Couplages et développements - Brian Flanagan

Table des matières

1 Algèbre et géométrie **2**

2 Analyse et probabilités **5**

3 Développements d'algèbre **8**
3.1 Décomposition de Dunford . . . 8
3.2 Décomposition polaire pour $O(p,q)$ . . . 10
3.3 Enveloppe convexe de $O_n(\mathbb{R})$ . . . 12
3.4 Forme normale de Smith . . . 12
3.5 Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$ . . . 13
3.6 Loi de réciprocité quadratique . . . 14
3.7 Par cinq points passe une conique . . . 15
3.8 Primalité des nombres de Mersenne . . . 15
3.9 Réduction de Frobenius . . . 16
3.10 Simplicité du groupe alterné . . . 18
3.11 Table des caractères de $\mathfrak{S}_4$ . . . 20
3.11.1 Isométries du cube et du tétraèdre . . . 20
3.11.2 Isométries du tétraèdre et table des caractères de $\mathfrak{S}_4$ . . . 21
3.11.3 Sous-groupes distingués et table des caractères . . . 24
3.12 Théorème de Sophie Germain . . . 27
3.13 Théorème de structure des groupes abéliens finis . . . 28
3.14 L'unique entier entre un carré et un cube . . . 28
3.15 Une version faible du théorème de Bézout . . . 29

4 Développements mixtes **31**
4.1 Cartan - Von Neumann . . . 31
4.2 Convergence des méthodes itératives hermitiennes . . . 33

5 Développements d'analyse **33**
5.1 Abel et Tauber faible . . . 33
5.2 Banach-Alaoglu . . . 36
5.3 Cauchy-Peano . . . 38
5.4 Développement asymptotique de la série harmonique . . . 39
5.5 Espace de Bergman . . . 40
5.6 Théorème de Fejér . . . 42
5.7 Formule des compléments . . . 43
5.8 Gradient à pas optimal . . . 45
5.9 Hadamard-Lévy . . . 46
5.10 Intégrale de Dirichlet . . . 48
5.11 Inversion de Fourier L^1 . . . 50
5.12 Lemme de Grothendieck . . . 52
5.13 Logarithme et Brouwer . . . 54
5.14 Marche aléatoire sur le N-gone . . . 56
5.15 Marche aléatoire sur $[0,1]$ . . . 59
5.16 Méthode de Newton . . . 61

5.17 Méthode des petits pas . . . 63
5.18 Séries lacunaires sans dérivées . . . 64
5.19 Théorème de Polya par le dénombrement . . . 66

6 Développements abandonnés **66**
6.1 Méthode de relaxation . . . 66
6.2 Un anneau principal non-euclidien . . . 67
6.3 Une suite d'extensions algébriques . . . 69

1 Algèbre et géométrie

101 Groupe opérant sur un ensemble. Exemples et applications.

Isométries du tétraèdre et table des caractères de $\mathfrak{S}_4$
Loi de réciprocité quadratique

---

102 Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

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

---

103 Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

Sous-groupes distingués et table des caractères
Simplicité du groupe alterné

---

104 Groupes finis. Exemples et applications.

Sous-groupes distingués et table des caractères
Théorème de structure des groupes abéliens finis

---

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

Isométries du tétraèdre et table des caractères de $\mathfrak{S}_4$
Simplicité du groupe alterné

---

106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.

Cartan - Von Neumann
Décomposition polaire pour $O(p, q)$

---

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

Isométries du tétraèdre et table des caractères de $\mathfrak{S}_4$
Simplicité du groupe alterné

---

120 Anneaux Z/nZ. Applications.

Primalité des nombres de Mersenne
Théorème de structure des groupes abéliens finis

---

121 Nombres premiers. Applications.

Primalité des nombres de Mersenne
Théorème de Sophie Germain

---

122 Anneaux principaux. Exemples et applications.

Forme normale de Smith
L'unique entier entre un carré et un cube

---

123 Corps finis. Applications.

Primalité des nombres de Mersenne
Loi de réciprocité quadratique

---

125 Extensions de corps. Exemples et applications.

Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$
Primalité des nombres de Mersenne

---

126 Exemples d'équations en arithmétique.

L'unique entier entre un carré et un cube
Théorème de Sophie Germain

---

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

Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$
Primalité des nombres de Mersenne

---

142 PGCD et PPCM, algorithmes de calcul. Applications.

Forme normale de Smith
L'unique entier entre un carré et un cube

---

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

Une version faible du théorème de Bézout
Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$

---

148 Exemples de décompositions de matrices. Applications.

Décomposition polaire pour $O(p, q)$
Forme normale de Smith

---

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

Par cinq points passe une conique
Réduction de Frobenius

---

152 Déterminant. Exemples et applications.

Une version faible du théorème de Bézout
Forme normale de Smith

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

Décomposition de Dunford
Réduction de Frobenius

---

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

Décomposition de Dunford
Réduction de Frobenius

---

155 Endomorphismes diagonalisables en dimension finie.

Décomposition de Dunford
Marche aléatoire sur le N-gone

---

156 Exponentielle de matrices. Applications.

Cartan - Von Neumann
Décomposition polaire pour $O(p,q)$

---

157 Endomorphismes trigonalisables. Endomorphismes nilpotents.

Décomposition de Dunford
Réduction de Frobenius

---

158 Matrices symétriques réelles, matrices hermitiennes.

Décomposition polaire pour $O(p,q)$
Convergence des méthodes itératives hermitiennes

---

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

Réduction de Frobenius
Enveloppe convexe de $O_n(\mathbb{R})$

---

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

Enveloppe convexe de $O_n(\mathbb{R})$
Décomposition polaire pour $O(p,q)$

---

161 Distances dans un espace affine euclidien. Isoméries.

Enveloppe convexe de $O_n(\mathbb{R})$
Isométries du cube et du tétraèdre

---

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

Convergence des méthodes itératives hermitiennes
Forme normale de Smith

---

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

Décomposition polaire pour $O(p,q)$
Loi de réciprocité quadratique

---

171 Formes quadratiques réelles. Coniques. Exemples et applications.

Décomposition polaire pour $O(p,q)$
Par cinq points passe une conique

---

181 Barycentres dans un espace affine réel de dimension finie, convexité. Applications.

Enveloppe convexe de $O_n(\mathbb{R})$
Par cinq points passe une conique

---

190 Méthodes combinatoires, problèmes de dénombrement.
Loi de réciprocité quadratique
Théorème de Polya par le dénombrement

---

191 Exemples d'utilisation de techniques d'algèbre en géométrie.

Isométries du cube et du tétraèdre
Une version faible du théorème de Bézout

2 Analyse et probabilités

201 Espaces de fonctions. Exemples et applications.

Espace de Bergman
Lemme de Grothendieck

---

203 Utilisation de la notion de compacité.

Banach-Alaoglu
Cauchy-Peano

---

204 Connexité. Exemples et applications.

Hadamard-Lévy
Logarithme et Brouwer

---

205 Espaces complets. Exemples et applications.

Banach-Alaoglu
Lemme de Grothendieck

---

206 Exemples d'utilisation de la notion de dimension finie en analyse.

Cauchy-Peano
Cartan - Von Neumann

---

208 Espaces vectoriels normés, applications linéaires continues. Exemples.

Banach-Alaoglu
Lemme de Grothendieck

---

209 Approximation d'une fonction par des fonctions régulières. Exemples et applications.

Théorème de Fejér
Marche aléatoire sur $[0,1]$

---

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

Banach-Alaoglu
Espace de Bergman

---

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

Cartan - Von Neumann
Hadamard-Lévy

---

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

Gradient à pas optimal
Hadamard-Lévy

---

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

Banach-Alaoglu
Gradient à pas optimal

---

220 Equations différentielles ordinaires. Exemples de résolution et d'études de solutions en dimension 1 et 2.

Cauchy-Peano
Hadamard-Lévy

---

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

Méthode de Newton
Méthode des petits pas

---

224 Exemples de développements asymptotiques de suites et de fonctions.

Méthode des petits pas
Développement asymptotique de la série harmonique

---

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 des petits pas
Méthode de Newton

---

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

applications.

Séries lacunaires sans dérivées
Méthode de Newton

---

229 Fonctions monotones. Fonctions convexes. Exemples et applications.

Gradient à pas optimal
Méthode de Newton

---

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

Théorème de Polya par le dénombrement
Développement asymptotique de la série harmonique

---

234 Fonctions et espaces de fonctions Lebesgue-intégrables.

Espace de Bergman
Lemme de Grothendieck

---

235 Problèmes d'interversion en analyse.

Intégrale de Dirichlet
Inversion de Fourier L^1

---

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

Formule des compléments
Intégrale de Dirichlet

---

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

Intégrale de Dirichlet
Inversion de Fourier L^1

---

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

Abel et Tauber faible
Séries lacunaires sans dérivées

---

243 Séries entières, propriétés de la somme. Exemples et applications.

Abel et Tauber faible
Espace de Bergman

---

245 Fonctions d'une variable complexe. Exemples et applications.

Espace de Bergman
Formule des compléments

---

246 Séries de Fourier. Exemples et applications.

Théorème de Fejér
Séries lacunaires sans dérivées

---

250 Transformation de Fourier. Applications.

Inversion de Fourier L^1
Séries lacunaires sans dérivées

---

253 Utilisation de la notion de convexité en analyse.

Banach-Alaoglu
Gradient à pas optimal

---

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

Marche aléatoire sur $[0, 1]$
Marche aléatoire sur le N-gone

---

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

Marche aléatoire sur $[0, 1]$
Marche aléatoire sur le N-gone

---

264 Variables aléatoires discrètes. Exemples et applications.

Théorème de Polya par le dénombrement
Marche aléatoire sur le N-gone

---

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

Formule des compléments
Marche aléatoire sur $[0, 1]$

---

266 Illustration de la notion d'indépendance en probabilités.

Marche aléatoire sur $[0, 1]$
Théorème de Polya par le dénombrement

---

267 Exemples d'utilisation de courbes en dimension 2 ou supérieure.

Formule des compléments
Logarithme et Brouwer

3 Développements d'algèbre

3.1 Décomposition de Dunford

Leçons concernées. $153, 154, 155, 157$.
Référence. *Les maths en tête, Algèbre*, Xavier Gourdon.
Remarques. Il est à noter que la décomposition de Dunford utilise la diagonalisation simultanée. Il est sans doute bon de savoir à quoi sert la décomposition de Dunford, notamment ne lien avec l'exponentielle d'une matrice.

