Développements

par

Corentin Kilque
ENS Rennes

28 novembre 2018

Remerciements

Je tiens à remercier tout particulièrement mes amis, qui se reconnaitront, avec qui j'ai travaillé durant cette année de préparation, au cours d'échanges mathématiques informels ou de discussions plus sérieuses sur des développements, des plans, ou des interrogations mathématiques. Les documents de développements et de plans que j'ai produit, ainsi que, de manière plus générale, cette année de préparation n'auraient pas été les mêmes sans eux.

Ma gratitude va également à Gabriel Lepetit, Adrien Laurent, Florian Lemonnier et Paul Alphonse pour leurs travaux d'agrégation dont je me suis souvent très largement inspiré. Là encore, je leur dois beaucoup pour cette année.

Enfin, merci à ma famille et mes amis pour leur soutien sans faille tout au long de l'année.

À propos

Ce document rassemble les développements que j'ai rédigés pour la concours de l'agrégation externe de mathématiques 2018. Apparaissent également les développements que j'avais rédigés mais qui ont été finalement écartés du couplage. Il contient le couplage utilisé le jour de l'oral, avec les deux développements choisis pour chaque leçon, puis éventuellement en italique les développements qui auraient pu être utilisés.

Chaque développement contient une liste, subjective, de leçons dans lesquelles il se recase, ainsi que d'éventuels compléments à ce développement.

Avec 4 impasses (181, 182 et 183 en algèbre et 233 en analyse), il y a 42 développements pour 71 leçons, soit un recasage moyen de 3,38 leçons par développement.

Il est fortement probable que ce document contienne des fautes de frappes, des erreurs mathématiques, des choix critiquables, notamment pour les développements écartés, il est donc à manier avec précaution. Tout signalement d'erreur est évidemment le bienvenu.

Table des matières

1 Couplage

1.1 Leçons d'algèbre et de géométrie

101 : Groupe opérant sur un ensemble. Exemples et applications.

- Loi de réciprocité quadratique.
- Table de caractères de $\mathfrak{S}_4$ et groupes d'isométrie du tétraèdre et du cube.

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

- Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$.
- Théorème de structure des groupes abéliens finis.

103 : Exemples de sous-groupes distingués et de groupes quotients. Applications.

- Automorphismes de $\mathfrak{S}_n$.
- Simplicité de $SO_3(\mathbb{R})$.

104 : Groupes finis. Exemples et applications.

- Automorphismes de $\mathfrak{S}_n$.
- Table de caractères de $\mathfrak{S}_4$ et groupes d'isométrie du tétraèdre et du cube.
- *Théorème de structure des groupes abéliens finis.*

105 : Groupe des permutations d'un ensemble fini. Applications.

- Automorphismes de $\mathfrak{S}_n$.
- Table de caractères de $\mathfrak{S}_4$ et groupes d'isométrie du tétraèdre et du cube.

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

- Simplicité de $SO_3(\mathbb{R})$.
- Étude de $O(p, q)$

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

- Table de caractères de $\mathfrak{S}_4$ et groupes d'isométrie du tétraèdre et du cube.
- Théorème de structure des groupes abéliens finis.

108 : Exemples de parties génératrices d'un groupe. Applications.

- Automorphismes de $\mathfrak{S}_n$.
- Simplicité de $SO_3(\mathbb{R})$.

110 : Structure et dualité des groupes abéliens finis. Applications.

- Théorème de structure des groupes abéliens finis.
- Formule de Poisson discrète.

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

- Théorème de Sophie-Germain.
- Théorème des deux carrés de Fermat.
- *Théorème de structure des groupes abéliens finis.*

121 : Nombres premiers. Applications.

- Loi de réciprocité quadratique.
- Théorème de Sophie-Germain.
- *Théorème des deux carrés de Fermat.*

122 : Anneaux principaux. Applications.

- Un anneau principal non euclidien.
- Théorème des deux carrés de Fermat.

123 : Corps finis. Applications.

- Loi de réciprocité quadratique.
- Polynômes irréductibles sur $\mathbb{F}_q$.
- *Algorithme de Berlekamp.*

125 : Extensions de corps. Exemples et applications.

- Polynômes irréductibles sur $\mathbb{F}_q$.
- Théorème d'Artin.

126 : Exemples d'équations diophantiennes.

- Théorème de Sophie-Germain.
- Théorème des deux carrés de Fermat.

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

- Algorithme de Berlekamp.
- Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$.
- *Polynômes irréductibles sur* $\mathbb{F}_q$.

142 : PGCD et PPCM, algorithmes de calcul. Applications.

- Théorème de Sophie Germain.
- Algorithme de Berlekamp.

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

- Borne de Bézout.
- Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$.

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

- Invariants de similitude.
- Étude de $O(p, q)$.

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

- Théorème d'Artin.
- Invariants de similitude.

152 : Déterminant. Exemples et applications.

- Borne de Bézout.
- Ellipsoïde de John-Loewner.

153 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

- Décomposition de Dunford.
- Invariants de similitude.

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

- Décomposition de Dunford.

- Invariants de similitude.

155 : Endomorphismes diagonalisables en dimension finie.

- Décomposition de Dunford.
- L'exponentielle induit un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ dans $\mathcal{S}_n^{++}(\mathbb{R})$.

156 : Exponentielle de matrices. Applications.

- Différentielle de l'exponentielle matricielle.
- L'exponentielle induit un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ dans $\mathcal{S}_n^{++}(\mathbb{R})$.
- *Étude de* $O(p,q)$.

157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

- Décomposition de Dunford.
- Méthodes itératives de résolution d'un système linéaire.
- *Invariants de similitude.*

158 : Matrices symétriques réelles, matrices hermitiennes.

- Ellipsoïde de John-Loewner.
- L'exponentielle induit un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ dans $\mathcal{S}_n^{++}(\mathbb{R})$.
- *Étude de* $O(p,q)$.

159 : Formes linéaires et dualité en dimension finie. Exemples et applications.

- Extrema liés.
- Invariants de similitude.

160 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

- Simplicité de $SO_3(\mathbb{R})$.
- L'exponentielle induit un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ dans $\mathcal{S}_n^{++}(\mathbb{R})$.
- *Étude de* $O(p,q)$.

161 : Isométries d'un espace affine euclidien de dimension finie. Applications en dimensions 2 et 3.

- Table de caractères de $\mathfrak{S}_4$ et groupes d'isométrie du tétraèdre et du cube.
- Simplicité de $SO_3(\mathbb{R})$.

162 : Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

- Méthodes itératives de résolution d'un système linéaire.
- Théorème d'Artin.

170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

- Ellipsoïde de John-Loewner.
- Loi de réciprocité quadratique.
- *Étude de* $O(p, q)$.

171 : Formes quadratiques réelles. Coniques. Exemples et applications.

- Ellipsoïde de John-Loewner.
- Étude de $O(p, q)$.

190 : Méthodes combinatoires, problèmes de dénombrement.

- Loi de réciprocité quadratique.
- Polynômes irréductibles sur $\mathbb{F}_q$.

1.2 Leçons d'analyse et de probabilités

201 : Espaces de fonctions. Exemples et applications.

- Théorème de Lax-Milgram et application.
- Espace de Bergman.
- *Théorème de Riesz-Fischer.*
- *Équation de Schrödinger.*
- *Théorème de Fourier-Plancherel.*
- *Densité des polynômes orthogonaux.*

202 : Exemples de parties denses et applications.

- Théorème de Fourier-Plancherel.
- Densité des polynômes orthogonaux.
- *Espace de Bergman.*
- *Équation de la chaleur sur le cercle.*

203 : Utilisation de la notion de compacité.

- Théorème de Hadamard-Lévy.
- Optimisation dans un Hilbert.

204 : Connexité. Exemples et applications.

- Simplicité de $SO_3(\mathbb{R})$.
- Théorème de Hadamard-Lévy.

205 Espaces complets. Exemples et applications.

- Théorème de Riesz-Fischer.
- Théorème de Lax-Milgram et application.
- *Espace de Bergman.*
- *Optimisation dans un Hilbert.*

207 : Prolongement de fonctions. Exemples et applications.

- Théorème de Fourier-Plancherel.
- Densité des polynômes orthogonaux.

208 : Espaces vectoriels normés, applications linéaires continues. Exemples.

- Théorème de Riesz-Fischer.
- Optimisation dans un Hilbert.
- *Espace de Bergman.*
- *Théorème de Fourier-Plancherel.*

209 : Approximation d'une fonction par des polynômes et des polynômes trigonométriques. Exemples et applications.

- Densité des polynômes orthogonaux.
- Équation de la chaleur sur le cercle.
- *Espace de Bergman.*

213 : Espaces de Hilbert. Bases hilbertiennes. Exemples et applications.

- Espace de Bergman.
- Théorème de Lax-Milgram et application.
- *Densité des polynômes orthogonaux.*
- *Optimisation dans un Hilbert.*

214 : Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.

- Extremas liés.
- Théorème de Hadamard-Lévy.

215 : Applications différentiables sur un ouvert de $\mathbb{R}^n$. Exemples et applications.

- Extremas liés.
- Théorème de Hadamard-Lévy.
- *Différentielle de l'exponentielle de matrices.*

218 : Applications des formules de Taylor.

- Fonction caractéristique et moments.
- Méthode de Newton.
- *Théorème central-limite.*

219 : Extremums : existence, caractérisation, recherche. Exemples et applications.

- Optimisation dans un Hilbert.
- Extrema liés.
- *Ellipsoïde de John-Loewner.*

220 : Équations différentielles $X' = f(t, X)$. Exemples d'étude en dimension 1 et 2.

- Théorème de Hadamard-Lévy.
- Nombre de zéro d'une solution d'une équation différentielle.

221 : Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

- Nombre de zéro d'une solution d'une équation différentielle.
- Différentielle de l'exponentielle de matrices.

222 : Exemples d'équations aux dérivées partielles linéaires.

- Théorème de Lax-Milgram et application.
- Équation de Schrödinger sur $\mathbb{R}$.
- *Équation de la chaleur sur le cercle.*

223 : Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.

- Méthode de Newton.
- Processus de Galton-Watson.

224 : Exemples de développements asymptotiques de suites et de fonctions.

- Développement asymptotique de la série harmonique.
- Nombre de zéro d'une solution d'une équation différentielle.

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.

- Méthode de Newton.
- Méthodes itératives de résolution d'un système linéaire.
- *Processus de Galton-Watson.*

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

- Fonction caractéristique et moments.
- Méthode de Newton.

229 : Fonctions monotones. Fonctions convexes. Exemples et applications.

- Ellipsoïde de John-Loewner.
- Optimisation dans un Hilbert.

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

- Développement asymptotique de la série harmonique.
- Théorème d'Abel angulaire et taubérien faible.

234 : Espaces L^p, $1 \leqslant p \leqslant +\infty$.

- Théorème de Riesz-Fischer.
- Théorème de Fourier-Plancherel.
- *Densité des polynômes orthogonaux.*
- *Théorème d'inversion de Fourier.*

235 : Problèmes d'interversion de limites et d'intégrales.

- Équation de la chaleur sur le cercle.
- Théorème d'inversion de Fourier.
- *Marche aléatoire dans* $\mathbb{Z}^d$.
- *Théorème de Fourier-Plancherel.*
- *Théorème d'Abel angulaire et taubérien faible.*

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

- Théorème d'inversion de Fourier.
- Étude de la loi Gamma.

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

- Théorème d'inversion de Fourier.
- Équation de Schrödinger sur $\mathbb{R}$.

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

- Équation de la chaleur sur le cercle.
- Théorème d'Abel angulaire et taubérien faible.

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

- Espace de Bergman.
- Théorème d'Abel angulaire et taubérien faible.

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

- Espace de Bergman.
- Densité des polynômes orthogonaux.
- *Étude de la loi Gamma.*

246 : Séries de Fourier. Exemples et applications.

- Équation de la chaleur sur le cercle.
- Formule sommatoire de Poisson.

250 : Transformation de Fourier. Applications.

- Théorème d'inversion de Fourier.

- Équation de Schrödinger sur $\mathbb{R}$.
- *Théorème de Fourier Plancherel.*
- *Densité des polynômes orthogonaux.*

253 : Utilisation de la notion de convexité en analyse.

- Ellipsoïde de John-Loewner.
- Optimisation dans un Hilbert.

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

- Fonction caractéristique et moments.
- Processus de Galton-Watson.
- *Marche aléatoire dans $\mathbb{Z}^d$.*
- *Théorème central limite.*

261 : Fonction caractéristique d'une variable aléatoire. Exemples et applications.

- Théorème central limite.
- Marche aléatoire dans $\mathbb{Z}^d$.
- *Fonction caractéristique et moments.*
- *Étude de la loi Gamma.*

262 : Modes de convergence d'une suite de variables aléatoires. Exemples et applications.

- Théorème central limite.
- Marche aléatoire dans $\mathbb{Z}^d$.

263 : Variables aléatoires à densité. Exemples et applications.

- Étude de la loi Gamma.
- Théorème central limite.

264 : Variables aléatoires discrètes. Exemples et applications.

- Marche aléatoire dans $\mathbb{Z}^d$.
- Processus de Galton-Watson.

2 Développements d'algèbre et de géométrie

2.1 Algorithme de Berlekamp

Référence : V. Beck, J. Malick, G. Peyré, *Objectif Agrégation*, H & K, 2005.

Leçons concernées : 123, 141, 142, *151.*

Soit $q = p^s$ où p est premier.

Théorème 1. *Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés. Alors si P n'est pas irréductible, il existe $V \in \mathbb{F}_q[X]$ non congru à un polynôme constant modulo P tel que*

$$P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, V - \alpha).$$

Démonstration. Étape 1 : on considère

$$S_P : \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P) \\ Q(X) \mod P & \mapsto & Q(X^q) \mod P \end{array}$$

qui est bien défini et correspond à l'élévation à la puissance q dans $\mathbb{F}_q[X]/(P)$. En effet, l'application

$$\delta_1 : \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q(X) & \mapsto & Q(X^q) \end{array}$$

est bien définie comme morphisme d'évaluation, et par propriété du morphisme de Frobenius, correspond à l'élévation à la puissance q dans $\mathbb{F}_q[X]$. On considère alors $\pi : \mathbb{F}_q[X] \to \mathbb{F}_q[X]/(P)$ et $\delta = \pi \circ \delta_1$ qui vérifie $\delta(P) = \pi(P^q) = \pi(P)^q = 0$ et donc par le premier théorème d'isomorphisme, δ passe au quotient en S_P qui vérifie, pour $Q \in \mathbb{F}_q[X]$, $S_P(Q \mod P) = S_P(\pi(Q)) = \pi(Q^q) = \pi(Q)^q$ d'où le résultat.

Étape 2 : soit $P = P_1 \cdots P_r$ la décomposition de P en produit d'irréductibles, alors par le théorème des restes chinois, si $K_i := \mathbb{F}_q[X]/(P_i)$, $\mathbb{F}_q[X]/(P)$ est isomorphe à $K_1 \times \cdots \times K_r$ via φ. On pose alors $\widetilde{S_P} = \varphi \circ S_P \circ \varphi^{-1} : K_1 \times \cdots \times K_r \to K_1 \times \cdots \times K_r$ qui correspond à l'élévation à la puissance q dans l'anneau produit. Ainsi,

$$(x_1, \ldots, x_r) \in \ker(\widetilde{S_P} - \text{Id}) \iff \forall 1 \leqslant i \leqslant r, x_i^q = x_i.$$

Or, les K_i sont des extensions de corps de F_q et l'image de $\mathbb{F}_q$ dans K_i est l'ensemble des éléments x de K_i tels que $x^q = x$ (en effet par le théorème de Lagrange tous les éléments de $\mathbb{F}_q$ vérifient cette relation, et puisque $X^q - X$ est de degré q sur le corps K_i il a au plus q racines.). Ainsi,

$$(x_1, \ldots, x_r) \in \ker(\widetilde{S_P} - \text{Id}) \iff \forall 1 \leqslant i \leqslant r, x_i \in \mathbb{F}_q \subset K_i$$

(où F_q est vu comme l'image de $\mathbb{F}_q$ dans K_i). Ainsi $\ker(\widetilde{S_P} - \mathrm{Id}) = (\mathbb{F}_q)^r$ et donc, puisque $\ker(\widetilde{S_P} - \mathrm{Id}) = \varphi(\ker(S_P - \mathrm{Id}))$ et φ étant un isomorphisme de $\mathbb{F}_q$-espace vectoriel, $r = \dim(\ker(S_P - \mathrm{Id}))$.

Étape 3 : par hypothèse $r > 1$, ainsi, l'espace des polynômes congrus à un polynôme constant modulo P étant de dimension un dans $\mathbb{F}_q[X]/(P)$, il existe $V \in \mathbb{F}_q[X]$ non congru à un polynôme constant modulo P tel que $(V \mod P) \in \ker(S_P - \mathrm{Id})$. On sait que

$$(V \mod P) \in \ker(S_P - \mathrm{Id}) \iff (V \mod P_1, \dots, V \mod P_r) \in (\mathbb{F}_q)^r.$$

On note alors $\alpha_i = V \mod P_i \in \mathbb{F}_q \subset K_i$. On considère ensuite, pour $\alpha \in \mathbb{F}_q$,

$$\mathrm{pgcd}(P, V - \alpha) = \prod_{i \in I_\alpha} P_i$$

étant un diviseur de P. Puisque les P_i sont premiers entre eux deux à deux (P étant sans facteur carré), le lemme de Gauss nous assure que

$$I_\alpha = \{i, P_i \mid V - \alpha\}.$$

Or pour tout i,

$$P_i \mid V - \alpha \iff V - \alpha = 0 \mod P_i \iff \alpha_i = \alpha,$$

d'où

$$\mathrm{pgcd}(P, V - \alpha) = \prod_{i,\ \alpha_i = \alpha} P_i.$$

On peut conclure :

$$P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \Big(\prod_{i,\ \alpha_i = \alpha} P_i \Big) = \prod_{\alpha \in \mathbb{F}_q} \Big(\mathrm{pgcd}(P, V - \alpha) \Big).$$

□

Proposition 2. *Soit Q un facteur irréductible de P de multiplicité μ. Alors Q un facteur irréductible de* $\mathrm{pgcd}(P, P')$ *de multiplicité μ^* où $\mu^* = \mu$ si $p \mid \mu$ et $\mu^* = \mu - 1$ sinon. Ainsi, si $P = \prod_{i=1}^{r} P_i^{\mu_i}$ est sa décomposition en facteurs irréductibles premiers entre-eux deux à deux, alors*

$$\mathrm{pgcd}(P, P') = \Big(\prod_{p \mid \mu_i} P_i^{\mu_i} \Big) \Big(\prod_{p \nmid \mu_i} P_i^{\mu_i - 1} \Big)$$

Démonstration. On note μ^* la multiplicité de Q dans $\mathrm{pgcd}(P, P')$, qui est inférieure ou égale à μ car $\mathrm{pgcd}(P, P') \mid P$. D'autre part on écrit $P = Q^\mu R$ avec Q et R premiers entre eux. On a alors $P' = Q^\mu R' + \mu Q' Q^{\mu - 1} R$ et donc $Q^{\mu - 1} \mid P'$ et ainsi $Q^{\mu - 1} \mid \mathrm{pgcd}(P, P')$ et donc $\mu^* \geqslant \mu - 1$. Enfin, $\mu^* = \mu$ si et seulement si $Q \mid \mu Q' R$, c'est-à-dire puisque Q et R sont premiers entre eux, $\mu^* = \mu$ si et seulement si $Q \mid \mu Q'$ et donc $\mu^* = \mu$ si et seulement si $\mu Q' = 0$ puisque $\deg \mu Q' < \deg Q$. Or puisque $Q' = 0$ si et seulement si $Q = U^p$ et que Q est irréductible, $\mu^* = \mu$ si et seulement si $p \mid \mu$. □

Remarque. Les deux résultats précédents justifient la correction de l'algorithme de factorisation suivant :

(1) Si P est constant, terminer l'algorithme

(2) Sinon, calculer $\text{pgcd}(P, P')$.

- Si $\text{pgcd}(P, P') = 1$, appliquer l'algorithme de Berlekamp à P
- Si $\text{pgcd}(P, P') = P$, calculer R tel que $P = R^p$ (s'obtient en prenant les racines p-èmes des coefficients de P) et revenir en (1) avec R
- Sinon, appliquer (1) à $\text{pgcd}(P, P')$ et $P/\text{pgcd}(P, P')$

où l'algorithme de Berlekamp est le suivant :

(1) Calculer la matrice de l'application $S_P - \text{Id}$ dans la base canonique $(1, \dots, x^{\deg P - 1})$ où $x = X \mod P$

(2) Le nombre de facteurs irréductibles de P est

$$r = \dim \ker(S_P - \text{Id}) = \deg P - \text{rg}(S_P - \text{Id})$$

(3) Si $r = 1$ renvoyer P

(4) Trouver $V \in \mathbb{F}_q[X]$ non congru à un polynôme constant modulo P tel que $(V \mod P) \in \ker S_P - \text{Id}$, appliquer (1) $\text{pgcd}(P, V - \alpha)$ pour $\alpha \in \mathbb{F}_q$.

Commentaire : le développement est un peu long mais il serait bien de faire la preuve de la proposition pour justifier le recasage dans la leçon PGCD, éventuellement admettre l'étape 1 dans un premier temps.

2.2 Automorphismes de $\mathfrak{S}_n$: $n \neq 6 \Rightarrow \mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$

Référence : D. Perrin, *Cours d'Algèbre*, Ellipses, 1996.

Leçons concernées : 103, 104, 105, 108

Proposition 1. *Si l'image par $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ de toute transposition est une transposition, alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.*

Démonstration. Soit un tel φ. On note $\tau_i := (1i), i \geqslant 2$, dont on sait qu'elles engendrent $\mathfrak{S}_n$. On remarque que les τ_i sont non disjoints donc ne commutent pas entre eux deux à deux, donc leurs images par φ ne commutent pas entre elles deux à deux, et donc ont deux à deux une orbite non disjointe, ces images sont d'autre part des transpositions par hypothèse, et distinctes car φ est un isomorphisme. Maintenant, on note $\varphi(\tau_2) = (a_1a_2)$ et $\varphi(\tau_3) = (a_1a_3), a_3 \neq a_2$ ce qui est possible d'après la première remarque. Ensuite, on a $\varphi(\tau_4) = (a_1a_4), a_4 \neq a_3, a_2$ car sinon $\varphi(\tau_4) = (a_2a_3)$ et on écrit

$$(a_1a_2)(a_1a_3)(a_2a_3) = (a_1a_3)$$

et donc par φ^{-1},

$$(12)(13)(14) = (13)$$

ce qui est impossible. De même $\varphi(\tau_i) = (a_1a_i)$. On a trouvé une permutation a telle que $\varphi(\tau_i) = a\tau_i a^{-1}$ et donc φ et i_a coïncident sur un ensemble générateur donc sont égales. □

Théorème 2. *Pour $n \neq 6$, on a $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.*

Démonstration. Étape 1 : on remarque tout d'abord qu'on peut supposer $n \geqslant 6$. En effet, si $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$, φ stabilise $\mathfrak{A}_n$ car $\mathfrak{A}_n = D(\mathfrak{S}_n)$ est caractéristique. L'image d'une transposition est donc impaire. D'autre part, l'image d'une transposition est d'ordre 2 donc elle se décompose en produit de k transpositions à supports disjoints, avec k impair par la première remarque. Si pour toute transposition, $k = 1$ c'est fini d'après la proposition précédente, dans le cas contraire, il y a un cas où $k \geqslant 3$ donc $n \geqslant 6$.

Étape 2 : pour $s \in \mathfrak{S}_n$, on note $c(s) := \{s' \in \mathfrak{S}_n \mid ss' = s's\}$ le centralisateur de s. Soit $\tau = (ab)$ une transposition. On a $\forall s \in \mathfrak{S}_n$, $s\tau s^{-1} = (s(a)s(b))$. Ainsi, si on note $E := \{1, \ldots, n\}$ et $F = E\backslash\{a, b\}$, $s \in c(\tau) \Leftrightarrow s(\{a, b\}) = \{a, b\} \Leftrightarrow s(F) = F$. On considère alors le morphisme de groupes

$$r : \begin{array}{ccc} c(\tau) & \to & \mathfrak{S}(F) \cong \mathfrak{S}_{n-2} \\ s & \mapsto & s_{|F} \end{array}$$

qui est bien défini par l'étude précédente, de noyau $\{1, \tau\}$ et surjectif.

Étape 3 : d'autre part, si $\tau = \tau_1 \cdots \tau_k$, avec $\tau_i = (a_{2i-1}a_{2i})$, est un produit d'un nombre impair k de transpositions à supports disjoints, on a $\tau_i \in c(\tau)$. On pose $N :=< \tau_i \mid 1 \leqslant i \leqslant$

$k>$. On a $|N| = 2^k$ et donc $N \cong (\mathbb{Z}/2\mathbb{Z})^k$ et d'autre part $N \lhd c(\tau)$. En effet, soit $s \in c(\tau)$, on a $s\tau s^{-1} = \tau = (s(a_1)s(a_2)) \cdots (s(a_{2k-1})s(a_{2k}))$ donc par unicité de la décomposition en produit de cycles à supports disjoints, $s\tau_i s^{-1} = \tau_j$ pour tout i.

Étape 4 : on considère alors τ une transposition telle que son image τ' par φ soit un produit d'un nombre impair $k \geqslant 3$ de transpositions à supports disjoints. On a $c(\tau) \cong c(\tau')$ via φ, donc il existe $N' \cong (\mathbb{Z}/2\mathbb{Z})^k \lhd c(\tau)$ via φ. On a alors $r(N') \lhd \mathfrak{S}_{n-2}$ avec

$$|r(N')| = \frac{|N'|}{|\ker r \cap N'|} = 2^k \text{ ou } 2^{k-1}.$$

Or si $n \geqslant 7$, $n-2 \geqslant 5$ et par l'étude des sous-groupes distingués de $\mathfrak{S}_m$ on trouve une absurdité par étude du cardinal. On peut alors conclure grâce à la proposition précédente. □

On donne ici l'étude des sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geqslant 5$.

Proposition 3. *Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}, \mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Démonstration. On considère $H \lhd \mathfrak{S}_n$. On a $H \cap \mathfrak{A}_n \lhd \mathfrak{A}_n$, donc $H \cap \mathfrak{A}_n = \{1\}$ ou $\mathfrak{A}_n$.

Si $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, alors $H = \mathfrak{A}_n$ ou $\mathfrak{S}_n$.

Si $H \cap \mathfrak{A}_n = \{1\}$, puisque le noyau de $\varepsilon : H \to \mathbb{Z}/2\mathbb{Z}$ est $H \cap \mathfrak{A}_n$, $\varepsilon : H \to \varepsilon(H)$ est un isomorphisme, de sorte que $|H| \leqslant 2$. Si $|H| = 2$, alors $H = \{1, \sigma\}$. Mais si $\tau \in \mathfrak{S}_n$, $\tau\sigma\tau^{-1} \in H$, et comme $\sigma \neq 1$, $\tau\sigma\tau^{-1} = \sigma$, et ce pour tout $\tau \in \mathfrak{S}_n$, et donc σ est dans le centre de $\mathfrak{S}_n$, qui est trivial, d'où l'absurdité.

On justifie que le centre de $\mathfrak{S}_n$ est trivial pour $n \geqslant 3$: si $\sigma \neq 1$ est dans le centre, alors il existe $i \in [|1, n|]$ tel que $\sigma(i) = j \neq i$. Alors si on choisit $k \neq i, j$, et que l'on pose $\tau = (j\ k)$, alors $\sigma\tau(i) = j$ et $\tau\sigma(i) = k$ et donc $\sigma\tau \neq \tau\sigma$, d'où l'absurdité. □

Commentaire : si c'est trop court on peut rajouter la dernière proposition.

2.3 Borne de Bézout

Références : [1] J.Y. Mérindol, *Nombres et algèbre*, EDP Sciences, 2006, A. Szpirglas, *Mathématiques L3*, Pearson Education, 2009.

Leçons concernées : 144, 152.

Théorème 1. *Soit k un corps infini et soit $A, B \in k[X,Y]$ premiers entre eux de degrés totaux respectifs m et n. Alors si on note $Z(A)$ l'ensemble des zéros de A, on a*

$$\mathrm{Card}(Z(A) \cap Z(B)) \leqslant mn.$$

Démonstration. Étape 1 : l'ensemble $Z(A) \cap Z(B)$ est fini. On note $R_X = \mathrm{res}_X(A,B)$ et $R_Y = \mathrm{res}_Y(A,B)$ qui sont des polynômes non nuls, puisque A et B sont premiers entre eux, respectivement de $k[Y]$ et $k[X]$. Pour tout $(x,y) \in Z(A) \cap Z(B)$, on a $R_X(y) = 0$ puisque x étant une racine de $A(X,y)$ et $B(X,y)$, ces deux polynômes ont un facteur commun. De même $R_Y(x) = 0$ et donc

$$\mathrm{Card}(Z(A) \cap Z(B)) \leqslant \deg R_X \deg R_Y.$$

Étape 2 : majoration de $\deg R_Y$. On écrit alors $A = \sum_{i=0}^{p} a_i(X)Y^i$ et $B = \sum_{j=0}^{q} b_j(X)Y^j$ où $\deg a_i \leqslant m-i$ et $\deg b_j \leqslant n-j$, et donc R_X est le déterminant de la matrice de Sylvester suivante :

$$C = (c_{i,j})_{1 \leqslant i,j \leqslant p+q} = \begin{pmatrix} a_p & & (0) & b_q & & & (0) \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_p & b_0 & & \ddots & \\ a_0 & & \vdots & & \ddots & & b_q \\ & \ddots & \vdots & & & \ddots & \vdots \\ (0) & & a_0 & (0) & & & b_0 \end{pmatrix}$$

avec

$$\forall j \in [|1; q|], \qquad c_{i,j} = \begin{cases} a_{p-(i-j)} & \text{si } 0 \leqslant i-j \leqslant p \\ 0 & \text{sinon} \end{cases}$$

$$\forall j \in [|q+1; p+q|], \qquad c_{i,j} = \begin{cases} b_{q-(i-(j-q))} & \text{si } 0 \leqslant i-j+q \leqslant q \\ 0 & \text{sinon} \end{cases}$$

1. adapté d'un développement rédigé de Harold Favreau et Lucien Grillet.

et donc pour tour $\sigma \in \mathfrak{S}_{p+q}$,

$$\begin{aligned}\deg\Big(\varepsilon(\sigma)\prod_{j=1}^{p+q} c_{\sigma(j),j}\Big) &= \sum_{j=1}^{q}\deg(c_{\sigma(j),j}) + \sum_{j=q+1}^{p+q}\deg(c_{\sigma(j),j}) \\ &\leqslant \sum_{j=1}^{q}\big(m-p+\sigma(j)-j\big) + \sum_{j=q+1}^{p+q}\big(n+\sigma(j)-j\big) \\ &= mq - pq + np = mn + (m-p)(q-n) \leqslant mn.\end{aligned}$$

En effet, si σ est tel qu'il existe $j \in [|1, p+q|]$ tel que $c_{\sigma(j),j}$, alors le produit est nul et donc son degré est $-\infty$. Sinon, on peut appliquer la majoration indiquée d'après l'expression de $c_{\sigma(j),j} = 0$ dans le cas non nul et les majorations des degrés de a_i et b_i. Un tel σ existe toujours car sinon R_Y serait nul ce que l'on a exclu par hypothèse. Ainsi, d'après la formule du déterminant, $\deg R_Y \leqslant mn$.

Étape 3 : changement de variables. On sait que pour tout $(x, y) \in Z(A) \cap Z(B)$, $R_X(y) = 0$. Ainsi, si toutes les abscisses des éléments de $Z(A) \cap Z(B)$ sont différentes on a le résultat souhaité. On va se ramener à ce cas par un changement de variables. On pose

$$\Gamma = \left\{ \frac{x-x'}{y-y'} \mid (x,y),(x',y') \in Z(A)\cap Z(B), y \neq y' \right\}$$

qui est un ensemble de cardinal fini, ainsi, comme k est infini il existe $u \in k^*\backslash\Gamma$. On effectue alors le changement de variables $X' = X + uY$ et $Y' = Y$ et on pose $\widetilde{A}(X', Y') = A(X, Y)$ et $\widetilde{B}(X', Y') = B(X, Y)$. On considère alors la fonction

$$\varphi : \begin{array}{ccc} Z(A)\cap Z(B) & \to & Z\big(\operatorname{res}_{Y'}(\widetilde{A},\widetilde{B})\big) \\ (x,y) & \mapsto & x+uy. \end{array}$$

La fonction φ est bien définie puisque si $(x, y) \in Z(A)\cap Z(B)$, alors $\widetilde{A}(x+uy, y) = A(x, y) = 0$ et $\widetilde{B}(x + uy, y) = B(x, y) = 0$ et donc $\operatorname{res}_{Y'}(\widetilde{A}, \widetilde{B})(x + uy) = 0$. D'autre part, puisque $u \notin \Gamma$, φ est injective. Ainsi

$$\operatorname{Card}\big(Z(A)\cap Z(B)\big) \leqslant \operatorname{Card}\big(Z\big(\operatorname{res}_{Y'}(\widetilde{A},\widetilde{B})\big)\big) \leqslant \deg\big(\widetilde{A}\big)\deg\big(\widetilde{B}\big) = \deg(A)\deg(B).$$

□

Remarques. Le théorème de Bézout plus général affirme que sous de bonnes hypothèses le cardinal de l'ensemble des zéros communs comptés avec multiplicités est exactement mn.

On peut travailler sur un corps quelconque et même sur un anneau intègre, il suffit pour cela de considérer la clôture algébrique du corps des fractions de l'anneau.

2.4 Décomposition de Dunford

Référence : X. Gourdon, *Les maths en tête, Algèbre*, Ellipses, 2009.

Leçons concernées : 153, 154, 155, 157.

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension finie.

Théorème 1. *Soit $f \in \mathcal{L}(E)$ tel que son polynôme caractéristique χ_f soit scindé sur $\mathbb{K}$. Alors il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que $f = d + n$, n soit nilpotent, d soit diagonalisable, et que $d \circ n = n \circ d$.*

De plus, d et n sont des polynômes en f.

Lemme 2. *Soit $f \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$ un polynôme annulateur de f. Soit $P = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ sa décomposition en facteurs irréductibles et $N_i := \ker M_i^{\alpha_i}(f)$. Alors on a $E = N_1 \oplus \cdots \oplus N_s$ et pour tout i, la projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en f.*

Démonstration. La première assertion résulte directement du lemme des noyaux.

Étape 1 : on note, pour tout i, $Q_i = \prod_{j \neq i} M_j^{\alpha_j}$, qui sont premiers entre eux dans leur ensemble, et donc, d'après le théorème de Bézout, il existe $U_1, \ldots, U_s \in \mathbb{K}[X]$ tels que $U_1 Q_1 + \cdots + U_s Q_s = 1$ et donc

$$\mathrm{id}_E = U_1 \circ Q_1(f) + \cdots + U_s \circ Q_s(f).$$

On note alors $P_i = U_i Q_i$ et $p_i = P_i(f)$ de sorte qu'on a $\mathrm{id}_E = \sum_{j=1}^s p_j$ $(*)$. On remarque que les p_i sont des polynômes en f. On commence par montrer que les p_i sont des projecteurs. Pour $j \neq i$, P divise $Q_i Q_j$ et donc

$$p_i \circ p_j = Q_i Q_j(f) \circ U_i U_j(f) = 0.$$

Ainsi, pour tout i, par $(*)$, $p_i = \sum_{j=1}^s p_i \circ p_j = p_i^2$.

Étape 2 : on montre ensuite par double inclusion que $\mathrm{Im}(p_i) = N_i$. Soit $y = p_i(x) \in \mathrm{Im}(p_i)$. On a

$$M_i^{\alpha_i}(f)(y) = M_i^{\alpha_i}(f) \circ P_i(f)(x) = U_i(f) \circ P(f)(x) = 0$$

et donc $\mathrm{Im}(p_i) \subset \ker M_i^{\alpha_i}(f) = N_i$. Réciproquement, si $x \in N_i$, on a d'après $(*)$, $x = \sum_{j=1}^s p_j(x)$. Or pour $j \neq i$, $p_j(x) = U_j Q_j(f)(x) = 0$ car $M_i^{\alpha_i}$ divise Q_j et donc $x = p_i(x) \in \mathrm{Im}(p_i)$.

Étape 3 : on montre enfin par double inclusion que $\ker(p_i) = \bigoplus_{j \neq i} N_j$. Soit $x \in N_j$, alors $p_i(x) = U_i Q_i(f)(x) = 0$ car $M_j^{\alpha_j}$ divise Q_i et donc $\bigoplus_{j \neq i} N_j \subset \ker(p_i)$. Réciproquement, si $x \in \ker(p_i)$, par $(*)$, $x = \sum_{j \neq i} p_j(x) \in \bigoplus_{j \neq i} \mathrm{Im}(p_j) = \bigoplus_{j \neq i} N_j$. Cela conclut la preuve du lemme. □

Démonstration (Théorème). Existence : on applique le lemme précédent à $P = \chi_f = \beta \prod_{i=1}^{s} (X - \lambda_i)^{\alpha_i}$ avec $M_i = X - \lambda_i$. On reprend les notations du lemme et on pose $d = \sum_{i=1}^{s} \lambda_i p_i$ qui est alors diagonalisable (diagonale dans une base adaptée à la décomposition $E = N_1 \oplus \cdots \oplus N_s$). On pose également $n = f - d = \sum_{i=1}^{s} (f - \lambda_i) p_i$ grâce à $(*)$. On sait que $p_i \circ p_j = 0$ si $i \neq j$, $p_i^2 = p_i$ et, puisque les p_i sont des polynômes en f, que les p_i et f commutent, ainsi, par récurrence, on obtient que pour tout $q \in \mathbb{N}$,

$$n^q = \sum_{i=1}^{s} (f - \lambda_i)^q p_i.$$

Or, si $q = \max_i \alpha_i$, pour tout i, $(f - \lambda_i)^q p_i(x) = \big((X - \lambda_i)^q P_i\big)(f)(x) = 0$ car χ_f divise $(X - \lambda_i)^q P_i$. Ainsi n est nilpotent et puisque ce sont des polynômes en f, d et n commutent, et on a l'existence.

Unicité : soit (d', n') un autre tel couple. Alors d' et n' commutent avec $d' + n' = f$ et donc avec d et n qui sont des polynômes en f. Ainsi, d et d' sont simultanément diagonalisables, et donc $d - d'$ est diagonalisable. Or on a $d - d' = n' - n$ qui est nilpotent par le binôme de Newton, puisque n et n' commutent. Ainsi $d = d'$ et donc $n = n'$. □

2.5 Étude de $O(p,q)$

Référence : P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométrie, Tome premier*, Calvage & Mounet, 2013.

Leçons concernées : 106, 150, 156, 158, 160, 170, 171.

Définition 1. Si $p+q=n$, on note $O(p,q)$ l'ensemble des isométries de $\mathrm{GL}_n(\mathbb{R})$ pour la forme quadratique $x_1^2+\cdots+x_p^2-x_{p+1}^2-\cdots-x_n^2$. Autrement dit, si on note $I_{p,q}$ la matrice diagonale par blocs $\mathrm{diag}(I_p,-I_q)$,

$$O(p,q)=\left\{P\in \mathrm{GL}_n(\mathbb{R}) \mid {}^tPI_{(p,q)}P=I_{(p,q)}\right\}.$$

Lorsque $q=0$, on note simplement $O(p)=O_p(\mathbb{R})$.

On aura besoin du résultat suivant :

Proposition 2. *L'exponentielle induit un homéomorphisme*

$$\exp : \mathcal{S}_n(\mathbb{R}) \xrightarrow{\cong} \mathcal{S}_n^{++}(\mathbb{R}).$$

Théorème 3. *Si $p,q\neq 0$, on a un homéomorphisme*

$$O(p,q)\cong O(p)\times O(q)\times \mathbb{R}^{pq}.$$

Démonstration. Étape 1 : on commence par montrer qu'il existe un homéomorphisme $O(p,q)\cong (O(p,q)\cap O(n))\times(O(p,q)\cap \mathcal{S}_n^{++}(\mathbb{R}))$. On utilise pour cela la décomposition polaire : soit $M\in O(p,q)$, il existe $(O,S)\in O_n(\mathbb{R})\times \mathcal{S}_n^{++}(\mathbb{R})$ tel que $M=OS$. On va montrer que O et S sont dans $O(p,q)$, et pour cela il suffit de vérifier que S l'est. On remarque tout d'abord que $O(p,q)$ est stable par transposition : on a ${}^tMI_{(p,q)}M=I_{(p,q)}$ donc par passage à l'inverse $M^{-1}I_{(p,q)}{}^tM^{-1}=I_{(p,q)}$ c'est-à-dire que ${}^tM^{-1}\in O(p,q)$, et donc ${}^tM\in O(p,q)$. Maintenant, si $T={}^tMM$, $T\in O(p,q)$, et d'autre part on vérifie que $S^2=T$, donc $S^2\in O(p,q)$. $T\in \mathcal{S}_n^{++}(\mathbb{R})$, soit donc $U\in\mathcal{S}_n(\mathbb{R})$ telle que $\exp U=T$. On a, par bijectivité de $\exp:\mathcal{S}_n(\mathbb{R})\to\mathcal{S}_n^{++}(\mathbb{R})$,

$$\begin{aligned}
T\in O(p,q) &\iff {}^t\exp(U)I_{(p,q)}\exp(U)=I_{(p,q)}\\
&\iff \exp({}^tU)=I_{(p,q)}\exp(-U)I_{(p,q)}=\exp\big(-I_{(p,q)}UI_{(p,q)}\big)\\
&\iff {}^tU=-I_{(p,q)}UI_{(p,q)}\\
&\iff \frac{{}^tU}{2}=-I_{(p,q)}\frac{U}{2}I_{(p,q)}\\
&\iff \exp(\frac{{}^tU}{2})=I_{(p,q)}\exp(-\frac{U}{2})I_{(p,q)}\\
&\iff \exp(\frac{U}{2})\in O(p,q).
\end{aligned}$$

Or $\left(\exp(\frac{U}{2})\right)^2 = T = S^2$, et par unicité de la racine carré d'une matrice définie positive, $S = \exp(\frac{U}{2}) \in O(p,q)$. Ainsi, la décomposition polaire nous fournit un homéomorphisme $O(p,q) \cong (O(p,q) \cap O(n)) \times (O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R}))$. On chercher alors à expliciter les deux groupes mis en jeu.

Étape 2 : on a l'homéomorphisme $O(p,q) \cap O(n) \cong O(p) \times O(q)$. En effet, si $O = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in O(p,q) \cap O(n)$, alors puisque

$$O \in O(p,q) \iff \begin{pmatrix} {}^tA & {}^tC \\ {}^tB & {}^tD \end{pmatrix} \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix},$$

on a, en particulier

$$\begin{cases} {}^tAA - {}^tCC = I_p \\ {}^tBB - {}^tDD = -I_q \end{cases}$$

et d'autre part puisque

$$O \in O(n) \iff \begin{pmatrix} {}^tA & {}^tC \\ {}^tB & {}^tD \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = I_n,$$

on a en particulier,

$$\begin{cases} {}^tAA + {}^tCC = I_p \\ {}^tBB + {}^tDD = I_q \end{cases}.$$

Ainsi, ${}^tCC = 0$, donc $\mathrm{Tr}\,{}^tCC = \sum c_{i,j}^2 = 0$, et ainsi $C = 0$. De même $B = 0$, donc $(A,D) \in O(p) \times O(q)$ et on obtient l'homéomorphisme annoncé $O \mapsto (A,D)$.

Étape 3 : on a l'homéomorphisme $O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R}) \cong \mathbb{R}^{pq}$. On a vu lors de la première étape que exp induit une bijection entre $\mathcal{S}_n(\mathbb{R}) \cap L$ et $\mathcal{S}_n^{++}(\mathbb{R}) \cap O(p,q)$ où $L = \{U \in \mathcal{M}_n(\mathbb{R}) \mid {}^tUI_{(p,q)} + UI_{(p,q)} = 0\}$. Puisque $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme, l'application précédente fournit un homéomorphisme. Enfin, si $U = \begin{pmatrix} A & B \\ {}^tB & C \end{pmatrix} \in \mathcal{S}_n(\mathbb{R})$ avec $A \in \mathcal{S}_p(\mathbb{R})$, $C \in \mathcal{S}_q(\mathbb{R})$ et $B \in \mathcal{M}_{p,q}(\mathbb{R})$, alors $U \in L \iff 2A = 0$ et $-2C = 0$, on a donc un homéomorphisme $\mathcal{S}_n(\mathbb{R}) \cap L \cong \mathbb{R}^{pq}$ donné par $U \mapsto B$, ce qui conclut la preuve. □

Proposition 4. *Pour toute matrice $T \in \mathcal{S}_n^{++}(\mathbb{R})$, il existe une unique matrice $S \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $S^2 = T$.*

Démonstration. Puisque $T \in \mathcal{S}_n^{++}(\mathbb{R})$, il existe $P \in {}_n(\mathbb{R})$ et $\lambda_i > 0$ tels que

$$T = P \begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix} {}^tP.$$

On pose alors

$$S = P \begin{pmatrix} \sqrt{\lambda_1} & & (0) \\ & \ddots & \\ (0) & & \sqrt{\lambda_n} \end{pmatrix} {}^tP$$

qui vérifie bien $S^2 = T$. On suppose maintenant que $S' \in \mathcal{S}_n^{++}(\mathbb{R})$ vérifie $S'^2 = T$. On considère $Q \in \mathbb{R}[X]$ tel que $\mathbb{Q}(\lambda_i) = \sqrt{\lambda_i}$ pour tout i. On a alors

$$\begin{aligned} S = P \begin{pmatrix} \sqrt{\lambda_1} & & (0) \\ & \ddots & \\ (0) & & \sqrt{\lambda_n} \end{pmatrix} {}^tP &= PQ \left(\begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix} \right) {}^tP \\ = Q \left(P \begin{pmatrix} \lambda_1 & & (0) \\ & \ddots & \\ (0) & & \lambda_n \end{pmatrix} {}^tP \right) &= Q(S^2) = Q(S'^2). \end{aligned}$$

Or S' commute avec $Q(S'^2)$, donc avec S, les deux matrices sont donc codiagonalisables : il existe $P_0 \in \mathrm{GL}_n(\mathbb{R})$ et $\mu_i > 0$, $\mu'_i > 0$ tels que

$$S = P_0 \operatorname{diag}(\mu_i) P_0^{-1} \quad \text{et} \quad S = P_0 \operatorname{diag}(\mu'_i) P_0^{-1}.$$

Or $S^2 = S'^2$, donc $\mu_i^2 = \mu_i'^2$ pour tout i, ainsi $\mu_i = \mu'_i$ pour tout i, et enfin $S = S'$. □

2.6 Formule de Poisson discrète

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

Leçons concernées : 110.

Définition 1. Soit G un groupe abélien fini. On note $\mathbb{C}[G]$ l'espace des fonctions $f : G \to \mathbb{C}$. Pour $f \in \mathbb{C}[G]$, on définit ses coefficients de Fourier $c_f(\chi) =< f, \chi >$ et sa transformée de Fourier $\widehat{f}$ comme, pour $\chi \in \widehat{G}$

$$\widehat{f}(\chi) = |G| c_f(\overline{\chi}) = \sum_{g \in G} f(g)\chi(g).$$

On a ainsi un morphisme (qui est en fait un isomorphisme)

$$\mathcal{F} : \begin{array}{ccc} \mathbb{C}[G] & \to & \mathbb{C}[\widehat{G}] \\ f & \mapsto & \widehat{f}. \end{array}$$

Proposition 2. *Pour G un groupe abélien fini, et pour $f \in \mathbb{C}[G]$, on a la formule d'inversion de Fourier suivante :*

$$f = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi^{-1} = \sum_{\chi \in \widehat{G}} c_f(\chi)\chi = \sum_{\chi \in \widehat{G}} < f, \chi > \chi.$$

On se donne G un groupe abélien fini, H un sous-groupe de G, et $f \in \mathbb{C}[G]$.

Définition 3. On note $H^\sharp$ le sous groupe de $\widehat{G}$ défini par

$$H^\sharp = \left\{ \chi \in \widehat{G} \mid \forall h \in H, \chi(h) = 1 \right\}$$

appelé l'*orthogonale de H*. C'est donc le sous-groupe de $\widehat{G}$ formé des caractères triviaux sur H.

Lemme 4. *Il existe un isomorphisme*

$$H^\sharp \cong \widehat{G/H}.$$

Démonstration. On pose

$$\varphi : \begin{array}{ccc} \widehat{G/H} & \to & H^\sharp \\ \chi & \mapsto & \widetilde{\chi} \end{array}$$

où $\widetilde{\chi}(g) = \chi(gH)$ pour tout $g \in G$. En particulier on voit que φ est bien défini puisque si $h \in H$, $\widetilde{\chi}(h) = \chi(H) = 1$. D'autre part on vérifie facilement que φ est morphisme de groupes.

Si $\gamma \in H^\sharp$, alors on définit $\chi \in \widehat{G/H}$ par $\chi(gH) = \gamma(g)$. L'application χ est bien définie puisque si $gH = g'H$, $gg'^{-1} \in H$, et donc $\gamma(g) = \gamma(g')$. D'autre part puisque γ est un morphisme de groupes de G dans $\mathbb{C}^*$, χ est un morphisme de groupe de G/H dans $\mathbb{C}^*$. Enfin, $\widetilde{\chi} = \gamma$, d'où la surjectivité de φ.

Si $\widetilde{\chi} = \widetilde{\chi'}$, alors de manière évidente $\chi = \chi'$, et donc φ est injective, d'où la conclusion. □

Théorème 5 (Formule de Poisson)**.** *On a la formule, pour $g \in G$,*

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

En particulier, si $g = 1$,

$$\sum_{h\in H} f(h) = \frac{|H|}{|G|} \sum_{\chi\in H^\sharp} \widehat{f}(\overline{\chi}).$$

Démonstration. On note S un système de représentants des classes d'équivalences de G/H. On définit $\widetilde{f} \in \mathbb{C}[G/H]$ par

$$\widetilde{f}(gH) = \sum_{h\in H} f(gh).$$

On remarque que $h \mapsto gh \in \mathfrak{S}(gH)$, et donc si $gH = g'H$, alors $\sum_{h\in H} f(gh) = \sum_{h\in H} f(g'h)$ et donc $\widetilde{f}$ est bien définie. On peut alors lui appliquer la formule d'inversion de Fourier et obtenir, pour $gH \in G/H$

$$\widetilde{f}(gH) = \sum_{\chi\in\widehat{G/H}} <\widetilde{f}, \chi> \chi(gH).$$

On explicite alors les coefficients de Fourier de $\widetilde{f}$: pour $\chi \in \widehat{G/H}$, on a

$$c_{\widetilde{f}} =<\widetilde{f}, \chi >= \frac{1}{|G/H|} \sum_{g\in S} \widetilde{f}(gH)\overline{\chi(gH)} = \frac{|H|}{|G|} \sum_{g\in S}\sum_{h\in H} f(gh)\overline{\chi(gH)}.$$

On remarque alors que l'application

$$\begin{array}{ccc} S \times H & \to & G \\ (g, h) & \mapsto & gh \end{array}$$

est une bijection, pour des raisons de cardinalité puisqu'elle est injective. Ainsi, puisque pour $h \in H$, $\chi(gH) = \chi(ghH)$, on a

$$<\widetilde{f}, \chi >= \frac{|H|}{|G|} \sum_{g\in G} f(g)\overline{\chi(gH)} = \frac{|H|}{|G|} \sum_{g\in G} f(g)\overline{\widetilde{\chi}(g)} = \frac{|H|}{|G|}\widehat{f}(\overline{\widetilde{\chi}})$$

où $\widetilde{\chi}$ a déjà été défini. Finalement,

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

d'après le lemme précédent. C'est la formule recherchée. □

Remarque. La formule de Poisson discrète trouve notamment son intérêt en théorie des codes correcteurs, puisqu'elle permet de montrer l'identité de MacWilliams qui met en relation les poids des mots d'un code de Hamming et ceux des mots de son orthogonal.

