se passe-t-il si on change les probas de transition ? Le nombre d'états ? La condition initiale ? Quelles sont les conditions nécessaires ?

R On cherche un vecteur propre à gauche associé à 1 pour $Q = \begin{pmatrix} 0 & 1/2 & 1/2 \\ 1/4 & 1/2 & 1/4 \\ 1/2 & 1/2 & 0 \end{pmatrix}$.
On sait que $Q^\top$ a 1 pour valeur propre de multiplicité 1 (par le théorème de PERRON-FROBENIUS). Donc Q aussi.

BIBLIOGRAPHIE

[BL07] P. BARBE et M. LEDOUX : *Probabilité*. EDP Sciences, 2007.

[Mé11] S. MÉLÉARD : *Aléatoire : introduction à la théorie et au calcul des probabilités*. Les éditions de l'École Polytechnique, 2011.

[Ouv09] J.-Y. OUVRARD : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[RS12] V. RIVOIRARD et G. STOLTZ : *Statistique mathématique en action*. Vuibert, 2 ème édition, 2012.

264 VARIABLES ALÉATOIRES DISCRÈTES. EXEMPLES ET APPLICATIONS.

Soit $(\Omega, \mathcal{A}, \mathbb{P})$ un espace probabilisé, et $(E, \mathcal{E})$ un espace probabilisable.

I. Généralités sur les variables aléatoires discrètes
[Ouv08, Ch1, p14–20]

I. A. Caractérisation d'une variable aléatoire discrète

Définition 1. [Variable aléatoire discrète]
Une variable aléatoire X est une fonction mesurable $X : (\Omega, \mathcal{A}) \longrightarrow (E, \mathcal{E})$.
Si de plus $X(\Omega)$ est dénombrable presque sûrement, alors on dit que X est discrète.
On note $\mathbb{P}_X$ la mesure image de $\mathbb{P}$ par X et on l'appelle loi de X.

Exemple 2. On lance une pièce, un dé, et on note X la variable aléatoire qui associe la face de la pièce ou la valeur du dé. Alors X est discrète.

Soit X une variable aléatoire discrète à valeurs dans E.

Proposition 3. *Enumérons $E' = (e_i)_{i\in I} \subset E$ où I est au plus dénombrable de sorte que $X(\Omega) \subset E'$ p.s.. Alors $\mathbb{P}_X$ est caractérisée par la famille $(p_i)_{i\in I}$ où $p_i = \mathbb{P}(X = e_i)$ et $\sum_{i\in I} p_i = 1$. De plus, on a $\mathbb{P}_X = \sum_{i\in I} p_i \delta_{e_i}$.*

I. B. 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 ($\mathbb{P}_X$, espérance, variance, ...). **[voir annexe]**

Application 4. [Modélisation par des variables aléatoires discrètes]
- on lance une pièce équilibrée et on note $X = 1$ si le résultat est « face », 0 sinon. Alors $X \sim \mathcal{B}(1/2)$,
- si on lance n fois la pièce de manière indépendante, le nombre X de succès suit $\mathcal{B}(n, 1/2)$,
- le résultat du jet d'un dé à 6 faces équilibré se modélise par $\mathcal{U}(\llbracket 1, 6 \rrbracket)$.
- 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 $\mathcal{P}(N\ell)$.
- on lance une pièce équilibrée et on note X le nombre de lancers nécessaires avant d'obtenir « face ». Alors $X \sim \mathcal{G}(1/2)$.

I. C. Variables aléatoires discrètes et indépendance
[Ouv08, Ch3/4, p51–86]

Définition 5. [Indépendance de variables aléatoires]
Soit I un ensemble et $(X_i)_{i\in I}$ des variables aléatoires telles que X_i est à valeurs dans $(E_i, \mathcal{E}_i)$. On dit que les $(X_i)_{i\in I}$ sont indépendantes si pour tout $J \subset I$ fini, on a :

$$\forall (A_i)_{i\in J} \in \prod_{i\in J} \mathcal{E}_i, \mathbb{P}(\cap_{i\in I} X_i \in A_i) = \prod_{i\in J} \mathbb{P}(X_i \in A_i)$$

Proposition 6. [Indépendance de variables aléatoires discrètes]
Soit I un ensemble et $(X_i)_{i\in I}$ des variables aléatoires discrètes à valeurs dans $(E_i, \mathcal{E}_i)_{i\in I}$.
Soit $(E_i')_{i\in I}$ des ensembles dénombrables tels que $\forall i \in I, X_i \in E_i'$ p.s..
Alors les $(X_i)_{i\in I}$ sont indépendantes si et seulement si pour tout $J \subset I$ fini, on a :

$$\forall (e_i)_{i\in J} \in \prod_{i\in J} E_i', \mathbb{P}(\cap_{i\in J} X_i = e_i) = \prod_{i\in J} \mathbb{P}(X_i = e_i)$$