On se donne un corps quelconque k et un k-espace vectoriel E de dimension finie.

Théorème 1 (Décomposition de Dunford)
Soit $u \in \mathcal{L}(E)$ tel que son polynôme caractéristique χ_u soit scindé sur k. Il existe un unique couple (d, n) d'endomorphismes tel que d est diagonalisable et n est nilpotent vérifiant

$$u = d + n \quad \text{et} \quad d \circ n = n \circ d.$$

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

Preuve.

Lemme 2 Soit $u \in \mathcal{L}(E)$ et $P \in k[X]$ un polynôme annulateur de u. Notons $P = a f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ sa décomposition en facteurs irréductibles et $N_i := \operatorname{Ker} f_i^{\alpha_i}(u)$. On a $E = N_1 \oplus \cdots \oplus N_r$ et pour tout $1 \leqslant i \leqslant r$, la projection sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$ est un polynôme en u.

Preuve. La décomposition $E = N_1 \oplus \cdots \oplus N_r$ découle du lemme des noyaux.

Pour tout $1 \leqslant i \leqslant r$, notons $Q_i = \prod_{j \neq i} f_j^{\alpha_j}$, de sorte que les Q_i sont premiers entre eux dans leur ensemble. D'après l'identité de Bézout, il existe donc des polynômes $U_1, \dots U_r$ tels que $U_1 Q_1 + \cdots + U_r Q_r = 1$, de sorte que

$$U_1(u) \circ Q_1(u) + \cdots + U_r(u) \circ Q_r(u) = \mathrm{Id}_E .$$

Pour tout i, notons alors $P_i = U_i Q_i$ et $p_i = P_i(u)$. Ainsi, l'égalité précédente s'écrit $\mathrm{Id}_E = p_1 + \cdots p_r$. Montrons que les p_i sont les projecteurs souhaités. On remarque que pour tout $j \neq i$, le polynôme P divise $Q_i Q_j$ et donc

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

Ainsi, on a pour tout i,

$$p_i = p_i \circ (p_1 + \cdots + p_r) = \sum_{j=1}^{r} p_i \circ p_j = p_i^2.$$

Les p_i sont donc bien des projecteurs. Il nous reste à montrer que pour tout i, $\operatorname{Im}(p_i) = N_i$ et $\operatorname{Ker}(p_i) = \bigoplus_{j \neq i} N_j$, ce que l'on fait par double inclusion.

Soit tout d'abord $y = p_i(x) \in \operatorname{Im}(p_i)$. On a

$$f_i^{\alpha_i}(u)(y) = f_i^{\alpha_i}(u) \circ P_i(u)(x) = U_i \circ P(u)(x) = 0,$$

ce qui montre que $\operatorname{Im} p_i \subset N_i$.
Réciproquement, si $x \in N_i$, alors on a $x = p_1(u) + \cdots + p_r(u)$. Or, pour tout $j \neq i$, on a que $f_i^{\alpha_i}$ divise Q_i, donc $p_j(x) = 0$. Dès lors, $x = p_i(x) \in \operatorname{Im}(p_i)$. D'où $\operatorname{Im}(p_i) = N_i$.

Ensuite, si $j \neq i$, on a vu que $N_j \subset \operatorname{Ker} p_i$ et donc $\bigoplus_{j \neq i} N_j \subset \operatorname{Ker}(p_i)$. Réciproquement, si $x \in \operatorname{Ker} p_i$, alors on a $x = \sum_{j \neq i} p_j(x)$ et donc $x \in \bigoplus_{j \neq i} N_j$.

✌

Nous voilà maintenant armés pour attaquer la preuve principale. On écrit $\chi_u = \prod_{i=1}^{s} (X - \lambda_i)^{\alpha_i}$ et on note $N_i := \operatorname{Ker}(u - \lambda_i \mathrm{Id}_E)^{\alpha_i}$, de sorte que d'après le lemme précédent appliqué à $P = \chi_u$, avec les mêmes notations, on dispose pour tout i de $p_i = P_i(u)$ le projecteur sur N_i parallèlement à $\bigoplus_{j \neq i} N_j$. On

pose alors $d := \lambda_1 p_1 + \cdots + \lambda_s p_s$ et $n := u - d = (u - \lambda_1 \mathrm{Id}_E)p_1 + \cdots + (u - \lambda_s \mathrm{Id}_E)p_s$. Puisque les p_i commutent avec u et vérifient $p_i \circ p_j = \delta_{ij} p_i$, on obtient que

$$\forall q \in \mathbb{N}^*, \quad n^q = \sum_{i=1}^{s} (u - \lambda_1 \mathrm{Id}_E)^q p_i.$$

Donc, si $q \geqslant \alpha_i$ pour tout $1 \leqslant i \leqslant s$, on a $(f - \lambda_i \mathrm{Id}_E)^q p_i = (X - \lambda_i)^q P_i(u) = 0$ et donc $n^q = 0$.

On a ainsi démontré l'existence de la décomposition de Dunford. Pour ce qui est de l'unicité, si l'on dispose de $u = d' + n'$ une autre décomposition de Dunford de u, alors puisque d' et n' commutent avec u, ils commutent avec d et n qui sont des polynômes en u. Donc d et d' sont codiagonalisables et ainsi, $n' - n = d' - d$ est diagonalisable. En outre, comme n et n' commutent, $n - n'$ est également nilpotent, et le seul endomorphisme nilpotent et diagonalisable et nilpotent est l'endomorphisme nul. Donc $n = n'$ et $d = d'$.

✌

Questions possibles :

- Quelle est la décomposition de Dunford de la matrice $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$? (attention, piège classique)
- Comment peut-on calculer pratiquement la décomposition de Dunford ? Il y a une méthode à partir de la décomposition du polynôme caractéristique sur $\mathbb{C}$ dans le Gourdon, et une autre par la méthode de Newton dans le *NH2G2, tome 1*.
- Résoudre l'équation $\exp(A) = I_2$ dans $\mathcal{M}_2(\mathbb{C})$.

3.2 Décomposition polaire pour $O(p, q)$

Leçons concernées. 106, 148, 156, 158, 160, 170, 171.
Référence. *Nouvelles histoires hédonistes de groupes et géométrie, tome 1*, Caldero et Germoni.
Remarques. Dans la preuve originale, on utilise l'unicité de la racine carrée sur $\mathcal{S}_n^{++}(\mathbb{R})$. Je m'en suis passé en définissant la matrice U à partir de S et non de T dans l'étape 1.
Dans la suite, on utilise fortement la décomposition polaire et l'homéomorphisme réalisé par l'exponentielle sur les matrices symétriques, dont on ne peut pas parler dans tous les plans concernés par ce développement.

Théorème 3 (Décomposition polaire et groupes orthogonaux)
Soient p, q des entiers naturels et $n = p+q$. Notons $O(p, q) \subset \mathrm{GL}_n(\mathbb{R})$ le groupe des isométries de la forme quadratique de $\mathbb{R}^n$ de signature (p, q), de matrice dans la base canonique

$$I_{(p,q)} = \mathrm{diag}(\underbrace{1, \ldots, 1}_{p}, \underbrace{-1, \ldots, -1}_{q}).$$

On dispose d'un homéomorphisme

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

Preuve.

Étape 1 (décomposition polaire). Soit $M \in O(p, q)$. Par décomposition polaire, il existe deux matrices $O \in O(n)$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$ telles que $M = OS$. Montrons que ces deux matrices sont elles aussi des éléments de $O(p, q)$. Notons qu'il suffit de montrer que c'est le cas de S.
Soit $T = {}^tMM \in S_n^{++}(\mathbb{R})$, de sorte que $S^2 = T$. La matrice T est un élément de $O(p, q)$, puisque ce groupe est stable par transposition. En effet, si $A \in O(p, q)$, alors ${}^tAI_{(p,q)}A = I_{(p,q)}$. En passant à l'inverse, on obtient

$$A^{-1} I_{(p,q)} {}^tA^{-1} = I_{(p,q)},$$

ce qui implique que ${}^tA^{-1} \in O(p,q)$ et donc que ${}^tA \in O(p,q)$.
À présent, on utilise le fait que l'exponentielle définit une bijection $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$ (et c'ets même un homéomorphisme). Dès lors, on peut se donner $U \in \mathcal{S}_n(\mathbb{R})$ tel que $\exp(U) = S$ et donc $\exp(2U) = S^2 = T$. Par conséquent, on a la suite d'équivalence suivante, en utilisant que l'exponentielle commute avec la transposition et avec la conjugaison,

$$\begin{aligned} S \in O(p,q) &\Leftrightarrow {}^tSI_{(p,q)}S = I_{(p,q)} \\ &\Leftrightarrow S = I_{(p,q)}S^{-1}I_{(p,q)} \\ &\Leftrightarrow \exp(U) = I_{(p,q)}\exp(-U)I_{(p,q)} \\ &\Leftrightarrow \exp(U) = \exp(-I_{(p,q)}UI_{(p,q)}) \\ &\Leftrightarrow U = -I_{(p,q)}UI_{(p,q)} \\ &\Leftrightarrow 2U = -I_{(p,q)}(2U)I_{(p,q)} \\ &\Leftrightarrow T = I_{(p,q)}T^{-1}I_{(p,q)} \Leftrightarrow T \in O(p,q) \end{aligned}$$

Donc puisque l'on a démontré que $T \in O(p,q)$, il en résulte que $S \in O(p,q)$. On remarque que l'on a au passage démontré la condition suivante, pour tout $A \in \mathrm{GL}_n(\mathbb{R})$,

$$A \in O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R}) \Leftrightarrow \exists U \in \mathcal{S}_n(\mathbb{R}) / \exp(U) = A \text{ et } I_{(p,q)}U + UI_{(p,q)} = 0.$$