2.7 Invariants de similitude (réduction de Frobenius)

Références : X. Gourdon, *Les maths en tête, Algèbre*, Ellipses, 2009
P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométrie, Tome premier*, Calvage & Mounet, 2013.

Leçons concernées : 150, 151, 153, 154, 157, 159.

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension finie.

Définition 1. Pour $f \in \mathcal{L}(E)$, on définit $\pi_{f,x}$ l'unique polynôme unitaire qui engendre l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ et $E_x = \{P(f)(x) \mid P \in \mathbb{K}[X]\}$ qui est alors de dimension $\deg \pi_{f,x} = k$ et dont une base est $(x, f(x), \dots, f^{k-1}(x))$.

Proposition 2. *Il existe $x \in E$ tel que $\pi_{f,x} = \pi_f$.*

Démonstration. On note $\pi_f = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ la décomposition de π_f en produit de facteurs irréductibles, $N_i = \ker P_i^{\alpha_i}(f)$ et $f_i = f_{|N_i}$. On remarque que $\pi_{f_i} = P_i^{\alpha_i}$. Par le lemme des noyaux, on a $E = N_1 \oplus \cdots \oplus N_r$. On montre d'abord la proposition sur les sous-espaces N_i : supposons par l'absurde que pour tout $x_i \in N_i$, π_{f_i,x_i} est différent de π_{f_i}. Soit $x_i \in N_i$, on a $\pi_{f_i,x_i} \mid \pi_{f_i} = P_i^{\alpha_i}$ et donc, puisque P_i est irréductible, $\pi_{f_i,x_i} \mid P_i^{\alpha_i - 1}$ et alors $P_i^{\alpha_i-1}(f_i)(x_i) = 0$. Ainsi $P_i^{\alpha_i-1}(f_i) = 0$ ce qui est absurde.

On montre alors que $x := x_1 + \cdots + x_r$ convient. On sait que $\pi_{f,x} \mid \pi_f$ et on montre donc que $\pi_f \mid \pi_{f,x}$. On a $\pi_{f,x}(f)(x) = 0 = \pi_{f,x}(f)(x_1) + \cdots + \pi_{f,x}(f)(x_r)$ et donc pour tout i, $\pi_{f,x}(f)(x_i) = 0$. Or $\pi_{f,x}(f)(x_i) = \pi_{f,x}(f_i)(x_i)$ puisque $x_i \in N_i$, et donc $\pi_{f_i,x_i} = \pi_{f_i} = P_i^{\alpha_i} \mid \pi_{f,x}$ et ainsi $\pi_f = P_1^{\alpha_1} \cdots P_r^{\alpha_r} \mid \pi_{f,x}$ ce qui conclut la preuve. □

Définition 3. On dit que $f \in \mathcal{L}(E)$ est cyclique si il existe $x \in E$ tel que $E_x = E$, c'est-à-dire, d'après la proposition précédente, si $\deg \pi_f = \dim E = n$, ou encore si $\pi_f = \chi_f$.

Remarque. Si f est cyclique, alors dans une certaine base, la matrice de f est la matrice compagnon associée à π_f. Il suffit de considérer pour cela $x \in E$ tel que $E_x = E$ et la base $(x, f(x), \dots, f^{n-1}(x))$.

Théorème 4. *Soit $f \in \mathcal{L}(E)$. Il existe une suite $(P_1, \dots, P_r)$ de polynômes unitaires et une suite $(F_1, \dots, F_r)$ de sous-espaces de E stables par f tels que*

(i) $E = F_1 \oplus \cdots \oplus F_r$

(ii) Pour tout $1 \leqslant i \leqslant r$, $f_i = f_{|F_i}$ soit cyclique de polynôme minimal P_i

(iii) $P_r \mid \cdots \mid P_1$.

La suite $(P_i)_i$ est unique, ses éléments sont appelés invariants de similitude *de f.*

Démonstration. Existence : on procède par récurrence sur $\dim E = n$. Pour $n = 1$, le théorème est trivial. On suppose alors le résultat vrai pour les espaces vectoriels G de dimension $\dim G \leqslant n-1$. On note $d = \deg \pi_f$. Soit $x \in E$ tel que $\pi_{f,x} = \pi_f$, que l'on note $P_1 = \pi_f$. On note également $F_1 = E_x = \mathrm{Vect}(x, f(x), \ldots, f^{d-1}(x))$ qui est stable par f. Alors $f_{|F_1}$ est cyclique et son polynôme minimal est de degré d (par la définition 3) et divise $\pi_f = P_1$ car celui-ci est un polynôme annulateur, il est ainsi égal à P_1.

Étape 1 : on cherche un supplémentaire f-stable à F_1. La famille

$$e_1 = x,\ e_2 = f(x),\ \ldots, e_d = f^{d-1}(x)$$

forme une base de F_1 que l'on complète en une base $(e_i)_i$ de E. On considère alors la base duale $(e_i^*)_i$ de E^* et on note $\varphi := e_d^*$ qui vérifie alors

$$\varphi(e_1) = \cdots = \varphi(e_{d-1}) = 0 \quad \text{et} \quad \varphi(e_d) = 1.$$

On vérifie facilement que la famille $(\varphi, \varphi \circ f, \ldots, \varphi \circ f^{d-1})$ est une famille libre de E^*. On considère alors $\Phi = \mathrm{Vect}(\varphi, \varphi \circ f, \ldots, \varphi \circ f^{d-1})$ qui est donc de dimension d et on pose $G = \Phi^0 = \{x \in E \mid \varphi(x) = 0\ \forall \varphi \in \Phi\}$ qui est alors de dimension $n-d$. Montrons que G convient.

Étape 2 : soit $y \in G$, vérifions que $f(y) \in G$. On a, par définition de G, pour $1 \leqslant k \leqslant d-2$, $\varphi \circ f^k(f(y)) = 0$ et d'autre part $\varphi \circ f^{d-1}(f(y)) = 0$ puisque, π_f étant de degré d, $f^d(y)$ s'exprime comme une combinaison linéaire de $(y, f(y), \ldots, f^{d-1}(y))$. Ainsi, G est stable par f.

Soit $y = \lambda_1 x + \cdots + \lambda_d f^{d-1}(x) \in F_1 \cap G$. On applique alors $\varphi \circ f^i$ à y pour i allant de 0 à $d-1$ pour obtenir $\lambda_1 = \cdots = \lambda_d = 0$ et donc $F_1 \cap G = \{0\}$.

Étape 3 : par dimension, on a ainsi montré que G est un supplémentaire f-stable à F_1. On applique alors l'hypothèse de récurrence à G et $f_{|G}$, et on trouve une suite $(P_2, \ldots, P_r)$ de polynômes unitaires et une suite $(F_2, \ldots, F_r)$ de sous-espaces de G (donc de E) stables par $f_{|G}$ (donc par f) tels que

(i) $G = F_2 \oplus \cdots \oplus F_r$, et ainsi $E = F_1 \oplus \cdots \oplus F_r$

(ii) Pour tout $2 \leqslant i \leqslant r$, $f_i = (f_{|G})_{|F_i} = f_{|F_i}$ soit cyclique de polynôme minimal P_i, et le résultat est vrai pour $i = 1$ d'après le début de la preuve

(iii) $P_r \mid \cdots \mid P_2$.

On conclut en remarquant que puisque $P_1 = \pi_f$ est un polynôme annulateur de $f_{|G}$, $\pi_{f_{|G}} = P_2 \mid P_1$.

Unicité : soit $(Q_1, \ldots, Q_s)$ et $(G_1, \ldots, G_s)$ deux autres suites satisfaisant le théorème. On remarque que $P_1 = \pi_f = Q_1$. Supposons par l'absurde que la liste $(Q_1, \ldots, Q_s)$ soit différente de la liste $(P_1, \ldots, P_r)$. Soit alors j le premier indice i tel que $P_i \neq Q_i$, qui existe même si $s \neq r$ puisque $\sum_{i=1}^r \deg P_i = n = \sum_{i=1}^s \deg Q_i$. On a, par (i), le fait que les F_i soient stables par f, et puisque pour $i \geqslant j$, $\pi_{f_{|F_i}} = P_i \mid P_j$ par (ii) et (iii),

$$P_j(f)(E) = P_j(f)(F_1) \oplus \cdots \oplus P_j(f)(F_{j-1}). \tag{1}$$

D'autre part, en utilisant $E = G_1 \oplus \cdots \oplus G_s$ qui est une décomposition en sous-espaces stables par f, on a

$$P_j(f)(E) = P_j(f)(G_1) \oplus \cdots \oplus P_j(f)(G_s). \tag{2}$$

Or, pour $1 \leqslant i \leqslant j-1$, d'après la remarque qui précède le théorème, il existe une base de F_i dans laquelle la matrice de $f_{|F_i}$ soit $\mathcal{C}(\pi_{f_{|F_i}}) = \mathcal{C}(P_i)$ et une base de G_i dans laquelle la matrice de $f_{|G_i}$ soit $\mathcal{C}(\pi_{f_{|G_i}}) = \mathcal{C}(Q_i) = \mathcal{C}(P_i)$ par hypothèse sur j et donc $\dim P_j(f)(F_i) = \dim P_j(f)(G_i)$. Ainsi, si on prend la dimension dans (1) et (2), on obtient

$$\dim P_j(f)(G_j) = \cdots = \dim P_j(f)(G_s) = 0$$

et donc

$$P_j(f)(G_j) = \cdots = P_j(f)(G_s) = \{0\}$$

ainsi, $Q_j \mid P_j$. Par symétrie on obtient $P_j \mid Q_j$ et donc $Q_j = P_j$ ce qui est absurde. □

Corollaire 5 (Réduction de Frobenius)**.** *Soit $f \in \mathcal{L}(E)$ et $(P_1, \ldots, P_r)$ la suite des invariants de similitude de f. Il existe une base dans laquelle la matrice de f est la matrice par blocs*

$$\begin{pmatrix} \mathcal{C}(P_1) & & (0) \\ & \ddots & \\ (0) & & \mathcal{C}(P_r) \end{pmatrix}$$

où $\mathcal{C}(P_i)$ désigne la matrice compagnon associée au polynôme P_i. Deux endomorphismes f et g sont semblables si et seulement si ils ont les mêmes invariants de similitude. Enfin, le polynôme minimal de f est P_1 et son polynôme caractéristique $P_1 \cdots P_r$.

Démonstration. Pour obtenir la matrice par blocs annoncée, il suffit de considérer une base adaptée à la décomposition $E = F_1 \oplus \cdots \oplus F_r$ et de voir que pour tout i il existe une base de F_i telle que la matrice de f_i dans cette base soit $\mathcal{C}(P_i)$.

Si f et g sont semblables d'invariants de similitudes respectifs $(P_i)_i$, $(Q_j)_j$, alors puisque la relation de similitude est transitive, les $(Q_j)_j$ sont aussi des invariants de similitude de f et on conclut par unicité. La réciproque s'obtient en remarquant que si f et g ont les mêmes invariants de similitude, alors ils sont semblables à la même matrice compagnon par blocs et sont donc semblables. □

Commentaire : on montre seulement le théorème 4 et éventuellement le corollaire 5, mais la preuve de la proposition 2 est à connaitre puisqu'elle est souvent demandée.

2.8 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$

Référence : D. Perrin, *Cours d'Algèbre*, Ellipses, 1996.

Leçons concernées : 102, 122, 141, 144.

Théorème 1. *Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.*

Démonstration. Étape 1 : soit $\zeta \in \mathbb{C}$ une racine primitive n-ème de l'unité, donc racine de Φ_n. Si p est premier et ne divise pas n, alors ζ^p est aussi une racine primitive n-ème de l'unité car $n \wedge p = 1$. Soit f, g les polynômes minimaux de ζ, ζ^p sur $\mathbb{Q}$. On décompose

$$\Phi_n(X) = f_1(X)^{\alpha_1} \cdots f_r(X)^{\alpha_r}$$

en produit d'irréductibles sur $\mathbb{Z}[X]$, unitaires puisque Φ_n l'est. Alors ζ est racine de l'un des f_i, irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$, ainsi f_i est le polynôme minimal de ζ sur $\mathbb{Q}$, et $f = f_i$. De même il existe j tel que $g = f_j$.

Étape 2 : montrons que $f = g$: supposons par l'absurde que ce n'est pas le cas, alors puisque f et g sont irréductibles, fg divise Φ_n. D'autre part, $g(\zeta^p) = 0$ donc ζ est racine de $g(X^p)$, ainsi, $f(X) \mid g(X^p)$ dans $\mathbb{Q}[X]$: il existe $h \in \mathbb{Q}[X]$ tel que

$$g(X^p) = f(X)h(X),$$

mais si on écrit $h = \frac{a}{b}h'$ avec $h' \in \mathbb{Z}[X]$ et $c(h') = 1$ (si $h(X) = \sum_i \frac{a_i}{b_i} X^i$, on prend $b := \mathrm{ppcm}(b_i)$ de sorte que $h(X) = \frac{1}{b}\sum_i a_i' X^i$, et on pose $a := \mathrm{pgcd}(a_i)$), on a

$$bg(X^p) = af(X)h'(X)$$

et en passant au contenu, $b = a$ puisque f et g sont unitaires, ainsi $f(X) \mid g(X^p)$ dans $\mathbb{Z}[X]$. Or par le morphisme de Frobenius, dans $\mathbb{F}_p[X]$, si $g = a_r X^r + \cdots + a_0$

$$\overline{g}(X^p) = \overline{a_r}X^{pr} + \cdots + \overline{a_0} = \overline{a_r}^p X^{pr} + \cdots + \overline{a_0}^p = (\overline{a_r}X^r + \cdots + \overline{a_0})^p = \overline{g}(X)^p.$$

Soit maintenant φ un facteur irréductible de $\overline{f}$ sur $\mathbb{F}_p$, alors avec

$$\overline{g}(X)^p = \overline{f}(X)\overline{h}(X)$$

dans $\mathbb{F}_p[X]$, φ divise $\overline{g}$ par le lemme d'Euclide. Ainsi, φ^2 divise $\overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$, qui aura donc une racine multiple dans son corps de décomposition, ce qui est impossible puisque $n \wedge p = 1$.

Étape 3 : soit maintenant ζ' une racine primitive n-ème de l'unité. Alors $\zeta' = \zeta^m$ où $m = p_1^{\beta_1} \cdots p_l^{\beta_l}$ avec $p_i \nmid n$. On a alors avec le paragraphe précédent et une récurrence immédiate que ζ' et ζ ont même polynôme minimal. Ainsi, $f(\zeta') = 0$, de sorte que toutes les racines primitives n-ème de l'unité annulent f, et donc $\deg(f) \geqslant \varphi(n)$, mais puisque $f \mid \Phi_n$, $f = \Phi_n$ et donc Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

□

2.9 L'exponentielle induit un homéomorphisme de $\mathcal{S}_n(\mathbb{R})$ dans $\mathcal{S}_n^{++}(\mathbb{R})$

Référence : P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométrie, Tome premier*, Calvage & Mounet, 2013.

Leçons concernées : 150, 155, 156, 158, 160.

Lemme 1. *Pour tout matrice $S \in \mathcal{S}_n(\mathbb{R})$,*

$$||S||_2 = \rho(S).$$

Démonstration. Puisque S est symétrique, il existe une base orthonormée $(v_i)_i$ formée de vecteurs propres de S tels que les valeurs propres associées vérifient $|\lambda_1| \geqslant \cdots \geqslant |\lambda_n|$. Soit $x = \sum_{i=1}^n x_i v_i$ de norme 1, alors $||Sx||_2 = ||\sum_{i=1}^n x_i \lambda_i v_i||_2 \leqslant |\lambda_1|$ et l'égalité est atteinte pour $x = v_1$. Ainsi $||S||_2 = \rho(S)$. □

Théorème 2. *L'application*

$$\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$$

est un homéomorphisme.

Démonstration. Étape 1 : soit $A \in \mathcal{S}_n(\mathbb{R})$, alors il existe $P \in O_n(\mathbb{R})$ et des réels $(\lambda_i)_i$ tels que $A = P \operatorname{diag}(\lambda_i) {}^tP$. On a alors

$$\exp A = P \exp\big[\operatorname{diag}\big(\lambda_i\big)\big] {}^tP = P \operatorname{diag}\big(\exp \lambda_i\big) {}^tP$$

qui est une matrice symétrique définie positive puisque $\exp \lambda_i > 0 \ \forall i$. Ainsi, exp envoie bien $\mathcal{S}_n(\mathbb{R})$ sur $\mathcal{S}_n^{++}(\mathbb{R})$ et l'application $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est continue par restriction.

Étape 2 : si $B \in \mathcal{S}_n^{++}(\mathbb{R})$, on peut, par diagonalisation et caractérisation des matrices symétriques définies positives, écrire $B = P \operatorname{diag}(\mu_i) {}^tP$ avec $P \in O_n(\mathbb{R})$ et $\mu_i > 0$ pour tout i. On a alors

$$\exp\big[P \operatorname{diag}\big(\ln \mu_i\big) {}^tP\big] = P \operatorname{diag}\big(\exp \ln \mu_i\big) {}^tP = P \operatorname{diag}\big(\mu_i\big) {}^tP = B$$

et donc $\exp \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est surjective.

Étape 3 : soit alors $A, B \in \mathcal{S}_n(\mathbb{R})$ telles que $\exp A = \exp B$. On écrit $A = P \operatorname{diag}(\lambda_i) {}^tP$ et on considère $Q \in \mathbb{R}[X]$ le polynôme interpolateur de Lagrange tel que pour tout i, $Q(\exp \lambda_i) = \lambda_i$. On a alors

$$\begin{aligned} Q[\exp B] = Q[\exp A] = Q\big[P \operatorname{diag}\big(\exp \lambda_i\big) {}^tP\big] &= P \cdot Q\big[\operatorname{diag}\big(\exp \lambda_i\big)\big] \cdot {}^tP \\ &= P \operatorname{diag}\big(Q(\exp \lambda_i)\big) {}^tP = P \operatorname{diag}\big(\lambda_i\big) {}^tP = A \end{aligned}$$

et donc puisque B commute avec $\exp B$ et donc avec $Q[\exp B]$, B commute avec A. Par le théorème de diagonalisation simultanée, il existe $P_0 \in O_n(\mathbb{R})$ telle que $A = P_0 \operatorname{diag}(\lambda_i) {}^tP_0$ et $B = P_0 \operatorname{diag}(\mu_i) {}^tP_0$. On a alors

$$P_0 \operatorname{diag}\big(\exp \lambda_i\big) {}^tP_0 = \exp A = \exp B = P_0 \operatorname{diag}\big(\exp \mu_i\big) {}^tP_0$$

et donc pour tout i, $\exp\lambda_i = \exp\mu_i$, c'est-à-dire que $\lambda_i = \mu_i$, et par suite $A = B$, d'où l'injectivité de $\exp\mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$.

Étape 4 : on montre enfin que $\exp\mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ est bicontinue. Soit $(B_p)_p = (\exp A_p)_p$ une suite de $\mathcal{S}_n^{++}(\mathbb{R})$ où $(A_p)_p \in \mathcal{S}_n(\mathbb{R})$, qui converge vers $B = \exp A$ dans $\mathcal{S}_n^{++}(\mathbb{R})$. Montrons que $(A_p)_p$ converge vers A. On a, pour $M \in \mathcal{S}_n(\mathbb{R})$,

$$||M||_2 = \rho(M).$$

Puisque $(B_p)_p$ converge vers B, $(B_p)_p$ est bornée en norme $||.||_2$ et donc toutes les valeurs propres des $(B_p)_p$ sont majorées par un certain $C > 0$. D'autre part, l'inverse étant continu, $(B_p^{-1})_p$ converge vers B^{-1}, et donc $(B_p^{-1})_p$ est bornée en norme $||.||_2$. Ainsi, toutes les valeurs propres des $(B_p^{-1})_p$ sont majorées par une certaine constante $C'' > 0$. Or les valeurs propres de B_p^{-1} étant les inverses des valeurs propres de B_p, les valeurs propres de B_p sont minorées par $C' = 1/C'' > 0$. Les valeurs propres de la suite $(B_p)_p$ sont donc comprises dans $[C', C]$, et donc les valeurs propres de $(A_p)_p$ sont comprises dans $[\ln C', \ln C]$ intervalle borné. Avec l'égalité

$$||M||_2 = \rho(M)$$

on déduit que $(A_p)_p$ est bornée pour la norme $||.||_2$. Or si $\widetilde{A}$ est une valeur d'adhérence de $(A_p)_p$, alors par continuité de l'exponentielle, $\exp(\widetilde{A}) = B = \exp(A)$ et par injectivité on obtient l'unicité de la valeur d'adhérence. On peut donc conclure que $(A_p)_p$ converge vers A, ce qui termine la preuve. □

2.10 Loi de réciprocité quadratique

Référence : P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométrie, Tome premier*, Calvage & Mounet, 2013.

Leçons concernées : 101, 121, 123, 150, 170, 190.

Définition 1. Pour p premier impair et $a \geqslant 1$, on définit le symbole de Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } p \mid a \end{cases}$$

Théorème 2 (Loi de réciprocité quadratique)**.** *Si p et q sont deux nombres premiers impairs distincts, alors*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Lemme 3. *Si p est premier impair et $a \in \mathbb{F}_p^*$, alors*

$$|\{x \in \mathbb{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Démonstration. Cela résulte du fait que si a est un carré modulo p si et seulement si a^{-1} est un carré modulo p et du fait que si b est un carré, le polynôme $X^2 - b$ admet deux racines distinctes dans $\mathbb{F}_p$. □

Démonstration (Théorème). L'idée de la preuve est de calculer de deux façons différentes le cardinal de l'ensemble suivant :

$$X = \Big\{(x_1, \ldots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^{p} x_i^2 = 1\Big\}.$$

La première méthode consiste à faire agir $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation sur les coordonnées : si $k \in \mathbb{Z}/p\mathbb{Z}$ et $(x_1, \ldots, x_p) \in X$,

$$k \cdot (x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{p+k})$$

où les indices sont vus modulo p. On étudie alors les orbites de cette action. Puisque $\mathbb{Z}/p\mathbb{Z}$ n'a que des sous-groupes triviaux, les seuls stabilisateurs possibles d'un élément sont $\{1\}$ et $\mathbb{Z}/p\mathbb{Z}$. Les orbites dont le stabilisateur des éléments est $\mathbb{Z}/p\mathbb{Z}$ sont les singletons $\{(x, \ldots, x)\}$ avec $x \in \mathbb{F}_q$ tel que $px^2 = 1$, elles sont donc au nombre de $1 + \left(\frac{p}{q}\right)$ par le lemme. Par la relation orbite stabilisateur, les orbites dont le stabilisateur des éléments est trivial sont de cardinal $|\mathbb{Z}/p\mathbb{Z}|/|\{1\}| = p$. Ainsi, pas la formule des classes, $|X| \equiv 1 + \left(\frac{p}{q}\right) \mod p$.

On va maintenant utiliser une forme quadratique équivalente sur $\mathbb{F}_q^p$ à $f(x) = \sum_i x_i^2$ dont la matrice dans la base canonique est I_p. On considère pour cela la matrice

$$A = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & (0) & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & (0) & & 1 & 0 & \\ & & & & & a \end{pmatrix}$$

où on a posé $a = (-1)^d$ avec $d = (p-1)/2$. Les matrices A et I_p ont même rang p et même déterminant 1, donc même discriminant, elles définissent donc des formes quadratiques équivalentes. Si P est la matrice de changement de base pour passer de l'une à l'autre, on a alors $X' = PX$ et donc $|X| = |X'|$ où on a posé

$$X' = \{(y_1, \ldots, y_d, z_1, \ldots, z_d, t) \in \mathbb{F}_q^p \mid 2(y_1 z_1 + \cdots + y_d z_d) + at^2 = 1\}.$$

On distingue alors deux types d'éléments $(y_1, \ldots, y_d, z_1, \ldots, z_d, t)$ de X :

- Ceux dont tous les y_i sont nuls. Le choix de $(z_1, \ldots, z_d)$ est alors quelconque et donne donc q^d possibilités et celui de t donne, d'après le lemme, $1 + \left(\frac{a}{q}\right)$ possibilités, d'où $q^d \left(1 + \left(\frac{a}{q}\right)\right)$ éléments de X' de cette forme.
- Ceux dont au moins un des y_i est non nul. On choisit donc un vecteur non nul de $\mathbb{F}_q^d$: $q^d - 1$ possibilités, puis on choisit t de manière quelconque dans $\mathbb{F}_q$: q possibilités, il nous reste alors à choisir $(z_1, \ldots, z_d)$ dans l'hyperplan affine d'équation $2(y_1 z_1 + \cdots + y_d z_d) + at^2 - 1 = 0$, il y a donc q^{d-1} possibilités, et $q^d(q^d - 1)$ éléments de ce type dans X'.

On peut alors conclure :

$$q^q \left(1 + \left(\frac{a}{q}\right)\right) + q^d(q^d - 1) \equiv 1 + \left(\frac{p}{q}\right) \mod p$$

c'est-à-dire, avec $\left(\frac{a}{q}\right) = a^{(q-1)/2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, et $\left(\frac{q}{p}\right) = q^{(p-1)/2} = q^d$,

$$\left(\frac{q}{p}\right)\left((-1)^{\frac{p-1}{2}\frac{q-1}{2}} + \left(\frac{q}{p}\right)\right) \equiv 1 + \left(\frac{p}{q}\right) \mod p$$

ainsi, en multipliant par $\left(\frac{q}{p}\right)$,

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} + \left(\frac{q}{p}\right) \equiv \left(\frac{q}{p}\right) + \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \mod p$$

et on a alors l'égalité modulo p. Or les éléments en jeu sont égaux à ± 1, donc l'égalité est en fait dans $\mathbb{Z}$. □

2.11 Polynômes irréductibles sur $\mathbb{F}_q$

Référence : S. Francinou, H. Gianella, *Exercices de mathématiques pour l'agrégation, Algèbre 1*, Masson, 1997.

Leçons concernées : 123, 125, 141, 190.

Soit p un nombre premier et q une puissance de p.

Théorème 1. *On note $\mathcal{P}_q(n)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$ et $I(q,n)$ son cardinal. Alors*

$$I(q,n) = \frac{1}{n}\sum_{d|n}\mu\Big(\frac{n}{d}\Big)q^d$$

et donc $I(q,n) \underset{n\to\infty}{\sim} \dfrac{q^n}{n}$.

Démonstration. On commence par montrer que

$$X^{q^n} - X = \prod_{d|n}\prod_{P\in\mathcal{P}_q(d)} P(X).$$

En effet, si $d \mid n$ et si $P \in \mathcal{P}_q(d)$, on considère $K = \mathbb{F}_q[X]/(P)$ qui est un corps de cardinal q^d, et donc, pour $x \in K$, $x^{q^d} = x$. Or, on a,

$$x^{q^n} = \underbrace{\big(\cdots\big(x^{q^d}\big)^{q^d}\cdots\big)^{q^d}}_{n/d \text{ fois}}$$

et donc pour $x \in K$, $x^{q^n} = x$, en particulier, $\overline{X}^{q^n} = \overline{X}$ et donc $\overline{X}^{q^n} - \overline{X} = 0$ dans $\mathbb{F}_q[X]/(P)$, c'est-à-dire que $P \mid X^{q^n} - X$. Par le lemme de Gauss, on déduit que $\prod_{d|n}\prod_{P\in\mathcal{P}_q(d)} P(X) \mid X^{q^n} - X$.

Réciproquement, soit P un diviseur irréductible de $X^{q^n} - X$ de degré d. Puisque $\mathbb{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$, P est scindé sur $\mathbb{F}_{q^n}$. Soit alors $x \in \mathbb{F}_{q^n}$ une racine de P. On a d'après le théorème de la base télescopique

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q].$$

Or P est irréductible sur $\mathbb{F}_q$ donc $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$, ainsi, $d \mid n$.

Enfin, $X^{q^n} - X$ n'a pas de facteurs multiples, en effet si c'était le cas il serait à racines multiples dans $\mathbb{F}_{q^n}$ son corps de décomposition sur $\mathbb{F}_q$. Or $(X^{q^n} - X)' = -1$ dans $\mathbb{F}_{q^n}$ (car $\mathrm{car}(\mathbb{F}_{q^n}) = p$) et donc $X^{q^n} - X$ est à racines simples sur $\mathbb{F}_{q^n}$.

On montre maintenant la proposition suivante :

Proposition 2. *Soit $f : \mathbb{N}^* \to \mathbb{C}$ et μ la fonction de Möbius. Si pour $n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} f(d)$, alors pour $n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.*

Démonstration. On remarque d'abord que ($d \mid n$ et $d' \mid \frac{n}{d}$) si et seulement si $dd' \mid n$. Ainsi, on a

$$\sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d).$$

Or on sait que si $m \neq 1$, $\sum_{d|m} \mu(d) = 0$ [1], d'où le résultat. □

On a, en prenant les degrés dans la factorisation de $X^{q^n} - X$,

$$q^n = \sum_{d|n} d \cdot I(q, d).$$

Ainsi, en appliquant la formule d'inversion de Möbius avec $g(d) = q^d$ et $f(d) = d \cdot I(q, d)$, on obtient

$$I(q, n) = \frac{1}{n} \sum_{d|n} \mu\Big(\frac{n}{d}\Big) q^d.$$

On note alors $r_n = \sum_{d|n,\ d<n} \mu(\frac{n}{d}) q^d$. On a,

$$|r_n| \leqslant \sum_{d|n,\ d<n} q^d \leqslant \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q - 1}$$

et donc $r_n \underset{+\infty}{=} o(q^n)$. Or $I(q, n) = \dfrac{q^n + r_n}{n}$, et donc $I(q, n) \underset{n \to \infty}{\sim} \dfrac{q^n}{n}$. □

1. Si $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\sum_{d|m} \mu(d) = \sum_{\beta \leqslant \alpha} \mu(p_1^{\beta_1} \cdots p_r^{\beta_r}) = \sum_{\beta \in \{0,1\}^r} (-1)^{|\beta|} = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = 0$

2.12 Table de caractères de $\mathfrak{S}_4$ et groupes d'isométrie du tétraèdre et du cube

Leçons concernées : 101, 103, 104, 105, 107, 161.

Proposition 1. *On note T un tétraèdre régulier et C un cube. Alors,*

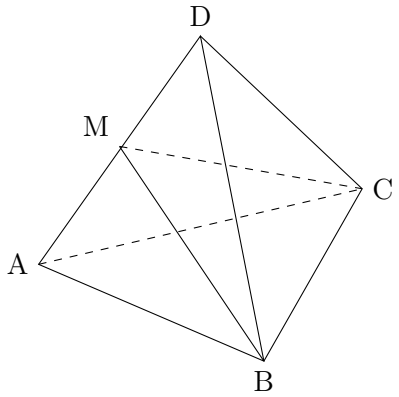
$$\mathrm{Isom}(T) \cong \mathfrak{S}_4 \quad et \quad \mathrm{Isom}^+(C) \cong \mathfrak{S}_4.$$

Démonstration. Puisqu'une isométrie conserve les longueurs, l'ensemble $S = \{A, B, C, D\}$ des sommets est conservé par toute isométrie de T, on a donc un morphisme

$$\varphi : \begin{array}{ccc} \mathrm{Isom}(T) & \to & \mathfrak{S}_4 \\ g & \mapsto & g_{|S}. \end{array}$$

Si $\varphi(g) = \mathrm{id}$, alors g conserve un repère affine, et donc $g = \mathrm{id}$, d'où l'injectivité de φ.

D'autre part, on considère s la symétrie orthogonale d'hyperplan (BMC). Alors $\varphi(r) = (AD)$. On peut de la même manière obtenir toutes les permutations de $\mathfrak{S}_4$, et donc puisqu'elles engendrent le groupe, on obtient la surjectivité.



Pour le cube, on remarque que puisque les grandes diagonales sont les plus grandes longueurs du cube, elles sont conservées par les isométries de C, et donc, si on note $S = \{D_1, D_2, D_3, D_4\}$, alors on a un morphisme

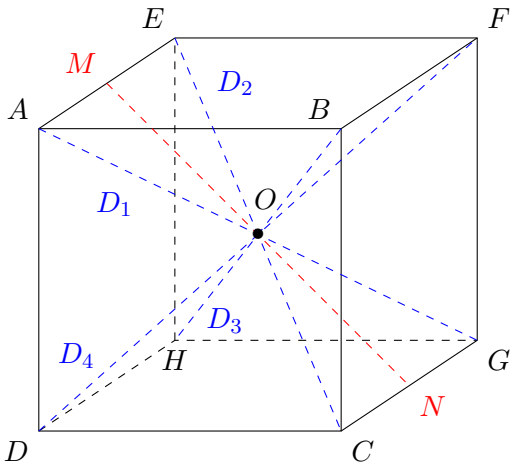
$$\varphi : \begin{array}{ccc} \mathrm{Isom}(C) & \to & \mathfrak{S}_4 \\ g & \mapsto & g_{|S}. \end{array}$$

On considère ρ la rotation d'axe (MN) et d'angle π. Alors $\varphi(\rho) = (D_1 D_2)$ et par le même procédé on obtient toutes les transpositions de $\mathfrak{S}_4$ et donc φ est surjective.

Soit $g \in \mathrm{Isom}(C)$ différente de l'identité telle que $\varphi(g) = \mathrm{id}$. Alors g échange au moins les sommets d'une grande diagonale, on peut donc supposer que $g(A) = G$. On a alors

$g(E) \in \{C, E\}$, et donc puisque g conserve les distances, $g(E) = C$. On obtient de la même manière que g échange les sommets de chaque grande diagonale, et donc g coïncide avec s_0 la symétrie de centre O le centre du cube, et donc $g = s_0$. Ainsi, $\ker \varphi = \{\mathrm{id}, s_0\}$ et on a,

$$\mathrm{Isom}^+(C) \cong \mathrm{Isom}(C)/\{\mathrm{id}, s_0\} \cong \mathfrak{S}_4.$$



□

On peut alors compléter la table de caractères de $\mathfrak{S}_4$.

Étape 1 : on détermine les classes de conjugaison de $\mathfrak{S}_4$ et leur cardinal. Puisque celles-ci sont caractérisées par le type, on obtient :

- la classe de l'identité qui contient 1 élément
- la classe des transpositions qui contient $\binom{4}{2} = 6$ éléments
- la classe des 3-cycles qui contient $2 \times \binom{4}{3} = 8$ éléments
- la classe des 4-cycles qui contient $3! = 6$ éléments
- et la classe des doubles transpositions qui contient 3 éléments [1].

Étape 2 : on connait deux représentations irréductibles de degré 1 : la représentation triviale, et la représentation donnée par la signature, on obtient donc les deux premières lignes suivantes :

	1 id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1

1. Il suffit de choisir l'élément qui sera dans la transposition avec 1 pour entièrement déterminer la double transposition.

Étape 3 : on considère maintenant la représentation par permutation ρ_p

$$\rho_p : \begin{array}{ccc} \mathfrak{S}_4 & \to & \mathrm{GL}(\mathbb{C}^4) \\ \sigma & \mapsto & (e_i \mapsto e_{\sigma(i)}) \end{array}$$

où on a noté $\mathcal{B} = \{e_1, e_2, e_3, e_4\}$ la base canonique de $\mathbb{C}^2$. Si χ_p est le caractère associé à ρ_p, on sait que $\chi_p(\sigma)$ est égal au nombre de points fixes de σ, ainsi, $\chi_p = (4, 2, 1, 0, 0)$, dont on vérifie qu'elle n'est pas irréductible. On considère alors $H_0 = \mathrm{Vect}((1, 1, 1, 1))$ stable par ρ_p, qui admet $H_1 = \{(x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$ pour supplémentaire stable par ρ. La représentation induite par ρ_p sur H_0 est la représentation triviale, et donc, si on note χ_s le caractère de la représentation induite sur H_1 par ρ_p, on a $\chi_p = \chi_1 + \chi_s$, et ainsi $\chi_s = (3, 1, 0, -1, -1)$ dont on vérifie qu'elle est irréductible. On peut alors compléter le tableau :

	1 id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1

Étape 3' : on utilise l'isomorphisme $\mathrm{Isom}^+(C) \cong \mathfrak{S}_4$ pour obtenir une action de $\mathfrak{S}_4$ sur l'espace $\mathbb{R}^3$ et donc une représentation de degré 3. On détermine alors son caractère χ_C. On sait que la trace d'une rotation d'angle θ est donnée par $1 + 2\cos\theta$. Ainsi, $\chi_C(\mathrm{id}) = 3$. Pour réaliser une transposition on réalise une rotation d'angle π autour de la diagonale joignant le milieu de deux côtés opposés, ce qui nous donne $\chi_C((12)) = -1$. Un 3-cycle s'obtient par rotation d'angle $2\pi/3$ autour de la grande diagonale invariante, et donc $\chi_C((123)) = 0$. Une rotation d'angle $\pi/2$ selon l'axe qui passe par le milieu de deux face opposées donne un 4-cycle, et donc $\chi_C((1234)) = 1$. Enfin, on obtient une double transposition grâce à la rotation d'angle π selon l'axe qui passe par le milieu de deux faces opposées et donc $\chi_C((12)(34)) = -1$, de sorte que $\chi_C = (3, -1, 0, 1, -1)$ qui est donc irréductible. On a alors le tableau :

	1 id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_C	3	-1	0	1	-1

Étape 4 : il nous reste encore deux caractères irréductibles à déterminer. De la relation sur les degrés des caractères $1^2 + 1^2 + 3^2 + n_4^2 + n_5^2 = 24$, on déduit qu'il y a un caractère de degré 2 et un de degré 3. On considère alors le produit tensoriel des représentations ε et ρ_s (resp. ρ_C) qui est irréductible, ce qui nous donne le tableau :

	1 id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
χ_C	3	-1	0	1	-1
χ_5	2				

Étape 5 : on utilise les relations d'orthogonalité des colonnes et ce que l'on sait du degré de χ_5 pour obtenir la dernière ligne :

	1 id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
χ_C	3	-1	0	1	-1
χ_5	2	0	-1	0	2

Remarque. À l'étape 4, on aurait pu considérer la représentation $\mathrm{Hom}(V_s, V_\varepsilon)$ dont le caractère est donné par $\overline{\chi_\varepsilon}\chi_s$ dont on doit vérifier qu'elle est irréductible.

Corollaire 2. *Les sous-groupes distingués non triviaux de* $\mathfrak{S}_4$ *sont* $\mathfrak{A}_4$ *et* $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong V_4$.

Démonstration. On applique la caractérisation des sous-groupes distingués à partir des caractères :

	1 id	6 (12)	8 (123)	6 (1234)	3 (12)(34)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
χ_C	3	-1	0	1	-1
χ_5	2	0	-1	0	2

la première ligne nous donne alors $\mathfrak{S}_4$, la seconde $\mathfrak{A}_4$, la troisième et la quatrième $\{\mathrm{id}\}$ et la dernière V_4 tandis que les intersections ne donnent pas de nouveau sous-groupe distingué. □

Commentaire : Faire l'étape 3 la plus adaptée à la leçon.

2.13 Théorème d'Artin

Références : A. Jeanneret, D. Lines, *Invitation à l'algèbre*, Cépaduès, 2008,
J. Calais, *Extensions de corps, théorie de Galois*, Ellipses, 2006.

Leçons concernées : 125, 151, 162.

Théorème 1 (Artin)**.** [1] *Soit L un corps et soit H un sous-groupe fini du groupe des automorphismes de L. Alors si on note $L^H := \{x \in L \mid \sigma(x) = x,\ \forall \sigma \in H\}$, L/L^H est une extension finie de degré $[L : L^H] = |H|$.*

Lemme 2 (Dedekind)**.** *Soit $n \geqslant 1$, K, L deux corps, et soit $\varphi_1, \dots, \varphi_n : K \to L$ n homomorphismes de corps distincts. Alors $(\varphi_1, \dots, \varphi_n)$ est libre sur L.*

Démonstration. On suppose par l'absurde que $(\varphi_1, \dots, \varphi_n)$ n'est pas libre et on se donne $(\lambda_1, \dots, \lambda_n) \in L^n \backslash \{0\}$ avec un nombre minimal r d'éléments non nuls tel que $\sum_{i=1}^n \lambda_i \varphi_i = 0$. On remarque que nécessairement $r \geqslant 2$, et quitte à renuméroter, on peut supposer que $\lambda_1, \dots, \lambda_r \neq 0$ et $\sum_{i=1}^r \lambda_i \varphi_i = 0$. Soit $y \in K$ tel que $\varphi_1(y) \neq \varphi_2(y)$. On a, pour $x \in K$,

$$\sum_{i=1}^{r} \lambda_i \varphi_i(x) = 0 \tag{1}$$

$$\sum_{i=1}^{r} \lambda_i \varphi_i(xy) = \sum_{i=1}^{r} \lambda_i \varphi_i(x)\varphi_i(y) = 0. \tag{2}$$

On réalise alors $(2) - \varphi_1(y) \times (1)$ et on obtient

$$\sum_{i=2}^{r} \lambda_i \big(\varphi_1(y) - \varphi_i(y)\big)\varphi_i = 0$$

ce qui nous fournit une contradiction par minimalité puisque $\lambda_2(\varphi_1(y) - \varphi_2(y)) \neq 0$. □

Démonstration (Théorème). On pose $m = [L : L^H]$ (éventuellement infini) et $n = |H|$. On veut montrer que $m = n$.

Étape 1 : $m \geqslant n$. On suppose par l'absurde que $m < n$. On se donne $(x_1, \dots, x_m)$ une L^H-base de L et on note $\sigma_1, \dots, \sigma_n$ les éléments de H. On considère le système d'équations

$$\sigma_1(x_j)y_1 + \cdots + \sigma_n(x_j)y_n = 0, \quad j \in [|1, m|].$$

Puisque le nombre d'inconnues est strictement supérieur au nombre d'équations, il existe une solution non nulle $(y_1, \dots, y_n)$ au système. Alors, pour tout $x = \sum_{j=1}^m \lambda_j x_j \in L$ avec $\lambda_j \in L^H$,

$$\sum_{i=1}^{n} y_i \sigma_i(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} y_i \sigma_i(x_j)\lambda_j = \sum_{j=1}^{m} \lambda_j \Big(\sum_{i=1}^{n} y_i \sigma_i(x_j) \Big) = 0$$

1. D'après le mathématicien autrichien Emil Artin ([artin]).

ce qui est absurde d'après le lemme précédent.

Étape 2 : $m \leqslant n$. On suppose par l'absurde que $m > n$, alors il existe une famille $(x_1, \dots, x_{n+1})$ de L libre sur L^H. Par le même raisonnement que précédemment, il existe une famille non nulle $(y_1, \dots, y_{n+1})$ de L telle que

$$\sigma_i(x_1)y_1 + \cdots + \sigma_i(x_{n+1})y_{n+1} = 0, \quad \forall i \in [|1, n|].$$

On choisit $(y_1, \dots, y_{n+1})$ tel que le nombre r de ses composantes non nulles soit minimal, et quitte à renuméroter on suppose que $y_1, \dots, y_r \neq 0$ et $y_{r+1}, \dots, y_{n+1} = 0$, et on suppose que $y_1 = 1$, ce qui nous donne le système

$$\sigma_i(x_1) + \cdots + \sigma_i(x_r)y_r = 0, \quad \forall i \in [|1, n|]. \tag{3}$$

On fait alors agir $\sigma \in H$ sur le système, pour obtenir

$$\sigma(\sigma_i(x_1)) + \cdots + \sigma(\sigma_i(x_r))\sigma(y_r) = 0, \quad \forall i \in [|1, n|]$$

et puisque $\tau \mapsto \sigma \circ \tau$ réalise une permutation des éléments de H le dernier système est équivalent à

$$\sigma_i(x_1) + \cdots + \sigma_i(x_r)\sigma(y_r) = 0, \quad \forall i \in [|1, n|]. \tag{4}$$

On réalise alors (3) − (4) ce qui nous donne

$$\sigma_i(x_2)(y_2 - \sigma(y_2)) + \cdots + \sigma_i(x_r)(y_r - \sigma(y_r)) = 0, \quad \forall i \in [|1, n|].$$

On a alors, par minimalité de r, $y_j - \sigma(y_j) = 0$ pour $j \in [|2, r|]$, c'est-à-dire que pour tout $j \in [|2, r|]$, $y_j \in L^H$. L'équation (3) pour $i \in [|1, n|]$ tel que $\sigma_i = \mathrm{id}_L$ devient alors

$$x_1 + x_2y_2 + \cdots + x_ry_r = 0$$

ce qui nous fournit une absurdité, par hypothèse sur $(x_1, \dots, x_{n+1})$ puisque $y_j \in L^H$. □

Corollaire 3. *Soit L un corps et soit H un sous-groupe fini du groupe des automorphismes de L. Alors H est le groupe des L^H-automorphismes de L, c'est-à-dire* $\mathrm{Gal}(L/L^H) = H$.

Démonstration. On note $G = \mathrm{Gal}(L/L^H)$. On a immédiatement $H \subset G$. Montrons que G est fini. Soient $a_1, \dots, a_n$ une L^H-base de L, m_i les polynômes minimaux sur L^H respectifs des a_i, et $f = m_1 \cdots m_n$. On note R l'ensemble des racines de f dans L. R contient évidemment $\{a_1, \dots, a_n\}$, et donc puisqu'ils constituent une L^H-base de L, $\sigma \in G$ est entièrement déterminé par ses valeurs sur R. Ainsi, l'application

$$\begin{array}{ccc} G & \to & \mathfrak{S}(R) \\ \sigma & \mapsto & \sigma_{|R} \end{array}$$

est injective, et donc puisque R étant fini, $\mathfrak{S}(R)$ est fini, G est fini.

Or on a les inclusions $L^H \subset L^G \subset L$ par définition de G, et $L^G \subset L^H \subset L$ car $H \subset G$. Ainsi $L^G = L^H$, et le théorème précédent appliqué à G et H nous donne

$$|G| = [L : L^G] = [L : L^H] = |H|$$

et donc $G = H$. □

Ce théorème s'inscrit dans la théorie de Galois, dont nous donnons quelques éléments afin de mettre en contexte le sujet.

Définition 4. On rappelle que si L/K est une extension de corps, on note $\mathrm{Gal}(L/K)$ l'ensemble des K-automorphismes de L, c'est-à-dire

$$\mathrm{Gal}(L/K) = \big\{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{id}_K \big\}.$$

Étant donné une extension L/K, on note $\mathcal{F}$ l'ensemble des corps intermédiaires de L/K et $\mathcal{H}$ l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$. Pour $H \in \mathcal{H}$, on note $\mathrm{Inv}(H)$ le sous-corps fixe de L par H l'ensemble

$$\mathrm{Inv}(H) = \big\{x \in L \mid \forall \sigma \in H, \sigma(x) = x\big\}.$$

On vérifie que $\mathrm{Inv}(H)$ est un corps intermédiaire de L/K pour tout $H \in \mathcal{H}$ et que pour tout $F \in \mathcal{F}$, $\mathrm{Gal}(L/F)$ est un sous-groupe de $\mathrm{Gal}(L/K)$. On peut donc considérer les applications

$$\mathrm{Gal} : \begin{array}{ccc} \mathcal{F} & \to & \mathcal{H} \\ F & \mapsto & \mathrm{Gal}(L/F) \end{array}, \qquad \mathrm{Inv} : \begin{array}{ccc} \mathcal{H} & \to & \mathcal{F} \\ H & \mapsto & \mathrm{Inv}(H). \end{array}$$

Définition 5. On dit qu'une extension L/K est galoisienne si elle est algébrique et que $K = \mathrm{Inv}(\mathrm{Gal}(L/K))$.

Le théorème d'Artin permet de montrer un premier théorème qui caractérise les extensions galoisiennes de degré fini.

Théorème 6. *Pour toute extension L/K, les assertions suivantes sont équivalentes*

(i) *L/K est galoisienne de degré fini*

(ii) *L/K est de degré fini, normale et séparable*

(iii) *$\mathrm{Gal}(L/K)$ est fini et $K = \mathrm{Inv}(\mathrm{Gal}(L/K))$.*

Lorsqu'une de ces conditions est vérifiée on a de plus $|\mathrm{Gal}(L/K)| = [L : K]$.

Exemple. (i) Les extension $\mathbb{C}/\mathbb{R}$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont galoisiennes.

(ii) L'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale donc n'est pas galoisienne.

Le théorème permet également d'obtenir la proposition suivante.

Proposition 7 (correspondance de Galois)**.** *Pour toute extension L/K, les deux assertions suivantes sont équivalentes*

(i) L/K *est galoisienne de degré fini*

(ii) L/K *est de degré fini et les applications* Gal *et* Inv *sont des bijections réciproques l'une de l'autre.*

Démonstration (partielle). L'implication $(ii) \Rightarrow (i)$ est évidente. On montre que si on suppose (i), alors $\mathrm{Gal} \circ \mathrm{Inv} = \mathrm{Id}$. D'après le théorème précédent, par hypothèse, $\mathrm{Gal}(L/K)$ est fini, ainsi, tout $H \in \mathcal{H}$ est fini, et on peut donc lui appliquer le corollaire du théorème d'Artin pour obtenir $H = \mathrm{Gal}(L/\mathrm{Inv}(H)) = \mathrm{Gal} \circ \mathrm{Inv}(H)$. □

On donne enfin le théorème central de la théorie de Galois.

Théorème 8 (fondamental de la théorie de Galois)**.** *Soit L/K est extension galoisienne de degré fini. Si F est un corps intermédiaire pour cette extension, alors*

(1) L/F *est une extension galoisienne de degré fini*

(2) $[F : K] = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)]$

(3) les assertions suivantes sont équivalentes

(i) F/K *est normale*

(ii) $\mathrm{Gal}(L/F) \lhd \mathrm{Gal}(L/K)$

(iii) F/K *est galoisienne.*

Remarque. La théorie de Galois a de nombreuses applications, notamment dans l'étude des polygones constructibles, et la résolution des équations par radicaux.

Commentaire : voir aussi les notes de J. Le Borgne sur le sujet.

2.14 Théorème de Sophie Germain

Référence : S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, Cassini, 2007.

Leçons concernées : 120, 121, 126, 142.