Exemple 7. Soient X, 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 8. *Soient X, Y des variables aléatoires discrètes indépendantes à valeurs dans $\mathbb{R}$. Alors $\mathbb{P}_{X+Y} = \mathbb{P}_X * \mathbb{P}_Y$ où $\mathbb{P}_X * \mathbb{P}_Y(z) = \sum_{x+y=z} \mathbb{P}_X(x)\mathbb{P}_Y(y)$.*

Exemple 9. Soient $p \in [0, 1]$, $n_1, n_2 \in \mathbb{N}$, $\lambda_1, \lambda_2 > 0$.
- Si $X \sim \mathcal{B}(n_1, p)$ et $Y \sim \mathcal{B}(n_2, p)$ avec $X \perp\!\!\!\perp Y$, alors $X + Y \sim \mathcal{B}(n_1 + n_2, p)$,
- Si $X \sim \mathcal{P}(\lambda_1)$ et $Y \sim \mathcal{P}(\lambda_2)$ avec $X \perp\!\!\!\perp Y$, alors $X + Y \sim \mathcal{P}(\lambda_1 + \lambda_2)$,

Application 10. [Marche aléatoire simple sur $\mathbb{Z}^d$]
Soient $(X_i)_{i\in\mathbb{N}^*}$ des variables aléatoires i.i.d. de loi $\mathcal{U}(\{\pm e_i, 1 \le i \le d\})$ où $e_i = (0, \dots, 0, 1, 0, \dots, 0) = (\delta_{i\,k})_{1\le k\le n}$. On pose $S_0 = 0$ et $S_n = \sum_{k=1}^n X_i$ pour $n \in \mathbb{N}^*$.
Alors si $d \le 2$, on a $\mathbb{P}(S_n = 0 \text{ i. s.}) = 1$ et si $d > 2$, on a $\mathbb{P}(|S_n| \to +\infty) = 1$.

I. D. Conditionnement
[Ouv08, Ch4, p87–115]

Définition 11. [Probabilité conditionnelle]
Soit $B \in \mathcal{A}$ tel que $\mathbb{P}(B) > 0$. On définit $\mathbb{P}_{\,|\,B}$ l'application qui à $A \in \mathcal{A}$ associe $\mathbb{P}_{\,|\,B}(A) = \mathbb{P}(A \,|\, B) = \frac{\mathbb{P}(A\cap B)}{\mathbb{P}(B)}$. C'est une probabilité sur $(\Omega, \mathcal{A})$ appelée probabilité sachant B.

Exemple 12. $\mathbb{P}_{\,|\,B}(A) = \mathbb{P}(A)$ si A et B sont indépendants.

Proposition 13. [Intersection d'événements]
Soit $(A_i)_{1\leq i\leq n}$ une famille d'événements tels que $\mathbb{P}(\cap_{i=1}^{n-1} A_i) \neq 0$. Alors :

$$\mathbb{P}(\cap_{i=1}^{n} A_i) = \mathbb{P}(A_1)\prod_{i=2}^{n} \mathbb{P}(A_i \mid \cap_{j=1}^{i-1} A_j)$$

Exemple 14. On tire successivement 4 cartes dans un jeu de 52 cartes (sans remise). Quelle est la probabilité de tirer les 4 as ?

Proposition 15. *Soit $(A_i)_{i\in I}$ une famille dénombrable d'événements disjoints deux à deux tels que $\mathbb{P}(\cap_{i\in I} A_i) = 1$ et pour tout $i \in I$, $\mathbb{P}(A_i) > 0$. Alors pour tout $A \in \mathcal{A}$:*

- **[Formule des probabilités totales]** $\mathbb{P}(A) = \sum_{i\in I} \mathbb{P}(A \mid A_i)\mathbb{P}(A_i)$,
- **[Formule de Bayes]** *Si $\mathbb{P}(A) > 0$, on a $\mathbb{P}(A_i \mid A) = \frac{\mathbb{P}(A \mid A_i)\mathbb{P}(A_i)}{\sum_{j\in I} \mathbb{P}(A \mid A_j)\mathbb{P}(A_j)}$ pour tout $i \in I$.*

Exemple 16. On place b_1 et n_1 (resp. b_2 et n_2) boules blanches et noires dans une urne U_1 (resp. U_2). On choisit une urne aléatoirement et on tire une boule dans cette urne. Quelle est la probabilité qu'elle soit noire ? que l'on ait choisi l'urne 1 sachant qu'elle est noire ?

Remarque 17. Ces formules sont très pratiques lorsque l'on prend pour $\mathbb{P}$ la loi d'une variable aléatoire discrète. Dans le cas où $\mathbb{P}$ n'est pas discrète, le fait d'avoir une famille satisfaisant les hypothèses de la proposition rend « moralement » cette probabilité discrète.