En outre, la décomposition polaire étant un homéomorphisme, on a démontré que l'on disposait de l'homéomorphisme suivant,

$$O(p,q) \cong (O(p,q) \cap O(n)) \times \left(O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R})\right).$$

Étape 2 (étude de $O(p,q) \cap O(n)$).
Considérons $O \in O(p,q) \cap O(n)$, que l'on décompose en blocs selon (p,q),

$$O = \begin{pmatrix} A & C \\ B & D \end{pmatrix}.$$

La relation $I_{(p,q)} = {}^tOI_{(p,q)}O$ nous donne, en inspectant respectivement les blocs supérieur gauche et inférieur droit,

$${}^tAA - {}^tBB = I_p \quad \text{et} \quad {}^tCC - {}^tDD = -I_q.$$

Or, puisque $O \in O(n)$, on obtient que $OI_{(p,q)} = I_{(p,q)}O$ et donc que O et $I_{(p,q)}$ commutent. Par conséquent, O laisse stable les sous espaces propre associés aux valeurs propres 1 et -1 de $I_{(p,q)}$. Si bien que nécessairement, $B = C = 0$. Dès, lors, on en déduit que

$${}^tAA = I_p \quad \text{et} \quad {}^tDD = I_q.$$

Il est alors aisé de conclure que l'on a l'homéomorphisme

$$O(p,q) \cap O(n) \cong \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \mid A \in O(p), D \in O(q) \right\} \cong O(p) \times O(q)$$

Étape 3 (étude de $O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R})$).
Puisque l'exponentielle réalise un homéomorphisme $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}(\mathbb{R})$, on a vu que l'on disposait de l'homéomorphisme

$$O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R}) \cong L := \{U \in \mathcal{S}_n(\mathbb{R}) \mid UI_{(p,q)} + I_{(p,q}U = 0\}$$

L'ensemble L est un espace vectoriel, dont il s'agit de calculer la dimension. Soit $U \in L$, que l'on décompose en blocs selon (p,q),

$$U = \begin{pmatrix} A & B \\ {}^tB & D \end{pmatrix}$$

avec A, D symétriques. La relation $UI_{(p,q)} + I_{(p,q}U = 0$ peut alors s'écrire

$$\begin{pmatrix} A+A & -B+B \\ {}^tB - {}^tB & D+D \end{pmatrix} = 0$$

On déduit donc que

$$L \cong \left\{ \begin{pmatrix} 0 & B \\ {}^tB & 0 \end{pmatrix} \mid B \in \mathcal{M}_{p,q}(\mathbb{R}) \right\} \cong \mathbb{R}^{pq}.$$

Questions possibles :

- A-t-on un résultat similaire sur $\mathbb{C}$? (plus généralement, lorsque l'on parle de matrice symétrique, il faut toujours être prêt à parler de matrices hermitiennes)
- Donner une idée de la preuve de la décompostion polaire.
- Donner une idée de la preuve de l'homéomorphisme exp : $S_n(\mathbb{R}) \to S_n^{++}(\mathbb{R})$.

3.3 Enveloppe convexe de $O_n(\mathbb{R})$

Leçons concernées. 159, 160, 161, 181.
Référence. *Objectif agrégation*, Beck, Malick & Peyré et *Algèbre, tome 2, groupes*, Aviva Szpirglas.
Remarques. Le résultat peut paraître anecdotique, mais il utilise ou illustre un certain nombre de résultats classiques (décomposition polaire, théorème de représentation de Riesz, Hahn-Banach géométrique, projection sur un convexe fermé...) et ouvre le champ assez large de la géométrie convexe (sur lequel il faut peut-être connaître quelques résultats, voir *Géométrie* de Patrice Tauvel par exemple).

Théorème 4 (Hahn-Banach géométrique, version Hilbert)
Soit H un espace de Hilbert (on peut également se placer en dimension finie).

i. Soit C un convexe fermé (non vide) de H et $x \in H \backslash C$. Il existe une forme linéaire (continue) f telle que
$$f(x) > \sup_{y \in C} f(y).$$

ii. Soit A une partie de H. On a la caractérisation suivante de l'enveloppe convexe fermée $\overline{\mathrm{Conv}(A)}$.
$$\forall x \in H, \qquad x \in \overline{\mathrm{Conv}(A)} \quad \text{ssi} \quad \forall f \in H',\ f(x) \leqslant \sup_{y \in C} f(y).$$

Théorème 5
Notons B la boule unitié de $\mathcal{M}_n(\mathbb{R})$ pour la norme subordonnée à la norme euclidienne sur $\mathbb{R}^n$. L'enveloppe convexe de $O_n(\mathbb{R})$ est égale à B.

Questions possibles :

- Pourquoi l'enveloppe convexe de ${}_n(\mathbb{R})$ est-elle fermée ? (une réponse possible est d'utiliser le résultat de compacité de Carathéodory sur l'enveloppe convexe)
- Quels sont les point extrémaux de B ? (réponse : c'est $O_n(\mathbb{R})$)
- Donner une idée de la preuve de la décomposition polaire.

3.4 Forme normale de Smith

Leçons concernées. 122, 142, 148, 152, 162.
Référence. *131 Développements pour l'oral* , D. Lesesvre, P. Montagnon, P. Le Barbenchon & T. Pierron .
Remarques. Travailler la forme normale de Smith et les modules sur les anneaux euclidiens (ou principaux) est à mon sens très rentable, étant donné le nombre d'applications à ce résultat. À peu près toute application usuelles du pivot de Gauss mais sur un anneau euclidien et non plus un corps (notamment la résolution de systèmes linéaires), théorème de la base adaptée (et donc étude des réseaux),

classification des modules de type fini (sur un anneau principal), classification des groupes abéliens de type fini, décomposition de Frobenius et de Jordan (attention, il faut étudier un peu plus précisément les $k[X]$-modules)... On peut trouver tout cela dans *Objectif agrégation* ainsi que dans *Géométrie* de Patrice Tauvel pour les réseaux.

Théorème 6 (Forme normale de Smith)
Soit A un anneau euclidien et $M \in \mathcal{M}_{m,n}(A)$. Il existe un unique entier r et d'uniques éléments $f_1, \dots, f_r \in A$ (uniques aux inversibles près) tels que $f_1 \mid \cdots \mid f_r$ et tels que M est équivalente à

$$\begin{pmatrix} f_1 & & & & & & \\ & f_2 & & & & & \\ & & \ddots & & & & \\ & & & f_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

Questions possibles :

- La preuve du développement n'est pas tout à fait effective. Existe-t-il un algorithme permettant de calculer la forme normale de Smith ?
- Donner la forme normale de Smith de la matrice $\begin{pmatrix} 4 & 2 & -3 \\ -2 & -2 & 0 \\ 0 & 2 & 3 \end{pmatrix}$. On trouve $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
- Donner la forme normale de Smith de la matrice $\begin{pmatrix} 12 & 0 & 0 \\ 0 & 18 & 0 \end{pmatrix}$. Attention, 12 ne divise pas 18.
- Comment calcule-t-on les invariants de similtude d'une matrice carrée A à coefficients dans un corps k ? On calcule la FNS de $XI_n - A$ dans $\mathcal{M}_n(k[X])$.
- Peut-on calculer la forme normale de Smith sur un anneau autre qu'Euclidien ? Oui, sur un anneau principal par les matrices de Bézout, mais il est à noter que ce n'est pas effectif (on n'a pas d'algorithme pour calculer ces matrices).

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

Leçons concernées. 102, 125, 141, 144.
Référence. *Cours d'algèbre*, Daniel Perrin.
Remarques. La preuve est assez courte, mais ce n'est pas forcément gênant, on peut prendre bien le temps d'expliquer les choses, ce qui est important lors d'un développement ! Pour bien justifier la présence de ce développement dans la leçon 125, il est nécessaire à mon avis de parler un peu d'extensions cyclotomiques et de leur importance en théorie de Galois (même brièvement) en les reliant par exemple aux extensions quadratiques (consulter le Gozart, par exemple).

Théorème 7
Soit $n \in \mathbb{N}^*$. Le polynôme $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.

Preuve. Soit $\zeta \in \mathbb{C}$ une racine n-ième primitive de l'unité. Si p est un nombre premier ne divisant pas n, alors ζ^p est elle aussi une racine n-ième primitive de l'unité. Soit f, g les polynômes minimaux respectifs de ζ et ζ^p sur Q. Par factorialité de $\mathbb{Z}[X]$, on décompose Φ_n en facteurs irréductibles sur $\mathbb{Z}[X]$,

$$\Phi_n = f_1^{\alpha_1} \cdots f_r^{\alpha_r}.$$

Le polynôme Φ_n étant unitaire, il en va de même pour les f_i. Or, ζ (resp. ζ^p) est racine de l'un des f_i, qui est unitaire et irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$. Dès lors, f et g sont parmi les f_i et en particuliers sont à coefficients entiers.

Montrons que $f = g$. Supposons par l'absurde que ce n'est pas le cas. Puisque f et g sont irréductibles et distincts, le produit $f \cdot g$ divise Φ_n dans $\mathbb{Z}[X]$. En outre, $g(\zeta^p) = 0$, donc f divise $g(X^p)$ dans $\mathbb{Q}[X]$. On dispose donc de $h \in \mathbb{Q}[X]$ tel que $g(X^p) = f(X)h(X)$.

Montrons que $h \in \mathbb{Z}[X]$. Puisque f est unitaire, on effectue la division euclidienne $g(X^p) = f(X) \cdot h_0(X) + r(X)$ de $g(X^p)$ par f dans $\mathbb{Z}[X]$, qui est également une division euclidienne dans $\mathbb{Q}[X]$. Par unicité de la division euclidienne dans $\mathbb{Q}[X]$, on a $r(X) = 0$ et $h(X) \in \mathbb{Z}[X]$.