Théorème 1. *Soit p premier impair tel que $q = 2p + 1$ soit premier (un tel nombre est dit premier de Sophie Germain). Alors il n'existe pas de triplet (x, y, z) de $\mathbb{Z}$ qui vérifie $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0[p]$.*

Démonstration. On raisonne par l'absurde et on suppose qu'il existe $(x, y, z) \in \mathbb{Z}^3$ tels que $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0[p]$. *Étape 1 :* si $d = \text{pgcd}(x, y, z)$, alors $(x', y', z') = (x/d, y/d, z/d)$ est encore solution du problème, et $\text{pgcd}(x', y', z') = 1$ de sorte qu'on peut supposer $\text{pgcd}(x, y, z) = 1$. D'autre part, si p_0 est un diviseur premier de x et y, alors p_0 divise $x^p + y^p$ et donc divise z^p. Ainsi d'après le lemme d'Euclide p_0 divise z, et donc $p_0 \mid \text{pgcd}(x, y, z) = 1$, ce qui est impossible. On peut appliquer le même raisonnement pour obtenir que x, y et z sont premiers entre-eux deux à deux.

Étape 2 : on montre alors par l'absurde que $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-k-1}y^k$ sont premiers entre eux : soit p_0 un diviseur premier de $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-k-1}y^k$. On a,

$$(y+z)\sum_{k=0}^{p-1}(-z)^{p-k-1}y^k = \sum_{k=0}^{p-1}\left((-z)^{p-k-1}y^{k+1} - (-z)^{p-k}y^k\right) = y^p + z^p = -x^p = (-x)^p \quad (1)$$

et donc p_0^2 divise $y^p + z^p = (-x)^p$ et donc p_0 divise x. D'autre part, puisque $y \equiv -z[p_0]$,

$$\sum_{k=0}^{p-1}(-z)^{p-k-1}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \equiv 0[p_0],$$

c'est-à-dire que $p_0 \mid py^{p-1}$, donc ou bien p_0 divise p, c'est-à-dire que $p_0 = p$ et donc $p \mid x$ ce qui est exclu par hypothèse, ou bien $p_0 \mid y^{p-1}$, et donc $p_0 \mid y$, et ainsi p_0 divise x et y ce qui est impossible. Puisque ($a \wedge b = 1$ et $ab = c^k$) implique que a et b sont des puissances k-èmes [1], alors de (1) on déduit qu'il existe a, α tels que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-k-1}y^k = \alpha^p$. De même, on montre que $x + y = b^p$ et $x + z = c^p$.

Étape 3 : soit maintenant m non divisible par q. Alors par le petit théorème de Fermat, $m^{q-1} \equiv (m^p)^2 \equiv 1[q]$. Ainsi, puisque $\mathbb{Z}/q\mathbb{Z}$ est un corps, $m^p \equiv \pm 1[q]$. On en déduit par l'absurde que q divise au moins un entier parmi x, y, z : en effet si ce n'était pas le cas, par le résultat précédent, on aurait $x^p \equiv \pm 1[q]$, $y^p \equiv \pm 1[q]$, $z^p \equiv \pm 1[q]$ et donc en sommant $0 \equiv -3, -1, 1, 3[q]$ ce qui est impossible car $q \geqslant 5$. Un seul des entiers x, y, z est divisible par q puisqu'ils sont premiers entre-eux, on suppose que c'est x.

1. En effet, si $a = \prod_p p^{\alpha_p}$, $b = \prod_p p^{\beta_p}$, $c = \prod_p p^{\gamma_p}$, alors pour tout p, $\alpha_p + \beta_p = k\gamma_p$, or pour tout p, $\alpha_p\beta_p = 0$, d'où le résultat.

Étape 4 : on sait que $y+z=a^p$, $x+y=b^p$ et $x+z=c^p$, ainsi, $b^p+c^p-a^p=2x\equiv 0[q]$. D'autre part, $x+y\equiv y\equiv b^p[q]$, or q ne divise pas y donc ne divise pas b, ainsi par un résultat précédent, $y\equiv b^p\equiv \pm 1[q]$. De même $z\equiv\pm 1[q]$. Si q ne divise pas a, alors $a^p\equiv\pm 1[q]$ et donc $b^p+c^p-a^p\equiv 0\equiv -3,-1,1,3[q]$ ce qui est impossible. Ainsi $q\mid a$, et donc $y+z=a^p\equiv 0[q]$, et donc

$$\sum_{k=0}^{p-1}(-z)^{p-k-1}y^k\equiv\sum_{k=0}^{p-1}y^{p-1}\equiv py^{p-1}\equiv p(\pm 1)^{p-1}\equiv p[q]$$

ce qui est absurde car d'après un résultat précédent, $\alpha^p\equiv 0,\pm 1[q]$. On a donc trouvé une absurdité, ce qui permet de conclure. □

Remarque. Ce théorème est un cas particulier du théorème de Fermat-Willes.

On conjecture qu'il existe une infinité de nombres premiers de Sophie Germain mais cela n'a pas encore été montré. Les nombres premiers 3,5,11 et 23 sont de Sophie Germain car $7,11,23,47$ sont premiers. En 2001, le plus grand nombre premier de Sophie Germain connu avait 20013 chiffres.

2.15 Théorème de structure des groupes abéliens finis

Référence : G. Peyré, *L'algèbre discrète de la transformée de Fourier*, Ellipses, 2004. [1]

Leçons concernées : 102, 104, 107, 110, *120.*

Lemme 1 (Prolongement des caractères)**.** *Soit G un groupe abélien fini, et soit $H \subset G$ un sous-groupe de G. Alors tout caractère χ de H peut être prolongé en un caractère de G.*

Démonstration. On montre le résultat par récurrence sur $[G : H]$ l'indice de H dans G. Si $[G : H] = 1$ alors $G = H$ et donc le résultat est trivial. Supposons maintenant que $[G : H] > 1$. Alors il existe $x \in G \backslash H$. On considère donc $K =< x, H >$. On note n le plus petit entier naturel non nul tel que $x^n \in H$, c'est-à-dire l'ordre de xH dans G/H, alors tout élément $z \in K$ s'écrit de façon unique $z = yx^k$ avec $y \in H$ et $k \in [|0, n-1|]$. En effet, l'existence d'une telle écriture est claire par définition de K et de n, et si $yx^k = y'x^{k'}$ avec $y, y' \in H$ et $0 \leqslant k \leqslant k' \leqslant n-1$, alors $x^{k-k'} = y'y^{-1} \in H$ et donc $k = k'$ par minimalité de n.

Soit alors $\chi \in \widehat{H}$, que l'on cherche à prolonger à K. On procède par analyse synthèse.

Analyse : soit $\widetilde{\chi} \in \widehat{K}$ un tel prolongement. On note $\zeta = \widetilde{\chi}(x)$, qui vérifie alors $\zeta^n = \widetilde{\chi}(x)^n = \widetilde{\chi}(x^n) = \chi(x^n)$. Ainsi, ζ est une racine n-ème de $\chi(x^n)$. Le prolongement $\widetilde{\chi}$ est ainsi défini par :

$$\widetilde{\chi}(yx^k) = \chi(y)\zeta^k.$$

Synthèse : soit ζ un racine n-ème de $\chi(x^n)$ et $\widetilde{\chi}$ défini comme précédemment. Il nous suffit alors de montrer que $\widetilde{\chi}$ est bien un morphisme de groupes. Soit $z = yx^k$ et $z' = y'x^{k'}$ deux éléments de K. On distingue alors deux cas :

- si $0 \leqslant k + k' \leqslant n-1$, alors

$$\widetilde{\chi}(zz') = \widetilde{\chi}(yy'x^{k+k'}) = \chi(yy')\zeta^{k+k'} = \chi(y)\zeta^k\chi(y')\zeta^{k'} = \widetilde{\chi}(z)\widetilde{\chi}(z')$$

- si $n \leqslant k + k' \leqslant 2n-1$, alors

$$\widetilde{\chi}(zz') = \widetilde{\chi}(yy'x^nx^{k+k-n'}) = \chi(y)\chi(y')\chi(x^n)\zeta^{k+k'-n} = \widetilde{\chi}(z)\widetilde{\chi}(z')$$

car $\chi(x^n) = \zeta^n$.

On a ainsi prolongé χ à K. Or, par multiplicativité des degrés, $[G : H] = [G : K][K : H]$ et donc puisque $[K : H] > 1$, $[G : K] < [G : H]$ et on peut appliquer l'hypothèse de récurrence et prolonger $\widetilde{\chi}$ à G, ce qui termine la preuve. □

1. Il n'y a que le lemme dedans, le reste étant inspiré de développements rédigés.

Théorème 2 (Structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini. Alors il existe $r \in \mathbb{N}^*$ et $n_1, \dots, n_r \in \mathbb{N}^*$ tels que $n_r \mid \cdots \mid n_1$ et*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

En particulier, $|G| = n_1 \cdots n_r$ et l'exposant de G est n_1.

Démonstration. On montre le résultat par récurrence sur $|G|$: si $|G| = 2$, alors $G \cong \mathbb{Z}/2\mathbb{Z}$ et le résultat est démontré. On suppose maintenant $|G| = n \geqslant 3$. On note n_1 l'exposant de G, et soit $x \in G$ d'ordre n_1 (qui existe car G est abélien). On considère $H =< x > \cong \mathbb{Z}/n_1\mathbb{Z} \cong \mathbb{U}_{n_1}$. Si $H = G$ alors le résultat est démontré, on suppose donc maintenant H différent de G. On note χ l'isomorphisme $H \cong \mathbb{U}_{n_1}$, qui est donc un caractère de H. On le prolonge par le lemme précédent à un caractère $\widetilde{\chi}$ de G. Par définition de l'exposant, pour tout $g \in G$, $g^{n_1} = 1$ et donc $\widetilde{\chi}$ est à valeurs dans $\mathbb{U}_{n_1}$, on peut donc considérer le morphisme de groupes suivant :

$$\varphi : \begin{array}{ccc} G & \to & H \times G/H \\ g & \mapsto & \left(\chi^{-1} \circ \widetilde{\chi}(g), gH\right) \end{array}$$

qui est un isomorphisme. En effet, si $g \in \ker(\varphi)$, alors $gH = H$ et donc $g \in H$, ainsi $1 = \chi^{-1} \circ \chi(g) = g$ et donc $g = 1$, c'est-à-dire que φ est injectif. Par cardinalité on conclut que φ est bijectif. On peut alors appliquer l'hypothèse de récurrence à G/H abélien fini d'ordre $|G/H| = |G|/n_1 < |G|$ pour obtenir $r \in \mathbb{N}^*$ et $n_2, \dots, n_r \in \mathbb{N}^*$ tels que $n_r \mid \cdots \mid n_2$ et

$$G/H \cong \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

ce qui nous donne l'isomorphisme recherché. Il nous reste à vérifier que $n_2 \mid n_1$, ce qui s'obtient grâce au fait que $(0, 1, 0, \dots, 0) \in \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ est d'ordre n_2 qui divise donc l'exposant du groupe n_1. □

Définition 3. L'exposant d'un groupe fini G est le plus petit entier n tel que $g^n = 1$ pour tout $g \in G$.

Proposition 4. *L'exposant d'un groupe abélien G est $N = \mathrm{ppcm}\{o(g), g \in G\}$ et il existe un élément d'ordre N dans G.*

Démonstration. On montre que pour tout x, y dans G d'ordre n, m, il existe un élément z de G d'ordre $\mathrm{ppcm}(n, m)$, ce qui montre la proposition à l'aide d'une récurrence immédiate.

On montre d'abord le résultat dans le cas où m et n sont premiers entre-eux. Il est clair que $(xy)^{nm} = 1$. D'autre part, si $(xy)^r = x^r y^r = 1$, alors en particulier, $x^{rm} y^{rm} = x^{rm} = 1$ ainsi n l'ordre de x divise rm et donc divise r car $m \wedge n = 1$. De même $m \mid r$ et ainsi $z = xy$ est d'ordre $mn = \mathrm{ppcm}(m, n)$.

Dans le cas général, on note

$$k = \prod_{\nu_p(n) \geqslant \nu_p(m)} p^{\nu_p(n)} \quad \text{et} \quad l = \prod_{\nu_p(m) > \nu_p(n)} p^{\nu_p(m)}.$$

On remarque alors que k et l sont premiers entre-eux, et que

$$kl = \prod_{\nu_p(n) \geqslant \nu_p(m)} p^{\nu_p(n)} \prod_{\nu_p(m) > \nu_p(n)} p^{\nu_p(m)} = \prod p^{\max(\nu_p(n), \nu_p(m))} = \text{ppcm}(n, m).$$

Or $k \mid n$ et $l \mid m$, donc $x' = x^{n/k}$ est d'ordre k et $y' = y^{m/l}$ est d'ordre l, et donc par le premier cas considéré, $z = x'y'$ est d'ordre $kl = \text{ppcm}(m, n)$. □

2.16 Théorème des deux carrés

Référence : D. Perrin, *Cours d'Algèbre*, Ellispes, 1996.

Leçons concernées : 120, 121, 122, 126.

On introduit $\mathbb{Z}[i] := \{a + ib, a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss et on pose $\Sigma := \{n \in \mathbb{N}^* \mid n = a^2 + b^2,\ a, b \in \mathbb{N}\}$. On pose également

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ z = a + ib & \mapsto & z\overline{z} = a^2 + b^2 \end{array}$$

où, pour $z = a + ib \in \mathbb{Z}[i]$, $\overline{z} = a - ib$.

Proposition 1. *Les inversibles de $\mathbb{Z}[i]$ sont $\{\pm 1, \pm i\}$, de sorte que $z \in \mathbb{Z}[i]^* \Leftrightarrow N(z) = 1$*

Démonstration. Il est clair que ces éléments sont inversibles, réciproquement, si $z = a+ib$ est inversible, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$, et donc $N(zz') = N(z)N(z') = N(1) = 1$ dans $\mathbb{N}$, donc $N(z) = N(z') = 1$. On a donc $a^2 + b^2 = 1$, donc ($a = \pm 1$ et $b = 0$) ou ($a = 0$ et $b = \pm 1$) ce qui nous fournit les quatre éléments annoncés. □

Théorème 2. *On a, pour p premier,*

(i) $\mathbb{Z}[i]$ est euclidien, donc principal.

(ii) $p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i] \Leftrightarrow p = 2$ ou $p \equiv 1 \mod 4$.

Démonstration. Pour la preuve du point (i), on montre que $\mathbb{Z}[i]$ est euclidien relativement à N. Soit $z, t \in \mathbb{Z}[i]\backslash\{0\}$, on considère $z/t = x + iy \in \mathbb{C}$, et on prend $q = a + ib$ avec $a, b \in \mathbb{Z}$ tels que a et b soient les entiers les plus proches de x et y, ainsi, $|x-a| \leqslant 1/2$ et $|y-b| \leqslant 1/2$ et donc $|z/t - q| \leqslant \sqrt{2}/2 < 1$ (c'est plus clair sur un dessin) d'où $|z - tq| < |t|$. Si on pose $r := z - tq$, on a $z = tq + r$ dans $\mathbb{Z}[i]$ et en passant au carré dans $|r| < |t|$, on obtient $N(r) < N(t)$.

On montre alors la première équivalence du point (ii) : pour le sens direct, si $p = a^2 + b^2$, alors $p = (a + ib)(a - ib)$ dans $\mathbb{Z}[i]$ et puisque a et b sont non nuls, $a + ib$ et $a - ib$ ne sont pas inversibles dans $\mathbb{Z}[i]$ et donc p n'est pas irréductible.

Réciproquement, si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^*$, $N(p) = p^2 = N(z)N(z')$ et puisque p est premier et $N(z), N(z') \neq 1$, $N(z) = N(z') = p$ et donc $p \in \Sigma$.

On montre maintenant la seconde équivalence. Puisque $\mathbb{Z}[i]$ est principal donc factoriel, p est irréductible dans $\mathbb{Z}[i]$ si et seulement si l'idéal $(p) = p\mathbb{Z}[i]$ est premier. On utilise alors les isomorphismes suivants : on sait que $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1)$. D'autre part,

$$(\mathbb{Z}[X]/(X^2 + 1))/(p) \cong \mathbb{Z}[X]/(p, X^2 + 1) \cong (\mathbb{Z}[X]/(p))/(X^2 + 1) \cong (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1)$$

d'après le troisième théorème d'isomorphisme. On obtient que (p) est premier dans $\mathbb{Z}[i]$ si et seulement si (X^2+1) est premier dans $\mathbb{F}_p[X]$, or (X^2+1) est premier dans $\mathbb{F}_p[X]$ si et seulement si (X^2+1) n'a pas de racine dans $\mathbb{F}_p[X]$ si et seulement si -1 n'est pas un carré modulo p. Or cette dernière condition est caractérisée par $p \equiv 3 \mod 4$, ce qui achève la démonstration du théorème. □

On peut maintenant conclure sur l'ensemble Σ :

Proposition 3. *On a $n \in \Sigma$ si et seulement si pour tout p premier tel que $p \equiv 3 \mod 4$, $\nu_p(n)$ est pair.*

Démonstration. On sait que $n \in \Sigma$ si et seulement si $\exists z \in \mathbb{Z}[i]$ tel que $n = N(z)$, et donc par multiplicativité de N on obtient la fait que Σ est stable par multiplication. Le sens réciproque s'obtient alors facilement avec le théorème 2.

Réciproquement, soit $p \equiv 3 \mod 4$. On montre par récurrence sur $k \in \mathbb{N}$ que pour tout $n \in \Sigma$ tel que $\nu_p(n) \leqslant k$, $\nu_p(n)$ est pair. Si $k = 0$, c'est clair. Sinon, soit $n \in \Sigma$ tel que $\nu_p(n) \leqslant k \in \mathbb{N}^*$. Si $\nu_p(n) = 0$ le résultat est clair, sinon $p \mid n = a^2 + b^2 = (a+ib)(a-ib)$, or p est irréductible dans $\mathbb{Z}[i]$ principal, donc $p \mid (a+ib)$ ou $p \mid (a-ib)$, disons que $p \mid (a+ib)$. Alors $p \mid a$ et $p \mid b$, ainsi $a = pa'$ et $b = pb'$, donc $n = p^2(a'^2 + b'^2)$ et donc $\frac{n}{p^2} \in \Sigma$. Or $\nu_p(\frac{n}{p^2}) = \nu_p(n) - 2$ et $\nu_p(\frac{n}{p^2})$ est pair par hypothèse de récurrence, donc $\nu_p(n)$ aussi, ce qui conclut la preuve. □

On montre maintenant la série d'isomorphismes donnée à la fin de la preuve du théorème.

Théorème 4 (Troisième théorème d'isomorphisme)**.** *Soit A un anneau, et soit I, J deux idéaux de A tels que $I \subset J$. Alors en tant qu'anneaux,*

$$(A/I)/(J/I) \cong A/J.$$

Démonstration. On note $\pi : A \to A/I$ le morphisme surjectif canonique. Puisque $I \subset J$, $\pi(J) = J/I$ et est un idéal de A/I. D'autre part, puisque $I \subset J$, on peut factoriser $\pi_2 : A \to A/J$ par I et obtenir le morphisme surjectif $\varphi : A/I \to A/J$, dont le noyau est exactement J/I, et donc par le premier théorème d'isomorphisme, $(A/I)/(J/I) \cong A/J$. □

On peut alors montrer :

Proposition 5. *Pour p premier on a*

$$(\mathbb{Z}[X]/(X^2+1))/(p) \cong \mathbb{Z}[X]/(p, X^2+1) \cong (\mathbb{Z}[X]/(p))/(X^2+1) \cong (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1).$$

Démonstration. On montre par exemple $\mathbb{Z}[X]/(X^2+1))/(p) \cong \mathbb{Z}[X]/(p, X^2+1)$ grâce au premier théorème d'isomorphisme appliqué à $A = \mathbb{Z}[X]$, $J = (p, X^2+1)$ et $I = (X^2+1)$ en remarquant que $(p, X^2+1)/(X^2+1) = (p)$. Le dernier isomorphisme s'obtient facilement avec le premier théorème d'isomorphisme. □

Remarque : on peut ne pas faire la première proposition sur la détermination des inversibles, et ne faire la proposition 3 que si il reste du temps. La partie sur le troisième théorème d'isomorphisme sert à se préparer à une éventuelle question sur ce point.

2.17 Un anneau principal non euclidien

Référence : D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

Leçons concernées : 122.

On cherche à montrer qu'un certain anneau est principal mais non euclidien. Pour cela on commence par énoncer une condition nécessaire lorsqu'un anneau A est euclidien.

Proposition 1. *Soit A un anneau euclidien pour le stathme v. Alors il existe $x \in A$ non inversible tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique $A \to A/(x)$ soit surjective.*

Démonstration. Si A est un corps $x = 0$ convient. Sinon on choisit $x \in A$ non nul non inversible tel que $v(x)$ soit minimal (c'est possible puisque $v : A \to \mathbb{N}$). Si $a \in A$, alors $a = xq + r$ avec $r = 0$ ou $v(r) < v(x)$, ainsi $a + (x) = r + (x)$. Si $r \neq 0$, alors puisque $v(r) < v(x)$, r est inversible. Ainsi, $a + (x) = r + (x)$ où $r \in A^\times \cup \{0\}$, d'où le résultat. □

Proposition 2. *L'anneau $A = \mathbb{Z}\left[\dfrac{1 + i\sqrt{19}}{2}\right]$ n'est pas euclidien.*

Démonstration. Étape 1 : on pose $\alpha = \frac{1+i\sqrt{19}}{2}$ qui est racine de $X^2 - X + 5$ puisque $\overline{\alpha} = \frac{1-i\sqrt{19}}{2}$ et donc $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$. On a alors

$$A = \mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$$

qui est intègre comme sous-anneau de $\mathbb{C}$. Avec $\overline{\alpha} = 1 - \alpha$ on sait que A est stable par conjugaison et on considère alors, pour $z = a + b\alpha$, $N(z) = z\overline{z} = a^2 + ab + 5b^2 \in \mathbb{N}$. On remarque que $N(zz') = N(z)N(z')$ et $N(z) > 0$ si $z \neq 0$.

Étape 2 : on détermine alors $A^\times$ le groupe des inversibles de A. Soit $z \in A^\times$, alors $N(zz^{-1}) = N(1) = 1 = N(z)N(z^{-1})$ et donc puisque N est à valeurs dans N, $N(z) = 1$. Ainsi, si $z = a + b\alpha$, $a^2 + ab + 5b^2 = 1$. Or

$$a^2 + ab + b^2 \geqslant a^2 + b^2 - |ab| \geqslant (|a| - |b|)^2 \geqslant 0$$

et donc $1 = a^2 + ab + 5b^2 \geqslant 4b^2$, ainsi $b = 0$ et donc $a = \pm 1$. On conclut que $A^\times = \{-1, 1\}$.

Étape 3 : on suppose enfin par l'absurde que A est euclidien. D'après la proposition précédente, il existe $x \in A$ tel que $A/(x)$ soit un corps à 2 ou 3 éléments. On a alors l'existence d'un morphisme d'anneaux $\varphi : \mathbb{Z}[\alpha] \to k$ où $k = \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. On remarque qu'alors φ restreint à $\mathbb{Z}$ est la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. On pose $\beta = \varphi(\alpha)$ qui est racine de $X^2 - X + 5$ dans k par propriété de morphisme d'anneaux de φ. Or, $X^2 - X + 5 = X^2 + X + 1$ dans $\mathbb{Z}/2\mathbb{Z}$ qui n'a pas de racines et $X^2 - X + 5 = X^2 - X - 1$ dans $\mathbb{Z}/3\mathbb{Z}$ qui n'admet pas non plus de racines : on a trouvé une absurdité. □

On montre maintenant que A est principal au moyen du lemme suivant.

Lemme 3. *Soient $a, b \in A\backslash\{0\}$, alors il existe $q, r \in A$ tels que :*

(i) $r = 0$ *ou* $N(r) < N(b)$

(ii) $a = bq + r$ *ou* $2a = bq + r$

Démonstration. On considère $x = \frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} \in \mathbb{C}$ que l'on écrit $x = u + v\alpha$ avec $u, v \in \mathbb{Q}$. On note $n = \lfloor v \rfloor$.

1) Si $v \notin]n + \frac{1}{3}, n + \frac{2}{3}[$, on pose s, t les entiers les plus proches de u et v respectivement. On a alors $|s - u| \leqslant \frac{1}{2}$, $|t - v| \leqslant \frac{1}{3}$. On pose $q = s + t\alpha \in A$ et on a

$$N(x - q) = (s - u)^2 + (s - u)(t - v) + 5(t - v)^2 \leqslant \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1$$

et donc $r = a - bq = b(x - q)$ convient.

2) Sinon, on a $2x = 2u + 2v\alpha$, et $2v \in]2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}[$ et ainsi si $m = \lfloor 2v \rfloor$, $2v \notin]m + \frac{1}{3}, m + \frac{2}{3}[$ et on conclut avec le cas précédent.

□

Proposition 4. *L'anneau A est principal.*

Démonstration. On montre d'abord que l'idéal (2) est maximal dans A. En effet on a par division euclidienne,

$$A \cong \mathbb{Z}[T]/(T^2 - T + 5)$$

et ainsi [1]

$$A/(2) \cong \mathbb{Z}[T]/(2, T^2 - T + 5) \cong \mathbb{Z}/2\mathbb{Z}[T]/(T^2 + T + 1)$$

et ce dernier est un corps puisque $T^2 + T + 1$ est irréductible sur $\mathbb{F}_2$.

Soit maintenant I un idéal non nul de A et $a \in I$ non nul tel que $N(a)$ soit minimal. Si $I = (a)$ on a terminé, sinon soit $x \in I\backslash(a)$. On applique alors le lemme précédent à x et a.

(i) Ou bien $x = aq + r$ avec $r = 0$ ou $N(r) < N(a)$, or $r \in I$, donc $r = 0$, ainsi $x \in (a)$, c'est impossible.

(ii) Ou bien $2x = aq + r$ avec $r = 0$ ou $N(r) < N(a)$ et de même $r = 0$ donc $2x = aq$. On a alors $aq \in (2)$ maximal donc premier, ainsi $a \in (2)$ ou $q \in (2)$. Si $q \in (2)$, alors $q = 2q'$ et donc $x = aq' \in (a)$ ce qui est impossible. Ainsi $a \in (2)$ et $q \notin (2)$, et donc $a = 2a'$ et $x = a'q$. Puisque (2) est maximal et ne contient pas q, $(2, q) = A$ et donc $1 = 2\lambda + q\mu$ avec $\lambda, \mu \in A$ et ainsi $a' = 2\lambda a' + \mu q a' = \lambda a + \mu x \in I$ car $a, x \in I$. On obtient une absurdité par minimalité de a.

□

Commentaire : c'est sûrement trop long : admettre le lemme, qui est technique et assez classique.

1. Une justification d'un résultat analogue est faite dans le développement "Théorème des deux carrés".

3 Développements d'analyse et de probabilités

3.1 Densité des polynômes orthogonaux

Références : V. Beck, J. Malick, G. Peyré, *Objectif Agrégation*, H & K, 2005,
S.D. Chatterji, *Cours d'analyse 3 : équations différentielles ordinaires et aux dérivées partielles*, Presses polytechniques et universitaires romandes, 1995.

Leçons concernées : 201, 202, 207, 209, 213, 234, 239, 245, 250.

Définition 1. Soit I un intervalle de $\mathbb{R}$. On considère ρ une fonction poids sur I, c'est-à-dire une fonction $\rho : I \to \mathbb{R}_+^*$ vérifiant

$$\forall n \in \mathbb{N}, \quad \int_I |x|^n \rho(x)\, dx < +\infty.$$

On note alors

$$L^2(I,\rho) = \left\{ f : I \to \mathbb{R} \mid \int_I |f(x)|^2 \rho(x)\, dx < +\infty \right\}$$

que l'on munit du produit scalaire

$$< f, g >= \int_I f(x)\overline{g(x)}\rho(x)\, dx$$

qui en fait un espace de Hilbert. On note alors $(P_n)_n$ l'unique suite de polynômes orthogonaux pour ce produit scalaire, échelonnée en degré.

Théorème 2. *On suppose qu'il existe $a > 0$ tel que*

$$\int_I e^{a|x|} \rho(x)\, dx < +\infty.$$

Alors $(P_n)_n$ est une base hilbertienne de $L^2(I,\rho)$.

Démonstration. On cherche à montrer que la suite $(P_n)_n$ est totale dans $L^2(I,\rho)$. On utilise pour cela le critère de densité valable dans les espaces de Hilbert, et on montre que $\big(\mathrm{Vect}(P_n, n \in N)\big)^\perp = \big(\mathrm{Vect}(x \mapsto x^n, n \in N)\big)^\perp = \{0\}$. On considère donc $f \in \big(\mathrm{Vect}(x \mapsto x^n, n \in N)\big)^\perp$.

Étape 1 : prolongement de la transformée de Fourier d'une fonction. On pose

$$\varphi(x) = \begin{cases} f(x)\rho(x) & \text{si } x \in I \\ 0 & \text{sinon.} \end{cases}$$

On remarque que $\varphi \in L^1(\mathbb{R})$ puisque pour $x \in I$, $|f(x)|\rho(x) \leqslant \frac{1}{2}(1 + |f(x)|^2)\rho(x) \in L^1(I)$, ce qui nous permet de considérer

$$\widehat{\varphi}(\xi) = \int_I f(x) e^{-i\xi x} \rho(x)\, dx$$

la transformée de Fourier de φ. On pose alors, pour $z \in B_a = \{z \in \mathbb{C} \mid |\Im(z)| < a/2\}$,

$$F(z) = \int_I e^{-izx} f(x)\rho(x)\,dx$$

qui est bien défini puisque pour $z \in B_a$,

$$\begin{aligned}\int_I |e^{-izx}||f(x)|\rho(x)\,dx &\leqslant \int_I e^{|x|a/2}|f(x)|\rho(x)\,dx \\ &\leqslant \left(\int_I e^{|x|a}\rho(x)\,dx\right)^{1/2}\left(\int_I |f(x)|^2\rho(x)\,dx\right)^{1/2} < +\infty\end{aligned}$$

par inégalité de Cauchy-Schwarz.

Étape 2 : F est holomorphe sur B_a. On applique le théorème d'holomorphie sous l'intégrale à la fonction $F(z) = \int_I g(x,z)\,dx$ où $g(x,z) = e^{-izx}f(x)\rho(x)$ pour $x \in I$ et $z \in B_a$. On a,

(i) pour tout $z \in B_a$, $x \mapsto g(x,z)$ est mesurable sur I,

(ii) pour tout $x \in I$, $z \mapsto g(x,z)$ est holomorphe sur l'ouvert B_a,

(iii) pour tout $x \in I$ et $z \in B_a$,

$$|g(x,z)| \leqslant h(x) = e^{|x|a/2}|f(x)|\rho(x)$$

et $h \in L^1(I)$.

Ainsi, F est holomorphe sur B_a.

Étape 3 : calcul des dérivées de F en 0. D'après le théorème d'holomorphie sous l'intégrale, pour $n \in \mathbb{N}$, et pour $z \in B_a$,

$$F^{(n)}(z) = \int_I (-i)^n x^n e^{-izx} f(x)\rho(x)\,dx$$

et donc $F^{(n)}(0) = (-i)^n \int_I x^n f(x)\rho(x)\,dx = (-i)^n < f, x \mapsto x^n >= 0$ par hypothèse sur f. Ainsi par unicité du développement en série entière d'une fonction holomorphe, F est nulle sur un voisinage de 0. Par le principe des zéros isolés, puisque B_a est connexe, F est nulle sur B_a, et donc, puisque $F = \widehat{\varphi}$ sur $\mathbb{R}$, $\widehat{\varphi}$ est nulle. Par injectivité de la transformée de Fourier sur L^1, φ est alors nulle sur $\mathbb{R}$, et donc finalement f est nulle sur I. □

Remarque. Il existe des fonctions poids dont les polynômes orthogonaux associés ne forment pas une base hilbertienne de $L^2(I,\rho)$, par exemple, pour la fonction poids $\rho(x) = x^{-\log(x)}$ sur $I =]0, +\infty[$, la fonction $f(x) = \sin(2\pi \log(x))$ est orthogonale à tous les polynômes, voir la référence pour plus de détails.

Exemple. On considère la fonction poids sur $I = \mathbb{R}$, $\rho(x) = e^{-x^2}$. Les polynômes orthogonaux associés sont appelés polynômes de Hermite. Les premiers polynômes de Hermite sont les suivants :

$$P_0 = 1, \quad P_1 = X, \quad P_2 = X^2 - \frac{1}{2}, \quad P_3 = X^3 - \frac{3}{2}X \text{ et } \quad P_4 = X^4 - 3X^2 + \frac{3}{4}.$$

On dispose d'une formule explicite [1] pour ces polynômes, en les imposant unitaires :

$$P_n(x) = \frac{(-1)^n}{2^n} e^{x^2} \frac{d^n}{dx^n}\Big(e^{-x^2}\Big).$$

Démonstration. On commence par montrer par récurrence que pour tout $n \in \mathbb{N}$, P_n est un polynôme unitaire de degré n. En effet le résultat est évident pour $n = 0$, et si il est vrai pour un certain $n \in \mathbb{N}$, alors

$$\begin{aligned} P_{n+1}(x) &= \frac{(-1)^{n+1}}{2^{n+1}} e^{x^2} \frac{d}{dx}\Big(\frac{d^n}{dx^n}\Big(e^{-x^2}\Big)\Big) = \frac{(-1)^{n+1}}{2^{n+1}} e^{x^2} \frac{d}{dx}\Big(\frac{2^n}{(-1)^n} e^{-x^2} P_n(x)\Big) \\ &= -\frac{1}{2} e^{x^2}\Big(-2x e^{-x^2} P_n(x) + e^{-x^2} \frac{d}{dx}\big(P_n(x)\big)\Big) = x P_n(x) - \frac{1}{2}\frac{d}{dx}\big(P_n(x)\big) \end{aligned}$$

et on obtient le résultat par hypothèse de récurrence. On montre alors que pour $m, n \in \mathbb{N}$, $< P_m, P_n >= \frac{\sqrt{\pi}\, n!}{2^n}\, \delta_n^m$. On écrit, en supposant que $m \leqslant n$,

$$\begin{aligned} < P_m, P_n > &= \int_{\mathbb{R}} P_m(x) P_n(x) e^{-x^2}\, dx = \frac{(-1)^n}{2^n} \int_{\mathbb{R}} P_m(x) \frac{d^n}{dx^n}\Big(e^{-x^2}\Big)\, dx \\ &= \frac{(-1)^{n+m}}{2^n} \int_{\mathbb{R}} \frac{d^m}{dx^m}\Big(P_m(x)\Big) \frac{d^{n-m}}{dx^{n-m}}\Big(e^{-x^2}\Big)\, dx \end{aligned}$$

grâce à m intégrations par parties. Maintenant, si $m = n$, on obtient le résultat puisque P_n est unitaire de degré m et que $\int_{\mathbb{R}} e^{-x^2}\, dx = \sqrt{\pi}$. D'autre part, si $m < n$, une autre intégration par partie nous donne $< P_m, P_n >= 0$ puisque P_m est un polynôme de degré m. □

On remarque que la fonction poids ρ vérifie les hypothèse du théorème précédent pour tout $a > 0$, et donc les polynômes de Hermite forment une base hilbertienne de $L^2(\mathbb{R}, \rho)$. Or les applications

$$\begin{array}{ccc} L^2(\mathbb{R}, \rho) & \to & L^2(\mathbb{R}) \\ f & \mapsto & f\sqrt{\rho} \\ g/\sqrt{\rho} & \leftarrow\!\shortmid & g \end{array}$$

sont des isométries bijectives réciproques l'une de l'autre. Ainsi $(P_n e^{-x^2/2})_n$ est, à renormalisation près, une base hilbertienne de $L^2(\mathbb{R})$ qui s'écrit explicitement

$$\frac{(-1)^n}{2^n} e^{x^2/2} \frac{d^n}{dx^n}\Big(e^{-x^2}\Big).$$

1. On a une formule plus explicite que cela pour ces polynômes, mais elle demande plus de travail, voir la référence.

3.2 Développement asymptotique de la série harmonique

Référence : S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, oraux X-ENS - Analyse 1*, Cassini, 2007.

Leçons concernées : 224, 230.

Théorème 1. *Si on note* $H_n = \sum_{k=1}^{n} \frac{1}{k}$*, alors on a,*

$$H_n = \log(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\Big(\frac{1}{n^2}\Big)$$

où $\gamma = \lim_{n+\infty} H_n - \log(n)$*.*

Démonstration. Étape 1 : on montre que la suite $(u_n)_n = (H_n - \log(n))_n$ est convergente. Pour cela on introduit $v_n := u_n - \frac{1}{n}$ et on montre que $(u_n)_n$ et $(v_n)_n$ sont adjacentes. En effet la différence $u_n - v_n = \frac{1}{n}$ est positive et tend vers 0. D'autre part,

$$u_n - u_{n+1} = \log(n+1) - \log(n) - \frac{1}{n+1} = -\frac{1}{n+1} - \log\Big(1 - \frac{1}{n+1}\Big) \geqslant 0$$

puisque $\log(1+x) \leqslant x$ pour tout $x > -1$ par concavité du logarithme. Par la même inégalité on obtient enfin

$$v_{n+1} - v_n = u_{n+1} - u_n - \frac{1}{n+1} + \frac{1}{n} = \log(n) - \log(n+1) + \frac{1}{n} = \frac{1}{n} - \log\Big(1 + \frac{1}{n}\Big) \geqslant 0.$$

Ainsi les suites $(u_n)_n$ et $(v_n)_n$ sont adjacentes et convergent donc vers une même limite γ.

Étape 2 : on a ainsi montré que $H_n = \log(n) + \gamma + o(1)$. On note alors $t_n = H_n - \log(n) - \gamma$ et on cherche un équivalent de t_n. On remarque que

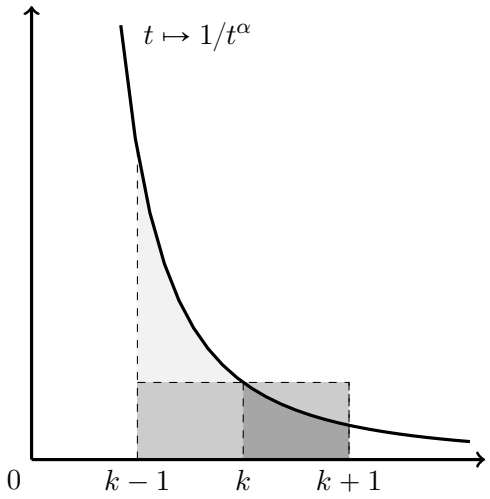
$$t_n - t_{n-1} = \frac{1}{n} + \log\Big(1 - \frac{1}{n}\Big) \sim -\frac{1}{2n^2}$$

et donc, puisque $(t_n)_n$ tend vers 0, on a par sommation des équivalents

$$\sum_{k=n+1}^{+\infty} (t_k - t_{k-1}) = -t_n \sim -\frac{1}{2} \sum_{k=n+1}^{+\infty} \frac{1}{k^2} \sim -\frac{1}{2n}.$$

Le dernier équivalent s'obtient de la manière suivante : si $\alpha > 1$, la décroissance de $t \mapsto \frac{1}{t^\alpha}$ sur $]0, +\infty[$ nous donne

$$\int_k^{k+1} \frac{1}{t^\alpha}\, dt \leqslant \frac{1}{k^\alpha} \leqslant \int_{k-1}^{k} \frac{1}{t^\alpha}\, dt$$



et donc

$$\frac{1}{\alpha-1}\frac{1}{(n+1)^{\alpha-1}} = \int_{n+1}^{+\infty} \frac{1}{t^\alpha}\,dt \leqslant \sum_{k=n+1}^{+\infty} \frac{1}{k^\alpha} \leqslant \int_{n}^{+\infty} \frac{1}{t\alpha}\,dt = \frac{1}{\alpha-1}\frac{1}{n^{\alpha-1}}$$

et alors $\displaystyle\sum_{k=n+1}^{+\infty} \frac{1}{k^\alpha} \sim \frac{1}{\alpha-1}\frac{1}{n^{\alpha-1}}$. Ainsi, on a $H_n = \log(n) + \gamma + \frac{1}{2n} + o\big(\frac{1}{n}\big)$.

Étape 3 : on précise encore le développement asymptotique : on note $w_n = t_n - \frac{1}{2n}$. On a alors

$$\begin{aligned} w_n - w_{n-1} &= \log\Big(1-\frac{1}{n}\Big) + \frac{1}{n} - \frac{1}{2n} + \frac{1}{2(n-1)} \\ &= -\frac{1}{n} - \frac{1}{2n^2} - \frac{1}{3n^3} + \frac{1}{n} - \frac{1}{2n} + \frac{1}{2n}\frac{1}{1-1/n} + o\Big(\frac{1}{n^3}\Big) \\ &= -\frac{1}{2n^2} - \frac{1}{3n^3} - \frac{1}{2n} + \frac{1}{2n}\Big(1 + \frac{1}{n} + \frac{1}{n^2}\Big) + o\Big(\frac{1}{n^3}\Big) \\ &= \frac{1}{6n^3} + o\Big(\frac{1}{n^3}\Big) \\ &\sim \frac{1}{6n^3} \end{aligned}$$

et donc par sommation des équivalents, puisque $(w_n)_n$ converge vers 0,

$$-w_n \sim \sum_{k=n+1}^{+\infty} \frac{1}{6n^3} \sim \frac{1}{12n^2}$$

et on peut donc conclure que $H_n = \log(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\big(\frac{1}{n^2}\big)$. □

Application 2. *Si on note* $k_n := \min\{k \in \mathbb{N}^* \mid H_k \geqslant n\}$*, alors*

$$\lim_{n\to+\infty} \frac{k_{n+1}}{k_n} = e.$$

Démonstration. On utilise le fait que $H_n = \log(n) + \gamma + \varepsilon_n$ où $(\varepsilon_n)_n$ est une suite qui tend vers 0. On a alors, par définition,

$$\log(k_n) + \gamma + \varepsilon_{k_n} \geqslant n$$

et

$$\log(k_n - 1) + \gamma + \varepsilon_{k_n-1} < n$$

et donc en passant à l'exponentielle,

$$e^n e^{-\gamma-\varepsilon_{k_n}} \leqslant k_n < e^n e^{-\gamma-\varepsilon_{k_n-1}} + 1.$$

Ainsi, $k_n \sim e^n e^{-\gamma}$ et donc en particulier

$$\lim_{n\to+\infty} \frac{k_{n+1}}{k_n} = e.$$

□

3.3 Équation de la chaleur sur le cercle

Références : H. Dym, H.P. McKean, *Fourier series and integrals*, Academic Press, 1972. [1]

Leçons concernées : 202, 209, 222, 235, 241, 246.

Théorème 1. *Il existe une unique solution $u \in \mathcal{C}^\infty(]0,+\infty[\times\mathbb{T})$ à l'équation*

$$\frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 \quad sur \quad]0,+\infty[\times\mathbb{T} \tag{1}$$

avec pour condition initiale

$$\lim_{\substack{t\to 0\\ t>0}} ||u-f||_\infty = \lim_{\substack{t\to 0\\ t>0}} \sup_{x\in\mathbb{T}} |u(t,x)-f(x)| = 0 \tag{2}$$

où $f \in \mathcal{C}^2(\mathbb{T})$.

Démonstration. On raisonne par analyse synthèse.

Analyse : supposons que $u \in \mathcal{C}^2(]0,+\infty[\times\mathbb{T})$ est solution de (1) et (2). Alors pour tout $t>0$, $x \mapsto u(t,x)$ est de classe $\mathcal{C}^1$ sur $\mathbb{T}$ et donc on peut écrire, avec convergence normale de la série en x,

$$\forall t>0, \forall x\in\mathbb{T}, \quad u(t,x) = \sum_{n\in\mathbb{Z}} c_n(t)e_n(x)$$

où $e_n : x \mapsto e^{inx}$ et où

$$\forall t>0, \forall n\in\mathbb{Z}, \quad c_n(t) = \frac{1}{2\pi}\int_0^{2\pi} u(t,x)e^{-inx}dx.$$

Pour $n \in \mathbb{Z}$, on cherche alors à déterminer c_n. On applique le théorème de dérivation sous l'intégrale sur tout compact de $]0,+\infty[$ puisque $[0,2\pi]$ est un compact et que $\frac{\partial u}{\partial t}$ est continue sur $]0,+\infty[\times\mathbb{T}$. On obtient alors $c_n \in \mathcal{C}^1(]0,+\infty[)$ et $\forall t>0$,

$$\begin{aligned}
c_n'(t) &= \frac{1}{2\pi}\int_0^{2\pi} \frac{\partial u}{\partial t}(t,x)e^{-inx}dx = \frac{1}{2\pi}\int_0^{2\pi} \frac{\partial^2 u}{\partial x^2}(t,x)e^{-inx}dx \\
&= \frac{1}{2\pi}\left[\frac{\partial u}{\partial x}(t,x)e^{-inx}\right]_0^{2\pi} + \frac{in}{2\pi}\int_0^{2\pi}\frac{\partial u}{\partial x}(t,x)e^{-inx}dx \\
&= 0 + \frac{in}{2\pi}\left[u(t,x)e^{-inx}\right]_0^{2\pi} - \frac{n^2}{2\pi}\int_0^{2\pi} u(t,x)e^{-inx}dx \\
&= 0 - n^2 c_n(t).
\end{aligned}$$

1. Merci à Michel Nassif pour l'idée et certains éléments du développement.

Par deux intégrations par parties, en utilisant la périodicité. On résout alors l'équation différentielle vérifiée par c_n et on trouve $c_n(t) = c_n^0 e^{-n^2 t}$ pour tout $t > 0$. Il nous faut alors déterminer c_n^0. On sait que $c_n^0 = \lim_{t\to 0} c_n(t)$. D'autre part, grâce à (2),

$$\Big|c_n(t) - \frac{1}{2\pi}\int_0^{2\pi} f(x)e^{-inx}dx\Big| \leqslant \sup_{x\in\mathbb{T}} |u(t,x) - f(x)| \underset{t\to 0}{\longrightarrow} 0.$$

Ainsi,

$$c_n^0 = \frac{1}{2\pi}\int_0^{2\pi} f(x)e^{-inx}dx.$$

On obtient finalement, $\forall t > 0, \forall x \in \mathbb{T}$,

$$u(t,x) = \sum_{n\in\mathbb{Z}} c_n^0 e^{-n^2 t}e^{inx} = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} \Big(\int_0^{2\pi} f(y)e^{-iny}dy\Big)e^{-n^2 t}e^{inx}$$

on peut alors intervertir somme et intégrale puisque $\forall t > 0, \forall x \in \mathbb{T}$,

$$\frac{1}{2\pi}\sum_{n\in\mathbb{Z}}\int_0^{2\pi} \big|f(y)e^{-n^2 t}\big|dy < +\infty$$

et on a ainsi $\forall t > 0, \forall x \in \mathbb{T}$,

$$u(t,x) = \frac{1}{2\pi}\int_0^{2\pi} \Big(\sum_{n\in\mathbb{Z}} e^{in(x-y)}e^{-n^2 t}\Big)f(y)dy = (K_t * f)(x)$$

où $K_t(x) = \sum_{n\in\mathbb{Z}} e^{inx}e^{-n^2 t}$. On a donc trouvé un candidat pour la solution.

Synthèse : l'analyse nous a montré qu'il n'y avait qu'une possibilité de solution, ce qui assure l'unicité. On montre alors que $u(t,x) = (K_t * f)(x)$ est solution de (1) et (2). On écrit $u(t,x) = \sum_{n\in\mathbb{Z}} u_n(t,x)$ où $u_n(t,x) = c_n^0 e^{-n^2 t}e^{inx}$ avec $c_n^0 = \int_0^{2\pi} f(y)e^{-iny}dy$ (on a l'égalité par une interversion limite intégrale qu'on a déjà justifiée). On remarque alors que u_n est une fonction de classe $\mathcal{C}^\infty$ sur $]0,+\infty[\times\mathbb{T}$ et qui vérifie (1). D'autre part, on a la majoration, pour $k, l \geqslant 0$, $t \geqslant a > 0$ et $x \in \mathbb{T}$,

$$\Big|\frac{\partial^{k+l} u_n}{\partial t^k \partial x^l}(t,x)\Big| \leqslant |c_n^0| n^{2k+l} e^{-n^2 a} \leqslant ||f||_\infty n^{2k+l} e^{-n^2 a}$$

qui est le terme général d'une série convergente. On peut donc appliquer le théorème de dérivation sous le signe somme pour obtenir que $u \in \mathcal{C}^\infty(]0,+\infty[\times\mathbb{T})$ et qu'elle vérifie (1).

On montre enfin que u vérifie (2). Puisque alors $f \in \mathcal{C}^1(\mathbb{T})$, on a, pour $x \in \mathbb{T}$

$$f(x) = \sum_{n\in\mathbb{Z}} c_n(f)e_n(x)$$

et d'autre part,

$$\forall t > 0, \forall x \in \mathbb{T}, \quad u(t,x) = \sum_{n\in\mathbb{Z}} c_n(f) e^{-n^2 t} e_n(x)$$

et donc

$$\forall t > 0, \quad \sup_{x\in\mathbb{T}} |u(t,x) - f(x)| \leqslant \sum_{n\in\mathbb{Z}} (1 - e^{-n^2 t}) |c_n(f)|.$$

Or on sait que, puisque $f \in \mathcal{C}^2(\mathbb{T})$,

$$c_n(f) = -\frac{1}{n^2} c_n(f'')$$

et ainsi

$$\forall t > 0, \quad \sup_{x\in\mathbb{T}} |u(t,x) - f(x)| \leqslant \sum_{n\in\mathbb{Z}} (1 - e^{-n^2 t}) \frac{1}{n^2} |c_n(f'')| \leqslant \sum_{n\in\mathbb{Z}} (1 - e^{-n^2 t}) \frac{1}{n^2} ||f''||_\infty$$

et on peut alors appliquer le théorème de convergence dominée pour conclure. □

Remarque. On peut en fait montrer le même théorème avec $f \in \mathcal{C}^0(\mathbb{T})$. L'analyse se fait de la même manière puisque l'on a seulement utilisé la continuité de f, et de même, la vérification que u vérifie (1) est identique. On montre enfin que u vérifie (2). On utilise pour cela le cas $\mathcal{C}^2(\mathbb{T})$ et on commence par montrer que K_t est positif pour tout $t > 0$. En effet, soit $t > 0$, la série

$$g_t(x) = \sum_{n\in\mathbb{Z}} e^{-(x-2\pi n)^2/4t}$$

converge normalement sur $\mathbb{T}$ puisqu'on a la majoration

$$e^{-(x-2\pi n)^2/4t} \leqslant e^{-2\pi(n-1)^2/4t}.$$

Ainsi $g_t \in \mathcal{C}(\mathbb{T})$ et on calcule ses coefficients de Fourier :

$$\begin{aligned}\widehat{g_t}(k) &= \frac{1}{2\pi} \int_0^{2\pi} \sum_{n\in\mathbb{Z}} e^{-(x-2\pi n)^2/4t} e^{-ikx} dx = \frac{1}{2\pi} \sum_{n\in\mathbb{Z}} \int_0^{2\pi} e^{-(x-2\pi n)^2/4t} e^{-ikx} dx \\ &= \frac{1}{2\pi} \sum_{n\in\mathbb{Z}} \int_{-2\pi n}^{-2\pi(n-1)} e^{-y^2/4t} e^{-iky} dy = \frac{1}{2\pi} \int_{\mathbb{R}} e^{-y^2/4t} e^{-iky} dy = \sqrt{\frac{t}{2\pi}} e^{-tk^2}\end{aligned}$$

par convergence normale de la série, par changement de variable $y = x - 2\pi n$ et par calcul de la transformée de Fourier d'une gaussienne. On a alors convergence absolue des coefficients de Fourier de g_t, et donc par un corollaire du théorème de Fejér, g_t est égale à sa série de Fourier, et on a donc,

$$\sqrt{\frac{2\pi}{t}} g_t(x) = \sqrt{\frac{2\pi}{t}} \sum_{n\in\mathbb{Z}} e^{-(x-2\pi n)^2/4t} = \sum_{n\in\mathbb{Z}} e^{-tn^2} e^{inx} = K_t(x).$$

On a d'autre part, par convergence normale de la série en $x \in \mathbb{T}$,

$$\frac{1}{2\pi}\int_0^{2\pi} K_t(x) = \frac{1}{2\pi}\sum_{n\in\mathbb{Z}} e^{-n^2t}\int_0^{2\pi} e^{inx}dx = 1$$

pour tout $t > 0$. Soit $\varepsilon > 0$, on prend alors $g \in \mathcal{C}^2(\mathbb{T})$ telle que $||f-g||_\infty < \varepsilon$. On a, par inégalité triangulaire, linéarité de la convolution, inégalité de convolution, et par le cas $\mathcal{C}^2(\mathbb{T})$,

$$\begin{aligned}
||K_t * f - f||_\infty &\leqslant ||K_t * f - K_t * g||_\infty + ||K_t * g - g||_\infty + ||g - f||_\infty \\
&= ||K_t * (f-g)||_\infty + ||K_t * g - g||_\infty + ||g-f||_\infty \\
&\leqslant ||K_t||_1 ||f-g||_\infty + ||K_t * g - g||_\infty + ||g-f||_\infty \\
&= 2||f-g||_\infty + ||K_t * g - g||_\infty \\
&\leqslant 3\varepsilon
\end{aligned}$$

pour t suffisamment petit, d'où la conclusion.