II. Moments et fonction génératrice

[Ouv08, Ch5, p115–178]

Soient X, Y deux variables aléatoires discrètes à valeurs dans $\mathbb{R}$.

II. A. Espérance et variance

Définition 18. [Espérance]
Si $\sum_{x\in\mathbb{R}} |x|\,\mathbb{P}(X = x) < +\infty$, on dit que X admet une espérance et on définit l'espérance de X par $\mathbb{E}[X] = \sum_{x\in\mathbb{R}} x\mathbb{P}(X = x)$.

Remarque 19. $\mathbb{E}$ est linéaire. Lorsque $X(\Omega) \subset \mathbb{N}$ p.s., on a $\mathbb{E}[X] = \sum_{n\geq 1} \mathbb{P}(X \geq n)$.

Exemple 20. Espérance de $\mathcal{B}(p), \mathcal{B}(n,p), \mathcal{P}(\lambda), \mathcal{G}(p)\ldots$ **[voir annexe]**

Proposition 21. [Lemme de transfert]
Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ borélienne. Alors $f(X)$ admet une espérance si et seulement si $\sum_{x\in\mathbb{R}} |f(x)|\,\mathbb{P}(X = x) < +\infty$ et dans ce cas $\mathbb{E}[f(X)] = \sum_{x\in\mathbb{R}} f(x)\mathbb{P}(X = x)$.

Exemple 22. Si $X \sim \mathcal{G}(1/2)$ et si $f : n \longmapsto \mathbb{1}_{n \text{ est pair}}$ alors $\mathbb{E}[f(X)] = \frac{1}{3}$.

Définition 23. [Covariance, variance]
On définit :

- la covariance de X et Y par $\mathrm{Cov}(X,Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])]$.
- la variance de X par $\mathrm{Var}(X) = \mathrm{Cov}(X,X) = \mathbb{E}[(X - \mathbb{E}[X])^2]$.

Proposition 24. *Cov est une forme bilinéaire symétrique positive et on a $\mathrm{Cov}(X,Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$ et $\mathrm{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2$.*

Exemple 25. Variance de $\mathcal{P}(\lambda), \mathcal{G}(p), \ldots$ **[voir annexe]**

Proposition 26. *Si $X \perp\!\!\!\perp Y$ alors $\mathrm{Cov}(X,Y) = 0$ et $\mathrm{Var}(X+Y) = \mathrm{Var}(X) + \mathrm{Var}(Y)$.*

Exemple 27. La réciproque est fausse : prendre $X \sim \mathcal{U}(\{-1,0,1\})$ et $Y = X^2$.

Remarque 28. Les inégalités classiques faisant intervenir espérance et variance sont valides dans le cas discret, notamment les inégalité de Markov, de Bienaymé-Tchebychev, de Jensen, de Cauchy-Schwarz, …. Ces résultats n'étant pas spécifiques aux variables aléatoires discrètes, nous ne nous étendons pas dessus.

Application 29. [Théorème de Weierstrass]
$\mathbb{R}[X]$ est dense dans $\mathcal{C}([a,b], \mathbb{C}, \|.\|_\infty)$ pour $a < b \in \mathbb{R}$.

II. B. Vers les fonctions génératrices

[CDGM16, p68–75]

On suppose X à valeurs dans $\mathbb{N}$ presque sûrement. Soit $p \in \mathbb{N}^*$.

Définition 30. [Moment et moment centré d'ordre p]
Si $\mathbb{E}[|X|^p] < +\infty$, on dit que X admet un moment d'ordre p (ou $X \in L^p$) et alors on appelle $\mathbb{E}[X^p]$ le moment d'ordre p et $\mathbb{E}[(X - \mathbb{E}[X])^p]$ le moment centré d'ordre p de X.

Proposition 31. *Si $X \in L^p$ alors $X \in L^q$ pour tout $1 \leq q \leq p$.*

Définition 32. [Fonction génératrice]
On définit g_X la fonction génératrice de X par $g_X(s) = \mathbb{E}[s^X] = \sum_{k\geq 0} \mathbb{P}(X = k)s^k$ (lorsque la série converge).

REMARQUE 33. Le rayon de convergence de cette série est au moins égal à 1 et $G_X(1) = 1$.

EXEMPLE 34. Fonctions génératrices de $\mathcal{B}(p), \mathcal{B}(n,p), \mathcal{P}(\lambda), \mathcal{G}(p)\dots$ **[VOIR ANNEXE]**

PROPOSITION 35. *G_X caractérise la loi de X. En particulier : $\forall k \in \mathbb{N}, \mathbb{P}(X=k) = \frac{G^{(k)}(0)}{k!}$.*

PROPOSITION 36. *X admet un moment d'ordre $p \in \mathbb{N}^*$ si et seulement si g_X est p fois dérivable en 1, et dans ce cas $G_X^{(p)}(1) = \mathbb{E}[X(X-1)\dots(X-p)]$.*

PROPOSITION 37. *Si $X \perp\!\!\!\perp Y$ alors $G_{X+Y} = G_X G_Y$.*

APPLICATION 38. Expression de l'espérance, la variance, ou plus généralement d'un moment en fonction des dérivées en 0 de G_X.