Posons $g(X) = a_r X^r + \cdots + a_0$ avec $a_i \in \mathbb{Z}$. On a alors en appliquant la projection $\bar{\cdot}$ dans $\mathbb{F}_p[X]$ et en utilisant le morphisme de Frobenius,

$$\overline{g}(X^p) = \overline{a_r} X^p r + \cdots + \overline{a_1} X^p + \overline{a_0} = \overline{a_r}^p X^p r + \cdots + \overline{a_1}^p X^p + \overline{a_0}^p = (\overline{a_r} X^r + \cdots + \overline{a_0})^p = \overline{g}(X)^p.$$

Soit alors $\varphi \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{f}$. On a $\overline{g}(X)^p = \overline{f} \cdot \overline{h}$, donc par le lemme d'Euclide, φ divise $\overline{g}$.
Puisque fg divise Φ_n, il en résulte que $\overline{f}\overline{g}$ divise $\overline{\Phi_n} = \Phi_{n,\mathbb{F}_p}$. Ainsi, φ^2 divise $\overline{\Phi_n}$ et donc dans un corps de rupture de φ, le polynôme $\overline{\Phi_n}$ admet une racine double.
Or, dans $\mathbb{F}_p[X]$, la dérivée de $X^n - 1$ est nX^{n-1}. Puisque $n \wedge p = 1$, la seule de racine de nX^{n-1} est 0, qui n'est pas racine de $X^n - 1$ et donc $X^n - 1$ est à racines simples dans son corps de décomposition. Puisque $\overline{\Phi_n}$ divise $X^n - 1$, il est lui aussi à racines simples, d'où notre contradiction. On a donc $f = g$.

Soit ζ' une racine primitive n-ième de l'unité. On a $\zeta' = \zeta^m$ pour un certain entier m premier avec n. Si l'on écrit $m = p_1^{\beta} \cdots p_s^{\beta^s}$ alors il est clair que par une récurrence immédiate, ζ' et ζ ont le mêmes polynôme minimal sur $\mathbb{Q}$. Ainsi, $f(\zeta') = 0$. Donc f admet toutes les racines primitives n-ième de l'unité comme racines. Ainsi, $\deg f \geqslant \varphi(n) = \deg \Phi_n$ et $f \mid \Phi_n$, donc $f = \Phi_n$. Par conséquent, Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

✌

Questions possibles :
- Pourquoi les polynômes cyclotomiques sur $\mathbb{Q}$ sont-ils à coefficients dans $\mathbb{Z}$?
- Soit m, n deux entiers premiers entre eux et α (resp. β) une racine primitive n-ième (resp. m-ième) de l'unité. Montrer que $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$. On peut trouver ce résultat dans le *Cours d'algèbre* de Perrin.
- Le résultat est-il vrai sur les corps finis ? (non, Φ_8 n'est irréductible sur aucun corps fini)

3.6 Loi de réciprocité quadratique

Leçons concernées. 101, 123, 170, 190.
Référence. *Nouvelles histoires hédonistes de groupes et de géométries, tome 1*, Caldero et Germoni.
Remarques. Un résultat incontournable, aux nombreuses démonstrations. Celle-ci présente l'avantage de mettre en oeuvre des outils assez surprenants (actions de groupes, formes quadratiques sur les coprs finis) et n'est pas très difficile à travailler.

Théorème 8 (Loi de réciprocité quadratique)
Soiit p, q deux nombres premiers impairs distincts. On a

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

Autrement dit, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ si et seulement si p ou q est congru à 1 modulo 4.

Questions possibles : (ce sont les questions que j'ai eues le jour J)
- Dans la démonstration, on utilise une action de $\mathbb{Z}/p\mathbb{Z}$, pourquoi pas un autre $\mathbb{Z}/n\mathbb{Z}$?
- À quoi sert la loi de réciprocité quadratique?
- Calculer un résidu quadratique.

3.7 Par cinq points passe une conique

Leçons concernées. 151, 152, 162, 171, 181, 191.
Référence. *Géométrie analytique classique*, Eiden.
Remarques. Ce développement a de nombreux recasages, ce qui ne veut pas forcément dire qu'il faut tous les exploiter mais montre surtout qu'il illustre énormément de leçon. C'est en outre un développement de géométrie, plus particulièrement sur les coniques, ce qui est un thème qui devrait faire plaisir au jury. Il faut être un minimum à l'aise avec les coordonnées barycentriques, qui sont de toute façon quasiment indispensables pour la leçon 181. Sur ce sujet, on pourra compléter la lecture du Eiden par celle de *Algèbre et géométries* de Pascal Boyer.
Il n'est à mon avis pas forcément nécessaire de démontrer la condition de non-dégénérescence, et peut-être pas absurde de prendre le temps de poser le cadre barycentrique en premier lieu.

Théorème 9
Soit $\mathcal{E}$ un plan affine et A, B, C, D, E cinq points distinct de $\mathcal{E}$. Par ces cinq points passe une conique. Elle est unique si et et seulement si 4 points quelconques parmi ces 5 points ne sont pas alignés.
Elle est non dégénérée si et seulement si 3 points quelconques parmi ces 5 points ne sont pas alignés.

Questions possibles :
- Montrer que deux coniques du plan affine s'intersectent en au plus 4 points ou ont une droite en commun.
- Démontrer la condition d'alignement de trois points utilisée dans le développement.

3.8 Primalité des nombres de Mersenne

Leçons concernées. 120, 121, 123, 125, 141.
Référence. *Cours de calcul formel. Corps finis, systèmes polynomiaux, applications*, Philippe Saux-Picart & Eric Rannou.
Remarques. Contrairement à ce qui est fait dans le Saux-Picart, on calcule directement le résidu quadratique de 3 modulo M_q au début de la preuve. Ceci raccourcit la démonstration et si c'est trop court on peut par exemple présenter le test de Lehmer-Lucas (qui est indispensable dans le plan, de toute façon) ou bien prendre son temps, ce qui jamais une mauvaise idée.

Théorème 10 (Un critère de primalité)
Soit q un nombre premier impair et $M_q := 2^q - 1$. Le nombre M_q est premier si et seulement si

$$(2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q,$$

où $\sqrt{3}$ est considérée dans une extension de l'anneau $\mathbb{Z}/M_q\mathbb{Z}$ que nous spécifierons.

Preuve. On suppose tout d'abord que M_q est un nombre premier. Montrons tout d'abord que 3 n'est une racine carrée dans $\mathbb{Z}/M_q\mathbb{Z}$. Pour cela, calculons le symbole de Legendre $\left(\frac{3}{M_q}\right)$ par la réciprocité quadratique.

$$\left(\frac{3}{M_q}\right) = \left(\frac{3}{2^q-1}\right) = -\left(\frac{2^q-1}{3}\right) = -\left(\frac{(-1)^q-1}{3}\right) = -\left(\frac{-2}{3}\right) = -1.$$

On pose donc $\mathcal{A} := \mathbb{F}_{M_q}[X]/(X^2-3)$ et l'on note $\sqrt{3}$ l'image de X dans $\mathcal{A}$. En outre, on a

$$(2^{\frac{q+1}{2}})^2 \equiv 2 \mod M_q,$$

donc $\sqrt{2} := 2^{\frac{q+1}{2}}$ est une racine carrée de 2. On note donc

$$\rho := \frac{1+\sqrt{3}}{\sqrt{2}} \quad \text{et} \quad \overline{\rho} := \frac{1-\sqrt{3}}{\sqrt{2}}.$$

De sorte que $\rho^2 = 2+\sqrt{3}$ et $\rho\overline{\rho} = -1$.
En outre, on a $\sqrt{3}^{M_q} = \sqrt{3}^{2\cdot\frac{M_q-1}{2}+1} = 3^{\frac{M_q-1}{2}}\sqrt{3} = -\sqrt{3}$, donc si $a, b \in \mathbb{F}_{M_q}$,

$$(a+b\sqrt{3})^{M_q} = a - b\sqrt{3},$$

puisque $\mathcal{A}$ est un corps de caractéristique M_q. Si bien que, comme $\sqrt{2} \in \mathbb{F}_{M_q}$, on a

$$(2+\sqrt{3})^{2^{q-1}} = \underbrace{(2+\sqrt{3})}_{=\rho^2}^{\frac{M_q+1}{2}} = \rho^{M_q+1} = \overline{\rho}\rho = -1.$$

Réciproquement, on suppose que dans une extension $\mathcal{A}$ contenant une racine carrée de 3 (à savoir $\mathbb{Z}/M_q\mathbb{Z}$ ou $(\mathbb{Z}/M_q\mathbb{Z})[X]/(X^2-3)$ selon que 3 est carré modulo M_q ou non), on a

$$(2+\sqrt{3})^{2^{q-1}} = -1.$$

Supposons par l'absurde que M_q n'est pas premier. On se donne donc p un diviseur premier de M_q qui lui est donc strictement inférieur. Puisque p est un diviseur de 0 dans $\mathcal{A}$, il est non inversible et est donc contenu dans un idéal maximal $\mathcal{M}$. Par conséquent, $\mathcal{A}/\mathcal{M}$ est un corps de caractéristique p, dans lequel on note α et β les images respectives de $2+\sqrt{3}$ et $2-\sqrt{3}$. Patr hypothèse, $\alpha^{2^{q-1}} = -1$, donc α est d'orde 2^q. De plus, le polynôme $Q = (X-\alpha)(X-\beta) = X^2 - 4X + 1$ est un polynôme à coefficients dans $\mathbb{F}_p$ et donc $Q(\alpha^p) = Q(\alpha)^p = 0$. Par conséquent, $\alpha^p = \alpha$ ou β.

— Si $\alpha^p = \alpha$, alors $\alpha^{p-1} = 1$ et donc 2^q divise $p-1$, si bien que $p \leqslant 2^q \leqslant p-1$, ce qui est absurde.
— Donc $\alpha^p = \beta$. Or, $\beta = \alpha^{-1} = \alpha^{2^q-1}$, donc $\alpha^{p+1} = \alpha^{2^q} = 1$, ce qui est à nouveau absurde, car alors $p < 2^q - 1 \leqslant p$.