Commentaire : pour justifier le recasage dans la leçon 235 : interversion de limites et d'intégrales, on note qu'on dérive deux fois sous l'intégrale, qu'il y a une interversion somme - intégrale et un théorème de convergence dominée.

3.4 Équation de Schrödinger sur $\mathbb{R}$

Référence : J. Rauch, *Partial differential equations*, Springer, 1991. [1]

Leçons concernées : 201, 222, 239, 250.

Théorème 1. *Soit $f \in \mathcal{S}(\mathbb{R})$. Alors il existe une unique fonction $u \in \mathcal{C}^2(\mathbb{R}^2)$ vérifiant*

(i) $\dfrac{\partial u}{\partial t}(x,t) = i\dfrac{\partial^2 u}{\partial x^2}(x,t), \quad \forall (x,t) \in \mathbb{R}^2$

(ii) $u(x,0) = f(x)$ *pour tout* $x \in \mathbb{R}$

(iii) $x \mapsto u(x,t)$ *appartient à* $\mathcal{S}(\mathbb{R})$ *uniformément par rapport à* t*, c'est-à-dire que pour tout* $T > 0$*,*

$$\forall k, l \geqslant 0, \quad M_{k,l}^T := \sup_{|t|<T} \sup_{x \in \mathbb{R}} \left| x^k \frac{\partial^l u}{\partial x^l}(x,t) \right| < +\infty.$$

De plus la solution est donnée par

$$\forall (x,t) \in \mathbb{R}^2, \quad u(x,t) = \frac{1}{2\pi} \int_{\mathbb{R}} \widehat{f}(\xi) e^{-i\xi^2 t} e^{ix\xi} d\xi.$$

Démonstration. On raisonne par analyse-synthèse.

Analyse : on suppose que $u \in \mathcal{C}^2(\mathbb{R}^2)$ est solution du problème. Puisque $u(.,t) \in \mathcal{S}(\mathbb{R})$ on peut considérer la transformée de Fourier partielle de u :

$$\forall t \in \mathbb{R}, \forall \xi \in \mathbb{R}, \quad \widehat{u}(\xi,t) = \int_{\mathbb{R}} u(x,t) e^{-ix\xi} dx.$$

Soit $\xi \in \mathbb{R}$, on applique alors le théorème de dérivation sous l'intégrale à $t \mapsto \widehat{u}(\xi,t)$ sur tout intervalle $]-T,T[$, pour $T > 0$:

(i) $\forall x \in \mathbb{R}$, $t \mapsto u(x,t)e^{-ix\xi}$ est dérivable sur $]-T,T[$

(ii) $\forall t \in]-T,T[$, $x \mapsto u(x,t)e^{-ix\xi} \in L^1(\mathbb{R})$ puisque $u(.,t) \in \mathcal{S}(\mathbb{R})$

(iii) $\forall x \in \mathbb{R}, \forall t \in]-T,T[$,

$$\left| \frac{\partial}{\partial t}\Big(u(x,t)e^{-ix\xi}\Big) \right| = \left| \frac{\partial u}{\partial t}(x,t) \right| = \left| \frac{\partial^2 u}{\partial x^2}(x,t) \right| \leqslant \frac{M_{0,2}^T + M_{2,2}^T}{1+|x|^2}$$

qui est intégrable sur $\mathbb{R}$ et ne dépend pas de t.

On obtient ainsi, pour $\xi, t \in \mathbb{R}$,

$$\frac{\partial \widehat{u}}{\partial t}(\xi,t) = \int_{\mathbb{R}} \frac{\partial}{\partial t}\Big(u(x,t)e^{-ix\xi}\Big) dx = i \int_{\mathbb{R}} \frac{\partial^2 u}{\partial x^2}(x,t) e^{-ix\xi} dx.$$

1. Merci à Michel Nassif pour l'idée et l'aide sur certains points du développement.

En réalisant deux intégrations par parties on obtient alors pour $\xi, t \in \mathbb{R}$,

$$\frac{\partial \widehat{u}}{\partial t}(\xi, t) = -i\xi^2 \widehat{u}(\xi, t)$$

et ainsi, pour tout $\xi \in \mathbb{R}$, il existe $A(\xi) \in \mathbb{R}$ tel que pour $t \in \mathbb{R}$,

$$\widehat{u}(\xi, t) = A(\xi) e^{-i\xi^2 t}.$$

Or, pour $\xi \in \mathbb{R}$,

$$\widehat{u}(\xi, 0) = A(\xi) = \int_{\mathbb{R}} u(x, 0) e^{-ix\xi} dx = \int_{\mathbb{R}} f(x) e^{-ix\xi} dx = \widehat{f}(\xi).$$

On obtient alors $\widehat{u}(\xi, t) = \widehat{f}(\xi) e^{-i\xi^2 t}$. Puisque pour tout $t \in \mathbb{R}$, $\xi \mapsto \widehat{f}(\xi) e^{-i\xi^2 t} \in \mathcal{S}(\mathbb{R})$, on peut appliquer l'inversion de Fourier pour avoir, pour $(x, t) \in \mathbb{R}^2$,

$$u(x, t) = \frac{1}{2\pi} \int_{\mathbb{R}} \widehat{f}(\xi) e^{-i\xi^2 t} e^{ix\xi} d\xi.$$

On a donc unicité de la solution.

Synthèse : on considère

$$u(x, t) = \frac{1}{2\pi} \int_{\mathbb{R}} \widehat{f}(\xi) e^{-i\xi^2 t} e^{ix\xi} d\xi$$

pour tout $(x, t) \in \mathbb{R}^2$. En appliquant le théorème de dérivation sous l'intégrale on obtient la régularité de u, qui est en fait $\mathcal{C}^\infty(\mathbb{R}^2)$ et le fait qu'elle vérifie l'équation de Schrödinger sur $\mathbb{R}^2$.

D'autre part, pour $x \in \mathbb{R}$,

$$u(x, 0) = \frac{1}{2\pi} \int_{\mathbb{R}} \widehat{f}(\xi) e^{ix\xi} d\xi = f(x)$$

par inversion de Fourier dans $\mathcal{S}(\mathbb{R})$.

Enfin, pour montrer le point (iii), on observe que pour tout $l \geqslant 0$, par dérivation sous le signe intégral,

$$\frac{\partial^l u}{\partial x^l}(x, t) = \frac{1}{2\pi} \int_{\mathbb{R}} i^l \xi^l \widehat{f}(\xi) e^{-i\xi^2 t} e^{ix\xi} d\xi$$

ainsi pour $k \geqslant 0$,

$$x^k \frac{\partial^l u}{\partial x^l}(x, t) = \frac{1}{2\pi} \int_{\mathbb{R}} i^l \xi^l \widehat{f}(\xi) e^{-i\xi^2 t} x^k e^{ix\xi} d\xi = \frac{1}{2\pi} \int_{\mathbb{R}} \frac{\partial^k}{\partial \xi^k} \left(i^l \xi^l \widehat{f}(\xi) e^{-i\xi^2 t} \right) i^k e^{ix\xi} d\xi$$

et donc pour $k, l \geqslant 0$, et pour $|t| < T$, où $T > 0$,

$$\begin{aligned}\left|x^k \frac{\partial^l u}{\partial x^l}(x,t)\right| &\leqslant \frac{1}{2\pi}\int_{\mathbb{R}} \left|\frac{\partial^k}{\partial \xi^k}\left(\xi^l \widehat{f}(\xi) e^{-i\xi^2 t}\right)\right| d\xi \leqslant \frac{1}{2\pi}\sum_{k'=0}^{k}\binom{k}{k'}\int_{\mathbb{R}}\left|\frac{\partial^{k'}}{\partial \xi^{k'}}\left(\xi^l \widehat{f}(\xi)\right)\right|\left|\frac{\partial^{k-k'}}{\partial \xi^{k-k'}}\left(e^{-i\xi^2 t}\right)\right| d\xi \\ &\leqslant \frac{1}{2\pi}\sum_{k'=0}^{k}\binom{k}{k'}\int_{\mathbb{R}}\left|\frac{\partial^{k'}}{\partial \xi^{k'}}\left(\xi^l \widehat{f}(\xi)\right)\right| P_{k'}(|\xi|,|t|) d\xi \\ &\leqslant \frac{1}{2\pi}\sum_{k'=0}^{k}\binom{k}{k'}\int_{\mathbb{R}}\left|\frac{\partial^{k'}}{\partial \xi^{k'}}\left(\xi^l \widehat{f}(\xi)\right)\right| P_{k'}(|\xi|,T) d\xi < +\infty\end{aligned}$$

où $P_{k'}$ est un polynôme à coefficients positifs en deux variables. Pour obtenir cette série de majoration on a appliqué l'inégalité triangulaire et la formule de Leibniz. La majoration est alors indépendante de t, et elle est valable puisque f étant dans $\mathcal{S}(\mathbb{R})$, il en est de même de $\widehat{f}$, et donc puisque $\mathcal{S}(\mathbb{R})$ est stable par dérivation et multiplication par un polynôme,

$$\xi \mapsto \frac{\partial^{k'}}{\partial \xi^{k'}}\left(\xi^l \widehat{f}(\xi)\right) P_{k'}(\xi, T) \in \mathcal{S}(\mathbb{R}) \subset L^1(\mathbb{R}).$$

□

Remarque. La même technique s'applique à l'équation de la chaleur sur $\mathbb{R}$, c'est cependant plus compliqué, puisque dans ce cas la condition initiale est une condition limite, il faut donc justifier un passage à la limite pour obtenir $A = \widehat{f}$. La justification de l'appartenance uniforme de u à $\mathcal{S}(\mathbb{R})$ est différente puisqu'on utilise l'expression de u comme produit de convolution avec un noyau.

3.5 Espace de Bergman du disque unité

Référence : F. Bayen, C. Margaria, *Espaces de Hilbert et opérateurs*, Ellipses, 1986.

Leçons concernées : 201, 202, 205, 208, 209, 213, 234, 243, 245.

On définit l'espace de Bergman $B^2(\mathbb{D}) := \mathcal{H}(\mathbb{D}) \cap L^2(\mathbb{D})$ l'ensemble des fonctions holomorphes sur le disque unité ouvert $\mathbb{D}$ de carré intégrable sur $\mathbb{D}$. On munit cet espace du produit scalaire $(.|.)$ de L^2 et de la norme $||.||_2$ induite. On commence par montrer

Lemme 1. *Pour tout K compact de $\mathbb{D}$, pour tout $f \in B^2(\mathbb{D})$,*

$$||f||_{\infty,K} \leqslant \frac{||f||_2}{\sqrt{\pi}\ d(K,\mathbb{S}^1)}$$

Démonstration. Soit $a \in \mathbb{D}$, et soit $r > 0$ tel que $D(a,r) \subset \mathbb{D}$. Par formule de la moyenne, pour $0 \leqslant \rho \leqslant r$, $f(a) = \frac{1}{2\pi}\int_0^{2\pi} f(a+\rho e^{i\theta})\ d\theta$ et donc, en multipliant par ρ et en intégrant par rapport à ρ :

$$\frac{r^2}{2}f(a) = \int_0^r f(a)\rho\ d\rho = \frac{1}{2\pi}\int_0^r\int_0^{2\pi} f(a+\rho e^{i\theta})\rho\ d\rho\ d\theta = \frac{1}{2\pi}\int_{D(a,r)} f(z)\ dz.$$

Ainsi, $f(a) = \frac{1}{\pi r^2}\int_{D(a,r)} f(z)\ dz$ et par inégalité de Hölder,

$$|f(a)| \leqslant \frac{1}{\pi r^2}\left(\int_{D(a,r)} |f(z)|^2\ dz\right)^{1/2}\left(\int_{D(a,r)} dz\right)^{1/2} \leqslant \frac{1}{\pi r^2}\sqrt{\pi r^2}||f||_2 = \frac{||f||_2}{\sqrt{\pi}r}.$$

On fait alors tendre r vers $d(a,\mathbb{S}^1)$, et on conclut avec $d(a,\mathbb{S}^1) \geqslant d(K,\mathbb{S}^1)$ pour $a \in K$. □

On utilise le lemme pour montrer la complétude de l'espace $B^2(\mathbb{D})$.

Proposition 2. *L'espace de Bergman $B^2(\mathbb{D})$ est un espace de Hilbert.*

Démonstration. On considère $(f_n)_n$ une suite de Cauchy dans $B^2(\mathbb{D})$. Pour tout K compact de $\mathbb{D}$, on a, d'après le lemme, pour tous $m, n \geqslant 0$,

$$||f_n - f_m||_{\infty,K} \leqslant \frac{||f_n - f_m||_2}{\sqrt{\pi}\ d(K,\mathbb{S}^1)}$$

et donc par hypothèse, $(f_n)_n$ vérifie le critère de Cauchy uniforme sur tout compact de $\mathbb{D}$ donc converge uniformément sur tout compact de $\mathbb{D}$ vers $f \in \mathcal{H}(\mathbb{D})$ d'après le théorème de Weierstrass. D'autre part, puisque $L^2(\mathbb{D})$ est complet d'après le théorème de Riesz-Fischer, il existe $g \in L^2(\mathbb{D})$ telle que f_n converge dans $L^2(\mathbb{D})$ vers g. De plus, d'après ce théorème, il existe $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(f_{\varphi(n)})_n$ converge presque partout vers g dans $\mathbb{D}$. Ainsi, par unicité de la limite simple, presque partout dans $\mathbb{D}$, $f = g$ et donc $f \in L^2(\mathbb{D}) \cap \mathcal{H}(\mathbb{D}) = B^2(\mathbb{D})$. □

On va enfin exhiber une base hilbertienne de l'espace $B^2(\mathbb{D})$. On pose, pour $n \geqslant 0$,

$$e_n : \begin{array}{ccc} \mathbb{D} & \to & \mathbb{C} \\ z & \mapsto & \sqrt{\frac{n+1}{\pi}} z^n. \end{array}$$

Proposition 3. *La famille $(e_n)_n$ est une base hilbertienne de $B^2(\mathbb{D})$.*

Démonstration. On commence par montrer que la famille est orthonormée : si $n, m \geqslant 0$, on a

$$(e_n, e_m) = \int_{\mathbb{D}} \sqrt{\frac{n+1}{\pi}} z^n \sqrt{\frac{m+1}{\pi}} \overline{z}^m \, dz = \frac{\sqrt{(n+1)(m+1)}}{\pi} \int_0^1 \int_0^{2\pi} r^{n+m} e^{i\theta(n-m)} r \, d\theta \, dr$$

par changement de variables. On conclut alors avec $\int_0^{2\pi} e^{i\theta(n-m)} \, d\theta = 2\pi\delta_m^n$ et $\int_0^1 r^{2n+1} \, dr = \frac{1}{2(n+1)}$.

On montre maintenant que la famille est totale, en utilisant le critère de densité : on montre que $(\mathrm{Vect}(e_n, n \geqslant 0))^\perp = \{0\}$. Soit $f \in (\mathrm{Vect}(e_n, n \geqslant 0))^\perp$. La fonction f est développable en série entière au voisinage de 0, on écrit alors, pour $z \in \mathbb{D}$, $f(z) = \sum_{k=0}^{\infty} a_k z^k$. Pour tout $0 < r < 1$, la série de droite est normalement convergente sur le disque fermé $\overline{D(0,r)}$. Alors, pour $n \geqslant 0$,

$$\begin{aligned} c_n = (e_n, f) = 0 &= \sqrt{\frac{n+1}{\pi}} \int_{\mathbb{D}} z^n \overline{f(z)} \, dz = \sqrt{\frac{n+1}{\pi}} \lim_{r\to 1} \int_{|z|<r} z^n \overline{f(z)} \, dz \\ &= \sqrt{\frac{n+1}{\pi}} \lim_{r\to 1} \int_{|z|<r} \sum_{k=0}^{\infty} a_k z^n \overline{z}^k \, dz = \sqrt{\frac{n+1}{\pi}} \lim_{r\to 1} \sum_{k=0}^{\infty} \int_{|z|<r} a_k z^n \overline{z}^k \, dz \end{aligned}$$

par convergence dominée et puisque sur $\overline{D(0,r)}$ la série $\sum_{k=0}^{\infty} a_k z^k$ est normalement convergente. Or,

$$\int_{|z|<r} z^n \overline{z}^k \, dz = \frac{2\pi r^{n+k+2}}{n+k+2} \delta_n^k = \frac{\pi r^{2n+2}}{n+1} \delta_n^k.$$

Ainsi, $c_n = \sqrt{\frac{\pi}{n+1}} a_n \lim_{r\to 1} r^{2n+2} = \sqrt{\frac{\pi}{n+1}} a_n = 0$, et donc $a_n = 0$ pour tout n et $f = 0$ sur $\mathbb{D}$ ce qui termine la preuve. □

Remarque. Puisque les coefficients d'un vecteur dans une base hilbertienne sont de carrés sommable, si $f \in B^2(\mathbb{D})$, $f = \sum_{n\geqslant 0} a_n z^n$, alors $\sum_{n\geqslant 0} |a_n|^2 \frac{\pi}{n+1} < +\infty$

3.6 Étude de la loi Gamma

Référence : Développement de Théo Pierron.

Leçons concernées : 236, 239, 245, 260, 261, 263.

Définition 1. La loi Gamma $\Gamma(a,\lambda)$ de paramètres $a>0, \lambda>0$ est la loi de probabilité de densité

$$\gamma_{a,\lambda}(x) = \frac{\lambda^a}{\Gamma(a)} e^{-\lambda x} x^{a-1} \mathbb{1}_{x\geqslant 0}.$$

Proposition 2. *La fonction caractéristique φ de la loi $\Gamma(a,\lambda)$ est donnée par*

$$\forall t\in\mathbb{R}, \quad \varphi(t) = \left(\frac{\lambda}{\lambda - it}\right)^a.$$

Démonstration. Étape 1 : on pose $D = \{z\in\mathbb{C} \mid \Re(z) < \lambda\}$, et pour $z\in D$, on considère

$$\psi(z) = \int_{\mathbb{R}} \gamma_{a,\lambda}(x) e^{xz}\, dx = \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{-(\lambda - z)x} x^{a-1}\, dx$$

qui est bien définie puisque si $z\in D$, $x\geqslant 0$,

$$\left|e^{-(\lambda-z)x} x^{a-1}\right| \leqslant e^{-(\lambda - \Re(z))x} x^{a-1}$$

et $x\mapsto e^{-(\lambda-\Re(z))x}x^{a-1} \in L^1(\mathbb{R}_+)$ puisque $\lambda - \Re(z) > 0$. On remarque que pour $t\in\mathbb{R}$, $\psi(it) = \varphi(t)$, on cherche donc à calculer ψ.

Étape 2 : on montre d'abord que ψ est holomorphe sur D en appliquant le théorème d'holomorphie sous l'intégrale sur tous les ouverts $D_\alpha = \{z\in\mathbb{C} \mid \Re(z) < \alpha < \lambda\}$:

(i) $\forall z\in D_\alpha$, $x\mapsto e^{-(\lambda-z)x}x^{a-1}$ est mesurable,

(ii) $\forall x\geqslant 0$, $z\mapsto e^{-(\lambda-z)x}x^{a-1}$ est holomorphe sur D_α,

(iii) $\forall z\in D_\alpha$, $\forall x\geqslant 0$,

$$\left|e^{-(\lambda-z)x}x^{a-1}\right| \leqslant e^{-(\lambda-\Re(z))x}x^{a-1} \leqslant e^{-(\lambda-\alpha)x}x^{a-1}$$

et $x\mapsto e^{-(\lambda-\alpha)x}x^{a-1}\in L^1(\mathbb{R}_+)$.

Étape 3 : on utilise ensuite le théorème du prolongement analytique : on calcule ψ sur $D\cap\mathbb{R}$. Soit $t<\lambda$, on a, en opérant le changement de variable $y = (\lambda - t)x$,

$$\psi(t) = \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{-(\lambda-t)x}x^{a-1}\, dx = \frac{\lambda^a}{\Gamma(a)} \int_0^{+\infty} e^{-y} \frac{y^{a-1}}{(\lambda-t)^a}\, dy = \frac{\lambda^a}{\Gamma(a)} \frac{\Gamma(a)}{(\lambda-t)^a} = \left(\frac{\lambda}{\lambda-t}\right)^a.$$

Ainsi, ψ et la fonction $z\mapsto \left(\frac{\lambda}{\lambda - z}\right)^a$ holomorphe sur D (en utilisant la détermination principale du logarithme) coïncident sur $D\cap\mathbb{R}$ et sont donc égales, d'où le résultat. □

Corollaire 3. *La transformée de Laplace de la loi $\Gamma(a,\lambda)$ est bien définie sur $]-\infty,\lambda[$ et est donnée par*

$$L(t) = \left(\frac{\lambda}{\lambda - t}\right)^a.$$

Démonstration. Cela a été démontré lors de la preuve de la proposition précédente. □

Corollaire 4. *La loi $\Gamma(a,\lambda)$ admet des moments à tout ordre donnés par :*

$$m_n = \frac{a(a+1)\cdots(a+n-1)}{\lambda^n}.$$

Démonstration. Puisque la fonction caractéristique est analytique, le théorème qui relie fonction caractéristique et moments nous donne l'existence des moments à tout ordre de la loi $\Gamma(a,\lambda)$ ainsi que leur expression. Or, puisque $\varphi(t) = \lambda^a(\lambda - it)^{-a}$, on obtient par récurrence

$$\varphi^{(n)}(t) = a(a+1)\cdots(a+n-1)\lambda^a i^n(\lambda - it)^{-a-n}$$

et on conclut avec

$$\varphi^{(n)}(0) = i^n m_n = i^n \frac{a(a+1)\cdots(a+n-1)}{\lambda^n}.$$

□

Remarque. On aurait pu raisonner de même avec la transformée de Laplace. Puisque celle-ci est définie au voisinage de 0, elle est analytique, et donc la loi $\Gamma(a,\lambda)$ admet des moments à tout ordre donnés par $m_n = L^{(n)}(0)$ et leur calcul est alors analogue.

Remarque. Le calcul des moments peut s'effectuer directement : par le changement de variable $y = \lambda x$ on obtient

$$\frac{\lambda^a}{\Gamma(a)}\int_0^{+\infty} e^{-\lambda x}x^a\,dx = \frac{\lambda^a}{\Gamma(a)\lambda^{a+1}}\int_0^{+\infty} e^{-y}y^{a-1}\,dy = \frac{\Gamma(a+1)}{\Gamma(a)\lambda} = \frac{a}{\lambda}.$$

et l'on procède de la même manière pour les moments d'ordres supérieurs.

3.7 Fonction caractéristique et moments

Référence : J.Y. Ouvrard, *Probabilités 2*, Cassini, 2009.

Leçons concernées : 218, 228, 239, 260, 216.

Théorème 1. *Soit X une variable aléatoire réelle et φ_X sa fonction caractéristique. Alors,*

(i) si X admet un moment d'ordre n, φ_X est de classe $\mathcal{C}^n$, et pour tout $k \in [|1, n|]$, $\forall t \in \mathbb{R}$,

$$\varphi_X^{(k)}(t) = i^k \int_\Omega X^k \exp(itX) d\mathbb{P}.$$

En particulier,

$$\varphi_X^{(k)}(0) = i^k \mathbb{E}[X^k].$$

(ii) Réciproquement, si φ_X est n ($n \geqslant 2$) fois dérivable en 0, alors X admet des moments d'ordre $1 \leqslant k \leqslant 2[\frac{n}{2}]$ vérifiant

$$\varphi_X^{(k)}(0) = i^k \mathbb{E}[X^k].$$

Démonstration. (i) Le premier point résulte d'une simple application du théorème de dérivation sous l'intégrale : soit $1 \leqslant k \leqslant n$, X admet un moment d'ordre k puisqu'il en admet un d'ordre n par hypothèse. D'autre part, on a

$$\frac{d^k}{dt^k} \exp(itX) = i^k X^k \exp(itX)$$

qui est majoré en module par $|X|^k$ qui est intégrable. On peut alors appliquer le théorème de dérivation sous l'intégrale itéré k fois pour obtenir φ_X de classe $\mathbb{C}^k$ et la formule

$$\varphi_X^{(k)}(t) = i^k \int_\Omega X^k \exp(itX) d\mathbb{P}.$$

(ii) On montre le résultat par récurrence sur $1 \leqslant k \leqslant [\frac{n}{2}]$: pour le cas $k = 1$, on cherche à montrer que X admet un moment d'ordre $2k = 2$, et on écrit pour cela la formule de Taylor-Young à l'ordre 2 en 0 de φ_X pour t et $-t$:

$$\varphi_X(t) = \varphi_X(0) + t\varphi_X'(0) + \frac{t^2}{2}\varphi_X''(0) + o(t^2)$$
$$\varphi_X(-t) = \varphi_X(0) - t\varphi_X'(0) + \frac{t^2}{2}\varphi_X''(0) + o(t^2).$$

Ainsi,

$$\varphi_X(t) + \varphi_X(-t) - 2 = t^2\varphi_X''(0) + o(t^2)$$

avec $\varphi_X(0) = 1$. c'est-à-dire que $\lim_{t\to 0} \dfrac{\varphi_X(t) + \varphi_X(-t) - 2}{t^2} = \varphi_X''(0)$. D'autre part, on sait que

$$\varphi_X(t) + \varphi_X(-t) = 2\Re(\varphi_X(t)) = 2\mathbb{E}[\cos(tX)].$$

Ainsi,

$$\lim_{t\to 0} 2\mathbb{E}\left[\frac{1-\cos(tX)}{t^2}\right] = -\varphi_X''(0).$$

Enfin, on sait que $X^2 = 2\lim_{t\to 0} \dfrac{1-\cos(tX)}{t^2}$, ainsi, par le lemme de Fatou, si $t_n \to 0$,

$$\int_\Omega X^2 = 2\mathbb{E}\left[\liminf_n \frac{1-\cos(t_nX)}{t_n^2}\right] \leqslant 2\liminf_n \mathbb{E}\left[\frac{1-\cos(t_nX)}{t_n^2}\right] = -\varphi_X''(0) < +\infty.$$

On fixe alors $1 \leqslant k \leqslant \left[\frac{n}{2}\right]$ et on suppose avoir montré l'existence des moments jusqu'à l'ordre $2(k-1)$ et on cherche à montrer que X admet un moment d'ordre $2k$: on applique le même raisonnement que précédemment à $\varphi_X^{(2k-2)}$ dérivable deux fois pour obtenir :

$$\lim_{t\to 0} \frac{\varphi_X^{(2k-2)}(t) + \varphi_X^{(2k-2)}(-t) - 2\varphi_X^{(2k-2)}(0)}{t^2} = \varphi_X^{(2k)}(0.)$$

D'autre part, par hypothèse de récurrence et par le point (i),

$$\varphi_X^{(2k-2)}(t) = i^{2k-2}\mathbb{E}[X^{2k-2}\exp(itX)]$$
$$\varphi_X^{(2k-2)}(-t) = i^{2k-2}\mathbb{E}[X^{2k-2}\exp(-itX)]$$

d'où

$$\varphi_X^{(2k-2)}(t) + \varphi_X^{(2k-2)}(-t) = (-1)^{k-1}2\mathbb{E}[X^{2k-2}\cos(tX)]$$

et d'autre part

$$\varphi_X^{(2k-2)}(0) = (-1)^{k-1}\mathbb{E}[X^{2k-2}].$$

Ainsi,

$$\lim_{t\to 0} 2\mathbb{E}\left[X^{2k-2}\frac{1-\cos(tX)}{t^2}\right] = (-1)^k\varphi_X^{(2k)}(0)$$

et on conclut avec le lemme de Fatou de la même manière que ci-dessus.

□

Application 2. *Si $X \sim \mathcal{N}(0,\sigma^2)$, alors pour $k \in \mathbb{N}$,*

$$\mathbb{E}\big[X^{2k}\big] = \frac{\sigma^{2k}(2k)!}{2^k k!} \quad \textit{et} \quad \mathbb{E}\big[X^{2k+1}\big] = 0.$$

Démonstration. On sait que $\varphi_X(t) = e^{-t^2\sigma^2/2}$, et donc d'après le théorème, X admet des moments de tout ordre. D'autre part, pour $t \in \mathbb{R}$,

$$\varphi_X(t) = e^{-t^2\sigma^2/2} = \sum_{k\geqslant 0} \frac{(-1)^k \sigma^{2k}}{2^k k!} t^{2k}.$$

Ainsi, pour $k \in \mathbb{N}$,

$$\varphi^{(2k)}(0) = \frac{(-1)^k \sigma^{2k}(2k)!}{2^k k!} \quad \text{et} \quad \varphi^{(2k+1)}(0) = 0$$

d'où le résultat d'après le théorème. □

3.8 Formule sommatoire de Poisson

Référence : X. Gourdon, *Les maths en tête, Analyse*, Ellipses, 2008.

Leçons concernées : 246, *241, 250.*

Théorème 1. *Soit $f \in \mathcal{S}(\mathbb{R})$. Alors pour x dans $\mathbb{R}$,*

$$\sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n) e^{2i\pi nx}$$

où on a noté $\widehat{f}(y) = \displaystyle\int_{\mathbb{R}} f(t)e^{-2i\pi yt}dt$ pour $y \in \mathbb{R}$.

Démonstration. Étape 1 : la série de fonctions $\sum_{n\in\mathbb{Z}} f(x+n)$ converge normalement sur tout compact de $\mathbb{R}$. En effet, puisque $f \in \mathcal{S}(\mathbb{R})$, il existe $C > 0$ telle que $|f(x)| \leqslant \frac{C}{x^2}$ pour $|x| \geqslant 1$, et donc pour tout $K > 0$, pour tout $n \in \mathbb{Z}$ tel que $|n| > K$, et tout $x \in [-K, K]$,

$$|f(x+n)| \leqslant \frac{C}{|x+n|^2} \leqslant \frac{C}{(|n|-|x|)^2} \leqslant \frac{C}{(|n|-K)^2}$$

qui est le terme général d'une série convergente. On note alors $G(x) = \sum_{n\in\mathbb{Z}} f(x+n)$ la somme de la série.

Un raisonnement analogue nous montre que la série $\sum_{n\in\mathbb{Z}} f'(x+n)$ converge également normalement sur tout compact de $\mathbb{R}$, et donc par le théorème de dérivation des suites de fonctions, G est de classe $\mathcal{C}^1(\mathbb{R})$ et $G'(x) = \sum_{n\in\mathbb{Z}} f'(x+n)$.

Enfin, G est 1-périodique. En effet, on a

$$G(x+1) = \sum_{n\in\mathbb{Z}} f(x+n+1) = \sum_{p\in\mathbb{Z}} f(x+p) = G(x)$$

par changement d'indice $p = n+1$.

Étape 2 : on obtient grâce à l'étape précédente que G est somme de sa série de Fourier qui converge normalement. On calcule alors ses coefficients de Fourier :

$$\begin{aligned}
\forall k \in \mathbb{Z}, \quad c_k(G) &= \int_0^1 G(t)e^{-2i\pi kt}\,dt = \int_0^1 \sum_{n\in\mathbb{Z}} f(t+n)e^{-2i\pi kt}\,dt \\
&= \sum_{n\in\mathbb{Z}} \int_0^1 f(t+n)e^{-2i\pi kt}\,dt = \sum_{n\in\mathbb{Z}} \int_n^{n+1} f(t)e^{-2i\pi kt}\,dt \\
&= \int_{-\infty}^{+\infty} f(t)e^{-2i\pi kt}\,dt
\end{aligned}$$

où on a interverti puisque G converge normalement, et la dernière somme converge puisque $f \in \mathcal{S}(\mathbb{R})$. On obtient alors le résultat annoncé. □

Corollaire 2. *On définit*

$$\theta(s) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 s}$$

pour $s > 0$. On déduit de la formule sommatoire de Poisson que

$$\forall s > 0, \quad \theta(s) = \frac{1}{\sqrt{s}}\theta(1/s).$$

Démonstration. On applique la formule sommatoire de Poisson en $x = 0$ à la fonction $f : x \mapsto e^{-\pi s x^2}$ pour $s > 0$. On a, pour $n \in \mathbb{Z}$,

$$\widehat{f}(n) = \int_{\mathbb{R}} e^{-\pi s t^2} e^{-2i\pi nt} dt = \frac{1}{\sqrt{\pi s}} \int_{\mathbb{R}} e^{-t^2} e^{-2i\pi nt/\sqrt{\pi s}} dt = \frac{1}{\sqrt{s}} e^{\pi n^2/s}$$

et donc

$$\forall s > 0, \quad \sum_{n\in\mathbb{Z}} e^{-\pi n^2 s} = \frac{1}{\sqrt{s}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/s}$$

d'où le résultat. □

Commentaire : c'est assez court, si besoin calculer la transformée de Fourier de la gaussienne.

3.9 Inversion de Fourier dans $L^1(\mathbb{R}^d)$

Référence : J.M. Bony, *Cours d'analyse - Théorie des distributions et analyse de Fourier*, les Éditions de l'École Polytechnique, 2001.

Leçons concernées : 234, 235, 236, 239, 250.

Lemme 1. *Soit $\chi \in L^1(\mathbb{R}^d)$ telle que $\int_{\mathbb{R}^d} \chi(x)dx = 1$ et pour tout $\varepsilon > 0$ soit $\chi_\varepsilon(x) := \varepsilon^{-d}\chi(x/\varepsilon)$. Alors pour tout $f \in L^1(\mathbb{R}^d)$, $f * \chi_\varepsilon$ converge vers f dans $L^1(\mathbb{R}^d)$.*

Démonstration. On commence par démontrer le résultat pour $f \in \mathcal{C}_c^0(\mathbb{R}^d)$. On prend $R > 0$ tel que $\text{supp}(f) \subset [-R, R]^d$. Soit $\alpha > 0$, par uniforme continuité, il existe $\delta > 0$ tel que $\forall x, y \in \mathbb{R}^d, |x - y| < \delta \Rightarrow |f(x) - f(y)| < \alpha$, et on suppose $\delta < 1$. On remarque alors que par un changement de variables on a $f * \chi_\varepsilon\ (x) = \int_{\mathbb{R}^d} f(x - \varepsilon t)\chi(t)dt$. On écrit donc, avec $\int_{\mathbb{R}^d} \chi(x)dx = 1$ et par inégalité triangulaire,

$$\begin{aligned}
\int_{\mathbb{R}^d} |f * \chi_\varepsilon\ (x) - f(x)|\, dx &\leqslant \iint_{\mathbb{R}^{2d}} |f(x - \varepsilon t) - f(x)||\chi(t)|dtdx \\
&= \int_{\mathbb{R}^d} |\chi(t)| \left(\int_{\mathbb{R}^d} |f(x - \varepsilon t) - f(x)|dx \right) dt \\
&= \int_{|t|<\delta/\varepsilon} |\chi(t)| \left(\int_{[-R-1,R+1]} |f(x - \varepsilon t) - f(x)|dx \right) dt \\
&+ \int_{|t|>\delta/\varepsilon} |\chi(t)| \left(\int_{\mathbb{R}^d} |f(x - \varepsilon t) - f(x)|dx \right) dt \\
&\leqslant \int_{|t|<\delta/\varepsilon} |\chi(t)| \left(\int_{[-R-1,R+1]} \alpha dx \right) dt + 2\int_{|t|>\delta/\varepsilon} |\chi(t)|||f||_1 dt \\
&\leqslant (2R + 2)||\chi||_1\alpha + 2||f||_1 \int_{|t|>\delta/\varepsilon} |\chi(t)|dt.
\end{aligned}$$

Or puisque $\chi \in L^1(\mathbb{R}^d)$, l'intégrale restante tend vers 0 lorsque ε tend vers 0, ainsi, il existe $\beta > 0$ tel que pour tout $\varepsilon < \beta$, $\int_{|t|>\delta/\varepsilon} |\chi(t)|dt < \alpha$ et on obtient donc la convergence voulue dans $L^1(\mathbb{R}^d)$. On obtient alors le résultat voulu par densité de $\mathcal{C}_c^0(\mathbb{R}^d)$ dans $L^1(\mathbb{R}^d)$, en utilisant la linéarité de la convolution, l'inégalité, pour deux fonctions $f, g \in L^1(\mathbb{R}^d)$ $||f * g||_1 \leqslant ||f||_1||g||_1$, et par inégalité triangulaire. □

Définition 2. Pour $f \in L^1(\mathbb{R}^d)$, on définit sa transformée de Fourier comme la fonction

$$\widehat{f}(x) = \mathcal{F}(f)(x) = \int_{\mathbb{R}^d} e^{-it\cdot x} f(t)dt.$$

Théorème 3. *Soit $f \in L^1(\mathbb{R}^d)$ telle que $\widehat{f} \in L^1(\mathbb{R}^d)$, alors, presque partout,*

$$f(x) = \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} e^{ix\cdot t} \widehat{f}(t) dt.$$

Proposition 4. *Soit $a > 0$, alors*

$$\mathcal{F}\left(t \mapsto e^{-a|t|^2}\right)(x) = \left(\frac{\pi}{a}\right)^{d/2} e^{-|x|^2/4a}.$$

Démonstration. On pose $g(x) := \mathcal{F}\left(e^{-t^2}\right)(x) = \int_{\mathbb{R}} e^{-itx} e^{-t^2} dt$. On vérifie facilement avec le théorème de dérivation sous le signe intégral que g est de classe $\mathcal{C}^1$ sur $\mathbb{R}$, et que $g'(x) = \int_{\mathbb{R}} -ite^{-itx} e^{-t^2} dt = \frac{1}{2} \int_{\mathbb{R}} ie^{-itx}(-2te^{-t^2}) dt = -x\frac{1}{2} \int_{\mathbb{R}} e^{-itx} e^{-t^2} dt$ par intégration par parties. Ainsi g vérifie $2g'(x) - xg(x) = 0$ et donc $g(x) = \sqrt{\pi} e^{-x^2/4}$ puisque $\int_{\mathbb{R}} e^{-t^2} dt = \sqrt{\pi}$.

D'autre part, si $f \in L^1(\mathbb{R})$,

$$\mathcal{F}\left(t \mapsto f(\lambda t)\right)(x) = \int_{\mathbb{R}} e^{-itx} f(t\lambda) dt = \left|\frac{1}{\lambda}\right| \int_{\mathbb{R}} e^{-it\cdot x/\lambda} f(t) dt = \left|\frac{1}{\lambda}\right| \mathcal{F}(f)\left(\frac{x}{\lambda}\right)$$

par changement de variables, d'où la formule voulue en dimension 1.

La dimension supérieure s'obtient facilement par le théorème de Fubini en remarquant que l'on peut écrire $e^{-a|t|^2} = e^{-at_1^2} \cdots e^{-at_d^2}$. □

Démonstration (Théorème). Étape 1 : on remarque que

$$\frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} e^{ix\cdot t} \widehat{f}(t) dt = \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} \left(\int_{\mathbb{R}^d} e^{it\cdot(x-y)} f(y) dy \right) dt$$

mais on ne peut pas appliquer le théorème de Fubini. On pose donc pour $\varepsilon > 0$,

$$I_\varepsilon(x) := \frac{1}{(2\pi)^d} \iint_{\mathbb{R}^{2d}} e^{i(x-y)\cdot t} e^{-\varepsilon^2|t|^2/4} f(y) dt dy.$$

On peut maintenant appliquer le théorème de Fubini :

$$\begin{aligned} I_\varepsilon(x) &= \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} \int_{\mathbb{R}^d} e^{i(x-y)\cdot t} e^{-\varepsilon^2|t|^2/4} f(y) dy dt \\ &= \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} e^{ix\cdot t} e^{-\varepsilon^2|t|^2/4} \left(\int_{\mathbb{R}^d} e^{-iy\cdot t} f(y) dy \right) dt = \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} e^{ix\cdot t} e^{-\varepsilon^2|t|^2/4} \widehat{f}(t) dt. \end{aligned}$$

On applique alors le théorème de convergence dominée puisque par hypothèse $\widehat{f} \in L^1(\mathbb{R}^d)$ pour obtenir :

$$I_\varepsilon(x) \underset{\varepsilon \to 0}{\longrightarrow} \frac{1}{(2\pi)^d} \int_{\mathbb{R}^d} e^{ix\cdot t} \widehat{f}(t) dt.$$

Étape 2 : d'autre part, si on intègre d'abord par rapport à t, on obtient

$$I_\varepsilon(x) := \frac{1}{(2\pi)^d}\int_{\mathbb{R}^d} G_\varepsilon(x-y)f(y)dy = G_\varepsilon * f\ (x).$$

En posant $G_\varepsilon(z) = \frac{1}{(2\pi)^d}\int_{\mathbb{R}^d} e^{iz\cdot t}e^{-\varepsilon^2|t|^2/4}dt$.

Étape 3 : or, d'après la proposition précédente,

$$G_\varepsilon(z) = \frac{1}{(2\pi)^d}\left(\frac{4\pi}{\varepsilon^2}\right)^{d/2} e^{-|z|^2/\varepsilon^2} = \varepsilon^{-d}G_1(z/\varepsilon)$$

avec $G_1(z) = \pi^{-d/2}e^{-|z|^2}$ dont on remarque qu'elle est d'intégrale 1. Ainsi, la famille $(G_\varepsilon)_\varepsilon$ vérifie les hypothèses du lemme. On obtient alors une convergence L^1 de I_ε vers f, donc une convergence simple presque partout à une sous-suite près. On a donc le résultat. □

Application 5. *La fonction caractéristique de la loi de Cauchy est*

$$\varphi(t) = e^{-|t|}.$$

Démonstration. On commence par calculer la fonction caractéristique de la loi de Laplace, c'est-à-dire la transformée de Fourier de la fonction $f : x \mapsto \frac{1}{2}e^{-|x|} \in L^1(\mathbb{R})$: pour $\xi \in \mathbb{R}$,

$$\begin{aligned}\widehat{f}(\xi) &= \frac{1}{2}\int_{\mathbb{R}} e^{-ix\xi}e^{-|x|}\,dx = \frac{1}{2}\int_{-\infty}^{0} e^{x(1-i\xi)}\,dx + \frac{1}{2}\int_0^{+\infty} e^{-x(1+i\xi)}\,dx \\ &= \frac{1}{2}\left[\frac{1}{1-i\xi}\,e^{x(1-i\xi)}\right]_{-\infty}^{0} + \frac{1}{2}\left[\frac{-1}{1+i\xi}\,e^{-x(1+i\xi)}\right]_0^{+\infty} = \frac{1}{2}\left(\frac{1}{1-i\xi} + \frac{1}{1+i\xi}\right) \\ &= \frac{1}{1+\xi^2} = \pi g(\xi)\end{aligned}$$

où $g \in L^1(\mathbb{R})$ est la densité de la loi de Cauchy. On cherche donc à calculer $\widehat{g}(x) = \frac{1}{\pi}\mathcal{F}(\mathcal{F}(f))(x)$. Or, d'après la formule d'inversion, pour $h \in L^1$ telle que $\widehat{h} \in L^1$,

$$\mathcal{F}(\mathcal{F}(x))(x) = 2\pi\, h(-x)$$

et donc $\widehat{g}(x) = 2f(-x) = e^{-|x|}$. □

Commentaire : la démonstration du théorème seule est un peut courte, on peut donc rajouter au choix celle du lemme ou de la proposition.

3.10 Marche aléatoire sur $\mathbb{Z}^d$, $d \geqslant 3$

Référence : Plan de leçon de Louis Garénaux et Michel Nassif.

Leçons concernées : 235, 260, 261, 262, 264.

Théorème 1. *Soit $(e_i)_{1\leqslant i\leqslant d}$ la base canonique dans $\mathbb{R}^d$, et $(X_i)_{i\in\mathbb{N}^*}$ une suite de variables aléatoires indépendantes et identiquement distribuées telles que*

$$\mathbb{P}(X_1 = e_i) = \mathbb{P}(X_1 = -ei) = \frac{1}{2d}$$

pour tout $1 \leqslant i \leqslant d$. On note $S_n := \sum_{i=1}^n X_i$, $S_0 = 0$. Alors pour $d \geqslant 3$,

$$\mathbb{P}(|S_n| \to +\infty) = 1.$$

Démonstration. On cherche à montrer que $\sum \mathbb{P}(S_n = 0)$ converge. En effet, si on note $R = \mathbb{E}[\sum_{n\geqslant 0} \mathbb{1}_{S_n=0}]$ l'espérance du nombre de retours en 0, on a par Fubini-Tonelli, $R = \sum_{n\geqslant 0} \mathbb{P}(S_n = 0)$, et l'on pourra aboutir à une conclusion.

Étape 1 : on cherche alors à calculer $\mathbb{P}(S_n = 0)$. On pose, pour $t = (t_1, \cdots, t_d) \in \mathbb{R}^d$,

$$\varphi(t) := \varphi_{X_1}(t) = \mathbb{E}[e^{iX_1\cdot t}] = \sum_{j=1}^{d} \frac{1}{2d}(e^{it\cdot e_j} + e^{-it\cdot e_j}) = \frac{1}{d}\sum_{j=1}^{d} \cos(t_j).$$

De plus, par indépendance, on a $\varphi_{S_n}(t) = (\varphi(t))^n$.

D'autre part, avec $\varphi_{S_n}(t) = \sum_{k\in\mathbb{Z}^d} \mathbb{P}(S_n = k)e^{ik\cdot t}$, si on pose $T := [-\pi, \pi]$, on a :

$$\frac{1}{(2\pi)^d}\int_{T^d} \varphi_{S_n}(t)dt = \frac{1}{(2\pi)^d}\sum_{k\in\mathbb{Z}^d}\int_{T^d} \mathbb{P}(S_n = k)e^{ik\cdot t}dt = \mathbb{P}(S_n = 0)$$

par Fubini puisque $\frac{1}{(2\pi)^d}\sum_{k\in\mathbb{Z}^d}\int_{T^d} |\mathbb{P}(S_n = k)e^{ik\cdot t}|dt = \sum_{k\in\mathbb{Z}^d} \mathbb{P}(S_n = k) = 1$ et puisque $\frac{1}{(2\pi)^d}\int_{T^d} e^{ik\cdot t}dt = \frac{1}{(2\pi)^d}\int_{T^d}\prod_{j=1}^d e^{ik_jt_j}dt = \delta_0^k$.

Étape 2 : on calcule alors R. Puisqu'il faut un nombre pair d'étapes à $(S_n)_n$ pour revenir en 0, on sait que pour n impair, $\mathbb{P}(S_n = 0) = 0$. On remarque que $|\varphi| \leqslant 1$ sur T^d et $|\varphi(t)| = 1$ si et seulement si $t = (0, \ldots, 0), \pm(\pi, \ldots, \pi)$. On obtient alors :

$$\begin{aligned}\sum_{n\geqslant 0} \mathbb{P}(S_n = 0) &= \frac{1}{(2\pi)^d}\sum_{n\geqslant 0}\int_{T^d} \varphi_{S_{2n}}(t)dt = \frac{1}{(2\pi)^d}\sum_{n\geqslant 0}\int_{T^d} \varphi(t)^{2n}dt \\ &= \frac{1}{(2\pi)^d}\int_{T^d}\sum_{n\geqslant 0} \varphi(t)^{2n}dt = \frac{1}{(2\pi)^d}\int_{T^d}\frac{1}{1-\varphi(t)^2}dt\end{aligned}$$

par Fubini-Tonelli puisqu'on a justifié que $\varphi(t)$ est réel et puisque $|\varphi| < 1$ presque partout sur T^d.

Étape 3 : justifions l'intégrabilité. Puisque $\frac{1}{1-\varphi^2}$ est continue sur $T^d\backslash\{(0,\dots,0),\pm(\pi,\dots,\pi)\}$, il nous reste maintenant à justifier l'intégrabilité de la fonction $\frac{1}{1-\varphi^2}$ en $(0,\dots,0),\pm(\pi,\dots,\pi)$. On se limite au point $(0,\dots,0)$ puisque pour tout $y\in\mathbb{R}$, $\cos(y\pm\pi)=-\cos(y)$.

Or, en 0,

$$\varphi(t)=\frac{1}{d}\sum_{j=1}^{d}\left(1-\frac{t_j^2}{2}+o(t_j^2)\right)=1-\frac{||t||^2}{2d}+o(||t||^2)$$

et ainsi

$$1-\varphi(t)^2=\frac{||t||^2}{d}+o(||t||^2)$$

donc

$$\frac{1}{1-\varphi(t)^2}\sim\frac{d}{||t||^2}$$

qui est intégrable en 0 dès que $d\geqslant 3$.