APPLICATION 39. $\mathcal{P}(\lambda) +^{\perp\!\!\!\perp} \mathcal{P}(\lambda) = \mathcal{P}(2\lambda)$.

APPLICATION 40. On ne peut pas truquer deux dés de sorte que la somme des points obtenue en les lançant suive une loi uniforme.

PROPOSITION 41. [PROCESSUS DE BRANCHEMENT DE GALTON-WATSON]
Soient $(X_i^j)_{i,j\geq 1}$ des v.a. i.i.d. à valeurs dans $\mathbb{N}$. On note μ leur loi, m leur espérance et 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 $n \in \mathbb{N}$. et enfin $\rho = \mathbb{P}(\exists n \geq 0 \mid Z_n = 0)$. Alors si $\mu \neq \delta_1$, on a :
- *si $m \leq 1$, $\rho = 1$ et on a extinction du processus presque surement,*
- *si $m > 1$, $\rho < 1$ et il y a une probabilité strictement positive de survie.*

REMARQUE 42. Lorsque la variable aléatoire n'est pas à valeur dans $\mathbb{N}$ p.s., on utilise alors la caractérisation par la fonction caractéristique, valable pour des variables aléatoires quelconques. Par exemple pour calculer la loi d'une variable aléatoire multinomiale dont le paramètre n n'est pas déterministe mais suit une loi $\mathcal{P}(\lambda)$.

APPLICATION 43. [LOI MULTINOMIALE POISSONNIFIÉE]
Soient $(p_j)_{1\leq j\leq d}$ des réels positifs tels que $\sum_{1\leq j\leq d} p_j = 1$. Soient $(Y^k)_{k\geq 1}$ des variables aléatoires indépendantes et identiquement distribuées telles que $\mathbb{P}(Y^k = j) = p_j$. Soit N indépendante des $(Y^k)_{k\geq 1}$ de loi $\mathcal{P}(\lambda)$ pour un $\lambda > 0$.
En posant $X^k = (\mathbb{1}_{Y^k=1}, \dots, \mathbb{1}_{Y^k=d})$, la loi de $S = \sum_{k=1}^N X^k$ est $\mathcal{P}(\lambda p_1) \otimes \dots \otimes \mathcal{P}(\lambda p_d)$.

III. Vers les Théorèmes limites

[BL07, §V.5, p131–147]

On considère des variables aléatoires discrètes à valeurs dans $\mathbb{R}$.

III. A. Théorèmes limites

PROPOSITION 44. *Soient $(X_i)_{i\in\mathbb{N}}$ et X des variables aléatoires discrètes. Alors $X_i \xrightarrow[i\to+\infty]{\mathcal{L}} X$ si et seulement si $\forall x \in F, \mathbb{P}(X_i = x) \underset{i\to+\infty}{\longrightarrow} \mathbb{P}(X = x)$, où $F = \cup_{i\in\mathbb{N}} E_i' \cup E'$ est dénombrable, avec $\forall i \in \mathbb{N}, X_i \in E_i'$ p.s. et $X \in E'$ p.s..*

THÉORÈME 45. [THÉORÈME CENTRAL POISSONIEN]
Soit $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires de loi $\mathcal{B}(i,p_i)$ avec $ip_i \underset{i\to+\infty}{\longrightarrow} \lambda > 0$.
Alors $X_i \xrightarrow[i\to+\infty]{\mathcal{L}} X$ où $X \sim \mathcal{P}(\lambda)$.

THÉORÈME 46. [THÉORÈME CENTRAL LIMITE]
Soit $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires réelles i.i.d. de carré intégrable. Alors :

$$\frac{1}{\sqrt{n}} \sum_{i=1}^n (X_i - \mathbb{E}[X_1]) \xrightarrow[n\to+\infty]{\mathcal{L}} Z \sim \mathcal{N}(0, \mathrm{Var}(X_1))$$

APPLICATION 47. [INTERVALLE DE CONFIANCE ASYMPTOTIQUE] [RS12, §3.4, p25]
Soient $(X_i)_{i\in\mathbb{N}^*}$ des réalisations i.i.d. de $\mathcal{B}(p)$ pour un $p \in [0,1]$ inconnu. Le théorème central limite donne un intervalle de confiance asymptotique de niveau α pour p en fonction de la moyenne empirique $\hat{p}_n = \frac{1}{n}\sum_{k=1}^n X_i : \mathrm{IC}_\alpha(p) = \left[\hat{p}_n \pm \frac{q_{1-\alpha/2}}{2}\frac{1}{\sqrt{n}}\right]$, où q_t est le quantile d'ordre t de $\mathcal{N}(0,1)$.