✌

Questions possibles :
— Montrer le test de primalité de Lehmer-Lucas. Quelle est sa complexité ?
— Calculer un résidu quadratique.
— Existe-t-il une infinité de nombres de Mersenne ? (on ne sait pas)

3.9 Réduction de Frobenius

Leçons concernées. 151, 153, 154, 157, 159.
Référence. *Les maths en tête, Algèbre*, Xavier Gourdon.
Remarques. Il vaut mieux être à l'aise avec la notion d'endomorphisme cyclique.

On se donne un corps quelconque k et un k-espace vectoriel E de dimension finie.

Théorème 11 (Invariants de similitude)
Soit $u \in \mathcal{L}(E)$. Il existe une unique suite $F_1, \dots, F_r$ de sous-espaces vectoriels de E stables par f tels que

i. $E = F_1 \oplus \cdots \oplus F_r$,

ii. pour tout $1 \leqslant i \leqslant r$, $f_i := f_{|F_i}$ est un endomorphisme cyclique,

iii. si P_i est le polynôme minimal de f_i, alors P_{i+1} divise P_i pour tout $i \in \{1, \dots, r-1\}$.

De plus, la suite de polynômes $P_1, \dots, P_r$ ne dépend que de f et on l'appelle suite des invariants de similitudes de f.

Preuve. **Existence :** Soit d le degré de μ_u et $x \in E$ de polynôme minimal local $\mu_{u,x}$ égal à μ. On note F le sous-espace $\mathrm{Vect}\{u^p(x) | p \in \mathbb{N}\}$ stable par u engendré par x, qui est donc de dimension d et dont $(e_1, \dots, e_d) := (x, u(x), \dots, u^{d-1}(x))$ forme une base. On la complète en une base $(e_1, \dots, e_n)$ de E. Soit alors $(e_1^*, \dots, e_n^*)$ la base duale associée, on note en outre

$$\Gamma := \{{}^t u^i(e_d^*) \mid i \in \mathbb{N}\} = \{e_d^* \circ u^i \mid i \in \mathbb{N}\} \quad \text{et} \quad G := \Gamma^\circ = \{x \in E \mid \forall \varphi \in \Gamma,\ \varphi(x) = 0\}.$$

Autrement dit, G est l'ensemble des éléments $x \in E$ tels que la $d-$ième coordonnée de $u^i(x)$ est nulle pour tout entier i. C'est un sous-espace vectoriel de E stable par u. Montrons alors que $E = F \oplus G$.

Tout d'abord, vérifions que $F \cap G = \{0\}$. Soit y un élément de cette intersection. Puisque $y \in F$, on écrit $y = a_1 e_1 + \cdots + a_d e_d$ avec $a_1, \dots, a_d \in k$. Supposons par l'absurde qu'il existe un indice $1 \leqslant p \leqslant d$ tel que $a_p \neq 0$ et donnons nous p l'indice maximal tel que cela est réalisé. Puisque $y \in F$, on a

$$0 = {}^t u^{d-p}(e_d^*)(y) = e_d^* \circ u^{d-p}(y) = e_d^*(a_1 e_{d-p+1} + \cdots + a_p e_d) = a_p,$$

ce qui est absurde. Donc $y = 0$.

Maintenant, montrons que $\dim F + \dim G = \dim E =: n$. Il s'agit donc de montrer que $\dim G = n - \dim F = n - d$. Or, $G = \Gamma^\circ$, donc il nous suffit de montrer que $\dim \mathrm{Vect}\,\Gamma = d$. On considère donc l'application linéaire

$$\varphi : \begin{cases} k[u] & \longrightarrow \mathrm{Vect}\,\Gamma \\ g & \longmapsto e_d^* \circ g \end{cases}.$$

Par définition de $\mathrm{Vect}\,\Gamma$, l'application φ est surjective. De plus, si $g \in \mathrm{Ker}\,\varphi$, on écrit $g = a_1 \mathrm{Id}_E + \cdots + a_d u^{d-1}$ avec $a_1, \dots, a_d \in k$. Supposons par l'absurde qu'il existe un indice $1 \leqslant p \leqslant d$ tel que $a_p \neq 0$ et donnons nous p l'indice maximal tel que cela est réalisé. On a

$$0 = \varphi(g)(f^{d-p}(x)) = e_d^* \circ g(f^{d-p}(x)) = e_d^*(a_1 f^{k-p}(x) + \cdots + a_p f^{d-1}(x)) = a_p,$$

ce qui est absurde. Donc $g = 0$ et φ est injective. Ainsi, φ est un isomorphisme et donc $\dim Gamma = d$.

On a donc trouvé G un supplémentaire de F stable par u. On note ainsi P_1 le polynôme minimal de $f_{|F}$ (de sorte que $P_1 = \mu_u$) et P_2 le polynôme minimal de $f_{|G}$, qui divise donc P_1. En travaillant par récurrence et en appliquant le résultat à G, on aboutit donc.

Unicité : Suppsons l'existence de deux suites de sous-espaces $F_1, \dots, F_r$ et $G_1, \dots, G_s$ stables par u et vérifiant les conditions i., ii. et iii. On note P_i (resp. Q_j) le polynôme minimal de $f_{|F_i}$ (resp. de $f_{|G_j}$). Supposons, disons $r \leqslant s$. D'après ii. on a $\sum \deg P_i = \sum \deg Q_j$, donc si l'on suppose les deux suites distinctes, il existe un indice $1 \leqslant i \leqslant r$ tel que $P_i \neq Q_i$, et on suppose que i est l'indice minimal où cela est vérifié. Da'après iii., pour tout $j \geqslant i$ on a $P_i(u)(F_j) = 0$ et donc d'après i.,

$$P_i(u)(E) = P_i(u)(F_1 \oplus \cdots \oplus F_r) = P_i(u)(F_1) \oplus \cdots \oplus P_i(u)(F_{i-1}).$$

Par ailleurs, on a également

$$P_i(u)(E) = P_i(u)(G_1) \oplus \cdots \oplus P_i(u)(G_{i-1}) \oplus P_i(u)(G_i) \oplus \cdots \oplus P_i(u)(G_s).$$

Or, pour tout $1 \leqslant j \leqslant i-1$, on a $P_i = Q_i$, donc puisque les $f_{|G_j}$ et les $f_{|F_j}$ sont cycliques, on a $\dim F_j = \dim G_j = \deg P_j$ et donc $\dim P_i(u)(F_j) = \dim P_i(u)(G_j)$. On en déduit donc que

$$0 = \dim P_i(u)(G_i) = \cdots = \dim P_i(u)(G_s).$$

Ainsi, Q_i divise donc P_i. Par symétrie des rôles, on a également que P_i divise Q_i et donc $P_i = Q_i$, ce qui est absurde. Finalement, on a donc $r = s$ et $Q_i = P_i$ pour tout i.

Théorème 12 (Réduction de Frobenius)
Soit $P_1, \dots, P_r$ la suite des invariants de similitude de $u \in \mathcal{L}(E)$. Il existe une base $\mathcal{B}$ de E dans laquelle

$$\mathcal{M}_{\mathcal{B}}(u) = \begin{pmatrix} C_{P_1} & & 0 \\ & \ddots & \\ 0 & & C_{P_r} \end{pmatrix},$$

où C_{P_i} est la matrice compagnon associée à P_i. De plus, $P_1 = \mu_u$ et $P_1 \cdots P_r = \chi_u$.
Deux endomorphismes u et v sont alors semblables si et seulement s'ils partagent les mêmes invariants de similitude.

Preuve. Pour obtenir la décomposition annoncée, il suffit de considérer une base adaptée à la décomposition $E = F_1 \oplus \cdots \oplus F_r$ et d'utiliser le fait qu'un endormophisme cyclique a pour matrice une matrice compagnon dans une certaine base.

Par transitivité de la relation de similitude et par unicité des invariants de similitude, il est clair que deux endomorphismes semblables partagent la même suite d'invariants de similitude. Réciproquement, si deux endomorphismes ont les mêms invariants de similitudes, alors ils sont semblables à la même matrice et donc semblables eux-mêmes par transitivité.

Questions possibles :
- Donner l'idée de la preuve du fait qu'il existe un polynôme minimal local égal au polynôme minimal.
- Quelle est la forme réduite de Frobenius de la matrice $\begin{pmatrix} \lambda & a \\ 0 & \mu \end{pmatrix}$?
- Quelle est la forme réduite de Frobenius d'une matrice diagonalisable ? (il est en tout cas bon de se poser la question, même si la réponse n'est pas forcément facile à formaliser/démontrer)
- Comment retrouve-t-on la réduction de Jordan à partir de celle de Frobenius ?
-
- Comment calcule-t-on les invariants de similtude d'une matrice carrée A à coefficients dans un corps k ? On calcule la FNS de $XI_n - A$ dans $\mathcal{M}_n(k[X])$.

3.10 Simplicité du groupe alterné

Leçons concernées. 103, 104, 105, 108.
Référence. *Cours d'algèbre*, Daniel Perrin.
Remarques. Il existe de nombreuses preuves de la simplicité de $\mathfrak{A}_n$, celle-ci est la plus élémentaire possible.

Théorème 13 (Simplicité de $\mathfrak{A}_n$)
Pour tout entier $n \geqslant 5$, le groupe alterné $\mathfrak{A}_n$ est simple.

Preuve.

Lemme 14 Pour tout $n \in \mathbb{N}$, le groupe $\mathfrak{A}_n$ est engendré par les 3−cycles.

Preuve. Le groupe $\mathfrak{S}_n$ est engendré par les transpositions, donc tout élément du groupe alterné est un produit de transposition. Une transposition étant de signature égale à -1, tout élément de $\mathfrak{A}_n$ s'écrit même comme un produit paire de transpositions. Il suffit donc de montrer que si $\tau_1, \tau_2 \in \mathfrak{S}_n$ sont deux transpositions, leur produit $\tau_1\tau_2$ s'écrit comme un produit de 3−cycles. Plusieurs cas de figures sont alors possibles.