Étape 4 : soit maintenant $k\in\mathbb{Z}^d$, on montre que $\sum_{n\geqslant 0}\mathbb{P}(S_n=k)$ converge en se ramenant en 0 : on pose $l=|k|$, on a, pour $n\geqslant l+1$

$$\begin{aligned}\mathbb{P}(S_n=0)&\geqslant\mathbb{P}(S_n=0\text{ et }S_l=-k)\\&\geqslant\mathbb{P}(X_1+\cdots+X_l=-k\text{ et }X_{l+1}+\cdots+X_n=k)\\&=\mathbb{P}(S_l=-k)\mathbb{P}(S_{n-l}=k)\end{aligned}$$

car les X_i sont i.i.d. Or, puisque $l=|k|$, $\mathbb{P}(S_l=-k)\geqslant\frac{1}{(2d)^l}>0$ donc

$$\sum_{n\geqslant 0}\mathbb{P}(S_n=k)=\sum_{n\geqslant 1}\mathbb{P}(S_n=k)=\sum_{n\geqslant l+1}\mathbb{P}(S_{n-l}=k)\leqslant\frac{1}{\mathbb{P}(S_l=-k)}\sum_{n\geqslant l+1}\mathbb{P}(S_n=0)<\infty.$$

Étape 5 : on peut alors conclure : pour $k\in\mathbb{Z}^d$, on note $N_k:=\sum_{n\geqslant 0}\mathbb{1}_{S_n=k}$ le nombre de retours de S_n en k, et puisque $\mathbb{E}[N_k]=\sum_{n\geqslant 0}\mathbb{P}(S_n=k)$, N_k est fini presque sûrement. On a alors

$$\begin{aligned}\mathbb{P}(|S_n|\to+\infty)&=\mathbb{P}(\forall A\in\mathbb{N}^*,\ \exists n_0,\ \forall n\geqslant n_0,\ |S_n|\geqslant A)\\&=\lim_{A\to+\infty}\mathbb{P}(\exists n_0,\ \forall n\geqslant n_0,\ |S_n|\geqslant A)\\&=\lim_{A\to+\infty}\mathbb{P}(\forall k,\ |k|\leqslant A,\ N_k\text{ est fini})\\&=1\end{aligned}$$

puisque $(\{\exists n_0,\ \forall n\geqslant n_0,\ |S_n|\geqslant A\})_{A\in\mathbb{N}^*}$ est décroissante, que $\{\exists n_0,\ \forall n\geqslant n_0,\ |S_n|\geqslant A\}=\{\forall k,\ |k|\leqslant A,\ N_k\text{ est fini}\}$ et puisque l'union dénombrable d'ensembles de mesure nulle est de mesure nulle. □

On justifie ici [1] l'intégrabilité de la fonction $x\mapsto\frac{1}{||x||^2}$ utilisée dans la preuve.

1. Merci à Michel Nassif pour cette preuve.

Proposition 2. *La fonction* $x \mapsto \frac{1}{||x||^2}$ *est intégrable au voisinage de* 0 *dans* $\mathbb{R}^d$ *si et seulement si* $d \geqslant 3$.

Démonstration. Il est clair que pour $d = 1, 2$, la fonction n'est pas intégrable en 0.

On montre alors l'intégrabilité pour $d = 3$: on considère le $\mathcal{C}^1$ difféomorphisme $\Psi(r, \theta, \varphi) = (r\cos(\theta)\sin(\varphi), r\sin(\theta)\sin(\varphi), r\cos(\varphi))$ de jacobien $-r^2\sin(\varphi)$. On a alors,

$$\iiint_{x^2+y^2+z^2\leqslant 1} \frac{1}{x^2+y^2+z^2}\, dx\, dy\, dz = \int_{\theta=0}^{2\pi}\int_{\varphi=0}^{\pi}\int_{r=0}^{1} \frac{1}{r^2}\, r^2\sin(\varphi)\, dr\, d\varphi\, d\theta = 4\pi.$$

Enfin, on se ramène au cas $d = 3$ lorsque $d \geqslant 3$:

$$\begin{aligned}\int\cdots\int_{x_1^2+\cdots+x_d^2\leqslant 1} \frac{1}{x_1^2+\cdots+x_d^2}\, dx_1\cdots dx_d &\leqslant \int\cdots\int_{x_1^2+\cdots+x_d^2\leqslant 1} \frac{1}{x_1^2+x_2^2+x_3^2}\, dx_1\cdots dx_d \\ &\leqslant \int_{x_4=-1}^{1}\cdots\int_{x_d=-1}^{1} \iiint_{x_1^2+x_2^2+x_3^2\leqslant 1} \frac{1}{x_1^2+x_2^2+x_3^2}\, dx_1\cdots dx_d = 2^{d-1}\pi\end{aligned}$$

car $\{x_1^2+\cdots+x_d^2 \leqslant 1, (x_1,\ldots,x_d) \in \mathbb{R}^d\} \subset \{x_1^2+x_2^3+x_3^2 \leqslant 1, (x_1,x_3,x_d) \in \mathbb{R}^3\} \times [-1,1]^{d-3}$. □

Remarque : pour obtenir $\frac{1}{(2\pi)^d}\int_{T^d}\varphi_{S_n}(t)dt = \mathbb{P}(S_n = 0)$ on pourrait utiliser les coefficients de Fourier de φ_{S_n} mais cela suppose d'introduire les séries de Fourier en dimension d, (cf H. Dym, H.P. McKean, D. Aldous, Y.L. Tong, *Fourier Series and integrals*, Academic Press, 1985).

Commentaire : pour justifier le recasage dans la leçon 235 : interversion de limites et d'intégrales, on note qu'on applique une fois le théorème de Fubini ainsi que deux fois le théorème de Fubini-Tonelli.

3.11 Méthode de Newton

Référence : F. Rouvière, *Petit guide de calcul différentiel*, Cassini, 2014.

Leçons concernées : 218, 223, 226, 228.

Théorème 1. *Soit $f : [c,d] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ qui possède un unique zéro $a \in [c,d]$ et telle que $f' > 0$ sur $[c,d]$. On considère $\varphi := x - \frac{f(x)}{f'(x)}$, et la suite récurrente $x_{n+1} = \varphi(x_n)$. Alors il existe $\alpha > 0$ tel que pour tout $x_0 \in [a-\alpha, a+\alpha]$, $(x_n)_n$ converge quadratiquement vers a.*

Si de plus $f'' > 0$ sur $[c,d]$, alors pour tout $x_0 \in [a,d]$, $(x_n)_n$ est décroissante et converge exactement à l'ordre 2 vers a.

Enfin, si on ne suppose plus $f' > 0$ et qu'on a $f'(a) = 0$, alors il existe $\alpha > 0$ tel que pour tout $x_0 \in [a-\alpha, a+\alpha]$, $(x_n)_n$ converge linéairement vers a.

Démonstration. Étape 1 : on observe que a est un point fixe de φ. On a alors, pour tout $x \in [c,d]$

$$\varphi(x) - a = x - a - \frac{f(x)}{f'(x)} = \frac{-f(x) - (a-x)f'(x)}{f'(x)}.$$

On applique alors la formule de Lagrange à l'ordre 2 à f, en utilisant $f(a) = 0$: il existe z compris strictement entre a et x tel que $-f(x) - (a-x)f'(x) = f(a) - f(x) - (a-x)f'(x) = \frac{1}{2}f''(z)(x-a)^2$. Ainsi :

$$\varphi(x) - a = \frac{1}{2}\frac{f''(z)}{f'(x)}(x-a)^2.$$

Étape 2 : on pose alors $C := \dfrac{1}{2}\dfrac{\max_{x\in[c,d]} |f''(x)|}{\min_{x\in[c,d]} |f'(x)|}$ ($\min_{x\in[c,d]} |f'(x)| > 0$ puisque f' est continue sur $[c,d]$ compact, non nulle) et on obtient, pour tout $x \in [c,d]$,

$$|\varphi(x) - a| \leqslant C|x-a|^2.$$

On prend alors $\alpha > 0$ tel que $C\alpha < 1$ et $I = [a-\alpha, a+\alpha] \subset [c,d]$. On obtient, pour tout $x \in I$, $|\varphi(x) - a| \leqslant C\alpha^2 < \alpha$ et donc I est stable par φ. On peut alors considérer la suite récurrente $x_{n+1} = \varphi(x_n)$ avec $x_0 \in I$, et on a

$$|x_{n+1} - a| \leqslant C|x_n - a|^2$$

d'où

$$C|x_n - a| \leqslant (C|x_0 - a|)^{2^n} \leqslant (C\alpha)^{2^n}$$

et on en déduit la convergence quadratique de x_n vers a avec $C\alpha < 1$.

Étape 3 : on suppose maintenant que $f'' > 0$ sur $[c,d]$. Pour tout $x \in [a,d]$, $f(x) \geqslant 0$ car f est croissante et $f'(x) > 0$ par hypothèse, ainsi,

$$\varphi(x) = x - \frac{f(x)}{f'(x)} \leqslant x$$

et d'autre part, comme on l'a montré plus haut,

$$\varphi(x) - a = \frac{1}{2}\frac{f"(z)}{f'(x)}(x-a)^2 \geqslant 0$$

par hypothèse. Ainsi, $[a,d]$ est stable par φ, et pour tout $x_0 \in [a,d]$, $(x_n)_n$ est décroissante minorée, elle converge donc vers $l \in [a,d]$. Or, $\varphi(l) = l$, donc $f(l) = 0$ et par unicité, $l = a$. La convergence est là encore quadratique puisqu'on a toujours

$$|x_{n+1} - a| \leqslant C|x_n - a|^2.$$

On ne peut pas obtenir de convergence plus que quadratique, en effet, si $a < x_0 \leqslant d$, on a $x_n > a$ pour tout $n \geqslant 0$ par bijectivité de φ, et

$$\frac{x_{n+1} - a}{(x_n - a)^2} = \frac{1}{2}\frac{f"(z_n)}{f'(x_n)}$$

or puisque $a < z_n < x_n$, z_n converge vers a, donc cette dernière fraction converge vers $\frac{1}{2}\frac{f''(a)}{f'(a)} > 0$.

Étape 4 : enfin, si $f'(a) = 0$, par hypothèse sur l'unicité du zéro a, $f' \neq 0$ au voisinage de a. Ainsi, φ est définie au voisinage de a mais a priori pas en a. Mais on a, en a, $f(x) = \frac{(x-a)^2}{2}f''(a) + o((x-a)^2)$ et $f'(x) = (x-a)f''(a) + o((x-a))$, d'où

$$\varphi(x) - a = \frac{(x-a)f'(x) - f(x)}{f'(x)} = \frac{\frac{(x-a)^2}{2}f''(a) + o((x-a)^2)}{(x-a)f''(a) + o((x-a))} = \frac{x-a}{2} + o((x-a))$$

ainsi φ est prolongeable par continuité en a. D'autre part,

$$\varphi'(x) = \frac{f(x)f''(x)}{f'(x)^2} = \frac{\frac{(x-a)^2}{2}f''(a) + o((x-a)^2)}{((x-a)f''(a) + o((x-a)))^2}(f''(a) + o(1)) = \frac{1}{2} + o(1)$$

donc par le théorème de la limite de la dérivée, φ est de classe $\mathcal{C}^1$ au voisinage de a et vérifie $\varphi'(a) = 1/2$. Ainsi, il existe $\alpha > 0$ tel que $|\varphi'| \leqslant k < 1$ sur $[a-\alpha, a+\alpha]$ et l'inégalité des accroissements finis nous assure que $[a-\alpha, a+\alpha]$ est stable par φ et que toute suite $(x_n)_n$ avec $x_0 \in [a-\alpha, a+\alpha]$, vérifie

$$|x_{n+1} - a| \leqslant k|x_n - a|$$

et on en déduit la convergence linéaire de x_n vers a. □

Remarque. Pour justifier la convergence exactement quadratique : si par l'absurde on avait de la convergence d'ordre $m \geqslant 3$, on aurait

$$|x_{n+1} - a| \leqslant C'|x_n - a|^m$$

et donc

$$\frac{|x_{n+1} - a|}{|x_n - a|^2} \leqslant C'|x_n - a|^{m-2}$$

qui tend vers 0 en $+\infty$.

3.12 Nombre de zéros d'une équation différentielle

Référence : H. Queffélec, C. Zuily, *Éléments d'analyse*, Dunod, 2002.

Leçons concernées : 220, 221, 224.

Théorème 1. *Soit $a \in \mathbb{R}$ et $q \in \mathcal{C}^1([a,+\infty[)$ avec $q > 0$ telle que $\int_a^{+\infty} \sqrt{q(u)}\ du = +\infty$ et $q'(x) = o(q^{3/2}(x))$ quand $x \to +\infty$. Alors si on considère y une solution réelle non nulle de l'équation $y'' + qy = 0$ sur $[a,+\infty[$ et $N(x)$ le nombre de zéros de y sur $[a,x]$, alors*

$$N(x) \underset{\infty}{\sim} \frac{1}{\pi} \int_a^x \sqrt{q(u)}\ du.$$

On a besoin du :

Lemme 2. *Soit $y_1, y_2 \in \mathcal{C}^1([a,+\infty[)$ sans zéros communs. Si $y_1(a) + iy_2(a) = r_0 e^{i\theta_0}$ alors il existe $r, \theta \in \mathcal{C}^1([a,+\infty[)$ telles que $y_1 = r\cos(\theta)$ et $y_2 = r\sin(\theta)$ où $r = \sqrt{y_1^2 + y_2^2}$ et $\theta(x) = \theta_0 + \int_a^x \frac{w(t)}{r^2(t)}\ dt$ où $w = y_1 y_2' - y_2 y_1'$.*

Démonstration. On pose $\varphi = y_1 + iy_2$ qui ne s'annule pas par hypothèse, on considère alors $\psi(x) = \int_a^x \frac{\varphi'(t)}{\varphi(t)}\ dt + \log(r_0) + i\theta_0$. On a $(\varphi e^{-\psi})' = (\varphi' - \varphi\psi')e^{-\psi} = 0$ et donc pour tout $x \geqslant a$, $\varphi(x)e^{-\psi(x)} = \varphi(a)e^{-\psi(a)} = r_0 e^{i\theta_0} r_0^{-1} e^{-i\theta_0} = 1$. Ainsi, $y_1 + iy_2 = \varphi = e^{\psi} = re^{i\theta}$ où $r = \sqrt{y_1^2 + y_2^2}$ et $\theta = \Im(\psi)$. Enfin,

$$\begin{aligned}
\psi(x) &= \log(r_0) + i\theta_0 + \int_a^x \frac{y_1'(t) + iy_2'(t)}{y_1(t) + iy_2(t)}\ dt \\
&= \log(r_0) + i\theta_0 + \int_a^x \frac{(y_1'(t) + iy_2'(t))(y_1(t) - iy_2(t))}{r^2(t)}\ dt \\
&= \log(r_0) + \int_a^x \frac{y_1'(t)y_1(t) + y_2(t)y_2'(t)}{r^2(t)}\ dt + i\theta_0 + i\int_a^x \frac{w(t)}{r^2(t)}\ dt
\end{aligned}$$

d'où le résultat. □

Démonstration (Théorème). Étape 1 : on commence par considérer $\tau(x) = \int_a^x \sqrt{q(u)}\ du$ pour $x \geqslant a$. La fonction τ est ainsi par hypothèse de classe $\mathcal{C}^1$ strictement croissante de $[a,+\infty[$ dans $[0,+\infty[$, qui est donc bijective. On pose alors $Y = y \circ \tau^{-1}$, c'est-à-dire $y(x) = Y(\tau(x))$ pour tout $x \geqslant a$. On a alors

$$\begin{aligned}
y'(x) &= \tau'(x)Y'(\tau(x)) = \sqrt{q(x)}Y'(\tau(x)) \\
y''(x) &= \frac{q'(x)}{2\sqrt{q(x)}}Y'(\tau(x)) + q(x)Y''(\tau(x))
\end{aligned}$$

ainsi,

$$y''(x)+q(x)y(x)=q(x)Y''(\tau(x))+\frac{q'(x)}{2\sqrt{q(x)}}Y'(\tau(x))+q(x)Y(\tau(x))=0$$

c'est-à-dire que, si on pose $\varphi(t)=\dfrac{q'(\tau^{-1}(t))}{2q^{3/2}(\tau^{-1}(t))}$, Y est solution sur $[0,+\infty[$ de

$$Y''+\varphi Y'+Y=0.$$

Étape 2 : on remarque maintenant que Y et Y' n'ont pas de zéro commun puisque sinon, par unicité de la solution, on aurait $Y\equiv 0$ et donc $y\equiv 0$ ce qui n'est pas possible par hypothèse. On peut alors appliquer le lemme et écrire $Y=r\sin(\theta)$ et $Y'=r\cos(\theta)$ avec $r,\theta\in\mathcal{C}^1([a,+\infty[)$. On obtient successivement

$$\begin{aligned}Y'&=r'\sin(\theta)+r\theta'\cos(\theta)=r\cos(\theta)\\ Y''&=r'\cos(\theta)-r\theta'\sin(\theta)=-\varphi r\cos(\theta)-r\sin(\theta).\end{aligned}$$

On multiplie la première égalité par $\cos(\theta)$ et la seconde par $-\sin(\theta)$, on ajoute les deux et on obtient : $r\theta'=r(1+\varphi\cos(\theta)\sin(\theta))$, c'est-à-dire $\theta'=1+\varphi\cos(\theta)\sin(\theta)$ et donc $|\theta'(t)-1|\leqslant\frac{1}{2}|\varphi(x)|$. Ainsi, puisque par hypothèse $\varphi(x)\underset{x\to+\infty}{\longrightarrow}0$, $\theta'(x)\underset{x\to+\infty}{\longrightarrow}1$ et donc par intégration des équivalents, $\theta(t)\sim t$ en $+\infty$.

Étape 3 : on note alors $M(t)$ le nombre de zéros de Y sur $[0,t]$. On commence par montrer par l'absurde que $M(t)<+\infty$ pour tout t. Si $M(t_0)=+\infty$, alors l'ensemble des zéros de Y dans $[0,t_0]$ admet un point d'accumulation u. Soit $(u_n)_n$ une suite de zéros de Y qui tend vers u par valeurs différentes, alors

$$0=\frac{Y(u_n)-Y(u)}{u_n-u}\underset{n\to+\infty}{\longrightarrow}Y'(u)$$

ce qui contredit le fait que Y et Y' n'aient pas de zéro commun.

Étape 4 : maintenant, soit $t_0\geqslant 0$ tel que pour tout $t\geqslant t_0$, $\theta'(t)>0$, alors $M(t)=\mathrm{Card}\{u\in[0,t_0],Y(u)=0\}+\mathrm{Card}\{u\in[t_0,t],\sin(\theta(u))=0\}$. Or, puisque θ est un $\mathcal{C}^1$ difféomorphisme sur $[t_0,+\infty[$,

$$\begin{aligned}\mathrm{Card}\{u\in[t_0,t],\sin(\theta(u))=0\}&=\mathrm{Card}\{v\in[\theta(t_0),\theta(t)],\sin(v)=0\}\\ &=\mathrm{Card}\{k\in\mathbb{Z},\theta(t_0)\leqslant k\pi\leqslant\theta(t)\}=\left\lfloor\frac{\theta(t)}{\pi}\right\rfloor-\left\lfloor\frac{\theta(t_0)}{\pi}\right\rfloor\underset{\infty}{\sim}\frac{t}{\pi}\end{aligned}$$

grâce à $\theta(t)\sim t$ en $+\infty$. Ainsi, $M(t)\sim\dfrac{t}{\pi}$ en $+\infty$.

Enfin, il est clair que $N(x)=M(\tau(x))$ et donc par composition des équivalents, on obtient le résultat. □

Remarque. Si on considère $a = 1$ et $q(x) = \frac{1}{4x^2}$, on a bien $\int_1^{+\infty} \sqrt{q(u)}\, du = +\infty$ mais $q'(x)q^{-3/2}(x) = -4$ et la solution de $y'' + \frac{1}{4x^2} y = 0$ est $y(x) = \sqrt{x}(a + b\log(x))$ qui a au plus un zéro sur $[1, +\infty[$.

Commentaire : c'est un peu long, on peut éventuellement passer rapidement sur le lemme (voire ne pas le faire), et simplement justifier que M est fini partout parce que la solution n'est pas nulle.

3.13 Optimisation dans un Hilbert

Référence : P.G. Ciarlet, *Introduction à l'analyse numérique matricielle et à l'optimisation*, Masson, 1982,
G. Allaire, *Analyse numérique et optimisation*, Éditions de l'École Polytechnique, 2005 [1].

Leçons concernées : 205, 208, 213, 219, 229, 253, *201, 203.*

Théorème 1 (Banach-Alaoglu)**.** *Soit H un espace de Hilbert séparable, et soit $(T_n)_n$ une suite bornée de H', alors il existe $T \in H'$ et une extractrice φ tels que $(T_{\varphi(n)})_n$ converge faiblement vers T, c'est-à-dire que pour tout $x \in H$,*

$$T_{\varphi(n)}(x) \underset{n\to+\infty}{\longrightarrow} T(x).$$

Démonstration. Étape 1 : on se donne $(x_k)_k$ une suite dense de H. Pour tout $k \in \mathbb{N}$, $(T_n(x_k))_{n\in\mathbb{N}}$ est bornée par $M\,||x_k||$, où on a noté $M = \sup_{n\in\mathbb{N}} ||T_n||$. Le procédé d'extraction diagonale nous assure ainsi l'existence d'une sous-suite de $(T_n)_n$ que l'on notera encore $(T_n)_n$ telle que pour tout $k \in \mathbb{N}$, $(T_n(x_k))_{n\in\mathbb{N}}$ converge vers une limite notée $T(x_k)$.

Étape 2 : on montre que $(T_n(x))_n$ converge pour tout $x \in H$. Soit $\varepsilon > 0$, et soit x_k tel que $||x - x_k|| < \varepsilon$. Pour $p, q \geqslant 0$

$$|T_p(x) - T_q(x)| \leqslant |T_p(x) - T_p(x_i)| + |T_p(x_i) - T_q(x_i)| + |T_q(x_i) - T_q(x)|,$$

or, $|T_p(x) - T_p(x_i)| \leqslant M||x - x_i||$, $|T_q(x) - T_q(x_i)| \leqslant M||x - x_i||$, et par le point précédent, il existe $N \geqslant 0$ tel que pour $p, q \geqslant N$, $|T_p(x_i) - T_q(x_i)| < \varepsilon$. Ainsi, pour $p, q \geqslant N$,

$$|T_p(x) - T_q(x)| < (2M + 1)\varepsilon.$$

La suite $(T_n(x))_n$ est donc de Cauchy dans $\mathbb{R}$ et converge ainsi vers une limite notée $T(x)$.

Étape 3 : comme limite de fonction linéaire, T est linéaire. D'autre part, pour $x \in H$,

$$|T(x)| = |\lim_{n\to+\infty} T_n(x)| \leqslant M||x||$$

et donc $T \in H'$, ce qui conclut la preuve du théorème. □

Théorème 2. *Soit H un espace de Hilbert séparable, et soit $J : H \to \mathbb{R}$ un fonction continue, convexe, et coercive, au sens où*

$$\lim_{||x||\to+\infty} J(x) = +\infty.$$

Alors il existe un minimum de J sur H.

1. La démonstration n'est faite de cette façon dans aucune des références, il faut adapter. Se reporter au développement rédigé d'Antoine Mouzard. Merci également à Michel Nassif pour ce développement.

Démonstration. Étape 1 : soit $(u_n)_n$ une suite minimisante. Puisque H est non vide, $\inf_{x\in H} J(x) < +\infty$, et donc par coercivité de J, $(u_n)_n$ est bornée. Ainsi, d'après le théorème de Banach-Alaoglu et le théorème de Riesz, quitte à extraire, $(u_n)_n$ converge faiblement vers $u \in H$.

Étape 2 : on prend $\alpha > \inf_{x\in H} J(x)$ et on pose $C_\alpha := \{x \in H \mid J(x) \leqslant \alpha\}$. La partie C_α est fermée car J est continue et convexe car J est convexe. Puisque $\lim J(u_n) = \inf_{x\in H} J(x) < \alpha$, $u_n \in C_\alpha$ à partir d'un certain rang, et en particulier C_α est non vide. On applique alors le théorème de projection à C_α sur H, et on note P_α le projection. À partir d'un certain rang, d'après le théorème de projection,

$$< u - P_\alpha(u), u_n - P_\alpha(u) > \leqslant 0.$$

On passe alors à la limite pour obtenir $||u - P_\alpha(u)||^2 = 0$, et donc $u = P_\alpha(u) \in C_\alpha$, c'est-à-dire que $J(u) \leqslant \alpha$. On a donc,

$$\forall \alpha > \inf_{x\in H} J(x), \quad J(u) \leqslant \alpha$$

et ainsi $J(u) = \inf_{x\in H} J(x)$. □

Remarque. L'hypothèse H séparable n'est pas nécessaire, puisque dans la preuve de la compacité faible on peut considérer $E = \overline{\text{Vect}(u_n, n \in \mathbb{N})}$ qui est un Hilbert séparable et conclure avec $H = E \oplus E^\perp$. On peut également minimiser J sur K un convexe fermé non vide au lieu de H, il faut pour cela montrer que la limite faible obtenue est dans K, ce qui se fait avec le théorème de la projection, de la même manière que dans l'étape 2 de la preuve.

Application 3. *Soit $f \in L^2(0,1)$, et $p \geqslant 1$. Alors il existe une unique fonction $u \in H_0^1(0,1)$ telle que*

$$-u'' + |u|^{p-1}u = f \tag{1}$$

dans $L^2(0,1)$.

Démonstration. On introduit la fonctionnelle $J : H_0^1(0,1) \to \mathbb{R}$ définie par

$$J(u) = \int_0^1 \Big(\frac{1}{2}u'(x)^2 + \frac{|u(x)|^{p+1}}{p+1} - f(x)u(x)\Big)dx$$

pour $u \in H_0^1$. On remarque tout d'abord que J est différentiable de différentielle [2]

$$dJ(u)(v) = \int_0^1 \Big(u'(x)v'(x) + |u(x)|^{p-1}u(x)v(x) - f(x)u(x)\Big)dx.$$

En particulier J est continue. D'autre part, puisque la dérivation est linéaire et que toutes les fonctions de u et de u' intervenant dans l'intégrale qui définit J sont convexes, J est

2. Cela demande un calcul non évident.

convexe. On montre alors que J est strictement convexe. Soit $\lambda \in]0,1[$, et $u, v \in H_0^1$. Si $J(\lambda u + (1-\lambda)v) = \lambda J(u) - (1-\lambda)J(v)$, alors puisque J est convexe, en particulier,

$$\int_0^1 |\lambda u(x) + (1-\lambda)v(x)|^{p+1} dx = \int_0^1 \lambda |u(x)|^{p+1} + (1-\lambda)|v(x)|^{p+1} dx$$

ce qui implique, par convexité de la fonction $t \mapsto |t|^{p+1}$ (si l'intégrale d'une fonction positive est nulle alors la fonction est nulle presque partout), que presque partout,

$$|\lambda u(x) + (1-\lambda)v(x)|^{p+1} = \lambda |u(x)|^{p+1} + (1-\lambda)|v(x)|^{p+1}$$

et donc, par strict convexité de $t \mapsto |t|^{p+1}$, $u = v$ presque partout, et on a montré la strict convexité de J.

On voit que $u \in H_0^1$ est solution de (1) si et seulement si $dJ(u)(v) = 0$, et donc, par convexité de J, $u \in H_0^1$ est solution de (1) si et seulement si u est un minimum de J sur H_0^1. Si on montre que J est coercive, on obtient alors l'existence en appliquant le théorème précédent, et l'unicité par strict convexité.

On a en effet, par inégalité de Cauchy-Schwarz, puis par inégalité de Poincaré,

$$J(u) \geqslant \int_0^1 \frac{1}{2} u'(x)^2 dx - ||u||_2 ||f||_2 \geqslant C||u||_{H^1}^2 - ||f||_2 ||u||_{H^1} \underset{||u|| \to +\infty}{\longrightarrow} +\infty.$$

□

Commentaire : on montre d'abord le théorème d'optimisation, puis le théorème de Banach-Alaoglu, et si il reste du temps on présente très succinctement l'application.

3.14 Processus de Galton-Watson

Références : W. Appel, *Probabilités pour les non probabilistes*, H & K, 2e édition. Plan de leçon Nassif-Garéneaux.

Leçons concernées : 223, 226, 260, 264, *229, 243, 253.*

Soit $(X_i^n)_{(i,n)}$ une suite double de variables aléatoires indépendantes et identiquement distribuées de même loi qu'une variable aléatoire X à valeurs dans $\mathbb{N}$. On note $p_k = \mathbb{P}(X = k)$ pour $k \in \mathbb{N}$ et on suppose $0 < p_0 = \mathbb{P}(X = 0) < 1$. Soit $Z_0 = 1$ et pour tout $n \geqslant 0$,

$$Z_{n+1} = \sum_{i=1}^{Z_n} X_i^n.$$

La suite (Z_n) représente le nombre d'individus au temps n d'une population issue d'un seul individu. On suppose que X est intégrable et on note $m = \mathbb{E}[X]$ et G la série génératrice de X. Enfin, soit M l'évènement $\{\exists n \geqslant 1, Z_n = 0\}$ d'extinction de la population.

Théorème 1. *On distingue deux cas :*

(i) si $m \leqslant 1$, alors $\mathbb{P}(M) = 1$

(ii) si $m > 1$, alors $\mathbb{P}(M)$ est l'unique point fixe de G sur $]0, 1[$.

Lemme 2. *Sur $]0, 1[$, G est*

(i) strictement croissante

(ii) convexe

(iii) strictement convexe si et seulement si $p_0 + p_1 = 1$.

Démonstration. On a, pour $t \in]-1, 1[$, $G(t) = \sum_{k\geqslant 0} p_k t^k$, $G'(t) = \sum_{k\geqslant 1} p_k k t^{k-1}$ et $G''(t) = \sum_{k\geqslant 2} p_k k(k-1)t^{k-2}$.

(i) Puisque $p_0 < 1$, il existe $k \geqslant 1$ tel que $p_k > 0$ et ainsi, pour $t \in]0, 1[$, $G'(t) \geqslant p_k k t^{k-1} > 0$.

(ii) Il est clair que $G'' \geqslant 0$ sur $]0, 1[$.

(iii) Enfin, si $p_0 + p_1 < 1$, alors il existe $k \geqslant 2$ tel que $p_k > 0$ et ainsi, pour $t \in]0, 1[$, $G''(t) \geqslant p_k k(k-1)t^{k-2} > 0$. Si $p_0 + p_1 = 1$, $G(t) = p_0 + p_1 t$ n'est pas strictement convexe.

□

Lemme 3. *On note G_n la série génératrice de Z_n. Alors, pour tout $n \geqslant 0$,*

$$G_{n+1} = G_n \circ G$$

et donc $G_n = G^n$.

Démonstration. Soit $n \geqslant 0$. Pour $l \geqslant 0$, on note $S_l^n := \sum_{i=1}^{l} X_i^n$. On a alors $G_{S_l^n} = G^l$ par indépendance. On a, pour $k \in \mathbb{N}$,

$$\mathbb{P}(Z_{n+1} = k) = \sum_{l=0}^{+\infty} \mathbb{P}(Z_{n+1} = k, Z_n = l) = \sum_{l=0}^{+\infty} \mathbb{P}(S_l^{n+1} = k, Z_n = l) = \sum_{l=0}^{+\infty} \mathbb{P}(S_l^{n+1} = k)\mathbb{P}(Z_n = l)$$

par indépendance de Z_n et S_l^{n+1}.

Soit maintenant $t \in [-1, 1]$, on a

$$\begin{aligned} G_{n+1}(t) &= \sum_{k=0}^{+\infty} \mathbb{P}(Z_{n+1} = k)t^k = \sum_{k=0}^{+\infty}\sum_{l=0}^{+\infty} \mathbb{P}(S_l^{n+1} = k)\mathbb{P}(Z_n = l)t^k \\ &= \sum_{l=0}^{+\infty} \mathbb{P}(Z_n = l) \sum_{k=0}^{+\infty} \mathbb{P}(S_l^{n+1} = k)t^k = \sum_{l=0}^{+\infty} \mathbb{P}(Z_n = l)G_{S_l^{n+1}}(t) \\ &= \sum_{l=0}^{+\infty} \mathbb{P}(Z_n = l)(G(t))^l = G_n \circ G(t) \end{aligned}$$

par Fubini. On conclut avec $G_0 = \mathrm{id}$. □

Lemme 4. *$\mathbb{P}(M)$ est le plus petit point fixe de G sur $[0, 1]$.*

Démonstration. Soit $x_n = \mathbb{P}(Z_n = 0)$. Puisque les intervalles $\{Z_n = 0\}$ sont croissants, on a $\mathbb{P}(M) = \mathbb{P}(\bigcup_{n\geqslant 0}\{Z_n = 0\}) = \lim_{n\to+\infty} \mathbb{P}(Z_n = 0) = \lim_{n\to+\infty} x_n$. Et de plus, (x_n) est croissante.

D'autre part, $x_{n+1} = \mathbb{P}(Z_{n+1} = 0) = G_{n+1}(0) = G^{n+1}(0) = G(G^n(0)) = G(x_n)$.

Enfin, soit α le plus petit point fixe de G sur $[0, 1]$ qui existe puisque $G(1) = 1$. Alors, puisque G est croissante sur $[0, 1]$ et vérifie $G(0) > 0$, la fonction G laisse stable l'intervalle $[0, \alpha]$. Ainsi, puisque $x_0 = 0$, $(x_n)_n$ est croissante majorée par α, donc elle converge et d'après la relation de récurrence vérifiée, la limite est un point fixe de G sur $[0, \alpha]$, c'est donc α. □

Démonstration (Théorème). Si $p_0 + p_1 = 1$, alors G est affine, et donc, puisque $p_0 > 0$, G admet au plus un point fixe sur $[0, 1]$, qui est donc 1. On remarque qu'alors $m = \mathbb{E}[X] = p_1 < 1$.

On suppose maintenant $p_0 + p_1 < 1$ et donc G est strictement convexe.

(i) Si $m \leqslant 1$, alors pour tout $u \in]0, 1[$, $G'(u) < G'(1) = m \leqslant 1$ et donc pour $t \in]0, 1[$,

$$1 - G(t) = \int_t^1 G'(u)\, du < \int_t^1 du = 1 - t$$

donc $G(t) > t$ et 1 est l'unique point fixe de G.

(ii) Si $m > 1$, pour $t \in [0,1]$, on pose $F(t) = G(t) - t$, on a alors $F'(t) = G'(t) - 1$. Puisque G' est strictement croissante sur $]0,1[$, F' l'est aussi et puisque $F'(0) = G'(0) - 1 = p_1 - 1 < 0$ et $F'(1) = G'(1) - 1 = m - 1 > 0$, F' s'annule en un unique point $\beta \in]0,1[$. On en déduit que F est strictement décroissante sur $]0,\beta[$, et strictement croissante sur $]\beta,0[$, avec $F(0) = p_0 > 0$, et $F(1) = 0$, on en déduit que $F(\beta) < 0$ et donc F s'annule en un unique point de $]0,\beta[\subset]0,1[$.

t	0		β		1
$F(t)$	$p_0 > 0$	$\searrow$	$F(\beta) < 0$	$\nearrow$	0
$F'(t)$	$p_1 - 1 < 0$	$-$	0	$+$	$m - 1 > 0$

□

Commentaire : on fait la démonstration du lemme le plus adapté à la leçon, puis celle du théorème, et si il reste du temps on démontre les autres lemmes.

3.15 Théorème central limite

Référence : H. Queffélec, C. Zuily, *Éléments d'analyse*, Dunod, 2002.

Leçons concernées : 218, 260, 261, 262, 263.

Théorème 1 (Central limite)**.** *Soit $(X_n)_n$ une suite de variables aléatoires indépendantes et identiquement distribuées admettant un moment d'ordre 2. On note $m = \mathbb{E}[X_1]$ et $\sigma^2 = \mathrm{Var}(X_1)$. Alors si $S_n = \sum_{k=1}^n X_n$,*

$$\frac{S_n - nm}{\sqrt{n}\sigma} \xrightarrow{\mathcal{L}} X$$

où $X \sim \mathcal{N}(0,1)$.

Lemme 2. *Soit $(z_n)_n$ une suite de nombres complexes de limite $z \in \mathbb{C}$, alors*

$$\left(1 + \frac{z_n}{n}\right)^n \underset{n\to+\infty}{\longrightarrow} e^z.$$

Démonstration. Pour $n \geqslant 0$, on a,

$$\exp(z_n) - \left(1 + \frac{z_n}{n}\right)^n = \sum_{k=0}^{+\infty} \frac{z_n^k}{k!} - \sum_{k=0}^{n} \binom{n}{k} \left(\frac{z_n}{n}\right)^k = \sum_{k=0}^{+\infty} a_k^{(n)} z_n^k$$

où

$$a_k^{(n)} = \begin{cases} \frac{1}{k!} & k \geqslant n+1 \\ \frac{1}{k!}\left(1 - \frac{n(n-1)\cdots(n-k+1)}{n^k}\right) & k \leqslant n \end{cases}$$

ainsi $a_k^{(n)} \geqslant 0$ pour tout n, k, et donc,

$$\left|\exp(z_n) - \left(1 + \frac{z_n}{n}\right)^n\right| \leqslant \sum_{k=0}^{+\infty} a_k^{(n)} |z_n|^k = \exp(|z_n|) - \left(1 + \frac{|z_n|}{n}\right)^n.$$

Enfin, avec pour $x \geqslant 0$, $\ln(1+x) \geqslant x - \frac{x^2}{2}$ et $1 - e^{-x} \leqslant x$,

$$\begin{aligned} \left|\exp(z_n) - \left(1 + \frac{z_n}{n}\right)^n\right| &\leqslant \exp(|z_n|) - \exp\left(n \ln\left(1 + \frac{|z_n|}{n}\right)\right) \\ &\leqslant \exp(|z_n|) - \exp\left(n\left(\frac{|z_n|}{n} - \frac{|z_n|^2}{2n^2}\right)\right) \\ &= \exp(|z_n|)\left(1 - \exp\left(-\frac{|z_n|^2}{2n}\right)\right) \\ &\leqslant \exp(|z_n|)\frac{|z_n|^2}{2n}. \end{aligned}$$

On peut alors conclure :

$$\begin{aligned}\left|\exp(z) - \left(1+\frac{z_n}{n}\right)^n\right| &\leqslant |\exp(z) - \exp(z_n)| + \left|\exp(z_n) - \left(1+\frac{z_n}{n}\right)^n\right| \\ &\leqslant |\exp(z) - \exp(z_n)| + \exp(|z_n|)\frac{|z_n|^2}{2n} \underset{n\to+\infty}{\longrightarrow} 0.\end{aligned}$$

□

Démonstration (Théorème). On peut sans perte de généralité se ramener au cas $m = 0$ et $\sigma = 1$. On utilise le théorème de Lévy et on cherche donc à montrer que $\varphi_{\frac{S_n}{\sqrt{n}}}(t) \to e^{-t^2/2}$ pour tout $t \in \mathbb{R}$.

On note $\varphi := \varphi_{X_1}$. Puisque X_1 admet un moment d'ordre 2, φ est de classe $\mathcal{C}^2$ et vérifie : $\varphi'(0) = \mathbb{E}[iX_1] = 0$ et $\varphi''(0) = \mathbb{E}[-X_1^2] = -1$. On a donc, par développement de Taylor à l'ordre 2 en 0, pour tout $t \in \mathbb{R}$,

$$\varphi(t) = 1 - \frac{t^2}{2} + o(t^2).$$

On a d'autre part, par indépendance et identique distribution,

$$\begin{aligned}\varphi_{\frac{S_n}{\sqrt{n}}}(t) &= \mathbb{E}\left[\prod_{k=1}^n e^{itX_k/\sqrt{n}}\right] = \prod_{k=1}^n \mathbb{E}\left[e^{itX_k/\sqrt{n}}\right] \\ &= \mathbb{E}\left[e^{itX_1/\sqrt{n}}\right]^n = \varphi\left(\frac{t}{\sqrt{n}}\right)^n.\end{aligned}$$

Ainsi, d'après le développement limité de φ en 0,

$$\varphi_{\frac{S_n}{\sqrt{n}}}(t) = \left(1 - \frac{t^2}{2n} + o(\frac{1}{n})\right)^n.$$

et on conclut avec le lemme. □

Application 3. *On a,*

$$\lim_{n\to+\infty} e^{-n}\sum_{k=0}^n \frac{n^k}{k!} = \frac{1}{2}.$$

Démonstration. Soit $(X_i)_i$ une suite de variables aléatoires i.i.d. de loi de Poisson $\mathcal{P}(1)$, et $S_n = X_1 + \cdots + X_n$ qui suit donc une loi de Poisson $\mathcal{P}(n)$. On a $\mathbb{E}[X_1] = \mathrm{Var}(X_1) = 1$ et on applique le théorème central limite pour obtenir :

$$Z_n = \frac{S_n - n}{\sqrt{n}} \xrightarrow{\mathcal{L}} Z \sim \mathcal{N}(0,1).$$

Or on remarque que

$$e^{-n}\sum_{k=0}^{n}\frac{n^k}{k!}=\sum_{k=0}^{n}\mathbb{P}(S_n=k)=\mathbb{P}(S_n\leqslant n)=\mathbb{P}(Z_n\leqslant 0)$$

et donc par convergence des fonctions de répartitions on obtient

$$\lim_{n\to+\infty}e^{-n}\sum_{k=0}^{n}\frac{n^k}{k!}=\lim_{n\to+\infty}\mathbb{P}(Z_n\leqslant 0)=\mathbb{P}(Z\leqslant 0)=\frac{1}{2}$$

puisque Z est symétrique. □

Proposition 4. *Si $X\sim\mathcal{N}(0,1)$, alors pour tout $t\in\mathbb{R}$, $\varphi_X(t)=e^{-t^2/2}$.*

Démonstration. On a

$$\varphi_X(t)=\frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}}e^{-itx}e^{-x^2/2}dx.$$

On applique alors le théorème de dérivation sous l'intégrale pour obtenir que φ_X est de classe $\mathcal{C}^1$ sur $\mathbb{R}$, et que

$$\varphi'_X(t)=\frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}}-ixe^{-itx}e^{-x^2/2}dx=\frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}}ie^{-itx}(-xe^{-x^2/2})dx=-\frac{t}{\sqrt{2\pi}}\int_{\mathbb{R}}e^{-itx}e^{-x^2/2}dx$$

par intégration par parties. Ainsi φ_X vérifie $\varphi'_X(t)-t\varphi_X(t)=0$ pour tout $t\in\mathbb{R}$ et donc $\varphi_X(t)=e^{-t^2/2}$ puisque $\varphi_X(0)=1$. □

3.16 Théorème d'Abel angulaire et théorème taubérien faible

Référence : X. Gourdon, *Les maths en tête, Analyse*, Ellipses, 2008.

Leçons concernées : 230, 235, 241, 243.

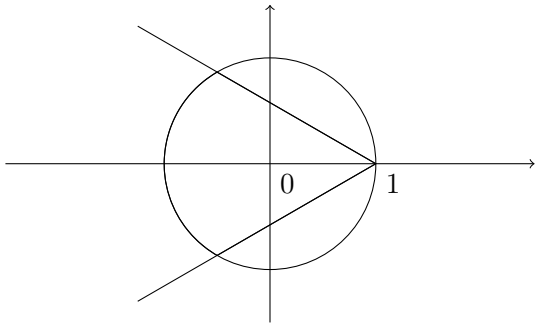
Théorème 1 (Abel angulaire)**.** *Soit $\sum_{n\geqslant 0} a_n z^n$ une série entière de rayon de convergence $R \geqslant 1$ telle que $\sum_{n\geqslant 0} a_n$ converge. On note f la somme de cette série entière sur le disque unité $\mathbb{D}$. Pour $\theta_0 \in [0, \pi/2[$, on note*

$$\Delta_{\theta_0} := \left\{ z \in \mathbb{C}, \exists \rho > 0, \theta \in [-\theta_0, \theta_0], z = 1 - \rho e^{i\theta} \right\}$$

alors

$$\lim_{\substack{z \to 1 \\ z \in \Delta_{\theta_0}}} f(z) = \sum_{n\geqslant 0} a_n.$$

Le domaine Δ_{θ_0} est représenté ici :



Démonstration. On note $S = \sum_{k\geqslant 0} a_k$, $S_n = \sum_{k=0}^{n} a_k$ les sommes partielles et $R_n = S - S_n$ les restes. En remarquant que pour tout $n \geqslant 0$ $a_n = R_{n-1} - R_n$, (en convenant que $R_{-1} = 0$), on a, pour tout $|z| < 1$,

$$\begin{aligned}\Big(\sum_{n=0}^{N} a_n z^n \Big) - S_N &= \sum_{n=0}^{N} (R_{n-1} - R_n)(z^n - 1) = \sum_{n=0}^{N-1} R_n (z^{n+1} - 1) - \sum_{n=0}^{N} R_n (z^n - 1) \\ &= \sum_{n=0}^{N-1} R_n (z^{n+1} - z^n) - R_N (z^N - 1) = (z-1) \sum_{n=0}^{N-1} R_n z^n - R_N (z^N - 1)\end{aligned}$$

et donc, en faisant tendre N vers $+\infty$, on obtient, puisque la série $\sum R_n z^n$ est absolument convergente sur $\mathbb{D}$,

$$f(z) - S = (z-1) \sum_{n=0}^{+\infty} R_n z^n.$$

Il s'agit alors de majorer cette quantité. Soit $\varepsilon > 0$ et $N \geqslant 0$ tel que pour tout $n > N$, $|R_n| < \varepsilon$. On observe alors que d'après la relation précédente, pour tout $|z| < 1$,

$$|f(z) - S| \leqslant |z-1| \left| \sum_{n=0}^{N} R_n z^n \right| + |z-1| \varepsilon \sum_{n=N}^{+\infty} |z|^n \leqslant |z-1| \sum_{n=0}^{N} |R_n| + \varepsilon \frac{|z-1|}{1-|z|}.$$

On se donne alors $z \in \Delta_{\theta_0}$, qui s'écrit donc $z = 1 - \rho e^{i\theta}$ avec $\rho > 0$ et $\theta \in [-\theta_0, \theta_0]$. On a $|z|^2 = (1 - \rho\cos(\theta))^2 + \rho^2 \sin(\theta)^2 = 1 - 2\rho\cos(\theta) + \rho^2$ et donc pour $\rho \leqslant \cos(\theta_0)$,

$$\frac{|z-1|}{1-|z|} = \frac{|z-1|}{1-|z|^2}(1+|z|) = \frac{\rho}{2\rho\cos(\theta) - \rho^2}(1+|z|) \leqslant \frac{2}{2\cos(\theta) - \rho} \leqslant \frac{2}{2\cos(\theta_0) - \cos(\theta_0)} = \frac{2}{\cos(\theta_0)}$$

par hypothèse sur ρ et par décroissance du cosinus sur $[0, \pi/2[$. On choisit alors $\alpha > 0$ tel que $\alpha \sum_{n=0}^{N} |R_n| < \varepsilon$ alors pour tout $z \in \Delta_{\theta_0}$ tel que $|z-1| \leqslant \min(\alpha, \cos(\theta_0))$,

$$|f(z) - S| \leqslant \varepsilon + \varepsilon \frac{2}{\cos(\theta_0)} = \varepsilon\Big(1 + \frac{2}{\cos(\theta_0)}\Big)$$

d'où le résultat. □

Application 2. *Le théorème d'Abel angulaire appliqué à la série entière* $\sum_{n\geqslant 1} \frac{(-1)^{n+1}}{n} z^n = \log(1+z)$ *sur* $\mathbb{D}$ *avec* $\sum_{n\geqslant 1} \frac{(-1)^{n+1}}{n}$ *convergente nous donne*

$$\sum_{n\geqslant 1} \frac{(-1)^{n+1}}{n} = \log(2).$$

De même,

$$\sum_{n\geqslant 1} \frac{(-1)^n}{2n+1} = \lim_{x\to 1} \sum_{n\geqslant 1} \frac{(-1)^n}{2n+1} x^n = \lim_{x\to 1} \arctan(x) = \frac{\pi}{4}.$$

Remarque. La réciproque du théorème est fausse comme le montre

$$\sum_{n\geqslant 0} (-1)^n z^n = \frac{1}{1+z} \underset{\substack{z\to 1 \\ |z|<1}}{\longrightarrow} \frac{1}{2}$$

alors que la série $\sum (-1)^n$ diverge. Le théorème suivant donne cependant une réciproque partielle.

Théorème 3 (taubérien faible)**.** *Soit* $\sum_{n\geqslant 0} a_n z^n$ *une série entière de rayon de convergence* $R \geqslant 1$. *On note* f *la somme de cette série entière sur le disque unité. On suppose qu'il existe* $S \in \mathbb{C}$ *tel que*

$$\lim_{\substack{x\to 1 \\ x<1}} f(x) = S.$$

Si $a_n = o(\frac{1}{n})$ *alors* $\sum_{n\geqslant 0} a_n$ *converge et* $\sum_{n\geqslant 0} a_n = S$.

Démonstration. On note $S_n = \sum_{k=0}^{n} a_k$ les sommes partielles. On a, pour $n \geqslant 1$, $x \in]0,1[$,

$$S_n - f(x) = \sum_{k=0}^{n} a_k(1-x^k) - \sum_{k=n+1}^{+\infty} a_k x^k.$$

Or pour $x \in]0,1[$, $(1-x^k) = (1-x)(1+x+\cdots+x^{k-1}) \leqslant k(1-x)$, ainsi,

$$|S_n - f(x)| \leqslant (1-x)\sum_{k=0}^{n} k a_k + \sum_{k=n+1}^{+\infty} \frac{k}{n}|a_k|x^k \leqslant (1-x)Mn + \frac{\sup_{k>n} k|a_k|}{n(1-x)}$$

en notant M un majorant de la suite $(ka_k)_k$ qui converge vers 0 par hypothèse. Soit alors $0 < \varepsilon < 1$. On a donc

$$\left|S_n - f\left(1-\frac{\varepsilon}{n}\right)\right| \leqslant M\varepsilon + \frac{\sup_{k>n} k|a_k|}{\varepsilon}.$$

Soit $N_0 \geqslant 0$ tel que $\sup_{k>N_0} k|a_k| \leqslant \varepsilon^2$, alors pour tout $n \geqslant N_0$,

$$\left|S_n - f\left(1-\frac{\varepsilon}{n}\right)\right| \leqslant \varepsilon(M+1).$$

Par hypothèse, puisque $\left(1-\frac{\varepsilon}{n}\right) \underset{n\to+\infty}{\longrightarrow} 1$, il existe $N_1 \geqslant N_0$ tel que pour tout $n \geqslant N_1$, $\left|f\left(1-\frac{\varepsilon}{n}\right) - S\right| < \varepsilon$. On conclut alors par inégalité triangulaire. □

3.17 Théorème de Fourier-Plancherel

Référence : W. Rudin, *Analyse réelle et complexe*, Dunod, 1998.

Leçons concernées : 201, 202, 207, 234, 235, 250.

Définition 1. Pour $f \in L^1(\mathbb{R})$ on définit sa transformée de Fourier

$$\mathcal{F}(f)(t) = \widehat{f}(t) = \int_{\mathbb{R}} f(x)e^{-ixt}dx.$$

Théorème 2. *Il existe un unique isomorphisme $\mathcal{F} : L^2(\mathbb{R}) \to L^2(\mathbb{R}), f \mapsto \widehat{f}$ qui prolonge la transformée de Fourier sur $L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. De plus, pour tout $f, g \in L^2(\mathbb{R})$, on a $(\widehat{f}, \widehat{g})_{L^2} = 2\pi\,(f, g)_{L^2}$ et si on note, pour $A > 0$,*

$$\varphi_A(t) = \int_{-A}^{A} f(x)e^{-ixt}dx \quad et \quad \psi_A(x) = \frac{1}{2\pi}\int_{-A}^{A} \widehat{f}(t)e^{ixt}dt$$

alors $||\varphi_A - \widehat{f}||_2 \underset{A\to+\infty}{\longrightarrow} 0$ et $||\psi_A - f||_2 \underset{A\to+\infty}{\longrightarrow} 0$.