III. B. Chaînes de MARKOV

Définition d'une CM, exemple d'une marche aléatoire
Existence et unicité d'une mesure invariante à constante multiplicative près si la chaîne est irréductible récurrente
Si de plus la chaîne est apériodique et admet une probabilité asymptotique μ, alors on a convergence en loi de X_n vers μ

ANNEXE

[BL07, Appendice, p229]
Tableau des principales lois discrètes
Soit X une loi discrète et $p \in [0,1], q \in]0,1[, n \in \mathbb{N}, \lambda > 0$.

$\mathcal{L}(X)$	$\mathbb{P}_X$	$\mathbb{E}[X]$	$\mathrm{Var}(X)$	$G_X(t)$
$\mathcal{U}(\llbracket 1,n \rrbracket)$	$\sum_{k=1}^{n} \frac{1}{n}\delta_k$	$\frac{n+1}{2}$	$\frac{n^2-1}{12}$	$\frac{1}{n}\frac{t-t^{n+1}}{1-t}$ $(t \neq 1)$
$\mathcal{B}(p)$	$p\delta_1 + (1-p)\delta_0$	p	$p(1-p)$	$1-p+pt$
$\mathcal{B}(n,p)$	$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} \delta_k$	np	$np(1-p)$	$(1-p+pt)^n$
$\mathcal{P}(\lambda)$	$\sum_{k=0}^{\infty} \frac{\lambda^k \mathrm{e}^{-\lambda}}{k!}\delta_k$	λ	λ	$\mathrm{e}^{(\lambda-1)t}$
$\mathcal{G}(q)$	$\sum_{k=1}^{\infty} q(1-q)^{k-1}\delta_k$	$\frac{1}{q}$	$\frac{1-q}{q^2}$	$\frac{pt}{1-(1-p)t}$

COMMENTAIRES

Voir également [Mé11].

QUESTIONS

Q Vous dites dans votre plan que l'on peut aussi utiliser la fonction caractéristique lorsque la variable aléatoire n'est plus à valeurs dans $\mathbb{N}$. Mais si elle l'est, peut-on aussi l'utiliser ? Quels résultats a-t-on ? Avez-vous un exemple de fonction caractéristique ?

R Oui bien sur, car la fonction génératrice n'est rien d'autre que la fonction caractéristique prise en certaines valeurs ! Donc on va avoir des résultats de caractérisation, etc … Je donne l'exemple de la fonction caractéristique d'une loi de Poisson, et dis que dans les autres cas ça revient souvent à remplacer le t de la fonction génératrice par e^{it}.

Q Avez-vous des exemples de processus discrets ?

R Les chaines de Markov, les marches aléatoires qui sont aussi une chaine de Markov d'ailleurs.

Q Pouvez-vous me donner la preuve de votre théorème pour montrer qu'il existe une unique mesure invariante ?

R Alors évidemment, il faudrait introduire tout ce qui est récurrence, transience, temps d'arrêt, mais en gros on va expliciter la mesure en question. On utilise Markov fort, puis si $x \in E$ est fixé, on considère $\nu : y \longmapsto \mathbb{E}[\sum_{n=0}^{T_x-1} \mathbb{1}_{X_n=y}]$.

Q Quelle définition de convergence en loi utilisez-vous et comment on montrez-vous le résultat sur la convergence en loi de variables discrètes.

R J'énonce à l'oral la condition de convergence en loi, puis je ne me souviens que d'un des deux sens, pour lequel je fais un dessin de la fonction à utiliser …

Q Pour montrer le théorème central limite, est-ce vous utilisez cette caractérisation-là ?

R Non il faut passer par la fonction caractéristique, on va pouvoir faire un développement limité à l'ordre 2 car la fonction caractéristique est $\mathcal{C}^2$, les variables aléatoires étant L^2.

Q Soient $(X_i)_i$ des vas indépendantes et identiquement distribuées de loi géométrique. Comment calculeriez-vous la loi de $\inf(X_i)_i$?

R On regarde la fonction de répartition.

Q Et que pouvez-vous me dire de la variable aléatoire qui modélise le temps d'attente avant un deuxième succès ?

R J'hésite un peu mais propose le calcul suivant où T_i est le temps de i-ième succès :

$$\mathbb{P}(X_2 = k) = \sum_{n=1}^{k-1} \mathbb{P}(X_2 = k \cap X_1 = n) = \ldots = (k-1)p^2(1-p)^{k-2}$$

On pouvait également passer par un systèmes complet d'événements : $X_2 = k$ si une seule des $k-1$ premières variables aléatoires indépendantes et identiquement distribuées $\mathcal{B}(p)$ est un succès, …

Q On regarde la marche aléatoire simple sur $\mathbb{Z}$ et A_n l'événement $|S_n| \leq \sqrt{2Cn\ln(n)}$ où C est une constante. On veut montrer que $\liminf A_n$ i.s..