- Si $\tau_1 = \tau_2$, alors $\tau_1\tau_2 = \mathrm{id}$ et le résultat est clair.
- Si $\tau_1 \neq \tau_2$ et leurs supports ont une intersection réduite à un singleton, alors il existe des éléments $x, y, z \in \{1, \dots, n\}$ distincts tels que $\tau_1 = (x\ y)$ et $\tau_2 = (x\ z)$.
  Dans ce cas, $\tau_1\tau_2 = (x\ y)(x\ z) = (x\ z\ y)$.
- Si $\tau_1 \neq \tau_2$ et leurs supports sont disjoints, alors il existe $x, y, z, t \in \{1, \dots, n\}$ distincts tels que $\tau_1 = (x\ y)$ et $\tau_2 = (z\ t)$.
  Dans ce cas, $\tau_1\tau_2 = (x\ y)(z\ t) = (x\ y)(y\ z)(y\ z)(z\ t) = (x\ y\ z)(y\ z\ t)$.

✌

Lemme 15 Pour tout entier $n \geqslant 5$, les 3−cycles sont conjugués dans le groupe $\mathfrak{A}_n$.

Preuve. Les 3−cycles sont conjugués dans $\mathfrak{S}_n$, donc si σ_1, σ_2 sont deux 3−cycles, il existe $\rho \in \mathfrak{S}_n$ tel que $\sigma_2 = \rho\sigma_1\rho^{-1}$. Puisque $n \geqslant 5$, on dispose de $x, y \in \{1, \dots, n\}$ non contenus dans le support de σ_2, de sorte que $((x\ y)\rho)\sigma_1(\rho(x\ y))^{-1} = (x\ y)\rho\sigma_1\rho^{-1}(x\ y) = (x\ y)\sigma_2(x\ y) = \sigma_2$.

Or, $\varepsilon(\rho) = -\varepsilon((x\ y)\rho)$, donc ρ ou $(x\ y)\rho$ est dans $\mathfrak{A}_n$ et donc σ_1 et σ_2 sont conjuguées dans $\mathfrak{A}_n$.

✌

La stratégie est maintenant claire. Considérons un sous-groupe distingué N non trivial de $\mathfrak{A}_n$ et montrons qu'il contient un 3−cycle. Puisque N est distingué, il les contiendra donc tous et puisqu'il contient un système de générateurs de $\mathfrak{A}_n$, il lui sera égal.

Considérons $\sigma \in N$ différent de l'identité (par hypothèse, N est non trivial). Il existe donc $x \in \{1, \dots, n\}$ tel que $y := \sigma(x) \neq x$. Considérons alors $z \in \{1, \dots, n\} \backslash \{\sigma^{-1}(x), x, y\}$ et posons $\gamma := (x\ z\ y)$, de sorte que

$$\gamma\sigma(x) = \gamma(y) = x \quad \text{et} \quad \sigma\gamma(x) = \sigma(z) \neq x.$$

Ainsi, $\sigma' := \sigma\gamma\sigma^{-1}\gamma^{-1} \neq \mathrm{id}$. De plus, puisque N est distingué, $\sigma' = \sigma(\gamma\sigma^{-1}\gamma^{-1}) \in N$ et on a

$$\begin{aligned}\sigma' &= (\sigma(x\ z\ y)\sigma^{-1})(y\ z\ x) \\ &= (\sigma(x)\ \sigma(y)\sigma(z))(y\ z\ x) = (y\ \sigma(y)\ \sigma(z))(y\ z\ x).\end{aligned}$$

Donc σ' est le produit de deux 3−cycles qui agissent sur l'ensemble à au plus 5 éléments $F := \{x, y, z, \sigma(y), \sigma(z)\}$. On considère donc la décomposition de σ' en produit de cycles à support disjoints sur F, plusieurs cas de figures se présentent, en prenant en compte le fait que $\varepsilon(\sigma') = 1$.

- Si σ' est un 3-cycle, on a terminé.
- Si σ' et un produit de deux 2−cycles $(x_1\ x_2)(x_3\ x_4)$, alors si $x_5 \in \{1, \dots, n\} \backslash \{x_1, x_2, x_3, x_4\}$, alors on pose $\tau := (x_1\ x_2\ x_5)$, de sorte que $\sigma'' := \sigma'\tau\sigma'^{-1}\tau^{-1} \in N$ et

$$\sigma'' = (\sigma(x_1)\ \sigma(x_2)\ \sigma(x_5))(x_5\ x_2\ x_1) = (x_2\ x_1\ x_5)(x_5\ x_2\ x_1) = (x_1\ x_2\ x_5).$$

- Enfin, si σ' est un 5−cycle $(x_1\ x_2\ x_3\ x_4\ x_5)$, alors on pose $\tau = (x_1\ x_2\ x_3)$, de sorte que $\sigma'' := \sigma'\tau\sigma'^{-1}\tau^{-1} \in N$ et

$$\sigma'' = (\sigma(x_1)\ \sigma(x_2)\ \sigma(x_3))(x_3\ x_2\ x_1) = (x_2\ x_3\ x_4)(x_3\ x_2\ x_1) = (x_1\ x_4\ x_2).$$

Questions possibles :

— Que peut-on dire dans le cas $n < 5$? Lister les sous-groupes distingués de $\mathfrak{A}_4$. Quels sont les endroits dans la preuve où l'on a utilisé l'hypothèse $n \geqslant 5$?
— Quels sont les sous-groupes distingués de $\mathfrak{S}_n$?
— Quels sont les sous-groupes d'indice 2 de $\mathfrak{S}_n$?
— Peut-on injecter $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+1}$? Et $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$? (exercices corrigés du Rombaldi)
— Quels sont les sous-groupes d'indice n de $\mathfrak{S}_{n+1}$ à isomorphisme près ? (idem)

3.11 Table des caractères de $\mathfrak{S}_4$

Les trois développements suivants ont une bonne moitié en commun, le reste est à adapter selon les leçons.

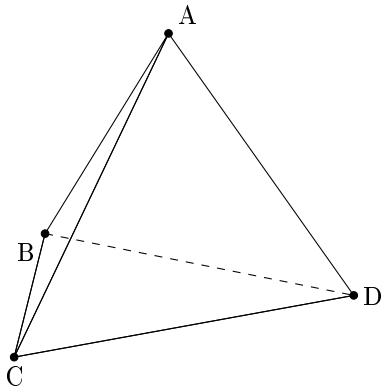
3.11.1 Isométries du cube et du tétraèdre

Leçons concernées. 161, 191.
Référence. *Nouvelles histoires hédonistes de groupes et géométrie, tome 2*, Philippe Caldero et Jérôme Germoni ou *Histoires hédonistes de groupes et géométrie, tome 1*, Philippe Caldero et Jérôme Germoni.
Remarques. Ce développement admet peu de recasages parce qu'il complète la détermination de la table de caractères de $\mathfrak{S}_4$.

Définition 16 (Groupe d'isométries)
Soit $X \subset \mathbb{R}^3$. Le groupe des isométries de X est le sous-groupe $\mathrm{Is}(X)$ des isométries de l'espace affine euclidien $\mathbb{R}^3$ qui stabilisent X.

Théorème 17 (Isométries du tétraèdre.)
Le groupe des isométries du tétraèdre Δ_4 est $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4$.

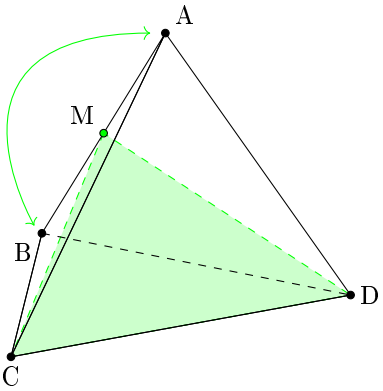
Preuve. Notons A, B, C, D les sommets du tétraèdre, comme dans la figure ci-dessous.



Les sommets du tétraèdre sont ses points extrémaux, donc le groupe $\mathrm{Is}(\Delta_4)$ agit par permutation sur l'ensemble $\{A, B, C, D\}$. Puisque (A, B, C, D) constitue une base affine de l'espace, on dispose donc d'une injection

$$\varphi : \mathrm{Is}(\Delta_4) \hookrightarrow \mathfrak{S}_{\{A,B,C,D\}} \simeq \mathfrak{S}_4.$$

Considérons M le milieu du segment $[AB]$ et soit r la réflexion selon la droite (AB) par rapport au plan (MCD). Alors r réalise la transposition $(A\ B)$ dans $\mathfrak{S}_{\{A,B,C,D\}}$ et $r \in \mathrm{Is}(\Delta_4)$.



Par symétrie des rôles de A, B, C et D, toutes les transpositions sont dans l'image de φ et par conséquent, φ est surjective et est donc un isomorphisme.

✌

Théorème 18 (Isométries et centre de symétrie)
Soit X une partie de $\mathbb{R}^3$ admettant un centre de symétrie O. Alors $\mathrm{Is}(X) \simeq \mathrm{Is}^+(X) \times \mathbb{Z}/2\mathbb{Z}$.

Théorème 19 (Isométries du cube)
Le groupe des isométries du cube C_6 est $\mathrm{Is}(C_6) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Questions possibles :
- Pourquoi la réflexion orthogonale par rapport au plan (MCD) est-elle une isométrie du tétraèdre ? (parce que (MCD) est un plan médiateur du tétraèdre)
- A-t-on $\mathrm{Is}(\Delta_4) \simeq \mathrm{Is}^+(\Delta_4) \times \mathbb{Z}/2\mathbb{Z}$? (non, car sinon $\mathfrak{S}_4$ aurait un sous-groupe distingué d'indice 2)
- Quel est le groupe d'isométries d'un triangle ?
- Peut-on avoir $\mathrm{Is}(X) = \mathrm{Is}^+(X) \neq \varnothing$? (oui, c'est un peu tordu)

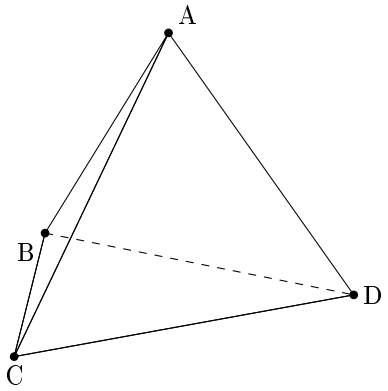
3.11.2 Isométries du tétraèdre et table des caractères de $\mathfrak{S}_4$

Leçons concernées. 101, 105, 108, 160, 161, 191.
Référence. *Nouvelles histoires hédonistes de groupes et géométrie, tome 2*, Philippe Caldero et Jérôme Germoni ou *Histoires hédonistes de groupes et géométrie, tome 1*, Philippe Caldero et Jérôme Germoni.
Remarques.