Lemme 3. *Pour $f \in L^2$, l'application*

$$y \mapsto \Big(\tau_y f : x \mapsto f(y + x)\Big)$$

est uniformément continue de $\mathbb{R}$ dans $L^2(\mathbb{R})$.

Démonstration. Soit $\varepsilon > 0$ et soit $g \in \mathcal{C}_c^0(\mathbb{R})$ telle que $||f - g||_2 < \varepsilon$. Soit $A > 0$ tel que $\mathrm{supp}(g) \subset [-A, A]$. Soit $\delta > 0$ un module d'uniforme continuité de g pour $(\varepsilon/3A)^{1/2}$. Quitte à restreindre on suppose $\delta < A$. On a alors

$$\int_{\mathbb{R}} |g(x - t) - g(x - s)|^2\, dx < \varepsilon(2A + \delta)/3A \leqslant \varepsilon$$

et on conclut par inégalité triangulaire. □

Définition 4. On note $H : t \mapsto e^{-|t|}$ qui appartient à $L^1 \cap L^2$, et pour $\lambda > 0$,

$$h_\lambda(x) = \int_{\mathbb{R}} H(\lambda t)e^{itx}dt.$$

Après calculs, on trouve

$$h_\lambda(x) = \frac{2\lambda}{\lambda^2 + x^2}$$

et donc

$$\int_{\mathbb{R}} h_\lambda(x)dx = 2\pi. \tag{1}$$

Démonstration. On a, pour $\lambda > 0$,

$$h_\lambda(x) = \int_{\mathbb{R}} e^{-|\lambda t|} e^{itx} dt = \int_{-\infty}^{0} e^{t(\lambda+ix)} dt + \int_{0}^{+\infty} e^{-t(\lambda-ix)} dt = \frac{1}{\lambda+ix} + \frac{1}{\lambda-ix} = \frac{2\lambda}{\lambda^2+x^2}$$

et

$$\int_{\mathbb{R}} h_\lambda(x)dx = \int_{\mathbb{R}} \frac{2\lambda}{\lambda^2+x^2}dx = \int_{\mathbb{R}} \frac{2}{1+y^2}dy = 2[\arctan(y)]_{-\infty}^{+\infty} = 2\pi.$$

□

Proposition 5. *Si $f \in L^1$, alors pour tout $x \in \mathbb{R}$,*

$$f * h_\lambda(x) = \int_{\mathbb{R}} H(\lambda t)\widehat{f}(t)e^{ixt}dt.$$

Démonstration. Par le théorème de Fubini, on obtient,

$$\begin{aligned} f * h_\lambda(x) &= \int_{\mathbb{R}} f(y) \int_{\mathbb{R}} H(\lambda t) e^{it(x-y)}\, dt\, dy \\ &= \int_{\mathbb{R}} H(\lambda t) e^{itx} \int_{\mathbb{R}} f(y) e^{-ity}\, dy\, dt = \int_{\mathbb{R}} H(\lambda t)\widehat{f}(t)e^{ixt}dt. \end{aligned}$$

□

Proposition 6. *Si $g \in L^\infty$ et est continue en $x \in \mathbb{R}$, alors*

$$g * h_\lambda(x) \underset{\lambda\to 0}{\longrightarrow} 2\pi\, g(x).$$

Démonstration. On a, avec (1),

$$\begin{aligned} g * h_\lambda(x) - 2\pi\, g(x) &= \int_{\mathbb{R}} \Big(g(x-y) - g(x)\Big) h_\lambda(y)\, dy \\ &= \int_{\mathbb{R}} \Big(g(x-y) - g(x)\Big) \frac{1}{\lambda} h_1(y/\lambda)\, dy = \int_{\mathbb{R}} \Big(g(x-\lambda s) - g(x)\Big) h_1(s)\, ds \end{aligned}$$

et cette dernière intégrale tend vers 0 lorsque $\lambda \to 0$ par convergence dominée en utilisant la continuité de g en x. □

Proposition 7. *Si $f \in L^2$, $||f * h_\lambda - 2\pi\, f||_2 \underset{\lambda\to 0}{\longrightarrow} 0$.*

Démonstration. On a, d'après (1), pour $x \in \mathbb{R}$

$$f * h_\lambda(x) - 2\pi\, f(x) = \int_{\mathbb{R}} \Big(f(x-y) - f(x)\Big) h_\lambda(y)\, dy$$

et donc, par inégalité de Jensen,

$$\Big(f*h_\lambda(x)-2\pi\, f(x)\Big)^2 = 4\pi^2\Big(\frac{1}{2\pi}\Big[f*h_\lambda(x)-2\pi\, f(x)\Big]\Big)^2 \leqslant 4\pi^2\Big(\frac{1}{2\pi}\int_{\mathbb{R}}\Big(f(x-y)-f(x)\Big)^2 h_\lambda(y)\,dy\Big)$$

on intègre alors par rapport à x et on applique le théorème de Fubini-Tonelli pour obtenir :

$$||f * h_\lambda - 2\pi\, f||_2 \leqslant 2\pi \int_{\mathbb{R}} ||\tau_{-y}f - f||_2^2\; h_\lambda(y)\,dy$$

or si on pose $g(y) = ||\tau_{-y}f - f||_2^2$ le lemme préliminaire nous assure que g est bornée, continue et que $g(0) = 0$ et en remarquant que

$$\int_{\mathbb{R}} ||\tau_{-y}f - f||_2^2\; h_\lambda(y)\,dy = g * h_\lambda(0)$$

on peut appliquer la proposition précédente pour obtenir la convergence souhaitée. □

Démonstration (Théorème). Étape 1 : on commence par montrer que pour tout $f \in L^1 \cap L^2$, $||\widehat{f}||_2 = \sqrt{2\pi}||f||_2$. Soit $f \in L^1 \cap L^2$ et $\widetilde{f} : x \mapsto \overline{f(-x)}$. On pose $g = f * \widetilde{f}$. On a

$$g(x) = \int_{\mathbb{R}} f(x-y)\overline{f(-y)}\,dy = \int_{\mathbb{R}} f(x+y)\overline{f(y)}\,dy = (\tau_x f, f).$$

On déduit de cette expression que g est continue, grâce au lemme préliminaire et la continuité du produit scalaire par rapport à la première variable. D'autre part par inégalité de Cauchy-Schwarz,

$$|g(x)| \leqslant ||\tau_x f||_2||f||_2 = ||f||_2^2$$

pour tout $x \in \mathbb{R}$ et donc g est bornée. Enfin, par propriété du produit de convolution, puisque f et $\widetilde{f}$ sont L^1, g est L^1. Ainsi, par la proposition 5,

$$g * h_\lambda(0) = \int_{\mathbb{R}} H(\lambda t)\widehat{g}(t)\,dt.$$

Or, puisque $\widehat{g} = \widehat{f}\widehat{\widetilde{f}} = \widehat{f}\overline{\widehat{f}} = |\widehat{f}|^2$, on peut appliquer le théorème de convergence monotone pour obtenir

$$\int_{\mathbb{R}} H(\lambda t)\widehat{g}(t)\,dt \underset{\lambda\to 0}{\longrightarrow} \int_{\mathbb{R}} |\widehat{f}|^2\,dt$$

Et d'autre part grâce à la proposition 6,

$$g * h_\lambda(0) \underset{\lambda\to 0}{\longrightarrow} 2\pi\, g(0) = 2\pi||f||_2^2$$

d'où le résultat.

Étape 2 : on note alors $Y = \mathcal{F}(L^1 \cap L^2)$ et on montre que Y est dense dans L^2 en montrant que $Y^\perp = \{0\}$. On remarque que pour tout $\lambda > 0$ et $\alpha \in \mathbb{R}$,

$$h_\lambda(\alpha - t) = \int_{\mathbb{R}} e^{i\alpha x} H(\lambda x) e^{-itx} dx$$

et donc $t \mapsto h_\lambda(\alpha - t) \in Y$ comme transformée de Fourier de $x \mapsto e^{i\alpha x} H(\lambda x)$ qui est dans $L^1 \cap L^2$. Ainsi, si $w \in Y^\perp$, alors pour tout $\lambda > 0$ et pour tout $\alpha \in \mathbb{R}$,

$$h_\lambda * \overline{w}(\alpha) = \int_{\mathbb{R}} h_\lambda(\alpha - t)\overline{w}(t) dt = 0$$

et donc $h_\lambda * \overline{w} = 0$, et en appliquant la proposition 7 on obtient $\overline{w} = 0$ et donc $w = 0$.

Étape 3 : puisque $\mathcal{F} : L^1 \cap L^2 \to Y$ est une isométrie (en renormalisant L^2 à l'arrivée) entre deux sous-espaces denses de L^2, il existe une unique isométrie $\mathcal{F} : L^2 \to L^2$ qui prolonge la transformée de Fourier. On déduit alors la formule de Parseval avec l'identité de polarisation.

Étape 4 : enfin, on note $k_A = \mathbb{1}_{[-A,A]}$ pour $A > 0$. Si $f \in L^2$, alors $fk_A \in L^1 \cap L^2$, et $\varphi_A = \widehat{fk_A}$ et donc

$$||\widehat{f} - \varphi_A||_2 = ||\widehat{f - fk_A}||_2 = \sqrt{2\pi}||f - fk_A||_2 \underset{A \to +\infty}{\longrightarrow} 0$$

par convergence dominée. De la même manière, par inversion de Fourier dans L^1, $\psi_A = \mathcal{F}^{-1}(k_A \mathcal{F}(f))$ et donc

$$\begin{aligned} ||f - \psi_A||_2 &= ||\mathcal{F}^{-1}(\mathcal{F}(f)) - \mathcal{F}^{-1}(k_A\mathcal{F}(f))||_2 \\ &= \left|\left|\mathcal{F}^{-1}\Big(\mathcal{F}(f) - k_A\mathcal{F}(f)\Big)\right|\right|_2 = \frac{1}{\sqrt{2\pi}}||\mathcal{F}(f) - k_A\mathcal{F}(f)||_2 \underset{A \to +\infty}{\longrightarrow} 0 \end{aligned}$$

par convergence dominée. □

Commentaire : le développement est très long, commencer les démonstrations à partir de la proposition 7 et éventuellement ne pas mettre les "formules d'inversion" dans le développement. Pour justifier le recasage dans la leçon 235 : interversion de limites et d'intégrales, on note qu'on applique une fois le théorème de convergence monotone dans la preuve même, ainsi qu'une fois le théorème de Fubini dans la preuve de la proposition qui précède, et deux fois le théorème de convergence dominée pour les formules de pseudo-inversion.

3.18 Théorème de Hadamard-Lévy

Référence : H. Queffélec, C. Zuily, *Éléments d'Analyse*, Dunod, 2002.

Leçons concernées : 203, 204, 214, 215, 220.

Théorème 1. *Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ de classe $\mathcal{C}^2$. On a équivalence entre :*

(i) f est une $\mathcal{C}^1$-difféomorphisme de $\mathbb{R}^n$ dans $\mathbb{R}^n$

(ii) f est propre et pour tout $x \in \mathbb{R}^n$, $df(x)$ est inversible.

Démonstration. Le sens direct (i) $\Rightarrow$ (ii) est facile puisque la continuité de f^{-1} nous donne le caractère propre de f et la différentiation des fonctions composées appliquée à $f^{-1} \circ f = \mathrm{id}$ implique l'inversibilité de $df(x)$ en tout point.

Pour le sens réciproque, on remarque que grâce au théorème d'inversion globale, il nous suffit de montrer que f est bijective. Pour cela, on montre que $S = f^{-1}(\{0\})$ est un singleton, ce qui, en l'appliquant à $x \mapsto f(x) - y$ pour tout $y \in \mathbb{R}^n$ conclura la preuve.

Pour $x \in \mathbb{R}^n$ on considère le problème de Cauchy

$$(1) : \begin{cases} u' = -df(u)^{-1}(f(u)) \\ u(0) = x \end{cases}$$

et le flot associé $\varphi(x,t)$ défini sur $\bigcup_{x\in\mathbb{R}^n}\{x\} \times I_x$, où I_x maximal pour la condition initiale x par théorème de Cauchy-Lipschitz local puisque $z \mapsto -df(z)^{-1}(f(z))$ est de classe $\mathcal{C}^1$.

Étape 1 : soit $x \in \mathbb{R}^n$, alors si $I_x =]T_*, T^*[$, on a $T^* = +\infty$. En effet, on considère la fonction

$$g : \begin{array}{ccc}]T_*, T^*[& \to & \mathbb{R}^n \\ t & \mapsto & f \circ \varphi(x,t) \end{array}$$

dérivable sur I_x de dérivée : $g'(t) = df(\varphi(x,t))\Big(\frac{\partial\varphi}{\partial t}(x,t)\Big) = -f(\varphi(x,t)) = -g(t)$ et donc $g(t) = g(0)e^{-t} = f(x)e^{-t}$. Ainsi, pour tout $t \geqslant 0$,

$$\varphi(x,t) \in f^{-1}\big(g([0,T^*[)\big) \subset f^{-1}\Big(\overline{B}\big(0, ||f(x)||\big)\Big)$$

or ce dernier ensemble est compact puisque f est propre. On conclut par le lemme de sortie de tout compact.

Étape 2 : tout $y \in S$ est un équilibre asymptotiquement stable. Il est clair que y est une équilibre. D'autre part, par le théorème d'inversion locale, quitte à restreindre, il existe U_y un voisinage de y et $\varepsilon_y > 0$ tels que f induise un difféomorphisme de U_y sur $B(0,\varepsilon_y)$. Soit maintenant $t_0 \geqslant 0, x \in \mathbb{R}^n$ tel que $\varphi(x,t_0) \in U_y$. Puisque

$$e^{-t_0} f(x) = f \circ \varphi(x,t_0) \in f(U_y) = B(0,\varepsilon_y),$$

pour tout $t \geqslant t_0$, $e^{-t}f(x) = f \circ \varphi(x,t) \in B(0,\varepsilon_y)$ et donc pour tout $t \geqslant t_0$,

$$\varphi(x,t) = f_{|U_y}^{-1}\big(f \circ \varphi(x,t)\big) = f_{|U_y}^{-1}\big(e^{-t}f(x)\big) \underset{t\to+\infty}{\longrightarrow} f_{|U_y}^{-1}(0) = y.$$

On pose maintenant, pour $y \in S$, $W_y = \Big\{x \in \mathbb{R}^n, \varphi(x,t) \underset{t\to+\infty}{\longrightarrow} y\Big\}$.

Étape 3 : on a $\mathbb{R}^n = \bigcup_{y\in S} W_y$. En effet, soit $x \in \mathbb{R}^n$. Pour tout $k \geqslant 0$, $\varphi(x,k) \in f^{-1}\Big(\overline{B}\big(0,||f(x)||\big)\Big)$ qui est compact, donc, quitte à extraire, $\varphi(x,k) \underset{k\to+\infty}{\longrightarrow} y \in \mathbb{R}^n$. Or, par continuité,

$$f(y) = \lim_k f \circ \varphi(x,k) = \lim_k e^{-k}f(x) = 0$$

et donc $y \in S$. Ainsi il existe $k_0 \geqslant 0$ tel que $\varphi(x,k_0) \in U_y$ et l'étape 2 nous donne $\varphi(x,t) \underset{t\to+\infty}{\longrightarrow} y$ et donc $x \in W_y$.

Étape 4 : pour $y \in S$, $W_y = \Big\{x \in \mathbb{R}^n, \varphi(x,t) \underset{t\to+\infty}{\longrightarrow} y\Big\}$ est un ouvert non vide. En effet, $u(t) = y$ est solution de (1) puisque $f(y) = 0$, et donc $y = \varphi(y,t)$ et $y \in W_y$. D'autre part,

$$W_y = \bigcup_{t\geqslant 0} \varphi(\,.\,,t)^{-1}(U_y).$$

En effet, si $x \in W_y$, il existe $t_0 > 0$ tel que $\varphi(x,t_0) \in U_y$. Réciproquement, si il existe $t_0 > 0$ tel que $\varphi(x,t_0) \in U_y$, par l'étape 2, $\varphi(x,t) \underset{t\to+\infty}{\longrightarrow} y$.

Étape 5 : on a écrit $\mathbb{R}^n$ comme une union d'ouverts disjoints (par unicité de la limite) non vides : $\mathbb{R}^n = \bigcup_{y\in S} W_y$ et donc, par connexité de $\mathbb{R}^n$, $|S| = 1$. □

Application 2. *L'application*

$$f : \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & \Big(\dfrac{x\exp(x^2+y^2)}{1+x^2+y^2}, \dfrac{y\exp(x^2+y^2)}{1+x^2+y^2}\Big) \end{array}$$

est un $\mathcal{C}^1$-difféomorphisme global.

Démonstration. Il est facile de voir que f est propre et de classe $\mathcal{C}^2$ et un logiciel de calcul formel nous permet de montrer que la différentielle est en tout point inversible. □

Commentaire : dans la référence, il est d'abord montré que S est fini et non vide, mais il semblerait que ce n'est pas nécessaire.

3.19 Théorème de Lax-Milgram et application

Références : F. Hirsch, G. Lacombe, *Éléments d'analyse fonctionnelle*, Dunod, 1999. H. Brézis, *Analyse fonctionnelle*, Dunod, 1999. [1]

Leçons concernées : 201, 205, 213, 222.

Théorème 1 (Lax-Milgram)**.** *Soit H un espace de Hilbert réel et a une forme bilinéaire sur H continue et coercive, c'est-à-dire telle qu'il existe $C, \alpha > 0$ telles que $\forall x, y \in H$,*

$$|a(x,y)| \leqslant C||x||||y|| \quad et \quad a(x,x) \geqslant \alpha||x||^2$$

alors pour toute forme linéaire continue L de H il existe un unique $u \in H$ tel que $\forall x \in H$

$$L(x) = a(u,x)$$

de plus si a est symétrique, en posant $J(x) = \frac{1}{2}\, a(x,x) - L(x)$ pour $x \in H$, u est caractérisé par

$$J(u) = \min_{x \in E} J(x).$$

Démonstration. Pour $x \in H$, $y \mapsto a(x,y)$ est une forme linéaire continue, ainsi, par le théorème de Riesz, il existe un unique vecteur $Tx \in H$ tel que pour tout $y \in H$, $a(x,y) = (Tx|y)$. Pour tout $x, y, z \in H$ et pour tout $\lambda \in \mathbb{R}$,

$$(Tx + \lambda Ty|z) = (Tx|z) + \lambda(Ty|z) = a(x,z) + \lambda a(y,z) = a(x + \lambda y, z)$$

et donc par unicité dans le théorème de Riesz $T(x + \lambda y) = T(x) + \lambda T(y)$ et T est linéaire. De plus, pour $x \in H$, par continuité de a,

$$||Tx||^2 = (Tx|Tx) = a(x,Tx) \leqslant C||x||||Tx||$$

et donc $||T|| \leqslant C$ et T est continu.

On montre alors que T est un isomorphisme : on commence par montrer que $T(H)$ est dense dans H par la caractérisation par l'orthogonal. Soit $z \in T(H)^{\perp}$, alors en particulier, par coercivité de a,

$$0 = (Tz|z) = a(z,z) \geqslant \alpha||z||^2 \geqslant 0$$

et donc $z = 0$. D'autre part, on remarque que pour tout $x \in H$,

$$||Tx||||x|| \geqslant |(Tx,x)| = a(x,x) \geqslant \alpha||x||^2$$

et donc $||Tx|| \geqslant \alpha||x||$. On en déduit que T est injectif. Enfin, si $(y_n)_n \in T(H)^{\mathbb{N}}$ converge vers $y \in H$, alors $(y_n)_n$ est de Cauchy dans H et donc en notant $x_n \in H$ tel que $y_n = Tx_n$,

1. Merci à Rudy Morel et Michel Nassif pour l'idée du développement et certains éléments de la preuve.

par l'inégalité précédente $(x_n)_n$ est aussi de Cauchy dans H complet, donc converge vers $x \in H$ et par continuité de T, $Tx = y$ de sorte que $T(H)$ est fermé. On peut alors conclure que T est un isomorphisme de H.

Soit maintenant L une forme linéaire continue sur H. Alors par le théorème de Riesz il existe un unique $v \in H$ tel que pour tout $x \in H$, $L(x) = (v|x)$. Ainsi, en notant $u = T^{-1}v$, pour tout $x \in H$, $L(x) = (Tu|x) = a(u, x)$. L'unicité de u s'obtient par l'unicité dans le théorème de Riesz : si pour tout $x \in H$, $L(x) = a(u', x)$, alors pour tout $x \in H$, $L(x) = (Tu', x)$ et donc $Tu' = Tu$ et $u' = u$.

Supposons de plus que a est symétrique, alors pour $v \in H$, si on écrit $v = u + w$, on obtient

$$J(v) = J(u+w) = J(u)+\frac{1}{2}\,a(w,w)-L(w)+a(u,w) = J(u)+\frac{1}{2}\,a(w,w)-L(w)+L(w) \geqslant J(u)$$

par coercivité. De plus si v est aussi minimum de J, alors si $w = u - v$, $J(u) = J(v)$ et par le calcul précédent $a(w, w) = 0$ et donc $w = 0$. □

On applique le théorème de Lax-Milgram pour résoudre une équation différentielle par une méthode variationnelle.

Proposition 2. *Soit $I =]0, 1[$, $p \in \mathcal{C}^1(\overline{I})$, $r, q \in \mathcal{C}^0(\overline{I})$ et $f \in L^2(I)$. On suppose que $p \geqslant \alpha > 0$, $q \geqslant 1$ et $r^2 \leqslant \alpha$, alors il existe une unique solution faible au problème*

$$\begin{cases} -(pu')' + ru' + qu = f \quad sur \quad I \\ u(0) = u(1) = 0 \end{cases} \tag{1}$$

c'est-à-dire qu'il existe un unique $u \in H_0^1(I)$ tel que

$$\forall v \in H_0^1(I), \quad \int_I pu'v' + \int_I ru'v + \int_I quv = \int_I fv.$$

Démonstration. Étape 1 : on définit la forme bilinéaire a par,

$$a(u, v) = \int_0^1 pu'v' + \int_0^1 ru'v + \int_0^1 quv$$

pour $u, v \in H_0^1$, et la forme linéaire φ par,

$$\varphi(v) = \int_0^1 fv.$$

pour $v \in H_0^1$. Il est immédiat que φ est continue. D'autre part, puisque p, q, r sont continues sur $\overline{I}$ donc bornées, a est aussi continue. Enfin, si $v \in H_0^1$, on a par inégalité de Cauchy-Schwarz

$$-\int_0^1 rv'v \leqslant \left|\int_0^1 rv'v\right| \leqslant \sqrt{\alpha}||v||_2||v'||_2$$

et donc

$$\begin{aligned} a(v,v) &= \int_0^1 pv'^2 + \int_0^1 rv'v + \int_0^1 qv^2 \geqslant \alpha||v'||_2^2 - \sqrt{\alpha}||v||_2||v'||_2 + ||v||_2^2 \\ &= \Big(\frac{\sqrt{\alpha}}{2}||v'||_2 - ||v||_2\Big)^2 + \frac{3\alpha}{4}||v'||_2^2 \geqslant \frac{3\alpha}{4}||v'||_2^2 \geqslant \frac{3\alpha}{4C^2}||v||_{H^1}^2 \end{aligned}$$

par inégalité de Poincaré et donc a est coercive. On peut ainsi appliquer le théorème de Lax-Milgram pour obtenir l'existence d'une unique solution faible $u \in H_0^1$. □

Remarque. On considère ici une forme bilinéaire non symétrique afin d'avoir une vraie application du théorème de Lax-Milgram. En effet si la forme bilinéaire considérée est symétrique, continue et coercive, elle constitue un produit scalaire dont la norme est équivalente à la norme $||.||_{H^1}$, et donc l'espace H_1^0 est complet pour cette nouvelle norme et on peut appliquer le théorème de Riesz. Cependant on perd ainsi le dernier point du théorème de Lax-Milgram qui est l'expression de u comme le minimum d'une fonctionnelle, ce qui peut-être utile pour obtenir des solutions approchées.

On voit maintenant comment montrer, avec des hypothèses de régularité, que l'unique solution faible est en fait une solution forte.

Proposition 3. *Soit $I =]0,1[$, $p \in \mathcal{C}^1(\overline{I})$ et $r, q, f \in \mathcal{C}^0(\overline{I})$. On suppose que $p \geqslant \alpha > 0$, $q \geqslant 1$ et $r^2 \leqslant \alpha$, alors il existe une unique fonction $u \in \mathcal{C}^2(\overline{I})$ vérifiant*

$$\begin{cases} -(pu')' + ru' + qu = f \quad sur \quad I \\ u(0) = u(1) = 0. \end{cases} \tag{2}$$

Démonstration. Étape 1 : par intégration par parties sur H_0^1, une solution forte de (2) est une solution faible de (2). La proposition précédente nous assure alors l'existence et l'unicité d'une solution faible $u \in H_0^1(I)$. On a donc unicité de la solution forte, il nous faut maintenant montrer que u est en fait une solution forte.

Étape 2 : puisque $\mathcal{D}(I) \subset H_0^1$ on a, par définition d'une solution faible,

$$-(pu')' + ru' + qu - f = 0 \tag{3}$$

au sens des distributions. Alors $(pu')' = ru' + qu - f \in L^2$ et donc $pu' \in H^1$ et ainsi $u' = \frac{1}{p}pu' \in H^1$. On obtient $u, u' \in \mathcal{C}^0(\overline{I})$ et donc [2] $u \in \mathcal{C}^1(\overline{I})$. Alors, puisque $(pu')' = p'u' + pu''$,

$$u'' = \frac{1}{p}\Big((pu')' - p'u'\Big) = \frac{1}{p}\Big(ru' + qu - f - p'u'\Big) \in \mathcal{C}^0(\overline{I})$$

donc $u' \in \mathcal{C}^1(\overline{I})$ et par suite, puisque $u \in \mathcal{C}^1(\overline{I})$, $u \in \mathcal{C}^2(\overline{I})$.

Étape 3 : puisque $u \in \mathcal{C}^2(\overline{I})$, la relation (3) est vérifiée au sens usuel (par injection de $\mathcal{C}^0(\overline{I})$ dans $\mathcal{D}'(I)$) et puisque $u \in H_0^1$, $u(0) = u(1) = 0$ et donc u est une solution classique. □

2. Cela provient de la formule $u(x) - u(y) = \int_y^x u'(t)dt$ qui relie le représentant continu de u et u'.

Proposition 4. *L'espace H_0^1 est stable par produit et si $u, v \in H_0^1$,*

$$(uv)' = u'v - uv'$$

et (en intégrant la précédente relation) pour tout $x, y \in \overline{I}$, on a la formule d'intégration par parties

$$\int_y^x u'v = u(x)v(x) - u(y)v(y) - \int_y^x uv'.$$

Démonstration. On remarque d'abord que puisque $H^1(I) \subset L^\infty(I)$, $uv \in H^1$, et puisque $uv(0) = uv(1) = 0$, $uv \in H_0^1$. On se donne alors $(u_n)_n, (v_n)_n$ deux suites de $\mathcal{C}_c^1(I)$ qui convergent dans H_0^1 vers u et v respectivement. Alors $u_n \to u$ et $v_n \to v$ dans $L^\infty(I)$, et ainsi, $u_n v_n$ converge vers uv dans $L^2(I)$. D'autre part, puisque $(u_n v_n)' = u_n' v_n + u_n v_n'$,

$$||(u_n v_n)' - u'v - uv'||_2 \leqslant ||u_n' v_n - u_n' v||_2 + ||u_n' v - u'v||_2 \leqslant ||u_n'||_2 ||v_n - v||_\infty + ||v||_2 ||u_n' - u||_\infty \to 0$$

d'où le résultat. La formule d'intégration par parties s'en déduit en intégrant, puisque uv est continue. □

Commentaires : le développement ne contient que le théorème de Lax-Milgram et l'existence et l'unicité d'une solution faible. L'existence et l'unicité d'une solution forte peut être faite si il reste du temps, mais c'est plus subtil.

3.20 Théorème de Riesz-Fischer

Références : H. Brézis, *Analyse fonctionnelle*, Dunod, 1999,
W. Rudin, *Analyse réelle et complexe*, Dunod, 1998.

Leçons concernées : 201, 205, 208, 234, 241, *262*.

Théorème 1. *Soit $(X, \mathcal{A}, \mu)$ un espace mesuré. Pour $1 \leqslant p \leqslant +\infty$, l'espace $(L^p(\mu), ||.||_p)$ est complet.*

Démonstration. Cas 1 : on commence par considérer le cas $p = +\infty$: soit $(f_n)_n$ une suite de Cauchy dans $L^\infty(\mu)$. Soit $k \in \mathbb{N}^*$, par définition il existe $N_k \geqslant 1$ tel que pour tout $m, n \geqslant N_k$,

$$||f_n - f_m||_\infty \leqslant \frac{1}{k}.$$

Ainsi, il existe un ensemble de mesure nulle E_k tel que pour tout $m, n \geqslant N_k$ et pour tout $x \in X \backslash E_k$,

$$|f_n(x) - f_m(x)| \leqslant \frac{1}{k}.$$

On pose alors $E = \bigcup_{k \in \mathbb{N}^*} E_k$ qui est de mesure nulle, et on obtient que pour tout $x \in X \backslash E$, pour tout $k \in \mathbb{N}^*$, il existe $N_k \geqslant 0$ tel que pour tout $m, n \geqslant N_k$,

$$|f_n(x) - f_m(x)| \leqslant \frac{1}{k} \tag{1}$$

c'est-à-dire que $(f_n(x))_n$ est de Cauchy dans $\mathbb{R}$. Par complétude de $\mathbb{R}$, cette suite admet une limite $f(x)$, et on peut donc construire la fonction f définie presque partout (on la prolonge par 0 sur E). En passant à la limite en m dans l'équation (1) on obtient que pour tout $x \in X \backslash E$, pour tout $k \in \mathbb{N}^*$, il existe $N_k \geqslant 0$ tel que pour tout $n \geqslant N_k$,

$$|f(x) - f_n(x)| \leqslant \frac{1}{k},$$

c'est-à-dire que pour tout $k \in \mathbb{N}^*$, il existe $N_k \geqslant 0$ tel que pour tout $n \geqslant N_k$,

$$||f - f_n||_\infty \leqslant \frac{1}{k},$$

et donc $f \in L^\infty$ par inégalité triangulaire, et $(f_n)_n$ converge vers f dans L^∞.

Cas 2 : soit maintenant $1 \leqslant p < +\infty$ et $(f_n)_n$ une suite de Cauchy dans $L^p(\mu)$. Il existe une suite extraite $(f_{n_k})_k$ telle que

$$\forall k \geqslant 1, \quad ||f_{n_{k+1}} - f_{n_k}||_p \leqslant \frac{1}{2^k}.$$

On pose alors

$$g_n = \sum_{k=1}^{n} \left| f_{n_{k+1}} - f_{n_k} \right| \quad \text{et} \quad g = \sum_{k \geqslant 1} \left| f_{n_{k+1}} - f_{n_k} \right|.$$

L'inégalité de Minkowski montre que pour $n \geqslant 1$, $||g_n||_p \leqslant 1$ et le lemme de Fatou appliqué à $(g_n^p)_n$ nous donne $||g||_p \leqslant 1$. Ainsi, en particulier, $|g| < +\infty$ presque partout de sorte que pour presque tout $x \in \mathbb{R}$, la série

$$f_{n_1}(x) + \sum_{k \geqslant 1} \left(f_{n_{k+1}}(x) - f_{n_k}(x) \right)$$

converge absolument dans $\mathbb{R}$ complet, donc converge vers $f(x) \in \mathbb{R}$. On note f la fonction ainsi obtenue (prolongée par 0 sur un ensemble de mesure nulle). On remarque que $f_{n_1} + \sum_{k=1}^{n} (f_{n_{k+1}} - f_{n_k}) = f_{n+1}$ et donc $(f_{n_k})_k$ converge presque partout vers f. On montre alors la convergence dans L^p. Soit $\varepsilon > 0$, par hypothèse il existe $N \geqslant 0$ tel que pour tout $n, m \geqslant N$, $||f_n - f_m||_p \leqslant \varepsilon$. Alors, grâce au lemme de Fatou, pour tout $m \geqslant N$,

$$\int_X |f - f_m|^p d\mu = \int_X \liminf_{k \to +\infty} |f_{n_k} - f_m|^p d\mu \leqslant \liminf_{k \to +\infty} \int_X |f_{n_k} - f_m|^p d\mu \leqslant \varepsilon^p$$

et donc $f - f_m \in L^p$ de sorte que $f \in L^p$ et d'autre part $||f - f_m||_p \leqslant \varepsilon$ et donc $(f_n)_n$ converge vers f dans L^p. □

Corollaire 2. *Soit $1 \leqslant p \leqslant +\infty$, et soit $(f_n)_n$ une suite convergente dans $L^p(\mu)$ vers f. Alors il existe une sous-suite $(f_{n_k})_k$ de $(f_n)_n$ qui converge presque sûrement vers f.*

Démonstration. Une suite convergente est de Cauchy, et dans la preuve précédente, dans chacun des deux cas, on obtient une sous-suite qui converge presque partout. □

4 Développements mixtes

4.1 Différentielle de l'exponentielle de matrice

Référence : F. Rouvière, *Petit guide de calcul différentiel*, Cassini, 2014.

Leçons concernées : 156, 215, 220, 221.

Théorème 1. *On note* $\operatorname{ad} X : \mathcal{M}_n(\mathbb{R}) \to \mathcal{M}_n(\mathbb{R}), H \mapsto [X,H] = XH - HX$. *La différentielle de l'application* $\exp : \mathcal{M}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ *est :*

$$\mathrm{d}\exp(X)\cdot(H) = \exp(X)\sum_{k=0}^{+\infty}\frac{(-\operatorname{ad} X)^k}{(k+1)!}H.$$

Démonstration. Étape 1 : on note $E = \mathcal{M}_n(\mathbb{R})$. Soit $H \in E$ et $A \in \mathcal{L}(E)$. On résout les équations d'inconnues $f, g : \mathbb{R} \to E$

$$f'(t) = Af(t), \quad f(0) = H$$

$$g'(t) = \exp(tA)H, \quad g(0) = 0.$$

On raisonne par analyse-synthèse. D'après la théorie des séries entières on sait que $t \to \exp(tA)$ est dérivable sur $\mathbb{R}$ de dérivée $A\exp(tA) = \exp(tA)A$. Ainsi, si $h(t) = \exp(-tA)f(t)$, $h'(t) = -A\exp(tA)f(t) + A\exp(tA)f(t) = 0$, et donc avec $h(0) = \exp(0\cdot A)f(0) = H$, on obtient $f(t) = \exp(tA)H$, et on vérifie que f est bien solution. Pour g, toujours d'après la théorie des séries entières on peut intégrer terme à terme pour obtenir, avec $g(0) = 0$,

$$g(t) = \Big(\sum_{k=0}^{+\infty}\frac{t^{k+1}A^k}{(k+1)!}\Big)H$$

et on vérifie que g est bien solution.

Étape 2 : pour tout $X, H \in E$, $\exp(X)H\exp(-X) = \exp(\operatorname{ad} X)H$. On pose $f(t) = \exp(tX)H\exp(-tX)$, et en dérivant on obtient

$$f'(t) = X\exp(tX)H\exp(-tX) - \exp(tX)H\exp(-tX)X = \operatorname{ad} X(f(t))$$

ainsi, d'après l'étape 1, puisque $f(0) = H$, on a $f(t) = \exp(t\operatorname{ad} X)H$, et donc, en évaluant en $t = 1$ on obtient

$$\exp(X)H\exp(-X) = \exp(\operatorname{ad} X)H.$$

Étape 3 : on pose

$$g(t) = \frac{\partial}{\partial u}\Big(\exp(-tX)\exp(t(X+uH)\Big)(t,0).$$

Alors $g'(t) = \exp(-t \operatorname{ad} X)H$. En effet, l'application exponentielle étant de classe $\mathcal{C}^2$, l'application $(t,u) \mapsto \exp(-tX)\exp(t(X+uH)$ est de classe $\mathcal{C}^2$ et d'après le lemme de Schwarz,

$$\begin{aligned} g'(t) &= \frac{\partial^2}{\partial t \partial u}\Big(\exp(-tX)\exp(t(X+uH)\Big)(t,0) = \frac{\partial^2}{\partial u \partial t}\Big(\exp(-tX)\exp(t(X+uH)\Big)(t,0) \\ &= \frac{\partial}{\partial u}\Big(-\exp(-tX)X\exp(t(X+uH) + \exp(-tX)(X+uH)\exp(t(X+uH)\Big)(t,0) \\ &= \frac{\partial}{\partial u}\Big(u\exp(-tX)H\exp(t(X+uH)\Big)(t,0) = \exp(-tX)H\exp(tX). \end{aligned}$$

Ainsi, d'après l'étape précédente, $g'(t) = \exp(-t \operatorname{ad} X)H$, et donc, puisque $g(0) = 0$, d'après la première étape, en évaluant en $t = 1$, on obtient

$$g(1) = \Big(\sum_{k=0}^{+\infty} \frac{(-\operatorname{ad} X)^k}{(k+1)!}\Big)H.$$

Or, $g(1) = h'(0)$ où $h(u) = \exp(-X)\exp(X+uH)$, et on sait que $h'(u) = \exp(-X)\,\mathrm{d}\exp(X+uH)(H)$ et donc enfin,

$$\exp(-X)\,\mathrm{d}\exp(X)(H) = \Big(\sum_{k=0}^{+\infty} \frac{(-\operatorname{ad} X)^k}{(k+1)!}\Big)H$$

d'où le résultat. □

Application 2. *Soit $X : \mathbb{R} \to E$ dérivable. Alors si X commute avec sa dérivée en tout point,*

$$(\exp(X))'(t) = \exp(X(t))X'(t)$$

mais ce n'est pas vrai en général.

Démonstration. Par dérivation des fonctions composées et le théorème précédent on a

$$(\exp(X))'(t) = \mathrm{d}\exp(X)(X') = \exp(X)\Big(X' - \frac{1}{2}[X,X'] + \frac{1}{6}[X,[X,X']] + \cdots\Big)$$

d'où l'égalité si $[X,X'] = 0$. Mais si on pose

$$X(t) = \begin{pmatrix} 1 & t \\ 0 & 0 \end{pmatrix}$$

alors on remarque que $X(t)^n = X(t)$ pour $n \geqslant 0$, et donc

$$\exp(X(t)) = \begin{pmatrix} e & (e-1)t \\ 0 & 1 \end{pmatrix}.$$

Ainsi

$$(\exp(X))'(t) = \begin{pmatrix} 0 & e-1 \\ 0 & 0 \end{pmatrix} \neq \exp(X)X' = \begin{pmatrix} 0 & e \\ 0 & 0 \end{pmatrix}.$$

□

4.2 Ellipsoïde de John-Loewner

Référence : S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 3*, Cassini, 2008.

Leçons concernées : 152, 158, 170, 171, 219, 229, 253.

Définition 1. Un ellipsoïde centrée en 0 est une surface de $\mathbb{R}^n$ définie par une équation $q(x) \leqslant 1$ où q est une forme quadratique définie positive. On notera $\mathcal{E}_q = \{x \in \mathbb{R}^n, q(x) \leqslant 1\}$ l'ellipsoïde centré en 0 associé à q définie positive.

Théorème 2. *Pour tout K compact de $\mathbb{R}^n$ d'intérieur non vide, il existe un unique ellipsoïde centré en 0 de volume minimal contenant K.*

Lemme 3. *Soit A, B deux matrices symétriques réelles définies positives et α, β positifs tels que $\alpha + \beta = 1$. Alors,*

$$\det(\alpha A + \beta B) \geqslant (\det A)^\alpha (\det B)^\beta,$$

c'est-à-dire que le déterminant est log-concave. De plus, si $\alpha \in]0,1[$ et $A \neq B$, l'inégalité est stricte.

Démonstration. D'après le théorème de pseudo-réduction simultanée, il existe $P \in \mathrm{GL}_n(\mathbb{R})$ et $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ avec $\lambda_i > 0$ telles que $A = {}^tPP$ et $B = {}^tPDP$. Ainsi,

$$(\det A)^\alpha (\det B)^\beta = (\det(P)^2)^\alpha (\det(P)^2 \det D)^\beta = \det(P)^2 (\det D)^\beta$$

et

$$\det(\alpha A + \beta B) = \det P^2 \det(\alpha I + \beta D).$$

On cherche donc à montrer que $\det(\alpha I + \beta D) \geqslant (\det D)^\beta$, c'est-à-dire

$$\prod_{i=1}^n (\alpha + \beta\lambda_i) \geqslant \left(\prod_{i=1}^n \lambda_i \right)^\beta$$

soit, en passant au logarithme,

$$\sum_{i=1}^n \log(\alpha + \beta\lambda_i) \geqslant \beta \sum_{i=1}^n \log(\lambda_i)$$

et cette inégalité s'obtient terme à terme par concavité du logarithme.

Enfin, si $\alpha \in]0,1[$ et $A \neq B$, alors au moins un des λ_i est différent de 1 et donc par stricte concavité du logarithme, au moins l'une des inégalités est stricte et on a donc le résultat. □

Démonstration (Théorème). On note $\mathcal{Q}$ (resp. $\mathcal{Q}_+$, $\mathcal{Q}_{++}$) l'ensemble des formes quadratiques (resp. positives, définies positives) de $\mathbb{R}^n$.

Étape 1 : on commence par calculer le volume de $\mathcal{E}_q$ pour q définie positive quelconque. Par le théorème spectral [1], il existe une base orthonormée $\mathcal{B}$ dans laquelle q s'écrit $q(x) = \sum_{i=1}^n a_i x_i^2$, $a_i > 0$. Soit P la matrice de passage orthogonale de la base canonique à $\mathcal{B}$. On considère le changement de variables $x = Py$, de jacobien le déterminant de P qui vaut 1, puis le changement de variables $(u_1, \dots, u_n) = (\sqrt{a_1}x_1, \dots, \sqrt{a_n}x_n)$ de jacobien $\sqrt{a_1 \cdots a_n}$, pour obtenir

$$\iint \cdots \int_{\mathcal{E}_q} dy = \iint \cdots \int_{a_1 x_1^2 + \cdots + a_n x_n^2 \leqslant 1} dx = \frac{1}{\sqrt{a_1 \cdots a_n}} \iint \cdots \int_{u_1^2 + \cdots + u_n^2 \leqslant 1} du = \frac{V_0}{\sqrt{D(q)}}$$

où V_0 est le volume de la boule unité dans $\mathbb{R}^n$ et $D(q) = a_1 \cdots a_n$ le déterminant de q (que l'on obtient en diagonalisant la matrice de q dans une base quelconque).

Le problème se reformule alors ainsi : pour tout K compact d'intérieur non vide de $\mathbb{R}^n$, il existe une unique $q \in \mathcal{Q}_{++}$ telle que $D(q)$ soit maximal et pour tout $x \in K$, $q(x) \leqslant 1$. On se donne alors K compact d'intérieur non vide de $\mathbb{R}^n$.

Étape 2 : soit $\mathcal{A} = \{q \in \mathcal{Q}_+, \forall x \in K, q(x) \leqslant 1\}$. On munit par ailleurs $\mathcal{Q}$ de la norme $N(q) := \sup_{||x|| \leqslant 1} |q(x)|$.

- $\mathcal{A}$ est convexe : on vérifie facilement que si $q, q' \in \mathcal{A}$, $\lambda q + (1-\lambda)q' \in \mathcal{A}$ pour $\lambda \in [0,1]$.
- $\mathcal{A}$ est fermé : soit $(q_n)_n$ une suite de $\mathcal{A}$ qui converge vers q, alors pour $x \in \mathbb{R}^n$, $|q_n(x) - q(x)| \leqslant N(q_n - q)||x||$ et donc $q_n(x) \underset{n \to +\infty}{\longrightarrow} q(x)$ et on en déduit la positivité de q et la condition $x \in K \Rightarrow q(x) \leqslant 1$ car ces conditions sont fermées.
- $\mathcal{A}$ est borné : puisque K est d'intérieur non vide, il existe $a \in K$ et $r > 0$ tel que $B(a, r) \subset K$. Soit $q \in \mathcal{A}$. Si $||x|| < r$, $a + x \in K$ et donc par inégalité de Minkowski et avec $q(-a) = q(a)$ on obtient $\sqrt{q(x)} \leqslant \sqrt{q(x+a)} + \sqrt{q(-a)} \leqslant 2$. Ainsi si $||x|| \leqslant 1$, $|q(x)| = q(x) = \frac{4}{r^2} q(\frac{rx}{2}) \leqslant \frac{16}{r^2}$ d'où $N(q) \leqslant \frac{16}{r^2}$.
- $\mathcal{A}$ est non vide : puisque K est compact il est borné par $M > 0$, et donc $q_0(x) = \frac{||x||^2}{M^2}$ convient.

Ainsi $q \mapsto D(q)$ est continue (par continuité du déterminant) sur $\mathcal{A}$ compact non vide, et donc admet un maximum $q_1 \in \mathcal{A}$. Or puisque $D(q_0) > 0$ car q_0 est définie positive, $D(q_1) > 0$ et $q_1 \in \mathcal{Q}_{++}$: on a prouvé l'existence.

Étape 3 : unicité. Soit q_1, q_2 deux telles formes quadratiques de $\mathcal{A}$. On suppose par l'absurde qu'elles sont différentes. Soit S_1 et S_2 leurs matrices dans la base canonique. Par convexité de $\mathcal{A}$, $\frac{q_1+q_2}{2} \in \mathcal{A}$ et est de matrice $\frac{S_1+S_2}{2}$ dans la base canonique. Alors, d'après

1. Ici on utilise un résultat plus fort que l'existence d'une base dans laquelle la forme quadratique est diagonale : la base peut être choisie orthonormée. C'est cependant différent du résultat de réduction des formes quadratique réelle, qui dit que la matrice peut être mise sous forme diagonale avec des 1 sur la diagonale, mais la base n'est alors pas forcément orthonormée

le lemme,

$$D\left(\frac{q_1+q_2}{2}\right) = \det\frac{S_1+S_2}{2} > (\det S_1)^{1/2}(\det S_2)^{1/2} = \sqrt{D(q_1)}\sqrt{D(q_2)} = D(q_1)$$

et on obtient une absurdité. □

Application 4. *Soit G un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$. Alors il existe $q \in \mathcal{Q}_{++}$ telle que $G \subset O(q)$.*

Démonstration. Soit B la boule unité de $\mathbb{R}^n$ et $K = \{g(x), x \in B, g \in G\}$ qui est un compact comme image continue de $G \times B$ compact et d'intérieur non vide puisque $B \subset K$ pour un $g = \mathrm{id}$. On applique le théorème précédent pour trouver $q \in \mathcal{Q}_{++}$ telle que $K \subset \mathcal{E}_q$. Soit maintenant $g \in G$ et $q' : x \mapsto q(g(x))$ qui est une forme quadratique définie positive. On a $K \subset \mathcal{E}_{q'}$ car $g(K) = K$ et $|\det(g)| = 1$ puisque det est borné sur G compact donc sur $\{g^p, p \in \mathbb{Z}\}$. Alors $D(q) = D(q')$ et donc par unicité dans le théorème précédent, $q' = q(g) = q$ et donc $g \in O(q)$. □

Remarque. On peut montrer que ce sont même tous les sous-groupes compacts maximaux de $\mathrm{GL}_n(\mathbb{R})$, cf H2G2.

Théorème 5 (pseudo réduction simultanée)**.** *Soit A, B des matrices symétriques définies positives. Alors il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que*

$$^tPAP = I_n \quad et \quad ^tPBP = D$$

où D est une matrice diagonale dont tous les coefficients sont strictement positifs.

Démonstration. Puisque A définit un produit scalaire, il existe $Q \in \mathrm{GL}_n(\mathbb{R})$ telle que $^tQAQ = I_n$. D'autre part ^tQBQ est encore symétrique et donc d'après le théorème spectral, il existe $R \in O_n(\mathbb{R})$ telle que $^tR\,^tQAQR = D$ où D est une matrice diagonale dont tous les coefficients sont strictement positifs. On peut alors conclure en prenant $P := QR$. □

4.3 Extrema liés (par les sous-variétés)

Références : F. Rouvière, *Petit guide de calcul différentiel*, Cassini, 2014,
J. Lafontaine, *Introduction aux variétés différentielles*, PUG, 1996,
V. Beck, J. Malick, G. Peyré, *Objectif Agrégation*, H & K, 2005. [1]

Leçons concernées : 159, 214, 215, 219.

Théorème 1. *Soit $f, g_1, \dots, g_r$ des fonctions réelles de classe $\mathcal{C}^1$ sur un ouvert U de $\mathbb{R}^n$. On note X l'ensemble de $x \in U$ tels que $g_1(x) = \cdots = g_r(x) = 0$. Si $f_{|X}$ admet un extremum local en a et les formes linéaires $dg_1(a), \dots, dg_r(a)$ sont indépendantes, alors il existe $\lambda_1, \dots, \lambda_r$ dans $\mathbb{R}$ tels que*

$$df(a) = \lambda_1 dg_1(a) + \cdots + \lambda_r dg_r(a),$$

autrement dit, les formes linéaires $df(a), dg_1(a), \dots, dg_r(a)$ sont liées.

Lemme 2. *Soit $g : U \subset \mathbb{R}^n \to \mathbb{R}^p$ une submersion en $a \in U$ (une application différentiable sur U dont la différentielle en a $dg(a) : \mathbb{R}^n \to \mathbb{R}^p$ est surjective). Alors il existe $V \subset U$ un ouvert contenant a tel que l'application*

$$h : \begin{array}{ccc} U & \longrightarrow & \mathbb{R}^n \\ x = (x_1, \dots, x_n) & \mapsto & (g_1(x), \dots, g_p(x), x_{p+1}, \dots, x_n). \end{array}$$

définisse un $\mathcal{C}^1$ difféomorphisme sur son image W.