R Ça nous fait penser à utiliser Borel-Cantelli, qui donne $\liminf A_n^c$ i.s.. Je cite ensuite l'inégalité de Hoeffding, on me dit non plus simple, j'écris celle de Bienaymé-Tchebychev mais ça ne suffit pas pour conclure, la majoration est trop grossière. Je repars sur Hoeffding.

Q Ok ça doit marcher comme ça mais est-ce que l'on peut utiliser plus simple ?

R Je ne vois pas. On me dit d'utiliser les fonctions génératrices, mais l'oral s'arrête là.

BIBLIOGRAPHIE

[BL07] P. Barbe et M. Ledoux : *Probabilité*. EDP Sciences, 2007.

[CDGM16] M. Cottrell, C. Duhamel, V. Genon-Catalot et T. Meyre : *Exercices de probabilités*. Cassini, 2016.

[Mé11] S. Méléard : *Aléatoire : introduction à la théorie et au calcul des probabilités*. Les éditions de l'École Polytechnique, 2011.

[Ouv08] J.-Y. Ouvrard : *Probabilités : Tome 1*. Cassini, 2ème édition, 2008.

[RS12] V. Rivoirard et G. Stoltz : *Statistique mathématique en action*. Vuibert, 2ème édition, 2012.

265 EXEMPLES D'ÉTUDES ET D'APPLICATIONS DE FONCTIONS USUELLES ET SPÉCIALES.

I. Utilisation des fonctions usuelles [RDO98, §4.4, p126]

I. A. Autour de l'exponentielle [Rud98, Prologue, p1–4] [AF93, §VI.7, p226]

Définition 1. [Exponentielle, cosinus et sinus]
On définit les séries entières suivantes :

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

Proposition 2.
(i) $\exp, \sin, \cos$ *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,*
(ii) Pour tout $z \in \mathbb{C}$, *on a* $\exp(iz) = \cos(z) + i\sin(z)$,
(iii) Pour $\theta \in \mathbb{R}$, $\cos(\theta)$ *et* $\sin(\theta)$ *sont réels et* $\left|\mathrm{e}^{i\theta}\right| = 1$.
(iv) $\exp$ *est un morphisme surjectif de* $(\mathbb{C}, +)$ *dans* $(\mathbb{C}^*, \times)$ *de noyau* $ia\mathbb{Z}$ *pour un* $a \in \mathbb{R}_+$.
(v) Pour $z_1, z_2 \in \mathbb{C}$, $\exp(z_1 + z_2) = \exp(z_1)\exp(z_2)$,

Remarque 3. On note alors $\mathcal{E} : \mathbb{R} \longrightarrow \mathbb{C}^*, t \longmapsto \mathrm{e}^{it}$ et $\pi = a/2$ (ainsi $\mathrm{e}^{i\pi} + 1 = 0$).
Cette application associe à un angle t l'unique point u de module 1 dont l'angle entre $[Ox)$ et $[Ou)$ est t.

Corollaire 4. [Formule de Moivre et d'Euler]
- *Pour* $n \in \mathbb{N}$ *et* $\theta \in \mathbb{R}$, *on a* $(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$.
- *Pour* $\theta \in \mathbb{R}$, *on a* $\cos(\theta) = \frac{\mathrm{e}^{i\theta} + \mathrm{e}^{-i\theta}}{2}$ *et* $\sin(\theta) = \frac{\mathrm{e}^{i\theta} - \mathrm{e}^{-i\theta}}{2i}$.

Application 5. Développement de $\cos(n\theta)$ et $\sin(n\theta)$ par la formule de Moivre. Linéarisation de $\cos^n(\theta)$ et $\sin^n(\theta)$ par les formules d'Euler. Exemples de $\cos^5(\theta)$ et $\sin(5\theta)$.

Application 6. Polynômes de Tchebychev.

Application 7. Calcul des noyaux de Dirichlet et Fejér :

$$D_N = \sum_{n=-N}^{N} \mathrm{e}^{in\cdot} = \frac{\sin\left(\frac{2N+1}{2}.\right)}{\sin(./2)} \quad \text{et} \quad K_N = \frac{1}{N}\sum_{n=0}^{N-1} D_n = \sum_{n=-N}^{N} \left(1 - \frac{|n|}{N}\right) e_n = \frac{\sin^2(N./2)}{\sin^2(./2)}$$

I. B. Fonctions usuelles et calculs d'intégrales

Calculs de primitives de fractions rationnelles : on se ramène par développements en éléments simples à certains types de primitives à calculer : apparait le $\ln$ et $\arctan$
Fractions rationnelles en $\cos, \sin$: règles de Bioche, on se ramène par changement de variables à une fraction rationnelle,
Dérivées des fonctions trigonométriques, hyperboliques, de leurs inverses
Calcul de l'intégrale de Dirichlet
Intégrales de Wallis
Intégrales d'une gaussienne

II. La fonction Γ d'Euler [QZ13, §IX.II.1, p312] [GS09, §2.1, p101]

II. A. Généralités [BMP05, §2.7, p82] [QZ13, §IX.II.1, p312]

Définition, relation de récurrence, calcul de $\Gamma(1), \Gamma(1/2)$

Proposition 8. Γ *est holomorphe sur* $\{\Re(z) > 0\}$.