Définition 20 (Groupe d'isométries)
Soit $X \subset \mathbb{R}^3$. Le groupe des isométries de X est le sous-groupe $\mathrm{Is}(X)$ des isométries de l'espace affine euclidien $\mathbb{R}^3$ qui stabilisent X.

Théorème 21 (Isométries du tétraèdre.)
Le groupe des isométries du tétraèdre Δ_4 est $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4$.

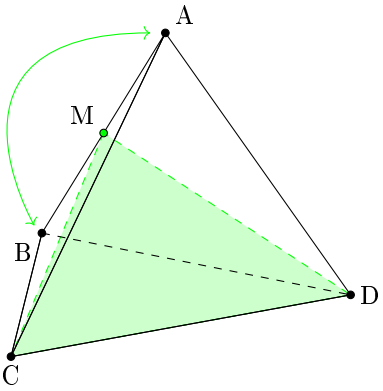
Preuve. Notons A, B, C, D les sommets du tétraèdre, comme dans la figure ci-dessous.



Les sommets du tétraèdre sont ses points extrémaux, donc le groupe $\mathrm{Is}(\Delta_4)$ agit par permutation sur l'ensemble $\{A, B, C, D\}$. Puisque (A, B, C, D) constitue une base affine de l'espace, on dispose donc d'une injection

$$\varphi : \mathrm{Is}(\Delta_4) \hookrightarrow \mathfrak{S}_{\{A,B,C,D\}} \simeq \mathfrak{S}_4.$$

Considérons M le milieu du segment $[AB]$ et soit r la réflexion selon la droite (AB) par rapport au plan (MCD). Alors r réalise la transposition $(A\ B)$ dans $\mathfrak{S}_{\{A,B,C,D\}}$ et $r \in \mathrm{Is}(\Delta_4)$.



Par symétrie des rôles de A, B, C et D, toutes les transpositions sont dans l'image de φ et par conséquent, φ est surjective et est donc un isomorphisme.

✌

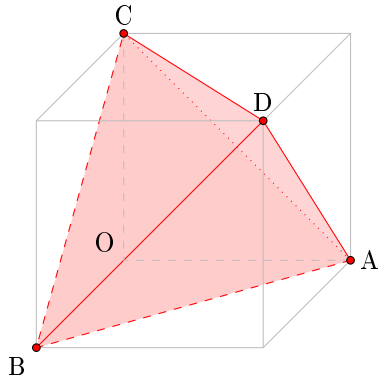
Théorème 22 (Table de caractères de $\mathfrak{S}_4$)
La table des caractères de $\mathfrak{S}_4$ est donnée par :

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_{Δ_4}	3	1	0	-1	-1
$\chi_{\Delta_4} \cdot \varepsilon$	3	-1	0	1	-1

Preuve. **Étape 1 :** (caractères de degré 1)
Les seuls caractères de degré 1 de $\mathfrak{S}_4$ sont les morphismes de $\mathfrak{S}_4$ dans $\mathbb{C}^*$, c'est-à-dire le morphisme trivial triv et la signature ε. On obtient donc le début de table

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1

Étape 2 : (une représentation par action sur le tétraèdre)
Fixons le tétraèdre inscrit dans le cube, en rouge dans la figure ci-dessous, de sorte que si O désigne l'origine de $\mathbb{R}^3$, les vecteurs $\overrightarrow{OA}, \overrightarrow{OB}$ et $\overrightarrow{OC}$ forment la base canonique de $\mathbb{R}^3$ en tant qu'espace vectoriel et que $\overrightarrow{OD}$ a pour coordonnées $(1,1,1)$.



Considérons la représentation $(\mathbb{R}^3, \rho)$ induite par l'isomorphisme $\mathfrak{S}_4 \simeq \mathrm{Is}(\Delta_4)$, dont on note χ_{Δ_4} le caractère.
Notons O' le barycentre des points A, B, C, D, de sorte que (O', A, B, C) forme une base affine de $\mathbb{R}^3$. Ainsi, si $\mathcal{B}$ est la base $(\overrightarrow{O'A}, \overrightarrow{O'B}, \overrightarrow{O'D})$, les matrices des $\rho(g)$ s'écrivent :

$$\mathscr{M}_{\mathcal{B}}(A\ B) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathscr{M}_{\mathcal{B}}(A\ B\ C) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathscr{M}_{\mathcal{B}}(A\ B\ C\ D) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix},$$

$$\mathscr{M}_{\mathcal{B}}(A\ B)(C\ D) = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}.$$

On en déduit donc le caractère χ_{Δ_4}, qui est bien irréductible puisque $\langle \chi_{\Delta_4}, \chi_{\Delta_4} \rangle = 1$, ce qui nous permet de continuer à remplire la table

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1
χ_{Δ_4}	3	1	0	-1	-1

Étape 3 : (multiplier par ε)
On remarque que si l'on considère le produit tensoriel entre la représentation standard et ε, on obtient une représentation dont le caractère est $\chi_{\Delta_4} \cdot \varepsilon$. Or,

$$\langle \chi_{\Delta_4} \cdot \varepsilon, \chi_{\Delta_4} \cdot \varepsilon \rangle = \frac{1}{|\mathfrak{S}_4|} \sum_{\sigma \in \mathfrak{S}_4} \chi_{\Delta_4}(\sigma) \cdot \varepsilon(\sigma) \overline{\chi_{\Delta_4}(\sigma) \cdot \varepsilon(\sigma)} = \frac{1}{|\mathfrak{S}_4|} \sum_{\sigma \in \mathfrak{S}_4} \chi_{\Delta_4}(\sigma) \overline{\chi_{\Delta_4}(\sigma)} = \langle \chi_{\Delta_4}, \chi_{\Delta_4} \rangle = 1,$$

donc $\chi_{\Delta_4} \cdot \varepsilon$ est un caractère irréductible, ce qui nous permet à nouveau de compléter notre table

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1
χ_{Δ_4}	3	1	0	-1	-1
$\chi_{\Delta_4} \cdot \varepsilon$	3	-1	0	1	-1

Enfin, on sait qu'il nous reste un dernier caractère à déterminer. Puisque la somme des carrés des dimension des caractères irréductibles est égale à l'ordre de $\mathfrak{S}_4$ (*i.e.* 24), le degré de ce dernier caractères est 2 et nous le nommerons donc χ_2. Comme précédemment, $\chi_2 \cdot \varepsilon$ est encore un caractère irréductible, nécessairement identique à χ_2 puisqu'il est lui aussi de degré égal à 2. Ainsi, on a $\chi_2(1\,2) = \chi(1\,2\,3\,4) = 0$, puisque la signature de ces éléments vaut -1. Notons pour le moment $a = \chi(1\,2\,3)$ et $b = \chi((1\,2)(3\,4))$. Les relations d'orthogonalité nous donnent

$$\langle \chi_2, \chi_{\Delta_4} \rangle = 0 = \frac{1}{24}(1 \cdot 2 \cdot 3 + 6 \cdot 0 \cdot 1 + 8 \cdot a \cdot 0 + 6 \cdot 0 \cdot (-1) + 3 \cdot b \cdot (-1)) = \frac{1}{24}(6 - 3b),$$

d'où l'on déduit que $b = 2$ et

$$\langle \chi_2, \mathrm{triv} \rangle = 0 = \frac{1}{24}(1 \cdot 2 \cdot 1 + 6 \cdot 0 \cdot 1 + 8 \cdot a \cdot 1 + 6 \cdot 0 \cdot 1 + 3 \cdot 2 \cdot 1) = \frac{1}{24}(2 + 8a + 6),$$

qui nous permet de conclure que $a = -1$. Finalement, on a bien la table annoncée.

✌

Questions possibles :

- Pourquoi la réflexion orthogonale par rapport au plan (MCD) est-elle une isométrie du tétraèdre ? (parce que (MCD) est un plan médiateur du tétraèdre)
- Quel est le groupe d'isométries d'un triangle ?
- Quelle est la table de caractères de $\mathfrak{S}_3$?
- Peut-on construire une représentation associée au caractère irréductible de dimension 2 ?

3.11.3 Sous-groupes distingués et table des caractères

Leçons concernées. 103, 104.
Référence. *Théorie des groupes*, Félix Ulmer.
Remarques. Au lieu d'appliquer le résultat à $\mathfrak{S}_4$ (ce qui n'est pas totalement inintéressant), on peut plutôt étudier les sous-groupes distingués du groupe diédral $\mathbb{D}_6$, ce qui est très fastidieux à faire à la main sinon. La construction de la table des caractères des groupes diédraux peut par exemple se trouver dans *Nouvelles histoires hédonistes de groupes et de géométries, tome 2.*

Dans la suite, on se place sur des $\mathbb{C}$-espaces vectoriels.

Définition 23 (Noyau d'un caractère)
Soit G un groupe fini et χ un caractère de G. On appelle noyau du caractère χ l'ensemble

$$\operatorname{Ker}\chi := \{g \in G \mid \chi(g) = \chi(\mathrm{id})\}.$$

Lemme 24 (Description du noyau d'un caractère) Soit G un groupe fini et (V, ρ) une représentation linéaire de G, de caractère χ. Pour tout $g \in G$,

i. $|\chi(g)| \leqslant \chi(\mathrm{id})$,
ii. $g \in \operatorname{Ker}\chi$ si et seulement si $g \in \operatorname{Ker}\rho$.