Démonstration. Quitte à permuter les coordonnées, on peut supposer que la matrice

$$B := \left(\frac{\partial g_i}{\partial x_j}(a) \right)_{1 \leqslant i,j \leqslant p}$$

est inversible. La matrice jacobienne en a de h est alors la matrice par blocs

$$\begin{pmatrix} B & (*) \\ 0 & I_{n-p} \end{pmatrix}$$

qui est inversible. Ainsi, d'après le théorème d'inversion locale, il existe $V \subset U$ contenant a tel que $h_{|V}$ soit un difféomorphisme sur son image $W \subset \mathbb{R}^n$. □

Démonstration (Théorème). Par hypothèse sur les g_i, X est lisse au point a (vérifie les hypothèses d'une sous-variété au point a). On définit $T_a X$ l'espace tangent de X en a comme :

$$T_a X := \Big\{ v \in \mathbb{R}^n, \exists \varepsilon > 0, \exists\ \gamma :]-\varepsilon, \varepsilon[\to X, \text{ de classe } \mathcal{C}^1, \gamma(0) = a \text{ et } \gamma'(0) = v \Big\}.$$

1. Merci à Adrian Petr pour son aide cruciale sur ce développement.

Étape 1 : l'application $df(a)$ est nulle sur l'espace tangent : soit $v \in T_aX$ associé à γ. La fonction de classe $\mathcal{C}^1$ $f \circ \gamma :]-\varepsilon, \varepsilon[\to X$ admet un extremum local en 0 par hypothèse, donc $f \circ \gamma'(0) = 0$, or,

$$f \circ \gamma'(0) = df(a) \cdot \gamma'(0) = df(a) \cdot v = 0.$$

Étape 2 : on montre que $T_aX = \bigcap_{i=1}^{r} \ker(dg_i(a))$. On procède par double inclusion. Soit $1 \leqslant i \leqslant r$, alors par définition, $\forall x \in X$, $g_i(x) = 0$, donc en particulier, si $v \in T_aX$ associé à γ, pour tout $t \in]-\varepsilon, \varepsilon[$, $g_i \circ \gamma(t) = 0$ et donc

$$g_i \circ \gamma'(0) = 0 = dg_i(a) \cdot \gamma'(0) = dg_i(a) \cdot v = 0.$$

Réciproquement, on sait par hypothèse que $g = (g_1, \ldots, g_p) : \mathbb{R}^n \to \mathbb{R}^p$ est une submersion, on considère alors $h : V \to W$ le $\mathcal{C}^1$ difféomorphisme donné par le lemme précédent : $h(x_1, \ldots, x_n) = (g_1(x), \ldots, g_p(x), x_{p+1}, \ldots, x_n)$. Soit $v \in \bigcap_{i=1}^{r} \ker(dg_i(a))$. On pose, pour $t \in \mathbb{R}$,

$$\widetilde{\gamma}(t) = h(a) + t\ dh(a) \cdot v.$$

Il est clair que $\widetilde{\gamma}$ est de classe $\mathcal{C}^1$. D'autre part, $\widetilde{\gamma}(0) = h(a) \in W$, ainsi, il existe $\varepsilon > 0$ tel que pour tout $|t| < \varepsilon$, $\widetilde{\gamma}(t) \in W$. Enfin, on remarque que

$$h(X \cap V) = W \cap (\{0\} \times \mathbb{R}^{n-p}).$$

Or, puisque $v \in \bigcap_{i=1}^{r} \ker(dg_i(a))$,

$$dh(a) \cdot v = (dg_1(a), \ldots, dg_p(a), \mathrm{id}, \ldots, id) \cdot v \in \{0\} \times \mathbb{R}^{n-p}.$$

Ainsi, puisque $h(a) \in \{0\} \times \mathbb{R}^{n-p}$, pour tout $|t| < \varepsilon$, $\widetilde{\gamma}(t) \in W \cap (\{0\} \times \mathbb{R}^{n-p})$. On considère alors $\gamma = h^{-1} \circ \widetilde{\gamma} :]-\varepsilon, \varepsilon[\to X$, de classe $\mathcal{C}^1$, qui vérifie

$$\gamma'(0) = dh^{-1}(h(a)) \cdot \widetilde{\gamma}'(0) = (dh(a))^{-1} \cdot dh(a) \cdot v = v$$

et donc $v \in T_aX$ [Faire un dessin].

Étape 3 : on conclut. On a montré que

$$T_aX = \bigcap_{i=1}^{r} \ker dg_i(a) \subset \ker df(a),$$

c'est-à-dire que

$$\big\{dg_1(a), \ldots, dg_p(a)\big\}^0 \subset \big\{df(a)\big\}^0$$

et donc,

$$\mathrm{Vect}\,\big(df(a)\big) \subset \mathrm{Vect}\,\big(dg_1(a), \ldots, dg_p(a)\big)$$

par passage à l'orthogonal, c'est la conclusion recherchée. □

On peut montrer le théorème spectral grâce au théorème des extrema liés (cf Beck, Malick, Peyré).

Application 3. *Soit E un espace euclidien et soit $u \in \mathcal{L}(E)$ symétrique. Alors il existe une base orthonormée de E formée de vecteurs propres de u.*

Démonstration. On considère

$$f : \begin{array}{ccc} E & \to & \mathbb{R} \\ x & \mapsto & < u(x), x > \end{array} \quad \text{et} \quad g : \begin{array}{ccc} E & \to & \mathbb{R} \\ x & \mapsto & < x, x > -1. \end{array}$$

Alors $S = \{x, g(x) = 0\}$ la sphère unité est compacte et donc f continue atteint son maximum sur S en e_1. D'autre part $df(x)(h) = 2 < u(x), h >$ et $dg(x)(h) = 2 < x, h >$ donc d'après le théorème des extrema liés, il existe λ_1 tel que $df(e_1) = \lambda_1 dg(e_1)$, c'est-à-dire $u(e_1) = \lambda_1 e_1$. On a donc trouvé une valeur propre λ_1 de vecteur propre e_1 de norme 1.

On raisonne alors par récurrence sur $F = e_1^{\perp}$. □

4.4 Méthodes itératives de résolution d'un système linéaire

Référence : L. Dumas, *Modélisation à l'oral de l'agrégation*, Ellipses, 1999.

Leçons concernées : 157, 162, 226, 233.

Soit $A \in \mathrm{GL}_n(\mathbb{R})$ et soit $b \in \mathbb{R}^n$. On s'intéresse au système $Ax = b$.

Définition 1. On suppose que $A = M - N$ où $M \in \mathrm{GL}_n(\mathbb{R})$ et $N \in \mathcal{M}_n(\mathbb{R})$. On dit que la méthode itérative associée à (M, N) converge si toute suite récurrente de la forme $u_{k+1} = M^{-1}(Nu_k + b)$ pour $k \geqslant 0$ et $u_0 \in \mathbb{R}^n$ converge vers u tel que $Au = b$.

Théorème 2. *La méthode associée à (M, N) converge si et seulement si $\rho(M^{-1}N) < 1$.*

La preuve repose entièrement sur le lemme suivant.

Lemme 3. *Soit $A \in \mathcal{M}_n(\mathbb{C})$ et soit $\varepsilon > 0$, alors il existe une norme subordonnée $||.||$ telle que*

$$||A|| \leqslant \rho(A) + \varepsilon.$$

Démonstration. On trigonalise A dans $\mathbb{C}$: soit $P \in \mathrm{GL}_n(\mathbb{C})$ telle que $P^{-1}AP = T = (t_{i,j})_{1 \leqslant i,j \leqslant n}$ soit triangulaire supérieure. On note également $D_\delta = \mathrm{diag}(1, \delta, \ldots, \delta^{n-1})$. On a [1]

$$T_\delta = D_\delta^{-1} T D_\delta = \begin{pmatrix} 1 & & & (0) \\ & \delta^{-1} & & \\ & & \ddots & \\ (0) & & & \delta^{1-n} \end{pmatrix} \begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,n} \\ & t_{2,2} & \cdots & t_{2,n} \\ & & \ddots & \vdots \\ (0) & & & t_{n,n} \end{pmatrix} \begin{pmatrix} 1 & & & (0) \\ & \delta & & \\ & & \ddots & \\ (0) & & & \delta^{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} t_{1,1} & \delta t_{1,2} & \cdots & \delta^{n-1} t_{1,n} \\ & t_{2,2} & \cdots & \delta^{n-2} t_{2,n} \\ & & \ddots & \vdots \\ (0) & & & t_{n,n} \end{pmatrix} = (\delta^{j-i} t_{i,j})_{1 \leqslant i,j \leqslant n}.$$

On définit alors la norme $||.||$ sur $\mathbb{R}^n$ par $||x|| = ||(PD_\delta)^{-1}x||_\infty$ et on note $|||.|||$ la norme subordonnée associée. On voit alors facilement que pour $B \in \mathcal{M}_n(\mathbb{C})$, $|||B||| = |||(PD_\delta)^{-1}BPD_\delta|||_\infty$, et on sait que si $B = (b_{i,j})_{i,j} \in \mathcal{M}_n(\mathbb{C})$, $|||B|||_\infty = \sup_{1 \leqslant i \leqslant n} \sum_{j=1}^n |b_{i,j}|$. Ainsi, si $\delta > 0$ est tel que pour tout $i \in [|1, n|]$, $\sum_{j=i+1}^n \delta^{j-i}|t_{i,j}| < \varepsilon$, alors

$$|||A||| = |||T_\delta|||_\infty = \sup_{1 \leqslant i \leqslant n} \sum_{j=1}^n \delta^{j-i}|t_{i,j}| \leqslant \rho(A) + \varepsilon.$$

□

1. On peut également voir cette égalité en remarquant que D_δ est une matrice de passage, exprimer l'endomorphisme T dans cette nouvelle base et utiliser les formules de changement de bases.

Démonstration (Théorème). Soit $u \in \mathbb{R}^n$ tel que $Au = b$, de telle sorte que $Mu = Nu + b$, et soit $e_k = u_k - u$. On a alors,

$$e_{k+1} = M^{-1}(Nu_k + b) - M^{-1}Nu - M^{-1}b = M^{-1}Ne_k$$

et donc par récurrence immédiate, $e_k = (M^{-1}N)^k e_0$. Deux cas se présentent alors.

- Ou bien $\rho(M^{-1}N) < 1$, et dans ce cas, d'après le lemme, il existe une norme subornée $||.||$ telle que $||M^{-1}N|| < 1$. On a alors, si on note aussi $||.||$ la norme sur $\mathbb{R}^n$ associée à $||.||$, $||e_k|| \leqslant ||(M^{-1}N)^k||\,||e_0|| \leqslant ||M^{-1}N||^k||e_0|| \underset{k\to+\infty}{\longrightarrow} 0$ et donc $(u_k)_k$ converge vers u.
- Ou bien $\rho(M^{-1}N) \geqslant 1$. Dans ce cas on note λ une valeur propre complexe de module supérieur ou égal à 1 et $v = v_1 + iv_2 \in \mathbb{C}^n$ le vecteur propre associé. On a alors $(M^{-1}N)^k\, v = \lambda^k\, v$ et donc la méthode ne converge pas pour $u_0 = u+v_1$ ou $u_0 = u+v_2$, puisqu'alors $e_k = \Re(\lambda^k\, v)$ ou $e_k = \Im(\lambda^k\, v)$ et $\lambda^k v$ ne converge pas vers 0, donc au moins sa partie réelle ou sa partie imaginaire ne converge pas vers 0.

□

Définition 4. Soit $A \in \mathrm{GL}_n(\mathbb{R})$ telle que $a_{i,i} \neq 0$ pour tout i. On note $D = \mathrm{diag}(a_{1,1}, \ldots, a_{n,n})$, $-E = (a_{i,j}\mathbb{1}_{i>j})$ et $-F = (a_{i,j}\mathbb{1}_{i<j})$ les parties diagonale, triangulaire inférieure stricte et triangulaire supérieure stricte de A. On définit alors les méthodes

- de Jacobi, où $M = D$ et $N = D - A$, et on pose $J = D^{-1}(D - A)$
- et de Gauss-Seidel, où $M = D - E$ et $N = F$ et on pose $\mathcal{L}_1 = (D - E)^{-1}F$.

Proposition 5. *Si A est une matrice tridiagonale, alors $\rho(\mathcal{L}_1) = (\rho(J))^2$.*

Démonstration. On commence par introduire la matrice $A(\mu)$ pour $\mu \neq 0$ définie par

$$A(\mu) = \begin{pmatrix} a_1 & \mu^{-1}\, c_2 & & (0) \\ \mu\, b_2 & a_2 & \ddots & \\ & \ddots & \ddots & \mu^{-1}\, c_n \\ (0) & & \mu\, b_n & a_n \end{pmatrix}$$

où $A(1) = A$. On remarque que si $Q(\mu) = \mathrm{diag}(1, \mu, \ldots, \mu^{n-1})$, $A(\mu) = Q(\mu)AQ(\mu)^{-1}$, et donc $\det(A(\mu)) = \det(A)$.

Les valeurs propres de J sont les racines du polynôme caractéristique $p_J(\lambda) = \det(D^{-1}(E+F) - \lambda I)$ qui sont aussi les racines du polynôme $q_J(\lambda) = \det(\lambda D - E - F)$. De même, les valeurs propres de $\mathcal{L}_1$ sont les racines du polynôme $p_{\mathcal{L}_1}(\lambda) = \det((D - E)^{-1}F - \lambda I)$ qui sont aussi celles du polynôme $q_{\mathcal{L}_1}(\lambda) = \det(\lambda D - \lambda E - F)$. Maintenant si $\lambda \in \mathbb{C}^*$, $q_{\mathcal{L}_1}(\lambda^2) = \det(\lambda^2 D - \lambda^2 E - F) = \lambda^n \det(\lambda D - \lambda E - \lambda^{-1}F) = \lambda^n \det(\lambda D - E - F) = \lambda^n q_J(\lambda)$ d'après le résultat préliminaire. Ainsi, les valeurs propres non nulles de $\mathcal{L}_1$ sont exactement les carrés des valeurs propres non nulles de J, d'où le résultat. □

Remarque. On justifie ici la formule utilisée pour la norme infinie subordonnée. Soit $A \in \mathcal{M}_n(\mathbb{R})$, alors, si $x \in \mathbb{R}^n$,

$$||Ax||_\infty = \max_{1\leqslant i\leqslant n} \Big| \sum_{j=1}^n a_{i,j}x_j \Big| \leqslant \Big(\max_{1\leqslant i\leqslant n} \sum_{j=1}^n |a_{i,j}| \Big) ||x||_\infty.$$

Ainsi, $||A||_\infty \leqslant \max_{1\leqslant i\leqslant n} \sum_{j=1}^n |a_{i,j}|$. D'autre part, si i_0 est tel que $\sum_{j=1}^n |a_{i_0,j}| = \max_{1\leqslant i\leqslant n} \sum_{j=1}^n |a_{i,j}|$, on définit $x = (x_j)_j$ par $x_j = a_{i_0,j}/|a_{i_0,j}|$ si $a_{i_0,j} \neq 0$ et $x_j = 1$ sinon, et on a alors $||x||_\infty = 1$, et

$$||Ax||_\infty = \max_{1\leqslant i\leqslant n} \Big| \sum_{j=1}^n a_{i,j}x_j \Big| \geqslant \Big| \sum_{j=1}^n a_{i_0,j}x_j \Big| = \sum_{j=1}^n |a_{i_0,j}| = \Big(\max_{1\leqslant i\leqslant n} \sum_{j=1}^n |a_{i,j}| \Big) ||x||_\infty$$

d'où le résultat.

4.5 Simplicité de $SO_3(\mathbb{R})$

Références : P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométrie, Tome premier*, Calvage & Mounet, 2013,
D. Perrin, *Cours d'Algèbre*, Ellipses, 1996.

Leçons concernées : 103, 106, 108, 160, 161, 204.

Théorème 1. *Le groupe $SO_3(\mathbb{R})$ est simple.*

Lemme 2. *Les retournements sont tous conjugués dans $SO_3(\mathbb{R})$.*

Démonstration. Soit r_D et $r_{D'}$ deux retournements de $SO_3(\mathbb{R})$ de droites D et D'. Soit $s \in SO_3(\mathbb{R})$ la rotation qui envoie D sur D', alors sr_Ds^{-1} est d'axe $s(D) = D'$ et d'angle π et est donc le retournement de droite D' i.e. $r_{D'}$. □

Lemme 3. *Le centre de $SO_3(\mathbb{R})$ est trivial.*

Démonstration. En effet soit $u \in Z(SO_3(\mathbb{R}))$. Alors pour tout retournement r_D de droite D, $ur_Du^{-1} = r_D$ est un retournement de droite $u(D)$, ainsi u stabilise toutes les droites du plan, et est donc une homothétie, et donc $u = \mathrm{id}$. □

Démonstration (Théorème). Soit H un sous-groupe non trivial distingué dans $SO_3(\mathbb{R})$. On sait que $SO_3(\mathbb{R})$ est engendré par les retournements, on montre alors que H contient un retournement. Cela suffit puisque ceux-ci sont tous conjugués dans $SO_3(\mathbb{R})$ et que H est distingué.

Soit $h \in H$ différent de l'identité. On considère

$$\varphi : \begin{array}{ccc} SO_3(\mathbb{R}) & \to & \mathbb{R} \\ g & \mapsto & \mathrm{Tr}(ghg^{-1}h^{-1}) \end{array}$$

qui est une application continue par continuité de la trace. Puisque tout élément de $SO_3(\mathbb{R})$ s'écrit dans une certaine base comme

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix},$$

la trace d'un élément de $SO_3(\mathbb{R})$ est de la forme $1 + 2\cos(\theta)$. Ainsi, puisque $SO_3(\mathbb{R})$ est connexe compact, son image par φ est un segment de $\mathbb{R}$ qui contient $\varphi(\mathrm{id}) = 3$, donc est de la forme $[a, 3]$, $a \leqslant 3$. Si par l'absurde $a = 3$, alors $\forall g \in SO_3(\mathbb{R})$, $ghg^{-1}h^{-1} = \mathrm{id}$ et donc $h \in Z(SO_3(\mathbb{R})) = \{\mathrm{id}\}$ ce qui est absurde. Ainsi, $a < 3$. On a $1 + 2\cos(\pi/n) \underset{n\to+\infty}{\longrightarrow} 3$, donc il existe $n \in \mathbb{N}^*$ tel que $a < 1 + 2\cos(\pi/n) < 3$. On considère alors g_n tel que $\varphi(g_n) = \mathrm{Tr}(g_nhg_n^{-1}h^{-1}) = 1 + 2\cos(\pi/n)$. Alors $h_n := g_nhg_n^{-1}h^{-1}$ est une rotation d'angle π/n de H puisque H est distingué, et donc h_n^n est une rotation d'angle π dans H, c'est-à-dire un retournement. □

Théorème 4. *Le groupe $SO_3(\mathbb{R})$ est connexe par arcs.*

Démonstration. Soit $u \in SO_3(\mathbb{R})$. On va montrer que u est dans la composante connexe par arcs de l'identité. On sait que dans une certaine base, u s'écrit

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

On pose alors, pour $t \in [0,1]$,

$$U_t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta t) & -\sin(\theta t) \\ 0 & \sin(\theta t) & \cos(\theta t) \end{pmatrix}.$$

Il est clair que $t \mapsto U_t$ est un chemin continu de $SO_3(\mathbb{R})$ reliant Id à U. □

Théorème 5. *Le groupe $O_n(\mathbb{R})$ est engendré par les réflexions et $SO_n(\mathbb{R})$ est engendré par les retournements.*

Démonstration. Soit $u \in O_n(\mathbb{R})$, et $F_u = \{x \in E, u(x) = x\}$ l'ensemble des points fixes de u. On raisonne par récurrence sur $p_u := n - \dim(F_u)$. Si $p_u = 0$, $u = \mathrm{id}$ et le résultat est évident. Si maintenant $p_u > 0$, soit $x \in F_u^\perp \backslash \{0\}$ et $y = u(x)$. Alors $x \neq y$, et $y \in F_u^\perp$ puisque F_u et donc $F_u^\perp$ sont stables par u. On a alors $< x - y, x + y >= 0$ puisque $||x|| = ||y||$, et donc $x - y$ est orthogonal à $x + y$. Soit τ la réflexion d'axe $x - y$. Alors $\tau(x - y) = y - x$ et $\tau(x + y) = x + y$ et donc $\tau(y) = x$. Enfin, $F_u \subset F_{\tau u}$ puisque $x - y \in F_u^\perp$ et l'inclusion est stricte puisque x est dans $F_{\tau u}$ et pas dans F_u. On applique alors l'hypothèse de récurrence pour obtenir $\tau u = \tau_1 \cdots \tau_k$, d'où le résultat.

Soit maintenant $u \in SO_n(\mathbb{R})$, alors $u = \tau_1 \cdots \tau_k$ est produit d'un nombre pair de réflexions (puisque leur déterminant est -1). Si $n = 3$, $-\tau_i$ est un renversement (considérer les matrices), d'où le résultat.

Si $n \geqslant 3$, il nous faut montrer que tout produit de deux réflexions $v = \tau_1\tau_2$ s'écrit comme un produit de retournements. Soient H_1, H_2 les hyperplans associés à τ_1, τ_2 et soit F un sous-espace de dimension $n - 3$ de $H_1 \cap H_2$. Alors $v_{|F} = \mathrm{id}$ et donc $V(F^\perp) \subset F^\perp$. Ainsi, d'après le premier cas, $v_{|F^\perp}$ est un produit $\sigma_1 \cdots \sigma_k$ de retournements, on prolonge alors les σ_i par l'identité sur V, et on obtient le résultat. □

Commentaire : le développement est un peu court, on peut suivant les leçons justifier la connexité par arcs de $SO_3(\mathbb{R})$ ou bien le fait que $SO_3(\mathbb{R})$ soit engendré par les retournements.

5 Développements non utilisés

5.1 Équation de la chaleur sur $\mathbb{R}$

Référence : E.M. Stein, M. Shakarchi, *Fourier analysis, an introduction*, Princeton University Press, 2003. [1]

Leçons concernées : 222, 239, 250.

Théorème 1. *Soit $f \in \mathcal{S}(\mathbb{R})$. Alors il existe une unique fonction $u \in \mathcal{C}^2(\mathbb{R} \times \mathbb{R}_+^*)$ vérifiant*

(i) $\dfrac{\partial u}{\partial t}(x,t) = \dfrac{\partial^2 u}{\partial x^2}(x,t), \quad \forall (x,t) \in \mathbb{R} \times \mathbb{R}_+^*$

(ii) $x \mapsto u(x,t)$ *tend uniformément vers f lorsque t tend vers 0, c'est-à-dire que*

$$\sup_{x \in \mathbb{R}} |u(x,t) - f(x)| \underset{t \to 0}{\longrightarrow} 0$$

(iii) $x \mapsto u(x,t)$ *appartient à $\mathcal{S}(\mathbb{R})$ uniformément par rapport à t, c'est-à-dire que pour tout $T > 0$,*

$$\forall k, l \geqslant 0, \quad M_{k,l}^T := \sup_{0<t<T} \sup_{x \in \mathbb{R}} \left| x^k \frac{\partial^l u}{\partial x^l}(x,t) \right| < +\infty.$$

De plus la solution est donnée par $u(x,t) = (f * \mathcal{H}_t)(x)$ où

$$\forall (x,t) \in \mathbb{R} \times \mathbb{R}_+^*, \quad \mathcal{H}_t(x) = \frac{1}{\sqrt{4\pi t}} e^{-x^2/4t}.$$

Démonstration. On raisonne par analyse-synthèse.

Analyse : on suppose que $u \in \mathcal{C}^2(\mathbb{R} \times \mathbb{R}_+^*)$ est solution du problème. Puisque $u(.,t) \in \mathcal{S}(\mathbb{R})$ on peut considérer la transformée de Fourier partielle de u :

$$\forall t > 0, \forall \xi \in \mathbb{R}, \quad \widehat{u}(\xi, t) = \int_{\mathbb{R}} u(x,t) e^{-ix\xi} dx.$$

Soit $\xi \in \mathbb{R}$, on applique alors le théorème de dérivation sous l'intégrale à $t \mapsto \widehat{u}(\xi, t)$ sur tout intervalle $]0, T[$, pour $T > 0$:

(i) $\forall x \in \mathbb{R}$, $t \mapsto u(x,t)e^{-ix\xi}$ est dérivable sur $]0,T[$

(ii) $\forall t \in]0,T[$, $x \mapsto u(x,t)e^{-ix\xi} \in L^1(\mathbb{R})$ puisque $u(.,t) \in \mathcal{S}(\mathbb{R})$

(iii) $\forall x \in \mathbb{R}, \forall t \in]0,T[$,

$$\left| \frac{\partial}{\partial t}\Big(u(x,t)e^{-ix\xi}\Big) \right| = \left| \frac{\partial u}{\partial t}(x,t) \right| = \left| \frac{\partial^2 u}{\partial x^2}(x,t) \right| \leqslant \frac{M_{0,2}^T + M_{2,2}^T}{1 + |x|^2}$$

qui est intégrable sur $\mathbb{R}$ et ne dépend pas de t.

1. Merci à Michel Nassif pour l'idée et l'aide sur certains points du développement.

On obtient ainsi, pour $\xi \in \mathbb{R}$ et $t > 0$,

$$\frac{\partial \widehat{u}}{\partial t}(\xi, t) = \int_{\mathbb{R}} \frac{\partial}{\partial t}\Big(u(x,t)e^{-ix\xi}\Big)dx = \int_{\mathbb{R}} \frac{\partial^2 u}{\partial x^2}(x,t)e^{-ix\xi}dx.$$

En réalisant deux intégrations par parties on obtient alors pour $\xi \in \mathbb{R}$ et $t > 0$,

$$\frac{\partial \widehat{u}}{\partial t}(\xi, t) = -\xi^2 \widehat{u}(\xi, t)$$

et ainsi, pour tout $\xi \in \mathbb{R}$, il existe $A(\xi) \in \mathbb{R}$ tel que pour $t > 0$,

$$\widehat{u}(\xi, t) = A(\xi)e^{-\xi^2 t}.$$

Or on a, pour $\xi \in \mathbb{R}$, puisque $f \in \mathcal{S}(\mathbb{R})$, pour tout $t > 0$,

$$\big|\widehat{u}(\xi, t) - \widehat{f}(\xi)\big| \leqslant \int_{\mathbb{R}} \big|u(x,t) - f(x)\big|dx.$$

Soit $\varepsilon > 0$. Puisque $f \in \mathcal{S}(\mathbb{R}) \subset L^1(\mathbb{R})$ et que pour $t \in]0,1[$, $|u(x,t)| \leqslant \frac{M^1_{0,0}+M^1_{2,0}}{1+|x|^2}$, il existe $A > 0$ tel que pour $t \in]0,1[$,

$$\int_{|x|>A} \big|u(x,t) - f(x)\big|dx \leqslant \int_{|x|>A} |u(x,t)|dx + \int_{|x|>A} |f(x)|dx < \varepsilon.$$

Ainsi, pour $t \in]0,1[$,

$$\begin{aligned}\int_{\mathbb{R}} \big|u(x,t) - f(x)\big|dx &= \int_{|x|>A} \big|u(x,t) - f(x)\big|dx + \int_{|x|\leqslant A} \big|u(x,t) - f(x)\big|dx \\ &< \varepsilon + 2A \sup_{x\in\mathbb{R}} |u(x,t) - f(x)| \underset{t\to 0}{\longrightarrow} \varepsilon\end{aligned}$$

d'après l'hypothèse (ii). Ainsi, en faisant $\varepsilon \to 0$, on obtient que pour tout $\xi \in \mathbb{R}$, $\widehat{u}(\xi, t) \underset{t\to 0}{\longrightarrow} \widehat{f}(\xi)$, et donc $A = \widehat{f}$. On obtient alors $\widehat{u}(\xi, t) = \widehat{f}(\xi)e^{-\xi^2 t}$. Puisque pour tout $t > 0$, $\xi \mapsto \widehat{f}(\xi)e^{-\xi^2 t} \in \mathcal{S}(\mathbb{R})$, on peut appliquer l'inversion de Fourier pour avoir, pour $(x,t) \in \mathbb{R} \times \mathbb{R}^*_+$,

$$\begin{aligned}u(x,t) &= \frac{1}{2\pi}\int_{\mathbb{R}} \widehat{f}(\xi)e^{-\xi^2 t}e^{ix\xi}d\xi = \frac{1}{2\pi}\int_{\mathbb{R}} \Big(\int_{\mathbb{R}} f(s)e^{-is\xi}ds\Big)e^{-\xi^2 t}e^{ix\xi}d\xi \\ &= \int_{\mathbb{R}} f(s)\Big(\frac{1}{2\pi}\int_{\mathbb{R}} e^{-\xi^2 t}e^{-i(s-x)\xi}d\xi\Big)ds = \int_{\mathbb{R}} f(s)\frac{1}{\sqrt{4\pi t}}e^{-(x-s)^2/4t}ds = (f * \mathcal{H}_t)(x)\end{aligned}$$

par théorème de Fubini et par transformée de Fourier d'une gaussienne. On a donc unicité de la solution.

Synthèse : on considère $u(x,t) = (f * \mathcal{H}_t)(x)$ pour tout $(x,t) \in \mathbb{R} \times \mathbb{R}_+^*$. D'après l'analyse on sait que

$$u(x,t) = \frac{1}{2\pi} \int_{\mathbb{R}} \widehat{f}(\xi) e^{-\xi^2 t} e^{ix\xi} d\xi$$

en appliquant le théorème de dérivation sous l'intégrale on obtient la régularité de u, qui est en fait $\mathcal{C}^\infty(\mathbb{R} \times \mathbb{R}_+^*)$ et le fait qu'elle vérifie l'équation de la chaleur sur $\mathbb{R} \times \mathbb{R}_+^*$.

La convergence uniforme de $u(.,t)$ vers f provient quant à elle du fait que $(\mathcal{H}_t)_{t>0}$ est une approximation de l'unité. En effet, il est clair que $\mathcal{H}_t$ est positive d'intégrale 1, et par changement de variable on obtient

$$\int_{|x|>\eta} \mathcal{H}_t(x) dx = \frac{1}{\sqrt{\pi}} \int_{|y|>\eta/\sqrt{4t}} e^{-y^2} dy \underset{t\to 0}{\longrightarrow} 0$$

et $f \in \mathcal{S}(\mathbb{R})$ donc est uniformément continue sur $\mathbb{R}$.

Enfin, pour montrer le point (iii),

$$\begin{aligned} |u(x,t)| &\leqslant \int_{|y|\leqslant |x|/2} |f(x-y)| \mathcal{H}_t(y)\, dy + \int_{|y|>|x|/2} |f(x-y)| \mathcal{H}_t(y)\, dy \\ &\leqslant \frac{C_N}{(1+|x|)^N} + C \frac{1}{\sqrt{t}} e^{-cx^2/t} \end{aligned}$$

en utilisant le fait que $f \in \mathcal{S}(\mathbb{R})$. Ainsi, pour tout $T > 0$,

$$\forall k \geqslant 0, \quad \sup_{0<t<T} \sup_{x\in\mathbb{R}} |x^k u(x,t)| < +\infty.$$

On obtient la même chose pour les dérivées partielles de u par rapport à x en appliquant un théorème de dérivation sous l'intégrale et en utilisant le fait que $f \in \mathcal{S}(\mathbb{R})$. □

Remarque. On peut raisonner de la même manière avec l'équation de Schrödinger, et c'est plus simple puisque dans ce cas la condition initiale est simplement la valeur de $u(.,t)$ en 0, puisque u est définie sur $\mathbb{R}^2$. On n'a donc pas besoin de justifier le passage à la limite dans la transformée de Fourier de u.

Commentaire : c'est sûrement trop long pour un développement, peut être préférer l'équation de Schrödinger qui manipule les mêmes outils mais est plus simple.

5.2 Équation de la chaleur sur la barre

Références : H. Queffélec, C. Zuily, *Éléments d'analyse*, Dunod, 2002.
L. C. Evans, *Partial differential equations*, American Mathematical Society, 1998.

Leçons concernées : 209, 222, 241, 246.

On se donne $L > 0$ et on note $Q =]0, L[\times]0, +\infty[$, $\widetilde{Q} = [0, L]\times]0, +\infty[$ et $\overline{Q} = [0, L] \times [0, +\infty[$. On considère le problème suivant, noté (EC) : trouver u qui vérifie

$$u \in \mathcal{C}^0(\overline{Q}), \quad u \in \mathcal{C}_1^2(\widetilde{Q}) \tag{1}$$

$$\frac{\partial u}{\partial t} - \frac{\partial^2 u}{\partial x^2} = 0 \quad \text{dans} \quad Q \tag{2}$$

$$u(0,t) = u(L,t) = 0, \quad t \in [0, +\infty[\tag{3}$$

$$u(x,0) = h(x), \quad x \in [0, L] \tag{4}$$

avec h une fonction $\mathcal{C}^1$ sur $]0, L[$, continue sur $[0, L]$ telle que $h(0) = h(L) = 0$ et ou $\mathcal{C}_1^2(\widetilde{Q})$ est l'ensemble des fonctions de classe $\mathcal{C}^1$ en temps et de classe $\mathcal{C}^2$ en espace sur $\widetilde{Q}$.

Théorème 1. *Le problème (EC) admet une solution $u \in \mathcal{C}^\infty(Q)$.*

Démonstration. Heuristique : on commence d'abord par chercher une solution de (2) sous la forme $u(x,t) = f(x)g(t)$. (2) se traduit alors par $f(x)g'(t) = f''(x)g(t)$. On suppose que f et g ne s'annulent pas sur $]0, +\infty[$. On a donc pour tout $(x,t) \in Q$

$$\frac{f''(x)}{f(x)} = \frac{g'(t)}{g(t)}$$

et donc les deux membres sont constants, égaux à $\lambda \in \mathbb{R}$. On a alors $f''(x) = \lambda f(x)$ et $g'(t) = \lambda g(t)$. On étudie alors la première équation :

(i) Si $\lambda > 0$, alors on obtient $f(x) = Ae^{\sqrt{\lambda}x} + Be^{-\sqrt{\lambda}x}$ et les conditions au bord (3) nous donnent $A + B = Ae^{\sqrt{\lambda}L} + Be^{-\sqrt{\lambda}L} = 0$ et donc $A = B = 0$ et $u = 0$ ce qui ne convient pas à (4) en général.

(ii) Si $\lambda = 0$, alors $f(x) = Ax + B$ et (3) nous donnent la encore $A = B = 0$ et $u = 0$.

(iii) Enfin, si $\lambda < 0$, alors on obtient en notant ξ une racine de $-\lambda$, $f(x) = A\cos(\xi x) + B\sin(\xi x)$. Les conditions au bord (3) donnent alors $A = 0$ et $B\sin(\xi L) = 0$ donc $\xi = \frac{n\pi}{L}$, $n \in \mathbb{Z}$. On résout alors l'équation que vérifie g pour trouver $g(t) = Ce^{-\xi^2 t}$.

Synthèse : on a donc trouvé une famille de solutions de la forme $u_n(x,t) = a_n \sin\left(\frac{n\pi}{L}x\right) e^{-\frac{n^2\pi^2}{L^2}t}$, $a_n \in \mathbb{R}$, $n \in \mathbb{Z}$. Cependant, ces solutions ne vérifient pas forcément (4), on va donc chercher une solution u sous la forme $u(x,t) = \sum_{n=0}^{+\infty} a_n \sin\left(\frac{n\pi}{L}x\right) e^{-\frac{n^2\pi^2}{L^2}t}$.

On prolonge h d'abord par imparité sur $[-L,0]$ puis par $2L$-périodicité sur $\mathbb{R}$ et on note encore h le prolongement obtenu. Celui-ci est continu et de classe $\mathcal{C}^1$ par morceaux puisque par hypothèse $h(0) = h(L) = 0$. Une conséquence du théorème de Fejér nous assure alors que la série de Fourier de h converge absolument vers h sur $\mathbb{R}$. Par imparité, on a, pour $x \in \mathbb{R}$

$$h(x) = \sum_{n=0}^{+\infty} a_n \sin\left(\frac{n\pi}{L}x\right)$$

avec $\sum_{n=0}^{+\infty} |a_n| < \infty$. Ainsi, la série $\sum a_n \sin\left(\frac{n\pi}{L}x\right) e^{-\frac{n^2\pi^2}{L^2}t}$ converge normalement sur $\overline{Q}$, sa somme

$$u(x,t) = \sum_{n=0}^{+\infty} a_n \sin\left(\frac{n\pi}{L}x\right) e^{-\frac{n^2\pi^2}{L^2}t}$$

est donc une fonction continue sur $\overline{Q}$. Il nous faut alors montrer que u est de classe $\mathcal{C}^\infty$ sur $\widetilde{Q}$. On pose pour cela $u_n(x,t) = a_n \sin\left(\frac{n\pi}{L}x\right) e^{-\frac{n^2\pi^2}{L^2}t}$. Pour tout $n \in \mathbb{N}$, u_n est $\mathcal{C}^\infty$ sur $\widetilde{Q}$. De plus, sur $[\varepsilon, +\infty[$, $\varepsilon > 0$, un dérivée d'ordre k de u_n est majorée par

$$C_k |a_n| n^{2k} e^{-\frac{n^2\pi^2}{L^2}\varepsilon}$$

qui est le terme général d'une série convergente puisque $n^{2k} e^{-\frac{n^2\pi^2}{L^2}\varepsilon}$ est borné et que la série $\sum |a_n|$ converge. Ainsi, par le théorème de dérivation sous le signe somme, sur tout compact de $\widetilde{Q}$, u admet des dérivées partielles à tout ordre, et est donc $\mathcal{C}^\infty$ sur $\widetilde{Q}$. D'autre part puisque tous les u_n vérifient (2) et par théorème de dérivation sous le signe somme, u vérifie (2). Les conditions (3) et (4) étant trivialement vérifiées, u est une solution de (EC). □

Théorème 2. *Le problème (EC) admet une unique solution.*

Démonstration. L'existence d'une solution ayant déjà été prouvé, on montre l'unicité. Soit u_1, u_2 deux solutions de (EC). On pose $w = u_1 - u_2$ qui vérifie alors (EC) pour la condition initiale $h = 0$. On considère $e(t) = \int_0^L w^2(x,t)\, dx$ pour $t \in [0, +\infty[$. On applique le théorème de dérivation sous l'intégrale sur tout compact de $]0, +\infty[$ pour obtenir, pour $t \in]0, +\infty[$,

$$\begin{aligned} e'(t) &= 2\int_0^L w(x,t)\frac{\partial w}{\partial t}(x,t)\, dx = 2\int_0^L w(x,t)\frac{\partial^2 w}{\partial x^2}(x,t)\, dx \\ &= 2\left[w(x,t)\frac{\partial w}{\partial x}(x,t)\right]_0^L - \int_0^L \left(\frac{\partial w}{\partial x}(x,t)\right)^2 dx = -\int_0^L \left(\frac{\partial w}{\partial x}(x,t)\right)^2 dx \leqslant 0 \end{aligned}$$

par (2), intégration par parties et (3), puisque $w \in \mathcal{C}_1^2(\widetilde{Q})$ et donc $x \mapsto \frac{\partial w}{\partial x}(x,t)$ est continue sur $[0,L]$. Ainsi, pour $t \in [0,+\infty[$, $e(t) \leqslant e(0) = 0$ par (4). Or on a aussi $e \geqslant 0$, donc $e(t) = 0$ pour $t \in [0,+\infty[$, et par continuité de $x \mapsto w(x,t)$ sur $[0,L]$, $w(x,t) = 0$ pour tout $x \in [0,L]$ et donc $u_1 = u_2$. □

On peut montrer l'unicité de la solution en les supposant seulement de classe $\mathcal{C}^2$ sur Q (et non sur $\widetilde{Q}$) par une méthode du maximum. On note (EC') le problème (EC) où les solutions sont cherchées dans $\mathcal{C}^0(\overline{Q}) \cap \mathcal{C}^2(Q)$.

Lemme 3. *Soit P l'opérateur $\frac{\partial^2}{\partial x^2} - \frac{\partial}{\partial t}$ et soit $u \in \mathcal{C}^0(\overline{Q}) \cap \mathcal{C}^2(Q)$ telle que $Pu \leqslant 0$ sur Q. Si $T > 0$ et $K := [0,L] \times [0,T]$, alors*

$$\sup_K u = \sup_{\partial Q \cap K} u.$$

Démonstration. On pose $\varepsilon > 0$ et $u_\varepsilon(x,t) = u(x,t) + \varepsilon x^2$. Alors $Pu_\varepsilon = Pu + 2\varepsilon \geqslant 2\varepsilon$ sur Q. On considère $m_\varepsilon = (x_\varepsilon, t_\varepsilon)$ le maximum de u_ε sur K. Si par l'absurde $m_\varepsilon \notin \partial Q \cap K$, alors $0 < x_\varepsilon < L$ et donc

$$\frac{\partial u_\varepsilon}{\partial x}(m_\varepsilon) = 0 \quad \text{et} \quad \frac{\partial^2 u_\varepsilon}{\partial x^2}(m_\varepsilon) \leqslant 0$$

et d'autre part $0 < t_\varepsilon \leqslant T$ donc

$$\frac{\partial u_\varepsilon}{\partial t}(m_\varepsilon) = \lim_{\substack{h \to 0 \\ <}} \frac{u_\varepsilon(x_\varepsilon, t_{\varepsilon+h}) - u_\varepsilon(x_\varepsilon, t_\varepsilon)}{h} \geqslant 0.$$

Ainsi $Pu_\varepsilon \leqslant 0$ d'où l'absurdité. On peut conclure :

$$\sup_K u \leqslant \sup_K u_\varepsilon = \sup_{\partial Q \cap K} u_\varepsilon \leqslant \sup_{\partial Q \cap K} u + \varepsilon L^2$$

et en faisant tendre ε vers 0 on obtient la conclusion. □

Proposition 4. *La problème (E'C) admet une unique solution.*

Démonstration. Soient u, v deux solutions de (EC') et soit $w = u - v$, qui vérifie (EC') avec comme condition initiale $h \equiv 0$, c'est-à-dire que $w = 0$ sur ∂Q. Soit $T > 0$, d'après (2), $Pw = 0$ sur Q et donc d'après le lemme $w \leqslant 0$ sur $[0,L] \times [0,T]$. D'autre part puisque $P(-w) = 0$ sur Q, le lemme donne également $w \geqslant 0$ sur $[0,L] \times [0,T]$ et donc, puisque T est arbitraire, $w = 0$ sur $\overline{Q}$. □

5.3 Extrema liés (par le calcul matriciel)

Références : X. Gourdon, *Les maths en tête, Analyse*, Ellipses, 2008.

Théorème 1. *Soit $f, g_1, \dots, g_r$ des fonctions réelles de classe $\mathcal{C}^1$ sur un ouvert U de $\mathbb{R}^n$. On note X l'ensemble de $x \in U$ tels que $g_1(x) = \cdots = g_r(x) = 0$. Si $f_{|X}$ admet un extremum local en a et les formes linéaires $dg_1(a), \dots, dg_r(a)$ sont indépendantes, alors il existe $\lambda_1, \dots, \lambda_r$ dans $\mathbb{R}$ tels que*

$$df(a) = \lambda_1 dg_1(a) + \cdots + \lambda_r dg_r(a),$$

autrement dit, les formes linéaires $df(a), dg_1(a), \dots, dg_r(a)$ sont liées.

Démonstration. On note $s = n - r$, et on identifie $\mathbb{R}^n$ et $\mathbb{R}^s \times \mathbb{R}^r$, on note en particulier $(x, y) = (x_1, \dots, x_s, y_1, \dots, y_r)$ les éléments de $\mathbb{R}^n$. Soit $(\alpha, \beta) = a$ et $g = (g_1, \dots, g_r)$. On remarque que par dimension de $(\mathbb{R}^n)^*$, $r \leqslant n$ et que le cas $r = n$ est trivial. Supposons alors $r < n$. Puisque les formes linéaires $dg_1(a), \dots, dg_r(a)$ sont supposées indépendantes, la matrice jacobienne de g,

$$\begin{pmatrix} \frac{\partial g_1}{\partial x_1}(a) & \cdots & \frac{\partial g_1}{\partial x_s}(a) & \frac{\partial g_1}{\partial y_1}(a) & \cdots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1}(a) & \cdots & \frac{\partial g_r}{\partial x_s}(a) & \frac{\partial g_r}{\partial y_1}(a) & \cdots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix}$$

est de rang r, on peut donc en extraire une sous matrice de taille $r \times r$ inversible, et quitte à permuter les variables on obtient

$$D_y g(a) = \begin{pmatrix} \frac{\partial g_1}{\partial y_1}(a) & \cdots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots \\ \frac{\partial g_r}{\partial y_1}(a) & \cdots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix}$$

inversible. On peut alors appliquer le théorème des fonctions implicites pour obtenir V un voisinage de α, W un voisinage de β tels que $V \times W \subset U$, et $\varphi : V \to W$ de classe $\mathcal{C}^1$ telle que $(x \in V, y \in W \text{ et } g(x, y) = 0) \Leftrightarrow (x \in V \text{ et } y = \varphi(x))$. Ainsi, au voisinage de a, X est le graphe de φ. Soit $h : x \mapsto f(x, \varphi(x))$. La fonction h est de classe $\mathcal{C}^1$ et admet un extremum local en α puisque $(x, \varphi(x)) \in X$ et $(\alpha, \varphi(\alpha)) = a$. Ainsi, pour $1 \leqslant i \leqslant s$,

$$\frac{\partial h}{\partial x_i}(\alpha) = \frac{\partial f}{\partial x_i}(a) + \sum_{j=1}^{r} \frac{\partial \varphi_j}{\partial x_i}(\alpha) \frac{\partial f}{\partial y_j}(a) = 0.$$

D'autre part, puisque pour tout $1 \leqslant k \leqslant r$, pour tout $x \in V$, $g_k(x, \varphi(x)) = 0$, on obtient, pour $1 \leqslant i \leqslant s$,

$$\frac{\partial g_k}{\partial x_i}(a) + \sum_{j=1}^{r} \frac{\partial \varphi_j}{\partial x_i}(\alpha) \frac{\partial g_k}{\partial y_j}(a) = 0.$$

Ainsi, les s premières colonnes de la matrice

$$M = \begin{pmatrix} \frac{\partial f}{\partial x_1}(a) & \cdots & \frac{\partial f}{\partial x_s}(a) & \frac{\partial f}{\partial y_1}(a) & \cdots & \frac{\partial f}{\partial y_r}(a) \\ \frac{\partial g_1}{\partial x_1}(a) & \cdots & \frac{\partial g_1}{\partial x_s}(a) & \frac{\partial g_1}{\partial y_1}(a) & \cdots & \frac{\partial g_1}{\partial y_r}(a) \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial g_r}{\partial x_1}(a) & \cdots & \frac{\partial g_r}{\partial x_s}(a) & \frac{\partial g_r}{\partial y_1}(a) & \cdots & \frac{\partial g_r}{\partial y_r}(a) \end{pmatrix}$$

sont des combinaisons linéaires des r dernières et donc la matrice est de rang $\mathrm{rg}(M) \leqslant r$. Ainsi, les $r+1$ lignes sont liées, ce qui donne l'existence de $\mu_0, \mu_1, \ldots, \mu_r$ dans $\mathbb{R}$ tels que $\mu_0 df(a) + \mu_1 dg_1(a) + \cdots + \mu_r dg_r(a) = 0$, or $\mu_0 \neq 0$ par liberté de la famille $dg_1(a), \ldots, dg_r(a)$ et on obtient le résultat. □

5.4 Formule des compléments

Référence : E. Amar, E. Matheron, *Analyse complexe*, Cassini, 2004.

Leçons concernées : 235, 236, 239, 245.

Théorème 1. *La fonction* Γ *définie par*

$$\forall z \in \{z \in \mathbb{C} \mid \Re(z) > 0\} \quad \Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t} dt$$

vérifie

$$\forall z \in \{z \in \mathbb{C} \mid 0 < \Re(z) < 1\} \quad \Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

Démonstration. D'après le théorème de prolongement analytique, il suffit de montrer que pour tout $\alpha \in]0,1[$, $\Gamma(\alpha)\Gamma(1-\alpha) = \frac{\pi}{\sin(\pi\alpha)}$. Soit alors $\alpha \in]0,1[$. D'après le théorème de Fubini-Tonelli, si $U = \{(t,s) \in \mathbb{R}^d \mid s > 0, t > 0\}$,

$$\begin{aligned}\Gamma(\alpha)\Gamma(1-\alpha) &= \int_0^{+\infty} t^{\alpha-1} e^{-t}\, dt \int_0^{+\infty} s^{-\alpha} e^{-s}\, ds \\ &= \int_U t^{\alpha-1} s^{-\alpha} e^{-t-s}\, dt\, ds = \int_U \left(\frac{t}{s}\right)^{\alpha} e^{-(t+s)}\, ds\, \frac{dt}{t}.\end{aligned}$$

On réalise alors le changement de variables $\varphi : (t,s) \mapsto (u,v) = \left(s+t, \frac{s}{t}\right)$ qui est un $\mathcal{C}^1$ difféomorphisme de U sur U d'inverse $\varphi^{-1}(u,v) = \left(\frac{u}{1+v}, \frac{uv}{1+v}\right)$. Le jabobien de φ en (t,s) est :

$$\left|\det \begin{pmatrix} 1 & 1 \\ \frac{1}{t} & -\frac{s}{t^2} \end{pmatrix}\right| = \frac{1}{t} + \frac{s}{t^2} = \frac{1}{t} + \frac{v}{t} = \frac{1+v}{t}.$$

On a donc, par le théorème de Fubini-Tonelli,

$$\Gamma(\alpha)\Gamma(1-\alpha) \;=\; \int_U v^{-\alpha} e^{-u} \frac{du\, dv}{1+v} \;=\; \int_0^{+\infty} \frac{dv}{v^{\alpha}(1+v)} \int_0^{+\infty} e^{-u} du \;=\; \int_0^{+\infty} \frac{dv}{v^{\alpha}(1+v)}$$

et on conclut à l'aide du lemme suivant. □

Lemme 2. *Pour tout* $\alpha \in]0,1[$*, on a*

$$\int_0^{+\infty} \frac{dt}{t^{\alpha}(1+t)} = \frac{\pi}{\sin(\pi\alpha)}.$$

Démonstration. Soit $\alpha \in]0,1[$. On note $I_\alpha = \int_0^{+\infty} \frac{dt}{t^\alpha(1+t)}$ dont on remarque qu'elle est bien définie comme l'intégrale de la fonction $u(t) = \frac{1}{t^\alpha(1+t)}$ positive. On a de plus $I_\alpha < +\infty$ puisque u est continue sur $]0,+\infty[$, et que $u(t) \underset{0}{\sim} \frac{1}{t^\alpha}$ intégrable en 0 et $u(t) \underset{+\infty}{\sim} \frac{1}{t^{\alpha+1}}$ intégrable en $+\infty$.