Application 9. Γ admet un unique prolongement méromorphe sur $\mathbb{C}$, holomorphe sur $\mathbb{C} \setminus -\mathbb{N}$.

Application 10. $\forall x \in \mathbb{R}_+^*, \Gamma(x) = \lim_{n\to+\infty} \frac{n! n^x}{x(x+1)\dots(x+n)}$ **[Formule de Gauss]**

Prolongement holomorphe, formule de Cauchy
$\ln$-convexité de Γ.

II. B. Applications

Formule de Stirling
Polynômes orthogonaux

II. C. Applications en probabilités

Loi Γ, β, stabilité par somme, ..., lien avec la loi exponentielle.
Exemples de modélisations

III. Transformée de Fourier

III. A. Généralités

III. B. Applications

Résolution de l'équation de la chaleur, de Schrödinger

III. C. Applications en probabilités [Ouv09, §12.2, p197]

On admet que $\phi_{\mathcal{N}(0,\sigma^2)} : \zeta \longmapsto \mathrm{e}^{-\frac{\sigma^2\zeta^2}{2}}$.

Proposition 11. *ϕ_X caractérise $\mathbb{P}_X$.*

Application 12. [Loi multinomiale poissonnifiée]
Soient $(p_j)_{1\leq j\leq d}$ des réels positifs tels que $\sum_{1\leq j\leq d} p_j = 1$. Soient $(Y^k)_{k\geq 1}$ des variables aléatoires indépendantes et identiquement distribuées telles que $\mathbb{P}(Y^k = j) = p_j$. Soit N indépendante des $(Y^k)_{k\geq 1}$ de loi $\mathcal{P}(\lambda)$ pour un $\lambda > 0$.
En posant $X^k = (\mathbb{1}_{Y^k=1}, \dots, \mathbb{1}_{Y^k=d})$, la loi de $S = \sum_{k=1}^N X^k$ est $\mathcal{P}(\lambda p_1) \otimes \cdots \otimes \mathcal{P}(\lambda p_d)$.

Convergence en loi, théorème de Lévy, théorème central limite, intervalles de confiance

QUESTIONS

Q Calculer $I = \int_0^1 \log(\frac{\sin(\pi x)}{\pi x})dx$ de deux manières différentes pour retrouver la formule de Stirling.

R On a $I = \int_0^1 \log(\sin(\pi x))dx - \int_0^1 \log(\pi x)dx$. La première intégrale se calcule par exemple en utilisant l'arc moitié.

BIBLIOGRAPHIE

[AF93] J.M. Arnaudiès et H. Fraysse : *Cours de mathématiques, Tome 1, Algèbre*. Dunod, 1993.

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[GS09] S. Groux et P. Soulat : *Les fonctions spéciales vues par les problèmes*. Cépaduès, 2009.

[Ouv09] J.-Y. Ouvrard : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[QZ13] H. Queffélec et C. Zuily : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[RDO98] E. Ramis, C. Deschamps et J. Odoux : *Cours de mathématiques 3, Topologie et éléments d'analyse*. Dunod, 1998.

[Rud98] W. Rudin : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

BIBLIOGRAPHIE

[AF91] J.M. Arnaudiès et H. Fraysse : *Cours de mathématiques, Tome 2, Analyse*. Dunod, 1991.

[AF93] J.M. Arnaudiès et H. Fraysse : *Cours de mathématiques, Tome 1, Algèbre*. Dunod, 1993.

[AK02] G. Allaire et S.-M. Kaber : *Algèbre linéaire numérique*. Ellipses, 2002.

[Ale99] M. Alessandri : *Thèmes de géométrie*. Dunod, 1999.

[All05] G. Allaire : *Analyse numérique et optimisation*. Les éditions de l'École Polytechnique, 2005.

[Aud06] M. Audin : *Géométrie*. EDP Sciences, 2006.

[Ave97] A. Avez : *Calcul différentiel*. Masson, 1997.

[Ber17] F. Berthelin : *Équations différentielles*. Cassini, 2017.

[BL07] P. Barbe et M. Ledoux : *Probabilité*. EDP Sciences, 2007.

[BMP05] V. Beck, J. Malick et G. Peyré : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Bon01] J.-M. Bony : *Théorie des distributions et analyse de* Fourier. Les éditions de l'École Polytechnique, 2001.

[BP15] M. Briane et G. Pagès : *Théorie de l'intégration*. Vuibert, 6ème édition, 2015.