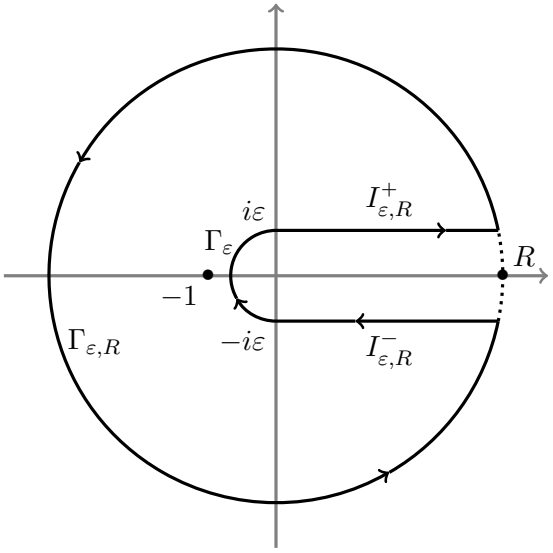
On considère alors $\Omega = \mathbb{C}\backslash[0,+\infty[$ et la fonction f définie sur $\Omega\backslash\{-1\}$ par

$$f(z) = \frac{1}{z^\alpha(1+z)}$$

où l'on convient que $z^\alpha = r^\alpha e^{i\alpha\theta}$ si $z = re^{i\theta}$ avec $0 < \theta < 2\pi$. La fonction f est holomorphe sur $\Omega\backslash\{-1\}$ avec un pôle simple en -1 de résidu

$$\mathrm{res}(f,-1) = \frac{1}{(-1)^\alpha} = e^{-i\pi\alpha}.$$

Pour $R > 1$ et $0 < \varepsilon < 1$ on définit alors le chemin orienté $I^-_{\varepsilon,R} \cup \Gamma_\varepsilon \cup I^+_{\varepsilon,R}\gamma_{\varepsilon,R} = \Gamma_{\varepsilon,R}\cup$ où $I^-_{\varepsilon,R} = [-i\varepsilon, -i\varepsilon + \sqrt{R^2-\varepsilon^2}]$, $\Gamma_\varepsilon = \{e^{i\theta} \mid \pi/2 < \theta < 3\pi/2\}$, $I^+_{\varepsilon,R} = [i\varepsilon, i\varepsilon + \sqrt{R^2-\varepsilon^2}]$ et $\Gamma_{\varepsilon,R} = \{Re^{i\theta} \mid \theta \in [-\pi,\pi], |\theta| > \theta_{\varepsilon,R}\}$ avec $\theta_{\varepsilon,R} = \arctan(\varepsilon/\sqrt{R^2-\varepsilon^2})$.



Puisque -1 est à l'intérieur de $\gamma_{\varepsilon,R}$, le théorème des résidus donne

$$\int_{\gamma_{\varepsilon,R}} f(z)dz = 2i\pi e^{-i\pi\alpha}.$$

- Sur Γ_ε, on a

$$\left|\int_{\Gamma_\varepsilon} f(z)dz\right| \leqslant \frac{1}{\varepsilon^\alpha(1+\varepsilon)} \times \pi\varepsilon = \frac{\pi\varepsilon^{1-\alpha}}{1+\varepsilon} \underset{\varepsilon\to 0}{\longrightarrow} 0,$$

- sur $\Gamma_{\varepsilon,R}$, on a

$$\left|\int_{\Gamma_{\varepsilon,R}} f(z)dz\right| \leqslant \frac{1}{R^\alpha(1+R)} \times (2\pi R - 2\theta_{\varepsilon,R}) \leqslant \frac{2\pi R^{1-\alpha}}{1+R} \underset{R\to+\infty}{\longrightarrow} 0,$$

- sur $I^+_{\varepsilon,R}$, on a

$$\int_{I^+_{\varepsilon,R}} f(z)dz = \int_0^{\sqrt{R^2-\varepsilon^2}} f(i\varepsilon+t)dt = \int_0^{\sqrt{R^2-\varepsilon^2}} \frac{dt}{(i\varepsilon+t)^\alpha(1+i\varepsilon+t)}$$

or $(i\varepsilon+t)^\alpha \underset{\varepsilon\to0^+}{\longrightarrow} t^\alpha$. Ainsi, avec

· $\mathbb{1}_{]0,\sqrt{R^2-\varepsilon^2}]} f(i\varepsilon+t) \underset{\varepsilon\to0^+}{\longrightarrow} \mathbb{1}_{]0,R]} \frac{1}{t^\alpha(1+t)}$

· $\left|\mathbb{1}_{]0,\sqrt{R^2-\varepsilon^2}]} f(i\varepsilon+t)\right| \leqslant \mathbb{1}_{]0,R]} \frac{1}{t^\alpha(1+t)}$ intégrable,

on obtient par convergence dominée

$$\lim_{\varepsilon\to0} \int_{I^+_{\varepsilon,R}} f(z)dz = \int_0^R \frac{dt}{t^\alpha(1+t)}$$

et donc

$$\lim_{R\to+\infty} \lim_{\varepsilon\to0} \int_{I^+_{\varepsilon,R}} f(z)dz = I_\alpha.$$

- De la même manière, puisque $(-i\varepsilon+t)^\alpha \underset{\varepsilon\to0^+}{\longrightarrow} e^{2i\pi\alpha}t^\alpha$, on a par convergence dominée

$$\lim_{R\to+\infty} \lim_{\varepsilon\to0} \int_{I^-_{\varepsilon,R}} f(z)dz = e^{-2i\pi\alpha} I_\alpha.$$

On conclut : d'après l'orientation du chemin, on a $(1-e^{-2i\pi\alpha})I_\alpha = 2i\pi e^{-i\pi\alpha}$ et donc

$$I_\alpha = \frac{\pi}{\sin(\pi\alpha)}.$$

□

Commentaire : pour justifier le recasage dans la leçon 235 : interversion de limites et d'intégrales, on note qu'on applique deux fois le théorème de Fubini-Tonelli ainsi que deux fois le théorème de convergence dominée.

5.5 Groupes d'ordre pq

Référence : D. Perrin, *Cours d'Algèbre*, Ellipses, 1996.

Leçons concernées : 103, 104, 120.

Théorème 1. *Soient $p < q$ deux nombres premiers. On a*

(i) Si $p \nmid (q-1)$, tout groupe d'ordre pq est cyclique.

(ii) Si $p \mid (q-1)$, il y a exactement deux groupes d'ordre pq non isomorphes, un groupe cyclique et un produit semi-direct non commutatif.

Proposition 2. *Soit*

$$1 \to N \xrightarrow{i} G \xrightarrow{\pi} Q \to 1$$

une suite exacte telle qu'il existe H un sous-groupe de G tel que $\pi_{|H} : H \to Q$ soit un isomorphisme. Alors on a $G \cong N \rtimes_\varphi Q$.

Démonstration. On note $K := i(N)$. On a $K \cap H = \{1\}$ et $G = KH$. En effet, $K \cap H = \ker(\pi) \cap H = \ker(\pi_{|H}) = \{1\}$ et si $g \in G$, $\pi(g) = \pi(h)$ pour un certain $h \in H$, et alors $gh^{-1} \in \ker(\pi) = K$. Ainsi, $G = K \rtimes H$, et donc, puisque $K \cong N$ et $H \cong Q$, $G \cong N \rtimes_\varphi Q$. □

Remarque. Étant donné une suite exacte $1 \to N \xrightarrow{i} G \xrightarrow{\pi} Q \to 1$ il est équivalent d'avoir H un sous-groupe de G tel que $\pi_{|H} : H \to Q$ soit un isomorphisme et un morphisme $s : Q \to G$, appelé *section*, tel que $\pi \circ s = \mathrm{id}_Q$. On dit alors que la suite exacte est *scindée*.

Démonstration (Théorème 1). On utilise les théorèmes de Sylow : soit G un groupe d'ordre pq. On sait que k le nombre de q-Sylow de G vérifie $k \mid p$ et $k \equiv 1 \mod (q)$, ainsi, $k = 1$ et il existe donc un unique q-Sylow Q distingué dans G. Puisqu'ils sont d'ordre premier, on a $Q \cong \mathbb{Z}/q\mathbb{Z}$ et $G/Q \cong \mathbb{Z}/p\mathbb{Z}$. On a alors une suite exacte

$$1 \to \mathbb{Z}/q\mathbb{Z} \to G \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \to 1.$$

De plus, si P est un p-Sylow de G, $\pi_{|P} : P \to \mathbb{Z}/p\mathbb{Z}$ est un isomorphisme car $\ker(\pi_{|P}) = Q \cap P = \{1\}$ et $|P| = |\mathbb{Z}/p\mathbb{Z}|$. On a donc d'après la proposition,

$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$$

où $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Or on sait que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$. On a alors deux cas possibles :

(i) Ou bien $p \nmid (q-1)$ et alors φ est trivial car sinon il serait injectif et on sait que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ n'admet pas de sous-groupe d'ordre p. On a alors $G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

(ii) Ou bien $p \mid (q-1)$, alors $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ possède un unique sous-groupe H d'ordre p. Ainsi, si φ est trivial, on a encore $G \cong \mathbb{Z}/pq\mathbb{Z}$. Maintenant, si $\varphi, \psi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ sont deux morphismes non triviaux, alors les morphismes $\widetilde{\varphi}, \widetilde{\psi} : \mathbb{Z}/p\mathbb{Z} \to H$ sont des isomorphismes, et donc $\beta := \widetilde{\psi}^{-1} \circ \widetilde{\varphi} \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ et

$$\begin{array}{ccc} G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/p\mathbb{Z} & \to & G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/p\mathbb{Z} \\ (a,b) & \mapsto & (a, \beta(b)) \end{array}$$

fournit un isomorphisme.

□

5.6 Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$.

Référence : D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

Lemme 1. *Les 3-cycles sont conjugués dans $\mathfrak{A}_5$, les doubles transpositions sont conjuguées dans $\mathfrak{A}_5$.*

Démonstration. Cela provient de la $n-2$-transitivité de $\mathfrak{A}_n$: si on se donne $\{a_1, \ldots, a_{n-2}\}$, $\{b_1, \ldots, b_{n-2}\}$ deux ensembles d'éléments distincts de $\{1, \ldots, n\}$, il existe $\sigma \in \mathfrak{A}_n$ telle que $\sigma(a_i) = b_i$. En effet, on considère $\sigma \in \mathfrak{S}_n$ telle que $\sigma(a_i) = b_i$. Si $\sigma \in \mathfrak{A}_n$ c'est terminé, sinon on compose par la transposition (a_{n-1}, a_n). La conjugaison annoncée est alors immédiate puisque si (abe) et $(a'b'e')$ sont deux trois cycles dans $\mathfrak{A}_5$ et $(ab)(cd)(e)$ et $(a'b')(c'd')(e')$, on a $\sigma(abe)\sigma^{-1} = (a'b'e')$ et $\sigma(ab)(cd)(e)\sigma^{-1} = (a'b')(c'd')(e')$ avec $\sigma \in \mathfrak{A}_n$ telle que $\sigma(a) = a'$, $\sigma(b) = b'$, $\sigma(e) = (e')$. □

Théorème 2. *Pour $n \geqslant 5$, $\mathfrak{A}_n$ est simple.*

Démonstration. On montre d'abord le théorème pour $n = 5$ et on utilisera ensuite ce cas en s'y ramenant pour $n > 5$.

Si $n = 5$: on sait que $\mathfrak{A}_5$ contient 60 éléments : le neutre, 15 doubles transpositions d'ordre 2, 20 3-cycles d'ordre 3, et 24 5-cycles d'ordre 5. Soit H distingué dans $\mathfrak{A}_5$ non réduit au neutre. On remarque que si H contient un élément d'ordre 2 (resp. 3, 5) alors il les contient tous. Pour 2 et 3 cela provient du fait que ces éléments sont tous conjugués dans $\mathfrak{A}_5$ et que H est distingué. Pour 5, on utilise qu'un élément d'ordre 5 engendre un 5-Sylow puisque $60 = 2^2 \times 3 \times 5$ et que ceux-ci sont tous conjugués, donc si H contient un élément d'ordre 5, il contient le 5-Sylow engendré, et donc tous les 5-Sylow et donc tous les éléments d'ordre 5. Enfin, on sait que H contient au moins deux de ces ensembles, puisque ni 25=24+1, ni 21=20+1, ni 16=15+1 ne divise 60, donc $|H| \geqslant 1 + 20 + 15 > 30$ et donc $H = \mathfrak{A}_5$.

Si $n > 5$, soit $H \lhd \mathfrak{A}_n$ non réduit au neutre, et $\sigma \in H$ différente de l'identité. Soit a tel que $b = \sigma(a) \neq a$. On prend c différent de $a, b, \sigma(b)$, et on considère $\tau = (acb)$, et donc $\tau^{-1} = (abc)$. On regarde alors $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$ qui appartient à H avec $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$. D'autre part, $\rho = (acb)(\sigma(a)\sigma(b)\sigma(c))$, donc, si $F = \{a, b, c, \sigma(a)\sigma(b)\sigma(c)\}$, $|F| \geqslant 5$, et $\rho(F) = F$ et $\rho_{|E\setminus F} = \mathrm{Id}_{E\setminus F}$, et on peut supposer $|F| = 5$ quitte à rajouter des éléments. On considère alors $\mathfrak{A}(F)$ l'ensemble des permutations paires de F, isomorphe à $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$, et son injection dans $\mathfrak{A}_n$ donnée par : $\Psi : u \mapsto \overline{u}$ donnée par $\overline{u}_{|F} = u$ et $\overline{u}_{|E\setminus F} = \mathrm{Id}_{E\setminus F}$. On pose $H_0 = \Psi^{-1}(H) = \{u \in \mathfrak{A}(F) | \overline{u} \in H\}$. Il est clair que $H_0 \lhd \mathfrak{A}(F)$, que $\rho_{|F} \neq \mathrm{Id}$ et $\rho_{|F} \in H_0$. Donc par le cas $n = 5$, $H_0 = \mathfrak{A}(F)$. Soit maintenant $u \in \mathfrak{A}(F)$ un 3-cycle, on a $u \in H_0$ donc $\overline{u} \in H$ et il est clair que $\overline{u}$ est toujours un 3-cycle dans $\mathfrak{A}_n$. Or les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$ et ils engendrent $\mathfrak{A}_n$, donc $H = \mathfrak{A}_n$. □

5.7 Sous-groupes distingués et table de caractères

Références : F. Ulmer, *Théorie des groupes*, Ellipses, 2012.
G. Peyré, *L'algèbre discrète de la transformée de Fourier*, Ellipses, 2004.

Leçons concernées : 103, 104, 107.

Théorème 1. *Soit G un groupe fini. Pour χ un caractère de G on note $\ker\chi := \{g \in G, \chi(g) = \chi(e)\}$. Alors si $\chi_1, \dots, \chi_m$ sont les caractères irréductibles de G, tout sous-groupe distingué H de G est de la forme $H = \bigcap_{j\in J} \ker\chi_j$, où $J \subset [|1, m|]$.*

Lemme 2. *Pour un caractère χ associé à la représentation (ρ, V), on a $|\chi(g)| \leqslant |\chi(e)|$ pour tout $g \in G$ et $\ker\chi = \ker\rho$.*

Démonstration. Soit $g \in G$. On note $n = \dim V$. On sait que $\rho(g)$ est diagonalisable à valeurs propres des racines de l'unité. Ainsi, $\chi(g) = \sum_{i=1}^n \lambda_i$ avec $\lambda_i \in \mathbb{U}$. Alors, par inégalité triangulaire,

$$|\chi(g)| = \Big|\sum_{i=1}^n \lambda_i\Big| \leqslant \sum_{i=1}^n |\lambda_i| = n = |\chi(e)|$$

avec égalité si et seulement si tous les λ_i sont égaux. Ainsi, $\chi(g) = \chi(e)$ si et seulement si $\lambda_i = 1$ pour $i \in [|1, n|]$ et donc $\rho(g) = \mathrm{id}$, c'est-à-dire $g \in \ker\rho$. □

Démonstration (Théorème). D'après le lemme, tous les ensembles de cette forme sont bien des sous-groupes distingués. Réciproquement, on se donne H distingué dans G.

Étape 1 : H est le noyau d'un caractère. On considère la représentation régulière de G/H de morphisme structurel $\psi : G/H \to \mathrm{GL}_{[G:H]}(\mathbb{C})$ et on note alors $\varphi = \psi \circ \pi : G \to \mathrm{GL}_{[G:H]}(\mathbb{C})$ la représentation de G ainsi obtenue. Puisque la représentation régulière est fidèle, on a $\ker\psi = H$ d'où le résultat.

Étape 2 : on note $V = \bigoplus_{i=1}^s \alpha_i V_i$ la décomposition de V en somme directe de G-modules irréductibles. On a alors $\chi = \sum_{i=1}^s \chi_i$ où χ_i est le caractère irréductible associé à V_i. Et donc, d'après le lemme préliminaire,

$$|\chi(g)| = \Big|\sum_{i=1}^s \chi_i(g)\Big| \leqslant \sum_{i=1}^s |\chi_i(g)| \leqslant \sum_{i=1}^s |\chi_i(e)| = \sum_{i=1}^s \dim V_i = \dim V = \chi(e).$$

Ainsi, si $g \in \ker\chi$, il y a égalité dans l'inégalité précédente, c'est-à-dire que $|\chi_i(g)| = |\chi_i(e)|$ pour tout i, et donc $\chi(g) = \chi(e)$, de sorte que $g \in \ker\chi_i$ pour tout i, d'où le résultat. □

Application 3. *Les sous-groupes distingués du groupe diédral $D_6 = < r, s \mid r^6, s^2, srsr >$ sont $\{e\}$, $< r >$, $< r^2, s >$, $< r^2, rs >$, $< r^2 >$, $< r^3 >$ et D_6.*

Démonstration. On commence par déterminer la table de caractères de D_6. Le groupe D_6 possède 6 classes de conjugaisons $\{e\}$, $\{r, r^5\}$, $\{r^2, r^4\}$, $\{r^3\}$, $\{s, r^2s, r^4s\}$ et $\{rs, r^3s, r^5s\}$.

Étape 1 : on commence par chercher des représentations de degré 1. Leur caractère χ vérifie $1 = \chi(e) = \chi(s^2) = \chi(s)^2$, donc $\chi(s) \in \{\pm 1\}$. De même $\chi(sr)^2 = 1$ et donc puisque $\chi(sr) = \chi(s)\chi(r)$, $\chi(r) \in \{\pm 1\}$. Enfin, $\chi(r)^6 = 1$ ne rajoute pas de conditions, et on obtient alors quatre représentations de degré 1.

Étape 2 : on sait que les degré n_1, n_2 des deux représentations restantes vérifient $4 + n_1^2 + n_2^2 = 12$, et donc $n_1 = n_2 = 2$. On pose $\omega = e^{i\pi/3}$ et on considère pour $h = 1, 2$ les représentations ρ_h données par

$$\rho_h(r) = \begin{pmatrix} \omega^h & 0 \\ 0 & \omega^{-h} \end{pmatrix} \quad \text{et} \quad \rho_h(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

ce qui donne

$$\rho_h(sr^k) = \begin{pmatrix} 0 & \omega^{hk} \\ \omega^{-hk} & 0 \end{pmatrix}.$$

On a alors $\chi_h(r^k) = 2\cos(hk\pi/3)$ et $\chi_h(sr^k) = 0$. On peut alors vérifier que les caractères sont irréductibles.

Étape 3 : on obtient la table de caractères

	1 $\{e\}$	2 $\{r, r^5\}$	2 $\{r^2, r^4\}$	1 $\{r^3\}$	3 $\{s, r^2s, r^4s\}$	3 $\{rs, r^3s, r^5s\}$	
ψ_1	1	1	1	1	1	1	D_6
ψ_2	1	1	1	1	-1	-1	$< r >$
ψ_3	1	-1	1	-1	1	-1	$< r^2, s >$
ψ_4	1	-1	1	-1	-1	1	$< r^2, rs >$
χ_1	2	1	-1	-2	0	0	$\{e\}$
χ_2	2	-1	-1	2	0	0	$< r^3 >$.

D'autre part $\ker \psi_3 \cap \ker \psi_4 =< r^2 >$, et les autres intersections ne donnent pas de nouveau groupe distingué, on obtient bien le résultat annoncé. □

5.8 Suite récurrente : convergence lente

Référence : S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, oraux X-ENS - Analyse 1*, Cassini, 2007.

Leçons concernées : 223, 224.

Théorème 1. *Soit f une fonction continue définie au voisinage de 0 et admettant un développement asymptotique en 0 de la forme*

$$f(x) = x - ax^\alpha + o(x^\alpha)$$

avec $a > 0$ et $\alpha > 1$. Alors il existe $\eta > 0$ tel que pour tout $u_0 \in [0, \eta]$, la suite $(u_n)_n$ définie par récurrence par $u_{n+1} = f(u_n)$ soit bien définie et admette un équivalent de la forme

$$u_n \underset{\infty}{\sim} (na(\alpha - 1))^{\frac{1}{1-\alpha}}.$$

Démonstration. On commence par montrer qu'il existe $\eta > 0$ tel que pour tout $u_0 \in [0, \eta]$, u_n converge vers 0 : le développement asymptotique de f nous apprend que $f(0) = 0$, que f est dérivable en 0 de dérivée égale à 1, et qu'il existe $\eta > 0$ tel que pour tout $x \in]0, \eta]$, $0 < f(x) < x$, ainsi, $[0, \eta]$ est stable par f et donc pour tout $u_0 \in [0, \eta]$, u_n est bien définie. De plus (u_n) est alors décroissante et converge donc vers l'unique point fixe de f sur cet intervalle, 0.

Le point 0 n'est pas attractif au sens de $|f'(a)| < 1$, il n'y a donc pas convergence géométrique : en effet, si c'était le cas, on aurait l'existence de $0 < k < 1$ tel que pour n assez grand $0 \leqslant u_n \leqslant k^n$, c'est-à-dire que $\frac{f(u_n)}{u_n} = \frac{u_{n+1}}{u_n} \leqslant k < 1$, or cette quantité converge vers $f'(0)$ puisque $u_n \to 0$ et on trouve une absurdité.

On précise alors la vitesse de convergence : on a, en 0,

$$\begin{aligned} f(x)^{1-\alpha} - x^{1-\alpha} &\underset{0}{=} (x - ax^\alpha + o(x^\alpha))^{1-\alpha} - x^{1-\alpha} \\ &\underset{0}{=} x^{1-\alpha}((1 - ax^{\alpha-1} + o(x^{\alpha-1}))^{1-\alpha} - 1) \\ &\underset{0}{=} x^{1-\alpha}(-a(1-\alpha)x^{\alpha-1} + o(x^{\alpha-1})) \\ &\underset{0}{\sim} -a(1-\alpha). \end{aligned}$$

Ainsi, puisque $u_n \to 0$, $(u_{n+1}^{1-\alpha} - u_n^{1-\alpha}) \underset{\infty}{\sim} -a(1-\alpha)$. Or $-a(1-\alpha)$ est le terme général d'une série divergente, ainsi, par équivalence des sommes partielles dans le cas d'une série divergente et puisque $\alpha > 1$ donc $u_n^{1-\alpha} \to +\infty$,

$$u_n^{1-\alpha} \underset{\infty}{\sim} u_n^{1-\alpha} - u_0^{1-\alpha} \underset{\infty}{\sim} -an(1-\alpha)$$

et on en déduit l'équivalent annoncé. □

Application 2. *Dans le cas où $f(x) = \log(1+x)$, c'est-à-dire $u_{n+1} = \log(1+u_n)$, on a $u_n \sim_{+\infty} \frac{2}{n}$, et on peut même obtenir :*

$$u_n = \frac{2}{n} + \frac{\log(n)}{3n^2} + o\left(\frac{\log(n)}{n^2}\right).$$

Démonstration. Le premier équivalent est une application directe en notant que $\log(1+x) = x - \frac{x^2}{2} + o(x^2)$. Pour le développement asymptotique, on applique la méthode générale en étudiant

$$\frac{1}{u_{n+1}} - \frac{1}{u_n} = \frac{1}{\log(1+u_n)} - \frac{1}{u_n}$$

et l'on réalise le développement limité de $\log(1+x)$ d'un ordre supérieur : à l'ordre 3 :

$$\begin{aligned}\frac{1}{\log(1+u_n)} - \frac{1}{u_n} = \frac{1}{u_n - \frac{u_n^2}{2} + \frac{u_n^3}{3} + o(u_n^3)} - \frac{1}{u_n} &= \frac{1}{u_n}\left(\frac{1}{1 - \frac{u_n}{2} + \frac{u_n^2}{3} + o(u_n^2)} - 1\right) \\ &= \frac{1}{u_n}\left(\frac{u_n}{2} - \frac{u_n^2}{12} + o(u_n^2)\right) = \frac{1}{2} - \frac{u_n}{12} + o(u_n)\end{aligned}$$

on a obtenu :

$$\frac{1}{u_{n+1}} - \frac{1}{u_n} - \frac{1}{2} = -\frac{u_n}{12} + o(u_n).$$

On a alors

$$\frac{1}{u_{n+1}} - \frac{1}{u_n} - \frac{1}{2} \underset{\infty}{\sim} -\frac{u_n}{12} \underset{\infty}{\sim} -\frac{1}{6n}$$

on peut alors appliquer l'équivalence des sommes partielles dans le cas de séries divergentes pour obtenir :

$$\frac{1}{u_n} - \frac{1}{u_1} - \frac{n-1}{2} \underset{\infty}{\sim} -\frac{1}{6}\sum_{1}^{n-1}\frac{1}{k} \underset{\infty}{\sim} -\frac{\log(n-1)}{6} \underset{\infty}{\sim} -\frac{\log(n)}{6}$$

d'où

$$\frac{1}{u_n} = \frac{n}{2} - \frac{\log(n)}{6} + \frac{1}{u_1} - \frac{1}{2} + o(\log(n)) = \frac{n}{2} - \frac{\log(n)}{6} + o(\log(n)) = \frac{n}{2}\left(1 + \frac{\log(n)}{3n} + o\left(\frac{log(n)}{n}\right)\right).$$

Enfin,

$$u_n = \frac{2}{n}\frac{1}{1 - \frac{\log(n)}{3n} + o\left(\frac{log(n)}{n}\right)} = \frac{2}{n}\left(1 + \frac{\log(n)}{3n} + o\left(\frac{log(n)}{n}\right)\right) = \frac{2}{n} + \frac{2\log(n)}{3n^2} + o\left(\frac{log(n)}{n^2}\right)$$

□

5.9 Théorème de Burnside

Définition 1 (Exposant fini)**.** On dit qu'un groupe G est d'exposant fini si il existe $N \in \mathbb{N}^*$ tel que pour tout $g \in G$, $x^N = 1$. Son exposant est alors défini comme le plus petit $N \in \mathbb{N}^*$ qui vérifie cela.

Lemme 2. *Soit A dans $\mathcal{M}_n(\mathbb{C})$ telle que pour tout $k \in \mathbb{N}^*$, $Tr(A^k) = 0$, alors A est nilpotente.*

Démonstration. Le corps $\mathbb{C}$ étant algébriquement clos, A est trigonalisable : on suppose par l'absurde que A n'est pas nilpotente, alors A admet des valeurs propres non nulles distinctes, notées $\lambda_1, \dots, \lambda_r$, de multiplicité $\alpha_1, \dots, \alpha_r$, il existe alors $P \in \mathrm{GL}_n(\mathbb{C})$ telle que

$$A = P \operatorname{diag}(\lambda_1, \dots, \lambda_1, \dots, \lambda_r, \dots, \lambda_r, 0, \dots, 0) P^{-1}.$$

On a ainsi :

$$A^k = PTP^{-1}$$

où T est une matrice triangulaire supérieure dont les coefficients diagonaux sont

$$\lambda_1, \dots, \lambda_1, \dots, \lambda_r, \dots, \lambda_r, 0, \dots, 0.$$

Par hypothèse, pour $1 \leqslant k \leqslant r$, on a $\sum_{i=1}^{r} \alpha_i \lambda_i^k = 0$, on a donc que $(\alpha_1, \dots, \alpha_r)$ est dans le noyau de la matrice de Vandermonde associée à $(\lambda_1, \dots, \lambda_r)$, inversible par hypothèse, et on obtient une absurdité. □

Théorème 3 (Burnside)**.** *Soit G un sous groupe de $\mathrm{GL}_n(\mathbb{C})$. G est fini si et seulement si G est d'indice fini.*

Démonstration. Si G est fini, par le théorème de Lagrange, il est d'exposant fini $\leqslant |G|$.

Réciproquement, on suppose G d'exposant fini N. On considère $F := \mathrm{Vect}(G) \subset \mathcal{M}_n(\mathbb{C})$ et on se donne $(M_1, \dots, M_m) \subset G^m$ une base de F. On pose l'application

$$\begin{array}{rccc} f: & F & \to & \mathbb{C}^m \\ & A & \mapsto & \begin{pmatrix} \mathrm{Tr}(AM_1) \\ \vdots \\ \mathrm{Tr}(AM_m) \end{pmatrix} \end{array}$$

Lemme 4. *Si tout élément $A \in G$ est diagonalisable, f est injective.*

Démonstration. Soit A, B dans G tels que $f(A) = f(B)$, par linéarité de la trace, on a $\mathrm{Tr}(AM) = \mathrm{Tr}(BM)$ pour tout M dans F et donc dans G. On pose $D := AB^{-1}$. On a pour tout $k \in \mathbb{N}^*$: $\mathrm{Tr}(D^k) = \mathrm{Tr}\left(AB^{-1}D^{k-1}\right) = \mathrm{Tr}(BB^{-1}D^{k-1}) = \mathrm{Tr}(D^{k-1}) = \mathrm{Tr}(I) = n$ puisque $B^{-1}D^{k-1} \in G$.

On a alors, par la formule du binôme de Newton, puisque D et I commutent,

$$\mathrm{Tr}\left((D-I)^k\right) = \mathrm{Tr}\left(\sum_{i=1}^{k}\binom{k}{i}(-1)^i D^{k-i}\right) = \sum_{i=1}^{k}\binom{k}{i}(-1)^i \mathrm{Tr}(D^{k-i})$$
$$= n\sum_{i=1}^{k}\binom{k}{i}(-1)^i = n(1-1) = 0.$$

On utilise le lemme préliminaire pour conclure que $D-I$ est nilpotente. On sait d'autre part que $D \in G$ est diagonalisable, donc $D-I$ l'est aussi, elle est donc nulle, et par suite, $A = B$. □

On conclut grâce au lemme précédent : on a, pour tout M dans G, $M^N = I$, donc $X^N - 1$ annule M, or il est scindé à racine simple sur $\mathbb{C}$, donc M est diagonalisable, et on applique le lemme 1. On a alors que G s'injecte dans X^m, où $X := \mathrm{Tr}(G)$. Or, les valeurs propres de éléments de G sont des racines N-ème de l'unité. Puisque la trace d'une matrice diagonalisable est la somme de ses valeurs propres, l'ensemble X est fini, et G l'est aussi. □

5.10 Théorème de Lévy

Référence : H. Queffélec, C. Zuily, *Éléments d'Analyse*, Dunod, 2002.

Leçons concernées : 250, 260, 261, 262.

Définition 1. On dit qu'une suite $(X_n)_n$ de variables aléatoires converge en loi vers X si pour toute fonction continue bornée f, $\mathbb{E}[f(X_n)] \underset{n\to+\infty}{\longrightarrow} \mathbb{E}[f(X)]$.

Pour une variable aléatoire X on note $\varphi_X(t) := \mathbb{E}[e^{itX}]$ sa fonction caractéristique. On note $\mathcal{C}_0(\mathbb{R})$ l'ensemble des fonctions f continues sur $\mathbb{R}$ telles que $f(x) \underset{|x|\to+\infty}{\longrightarrow} 0$.

Théorème 2 (Lévy)**.** *Soit $X, X_1, \dots, X_n, \dots$ des variables aléatoires. Alors on a équivalence entre*

(i) La suite $(X_n)_n$ converge en loi vers X

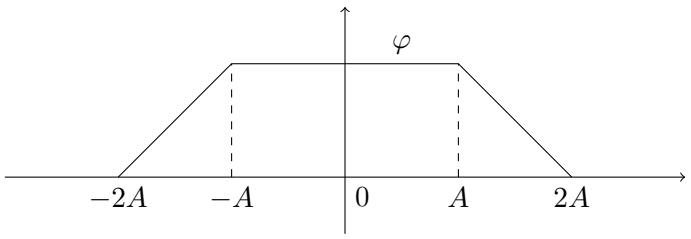
(ii) La suite de fonctions $(\varphi_{X_n})_n$ converge simplement vers φ_X.

On commence par montrer la proposition suivante :

Proposition 3. *Une suite $(X_n)_n$ de variables aléatoires converge en loi vers X si et seulement si pour toute fonction $f \in \mathcal{C}_0(\mathbb{R})$, $\mathbb{E}[f(X_n)] \underset{n\to+\infty}{\longrightarrow} \mathbb{E}[f(X)]$.*

Démonstration. Le sens direct est évident puisqu'une fonction de $\mathcal{C}_0(\mathbb{R})$ est bornée.

Réciproquement, soit $\varepsilon > 0$, $f \in \mathcal{C}_b^0(\mathbb{R})$ et soit $A > 0$ tel que $\mathbb{P}_X(x, |x| \geqslant A) \leqslant \varepsilon$. On pose $\varphi \in \mathcal{C}_0(\mathbb{R})$ la fonction valant 1 sur $[-A, A]$, 0 en dehors de $[-2A, 2A]$, et affine entre $-2A$ et $-A$ et entre A et $2A$:



On a

$$\int_{\mathbb{R}} (1-\varphi) d\mathbb{P}_X \leqslant \mathbb{P}_X(x, |x| \geqslant A) \leqslant \varepsilon.$$

On écrit alors

$$\int_{\mathbb{R}} f d\mathbb{P}_{X_n} - \int_{\mathbb{R}} f d\mathbb{P}_X = \int_{\mathbb{R}} f(1-\varphi) d\mathbb{P}_{X_n} + \left[\int_{\mathbb{R}} f\varphi d\mathbb{P}_{X_n} - \int_{\mathbb{R}} f\varphi d\mathbb{P}_X\right] + \int_{\mathbb{R}} f(1-\varphi) d\mathbb{P}_X =: A_n + B_n + C_n.$$

On a alors $|A_n| \leqslant ||f||_\infty \int_{\mathbb{R}}(1-\varphi)d\mathbb{P}_{X_n} = ||f||_\infty \left(1 - \int_{\mathbb{R}} \varphi d\mathbb{P}_{X_n}\right)$ d'où $\limsup_n |A_n| \leqslant ||f||_\infty \left(1 - \int_{\mathbb{R}} \varphi d\mathbb{P}_X\right) = ||f||_\infty \int_{\mathbb{R}}(1-\varphi)d\mathbb{P}_X \leqslant \varepsilon ||f||_\infty$ par hypothèses. D'autre part, $|B_n| \underset{n\to+\infty}{\longrightarrow} 0$ puisque $f\varphi \in \mathcal{C}_0(\mathbb{R})$ et $|C_n| \leqslant \varepsilon ||f||_\infty$. On a alors

$$\limsup_n \left| \int_{\mathbb{R}} f d\mathbb{P}_{X_n} - \int_{\mathbb{R}} f d\mathbb{P}_X \right| \leqslant 2\varepsilon ||f||_\infty$$

et donc $|\mathbb{E}[f(X_n)] - \mathbb{E}[f(X)]| \underset{n\to+\infty}{\longrightarrow} 0$. □

Démonstration (Théorème). L'implication (i) ⇒ (ii) est directe en remarquant que $f(x) := e^{itx}$ est continue bornée pour tout $t \in \mathbb{R}$.

Réciproquement, on se donne f de la forme $f(x) = \int_{\mathbb{R}} e^{itx}\varphi(t)dt$ avec $\varphi \in L^1(\mathbb{R})$. Par les théorèmes de Fubini et de convergence dominée, on a

$$\mathbb{E}[f(X_n)] = \mathbb{E}\left[\int_{\mathbb{R}} e^{itX_n}\varphi(t)dt\right] = \int_{\mathbb{R}} \varphi(t)\mathbb{E}\left[e^{itX_n}\right]dt$$
$$\underset{n\to+\infty}{\longrightarrow} \int_{\mathbb{R}} \varphi(t)\mathbb{E}\left[e^{itX}\right]dt = \mathbb{E}\left[\int_{\mathbb{R}} e^{itX}\varphi(t)dt\right] = \mathbb{E}[f(X)].$$

Maintenant, si $f \in \mathcal{C}_0(\mathbb{R})$ et $\varepsilon > 0$, on sait qu'il existe $g \in \mathcal{C}_c^\infty(\mathbb{R})$ telle que $||f-g||_\infty \leqslant \varepsilon$. Or $\mathcal{C}_c^\infty(\mathbb{R}) \subset \mathcal{S}(\mathbb{R})$, et donc par bijectivité de la transformée de Fourier sur $\mathcal{S}(\mathbb{R})$, g s'écrit $g(x) = \int_{\mathbb{R}} e^{itx}\varphi(t)dt$ avec $\varphi \in \mathcal{S}(\mathbb{R}) \subset L^1(\mathbb{R})$, et on conclut par inégalité triangulaire en remarquant que pour toute variable aléatoire Y, $\mathbb{E}[(f-g)(Y)] \leqslant ||f-g||_\infty$. □

On peut déduire de ce théorème le théorème central limite, au moyen du lemme suivant :

Lemme 4. *Soit $(z_n)_n$ une suite de nombres complexes de limite $z \in \mathbb{C}$, alors*

$$\left(1 + \frac{z_n}{n}\right)^n \underset{n\to+\infty}{\longrightarrow} e^z.$$

Théorème 5 (Central limite)**.** *Soit $(X_n)_n$ une suite de variables aléatoires indépendantes et identiquement distribuées admettant un moment d'ordre 2. On note $m = \mathbb{E}[X_1]$ et $\sigma^2 = \mathrm{Var}(X_1)$. Alors si $S_n = \sum_{k=1}^n X_n$,*

$$\frac{S_n - mn}{\sqrt{n}\sigma} \xrightarrow{\mathcal{L}} \mathcal{N}(0,1).$$

Démonstration. On peut sans perte de généralité se ramener au cas $m = 0$ et $\sigma = 1$. On utilise le théorème précédent et on cherche donc à montrer que $\varphi_{\frac{S_n}{\sqrt{n}}}(t) \to e^{-t^2/2}$ pour tout $t \in \mathbb{R}$.

On note $\varphi := \varphi_{X_1}$. Puisque X_1 admet un moment d'ordre 2, φ est de classe $\mathcal{C}^2$ et vérifie : $\varphi'(0) = \mathbb{E}[iX_1] = 0$ et $\varphi''(0) = [-X^2] = -1$. On a d'autre part

$$\begin{aligned}\varphi_{\frac{S_n}{\sqrt{n}}}(t) &= \mathbb{E}\left[\prod_{k=1}^{n} e^{itX_k/\sqrt{n}}\right] = \prod_{k=1}^{n} \mathbb{E}\left[e^{itX_k/\sqrt{n}}\right] \\ &= \mathbb{E}\left[e^{itX_1/\sqrt{n}}\right]^n = \varphi\left(\frac{t}{\sqrt{n}}\right)^n = \left(1 - \frac{t^2}{2n} + o(\frac{1}{n})\right)^n.\end{aligned}$$

On conclut donc avec le lemme. □

5.11 Théorème de Stone-Weierstrass

Référence : F. Hirsch, G. Lacombe, *Éléments d'analyse fonctionnelle*, Dunod, 1999.

Leçons concernées : 201, 202, 203, 209.

Proposition 1. *Il existe une suite de polynômes $(P_n)_n$ qui converge uniformément vers la valeur absolue sur $[-1,1]$.*

C'est une conséquence du théorème de Weierstrass mais cela peut être démontré indépendamment :

Démonstration. On définit par récurrence $(P_n)_n$ sur $[-1,1]$ par $P_0 = 0$ et

$$P_{n+1}(x) = P_n(x) + \frac{1}{2}\big(x^2 - P_n^2(x)\big).$$

Pour tout $x \in [-1,1]$ on montre alors par récurrence que pour tout $n \geqslant 0$, $0 \leqslant P_n(x) \leqslant P_{n+1}(x) \leqslant |x|$. Pour $n = 0$ le résultat est clair. Soit maintenant $n \geqslant 0$, alors par hypothèse de récurrence il est clair que $0 \leqslant P_{n+1}(x) \leqslant P_{n+2}(x)$ et d'autre part

$$P_{n+2} = |x| - \big(|x| - P_{n+1}(x)\big)\Big(1 - \frac{1}{2}\big(|x| + P_{n+1}(x)\big)\Big) \leqslant |x|$$

par hypothèse de récurrence. Ainsi pour tout $x \in [-1,1]$, $(P_n(x))_n$ est croissante majorée donc converge vers $f(x) \geqslant 0$, et en passant à la limite dans la relation de récurrence on obtient que $f(x)^2 = x^2$ et donc $f(x) = |x|$. Enfin, on applique le théorème de Dini pour obtenir la convergence uniforme. □

Soit X un espace métrique compact non vide et $\mathcal{C}(X)$ l'espace des fonctions continues de X à valeurs dans $\mathbb{R}$ munit de la norme de la convergence uniforme.

Définition 2. On dit qu'une partie H de $\mathcal{C}(X)$ est *séparante* si pour tout $x, y \in X$, il existe $h \in H$ telle que $h(x) \neq h(y)$. D'autre part une partie H de $\mathcal{C}(X)$ est dite *réticulée* si pour tout $f, g \in H$, les fonctions $\inf(f,g)$ et $\sup(f,g)$ sont dans H.

Théorème 3. *On suppose que X contient au moins deux éléments. Soit H une partie de $\mathcal{C}(X)$ réticulée telle que pour tout $x, y \in X$ $x \neq y$, $\alpha, \beta \in \mathbb{R}$, il existe $h \in H$ telle que $h(x) = \alpha$ et $h(y) = \beta$. Alors H est dense dans $\mathcal{C}(X)$.*

Démonstration. Soit $f \in \mathcal{C}(X)$ et $\varepsilon > 0$. Soit $x \in X$. Par hypothèse, pour tout $y \in X$, $y \neq x$, il existe $h_y \in H$ telle que $h_y(x) = f(x)$ et $h_y(y) = f(y)$. On pose

$$O_y = \{z \in X, h_y(z) > f(z) - \varepsilon\}$$

qui est un ouvert de X contenant x et y. Ainsi $X = \bigcup_{y \neq x} O_y$ et par propriété de Borel-Lebesgue, $X = \bigcup_{i=1}^{k} O_{y_i}$ avec les y_i distincts et différents de x. On pose alors $g_x :=$

$\sup(h_{y_1}, \ldots, h_{y_k})$ qui est dans H par hypothèse. D'autre part $g_x(x) = f(x)$ et pour tout $z \in X$, $g_x(z) > f(z) - \varepsilon$. On considère alors

$$\Omega_x = \{z \in X, g_x(z) < f(z) + \varepsilon\}$$

qui est un ouvert de X contenant x. Par le même raisonnement que précédemment on a alors $X = \bigcup_{i=1}^{n} \Omega_{x_i}$. On pose maintenant $g = \inf(g_{x_1}, \ldots, g_{x_n})$ qui appartient à H par hypothèse. On vérifie alors que $f - \varepsilon < g < f + \varepsilon$ ce qui conclut la preuve. □

Théorème 4. *Tout sous-espace vectoriel H de $\mathcal{C}(X)$ réticulé, séparant et contenant les constantes est dense dans $\mathcal{C}(X)$.*

Démonstration. Si X est réduit à un seul élément le résultat est clair. Sinon on montre que H vérifie les conditions du théorème précédent : soient $x, y \in X$ distincts. Puisque H est séparant, il existe $h \in H$ telle que $h(x) \neq h(y)$. Pour $\alpha, \beta \in \mathbb{R}$ on considère alors le système

$$\begin{cases} \lambda\, h(x) + \mu = \alpha \\ \lambda\, h(y) + \mu = \beta \end{cases}$$

qui admet un unique couple de solution (λ, μ) puisque $h(x) \neq h(y)$. La fonction $g : z \mapsto \lambda\, z + \mu$ est alors solution du problème et appartient à H puisque H est un sous-espace vectoriel qui contient les constantes. □

Théorème 5 (Stone-Weierstrass)**.** *Toute sous-algèbre H de $\mathcal{C}(X)$ séparante et contenant les constantes est dense dans $\mathcal{C}(X)$.*

Démonstration. On remarque que si H est une sous-algèbre H de $\mathcal{C}(X)$ séparante et contenant les constantes, alors il en est de même de $\overline{H}$. On montre alors que $\overline{H}$ vérifie les hypothèses du théorème précédent. Or les relations suivantes

$$|h| = \sup(h, 0) - \inf(h, 0)$$

$$\inf(f, g) = \frac{1}{2}\Big(f + g - |f - g|\Big)$$

et

$$\sup(f, g) = \frac{1}{2}\Big(f + g + |f - g|\Big).$$

montrent que $\overline{H}$ est réticulé si et seulement si $|h| \in \overline{H}$ pour tout $h \in \overline{H}$. Soit alors $h \in \overline{H}$. D'après la première proposition (ou par le théorème de Weierstrass), il existe une suite de polynômes $(P_n)_n$ qui converge uniformément vers la valeur absolue sur $[-1, 1]$. La suite de fonctions $\big(P_n(h/||h||)\big)_n$ appartient à $\overline{H}$ par hypothèses et converge alors uniformément vers $|h|/||h||$ qui appartient à $\overline{H}$ car celui-ci est fermé. On conclut avec $|h| = ||h|| \times |h|/||h|| \in \overline{H}$. □

Application 6. *L'ensemble des fonctions lipschitziennes de X dans $\mathbb{R}$ est dense dans $\mathcal{C}(X)$. Si $X \subset \mathbb{R}^d$ est compact alors*

$$H = \{x \in X \mapsto P(x), P \in \mathbb{R}[X_1, \ldots, X_d]\}$$

est dense dans $\mathcal{C}(X)$.

Démonstration. Il est clair que l'ensemble des fonctions lipschitzienne est une sous-algèbre de $\mathcal{C}(X)$ contenant les constantes, et d'autre part si $x \neq y$, alors $f : z \mapsto d(x, z)$ est 1-lipschitzienne et vérifie $f(x) = 0 \neq f(y)$ donc l'ensemble des fonctions lipschitziennes est séparant et on peut donc lui appliquer le théorème de Stone-Weierstrass. De la même manière, H est une sous-algèbre de $\mathcal{C}(X)$ contenant les constantes, et si $x \neq y$, alors ils différent au moins selon l'une de leurs composantes : $x_i \neq y_i$ et le polynôme X_i sépare x et y. □

Enfin, on donne une preuve du théorème de Stone-Weierstrass dans le cas complexe. On note $\mathcal{C}^{\mathbb{C}}(X)$ l'ensemble des fonctions continues sur X à valeurs dans $\mathbb{C}$. Enfin une partie $H \subset \mathcal{C}^{\mathbb{C}}(X)$ est dite *auto-conjuguée* si pour tout $h \in H$, $\overline{h} \in H$.

Théorème 7 (Stone-Weierstrass, cas complexe)**.** *Toute sous-algèbre H de $\mathcal{C}^{\mathbb{C}}(X)$ séparante, auto-conjuguée et contenant les constantes est dense dans $\mathcal{C}^{\mathbb{C}}(X)$.*

Démonstration. On note $H^{\mathbb{R}} = \{f \in H, \forall x \in X, f(x) \in \mathbb{R}\}$. Alors $H^{\mathbb{R}}$ vérifie les hypothèses du théorème de Stone-Weierstrass dans le cas réel. En effet c'est bien une sous-algèbre de $\mathcal{C}(X)$ qui contient les constantes. D'autre part, si $x \neq y$, alors il existe par hypothèse il existe $g \in H$ telle que $g(x) \neq g(y)$. Ainsi par exemple $\Re(g)(x) \neq \Re(g)(y)$. Or

$$\Re(g) = \frac{g + \overline{g}}{2} \in H$$

par hypothèse sur H et donc $\Re(g) \in H^{\mathbb{R}}$ et $H^{\mathbb{R}}$ est ainsi séparant. On peut appliquer le théorème de Stone-Weierstrass dans le cas réel. Or $\mathcal{C}^{\mathbb{C}}(X) = \mathcal{C}(X) + i\mathcal{C}(X)$ et $H = H^{\mathbb{R}} + iH^{\mathbb{R}}$ et donc H est dense dans $\mathcal{C}^{\mathbb{C}}(X)$. □

5.12 Théorème de Sylow

Référence : D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

Leçons concernées : 103 (ss-gr. distingués), 104 (groupes finis), 106 (GL(E)).

Soit p premier et soit G un groupe fini d'ordre $p^\alpha m$ où $p \nmid m$.

Définition 1. Un p-sous groupe de Sylow P est un sous-groupe de G d'ordre $n = p^\alpha$.

Théorème 2 (Sylow)**.** *(i) G possède un p-sous groupe de Sylow*

(ii) Si H est un sous-groupe d'ordre p^γ de G, alors il existe un p-Sylow S qui contient H, et les p-Sylow sont tous conjugués, donc leur nombre k divise n

(iii) On a $k \equiv 1 \mod p$

La démonstration repose en grande partie sur le lemme suivant :

Lemme 3. *Soit H un sous-groupe de G et S un p-Sylow de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Démonstration. Le groupe G agit sur G/S par translation à gauche, et H aussi par restriction de l'action. Pour tout $a \in G$, le stabilisateur de aS sous l'action de G est aSa^{-1} et donc celui de aS sous l'action de H est $aSa^{-1} \cap H$. Soit $a_1, \dots, a_r$ des représentants des orbites sous cette action, on a, par formule des classes,

$$\sum_{i=1}^{r} |H/a_i S a_i^{-1} \cap H| = |G/S| = m.$$

Ainsi, puisque $p \nmid m$, il existe $a := a_{i_0}$ tel que $p \nmid |H/aSa^{-1} \cap H| = \frac{|H|}{|aSa^{-1} \cap H|}$ ce qui signifie que $aSa^{-1} \cap H$ est un p-sous-groupe de Sylow de H. □

Il ne nous reste plus qu'a plonger G dans un groupe dont on sait qu'il possède un p-Sylow.

Démonstration. (i) Par le théorème de Cayley, G se plonge dans $\mathfrak{S}_n$, et on plonge ensuite $\mathfrak{S}_n$ dans $\mathrm{GL}_n(\mathbb{F}_p)$ avec les matrices de permutations. Il ne nous reste plus qu'a montrer que $\mathrm{GL}_n(\mathbb{F}_p)$ possède un p-Sylow.

On a $|G| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{n(n-1)/2} \prod_{i=0}^{n-1}(p^{n-i}-1)$ et $p \nmid \prod_{i=0}^{n-1}(p^{n-i}-1)$.

Et d'autre part, le sous-groupe T des matrices triangulaires supérieures de la forme

$$\begin{pmatrix} 1 & & (*) \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$$

$T = \{(a_{i,j} \in \mathrm{GL}_n(\mathbb{F}_p) | i > j \Rightarrow a_{i,j} = 0, a_{i,i} = 1\}$ est d'ordre $p^{n(n-1)/2}$ et donc un p-Sylow. On conclut alors avec le lemme.

(ii) On se donne H un p-groupe et S un p-Sylow. Par le lemme 3, il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H, or $|H| = a^\gamma$, donc $|aSa^{-1} \cap H| = |H|$ et $H = aSa^{-1} \cap H$, par suite, H est contenu dans aSa^{-1}, qui est un p-Sylow. On a montré le premier point, pour le deuxième, il suffit de considérer H un p-Sylow, et on a par cardinalité $H = aSa^{-1}$.

(iii) G agit par conjugaison sur l'ensemble X des p-Sylow de G, et donc, si S est un p-Sylow, S agit aussi sur X. On sait alors que $|X| \equiv |X^S| \mod p$. Soit maintenant $T \in X^S$. On pose N le sous-groupe de G engendré par S et T, qui sont alors des p-Sylow de N. Puisque par hypothèse $\forall s \in S, sTs^{-1} = T$, $T \lhd N$, donc d'après le point (ii), T est l'unique p-Sylow de N, et $S = T$. Ainsi, $X^S = S$ et $|X| \equiv 1 \mod p$. □