[Bre99] H. Brezis : *Analyse fonctionnelle : théorie et applications*. Dunod, 1999.

[CDGM16] M. Cottrell, C. Duhamel, V. Genon-Catalot et T. Meyre : *Exercices de probabilités*. Cassini, 2016.

[CG13] P. Caldero et J. Germoni : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Cog00] M. Cognet : *Algèbre linéaire*. Bréal, 2000.

[Col11] P. Colmez : *Éléments d'analyse et d'algèbre*. Les éditions de l'École Polytechnique, 2 ème édition, 2011.

[Com98] F. Combes : *Algèbre et géométrie*. Bréal, 1998.

[De 11] C. De Seguins Pazzis : *Invitation aux formes quadratiques*. Calvage et Mounet, 2011.

[Dem96] J.-P. Demailly : *Analyse numérique et équations différentielles*. Collection Grenoble Sciences, 1996.

[Dem09] M. Demasure : *Cours d'algèbre*. Cassini, 2009.

[Duv07] D. Duverney : *Théorie des nombres*. Dunod, 2007.

[El 11] M. El Amrani : *Suites et séries numériques, suites et séries de fonctions*. Ellipses, 2011.

[Far00] J. Faraut : *Calcul intégral*. Belin, 2000.

[FG97] S. Francinou et H. Gianella : *Exercices de mathématiques pour l'agrégation - Algèbre 1*. Masson, 1997.

[FGN07a] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[FGN07b] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Algèbre 2*. Cassini, 2007.

[FGN07c] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 1*. Cassini, 2007.

[FGN07d] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 2*. Cassini, 2007.

[FGN12] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 4*. Cassini, 2012.

[FGN14] S. Francinou, H. Gianella et S. Nicolas : *Oraux X-ENS - Analyse 3*. Cassini, 2ème édition, 2014.

[Gou08] X. Gourdon : *Les maths en tête - Analyse*. Ellipses, 2ème édition, 2008.

[Gou09] X. Gourdon : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Gri15] J. Grifone : *Algèbre linéaire*. Cépaduès, 5ème édition, 2015.

[GS09] S. Groux et P. Soulat : *Les fonctions spéciales vues par les problèmes*. Cépaduès, 2009.

[Hau07] D. Hauchecorne : *Les contre-exemples en Mathématiques*. Ellipses, 2ème édition, 2007.

[HL09] F. Hirsch et G. Lacombe : *Eléments d'analyse fonctionnelle*. Dunod, 2009.

[Lan14] S. Lang : *Algèbre*. Dunod, 3ème édition, 2014.

[MM16] R. Mansuy et R. Mneimné : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Mé11] S. Méléard : *Aléatoire : introduction à la théorie et au calcul des probabilités*. Les éditions de l'École Polytechnique, 2011.

[Ouv08] J.-Y. Ouvrard : *Probabilités : Tome 1*. Cassini, 2ème édition, 2008.

[Ouv09] J.-Y. Ouvrard : *Probabilités : Tome 2*. Cassini, 3ème édition, 2009.

[Per96] D. Perrin : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. Peyré : *L'algèbre discrète de la transformée de* Fourier. Ellipses, 2004.

[QZ13] H. Queffélec et C. Zuily : *Analyse pour l'agrégation*. Dunod, 4ème édition, 2013.

[RDO98a] E. Ramis, C. Deschamps et J. Odoux : *Cours de mathématiques 3, Topologie et éléments d'analyse*. Dunod, 1998.

[RDO98b] E. Ramis, C. Deschamps et J. Odoux : *Cours de mathématiques 4, Séries et équations différentielles*. Dunod, 1998.

[Rom17] J.-E. Rombaldi : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Rou99] F. Rouvière : *Petit guide de calcul différentiel*. Cassini, 1999.

[RS12] V. Rivoirard et G. Stoltz : *Statistique mathématique en action*. Vuibert, 2 ème édition, 2012.

[Rud98] W. Rudin : *Analyse réelle et complexe*. Dunod, 2ème édition, 1998.

[Ser98] J.-P. Serre : *Représentations linéaires des groupes finis*. Hermann, 1998.

[Ser01] D. Serre : *Les Matrices*. Dunod, 2001.

[SS03] E. Stein et R. Shakarchi : *Complex Analysis*. Princeton University Press, 2003.

[Szp09] A. Szpriglas : *Algèbre L3*. Pearson Education, 2ème édition, 2009.

[Tau00] P. Tauvel : *Cours de géométrie*. Dunod, 2000.

[Tau06] P. Tauvel : *Analyse complexe pour la Licence 3*. Dunod, 2006.

[Tau07] P. Tauvel : *Mathématiques générales pour l'agrégation*. Masson, 2007.

[Ulm12] F. Ulmer : *Théorie des groupes*. Ellipses, 2012.

[Zé17] G. Zémor : *Cours de cryptographie*. Cassini, 2017.