Preuve. Notons n la dimension de V.
Puisque $\rho(g)$ est annulé par $X^{|G|} - 1$, il est diagonalisable et ses valeurs propres $\lambda_1, \dots, \lambda_n$ (comptées avec multiplicités) sont des racines de l'unité. Par conséquent, $\chi(g) = \sum_{j=1}^{n} \lambda_j$ et donc

$$|\chi(g)| \leqslant \sum_{j=1}^{n} |\lambda_j| = n = \dim V = \chi(\mathrm{id})$$

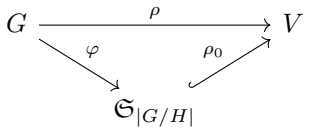
avec égalité si et seulement si toutes les valeurs propres λ_j sont égales (c'est le cas d'égalité de l'inégalité triangulaire). Ainsi, $\chi(g) = \chi(\mathrm{id})$ si et seulement si $\lambda_1 = \cdots = \lambda_n = 1$ si et seulement si $\rho(g) = \mathrm{Id}_V$.

Théorème 25 (Sous-groupes distingués et table des caractères)
Soit G un groupe fini admettant m classes de conjugaison et de caractères irréductibles $\chi_1, \dots, \chi_m$. Tout sous-groupe distingué H de G est de la forme

$$H = \bigcap_{j \in J} \mathrm{Ker}(\chi_j), \quad J \subset \{1, \dots, m\}.$$

Preuve. Le lemme 24 assure que pour $J \subset \{1, \dots, m\}$, $\bigcap_{j\in J} \mathrm{Ker}(\chi_j) = \bigcap_{j\in J} \mathrm{Ker}(\rho_j)$ est un sous-groupe distingué de G (où ρ_j est une représentation de caractère est χ_j).

Soit $H \lhd G$. Considérons l'action par translation à gauche de G sur G/H, de morphisme $\varphi : G \to \mathfrak{S}_{|G/H|}$. Considérons (V, ρ_0) la représentation par permutation de $S_{|G/H|}$ et (V, ρ) la représentation de G qui en résulte, de caractère χ :



On a $H = \mathrm{Ker}\,\varphi$ et donc d'après le lemme 24,

$$\mathrm{Ker}(\chi) = \mathrm{Ker}(\rho) = \mathrm{Ker}(\varphi) = H$$

Par conséquent, tout sous-groupe distingué est le noyau d'un caractère de G.

Soit maintenant $V = \bigoplus_{j=1}^{s} a_j V_j$ une décomposition de V en représentation irréductibles. On note ρ_j le morphisme associé à V_j et χ_j le caractère (irréductible) associé. Pour tout $g \in G$,

$$g \in \mathrm{Ker}\,\chi \text{ ssi } g \in \mathrm{Ker}\,\rho \text{ ssi } \forall j \in \{1, \dots, m\},\ g \in \mathrm{Ker}\,\rho_j \text{ ssi } g \in \bigcap_{j=1}^{s} \mathrm{Ker}\,\chi_j.$$

Par conséquent, $H = \bigcap_{j=1}^{s} \mathrm{Ker}\,\chi_j$.

Théorème 26 (Table de caractères de $\mathfrak{S}_4$)
La table des caractères de $\mathfrak{S}_4$ est donnée par :

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_{std}	3	1	0	-1	-1
$\chi_{\mathrm{std}} \cdot \varepsilon$	3	-1	0	1	-1

et ses sous groupes distingués sont donc $\mathfrak{S}_4$, $\mathfrak{A}_4$, $(\mathbb{Z}/2\mathbb{Z})^2$ le groupe des doubles transpositions et $\{\mathrm{id}\}$.

Preuve. **Étape 1 :** (caractères de degré 1)
Les seuls caractères de degré 1 de $\mathfrak{S}_4$ sont les morphismes de $\mathfrak{S}_4$ dans $\mathbb{C}^*$, c'est-à-dire le morphisme trivial triv et la signature ε. On obtient donc le début de table

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1

Étape 2 : (la représentation standard)
Considérons la représentation par permutation $\rho : \mathfrak{S}_4 \to \mathbb{C}^4$ de caractère χ. Elle se décompose en deux sous-représentation donnée par $H = \{x_1 + x_2 + x_3 + x_4 = 0\}$ et $\mathbb{C} \cdot (1,1,1,1) \cong$ triv.
Donc si χ_{std} désigne le caractère de H, on a $\chi = \chi_{\text{std}} + 1$. Puisque pour $\sigma \in \mathfrak{S}_4$, $\text{Tr}(\rho(\sigma))$ vaut le nombre de point fixes de σ, on en déduit la suite de la table

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1
χ_{std}	3	1	0	-1	-1

et χ_{std} est bien irréductible, puisque $\langle \chi_{\text{std}}, \chi_{\text{std}} \rangle = 1$.

Étape 3 : (multiplier par ε)
On remarque que si l'on considère le produit tensoriel entre la représentation standard et ε, on obtient une représentation dont le caractère est $\chi_{\text{std}} \cdot \varepsilon$. Or,

$$\langle \chi_{\text{std}} \cdot \varepsilon, \chi_{\text{std}} \cdot \varepsilon \rangle = \frac{1}{|\mathfrak{S}_4|} \sum_{\sigma \in \mathfrak{S}_4} \chi_{\text{std}}(\sigma) \cdot \varepsilon(\sigma) \overline{\chi_{\text{std}}(\sigma) \cdot \varepsilon(\sigma)} = \frac{1}{|\mathfrak{S}_4|} \sum_{\sigma \in \mathfrak{S}_4} \chi_{\text{std}}(\sigma) \overline{\chi_{\text{std}}(\sigma)} = \langle \chi_{\text{std}}, \chi_{\text{std}} \rangle = 1,$$

donc $\chi_{\text{std}} \cdot \varepsilon$ est un caractère irréductible, ce qui nous permet à nouveau de compléter notre table

	id [1]	(1 2) [6]	(1 2 3) [8]	(1 2 3 4) [6]	(1 2)(3 4) [3]
triv	1	1	1	1	1
ε	1	-1	1	-1	1
χ_{std}	3	1	0	-1	-1
$\chi_{\text{std}} \cdot \varepsilon$	3	-1	0	1	-1

Enfin, on sait qu'il nous reste un dernier caractère à déterminer. Puisque la somme des carrés des dimension des caractères irréductibles est égale à l'ordre de $\mathfrak{S}_4$ (*i.e.* 24), le degré de ce dernier caractères est 2 et nous le nommerons donc χ_2. Comme précédemment, $\chi_2 \cdot \varepsilon$ est encore un caractère irréductible, nécessairement identique à χ_2 puisqu'il est lui aussi de degré égal à 2. Ainsi, on a $\chi_2(1\,2) = \chi(1\,2\,3\,4) = 0$, puisque la signature de ces éléments vaut -1. Notons pour le moment $a = \chi(1\,2\,3)$ et $b = \chi((1\,2)(3\,4))$. Les relations d'orthogonalité nous donnent

$$\langle \chi_2, \chi_{\text{std}} \rangle = 0 = \frac{1}{24}(1 \cdot 2 \cdot 3 + 6 \cdot 0 \cdot 1 + 8 \cdot a \cdot 0 + 6 \cdot 0 \cdot (-1) + 3 \cdot b \cdot (-1)) = \frac{1}{24}(6 - 3b),$$

d'où l'on déduit que $b = 2$ et

$$\langle \chi_2, \varepsilon \rangle = 0 = \frac{1}{24}(1 \cdot 2 \cdot 1 + 6 \cdot 0 \cdot (-1) + 8 \cdot a \cdot 1 + 6 \cdot 0 \cdot 1 + 3 \cdot 2 \cdot 1) = \frac{1}{24}(2 + 8a + 6),$$

qui nous permet de conclure que $a = -1$. Finalement, on a bien la table annoncée, où il nous suffit de lire les sous-groupes distingués de $\mathfrak{S}_4$.

✌

Questions possibles :
- Y-a-t-il une autre manière de déterminer les sous-groupes distingués de $\mathfrak{S}_4$?
- Appliquer le résultat au groupe diédral D_6.
- Quels sont les groupes distingués de $\mathfrak{S}_n$ en général ?

3.12 Théorème de Sophie Germain

Leçons concernées. 120, 121, 126, 142.
Référence. *Oraux X-ENS, algèbre 1*, FGN.
Remarques. Le théorème de Sophie Germain est une version faible du théorème de Fermat-Wiles. La preuve peut sembler un peu sortir de nulle part, mais après l'avoir bien travaillée elle est finalement presque naturelle. On ramène l'équation $x^p + y^p + z^p = 0$ à une même équation modulo q, où l'on remarque qu'elle est bien plus simple.

Théorème 27 (Sophie Germain)
Soit p un nombre premier impair tel que $q = 2p + 1$ soit premier. Il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \neq 0 \mod p$ et $x^p + y^p + z^p = 0$.

Preuve. Raisonnons par l'absurde. Soit $(x, y, z) \in \mathbb{Z}^3$ tel que $x^p + y^p + z^p = 0$ et $xyz \neq 0 \mod p$. Notons $d := x \wedge y \wedge z$ et $t' := t/d$ pour $t = x, y, z$. Quitte à remplacer (x, y, z) par (x', y', z') on peut alors supposer que $d = 1$.
Alors, si p_0 est un diviseur premier commun de x et y, il advient que p_0 divise $z^p = -(x^p + y^p)$ et donc z, ce qui est impossible. Ainsi, $x \wedge y = 1$ et par symétrie des rôles, $x \wedge z = y \wedge z = 1$.

Montrons que les quantités $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont des puissances p-ième parfaites. On remarque tout d'abord que

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

Par conséquent, si p_0 était un diviseur commun de ces deux quantités, ce serait également un diviseur de x. En réduisant modulo p_0, on obtient alors $y = -z \mod p_0$ et donc

$$0 = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \sum_{k=0}^{p-1} y^{p-1} = py^{p-1} \mod p_0.$$

Par conséquent, p_0 divise p et donc par le lemme de Gauss, p_0 divise p ou y. Dans le premier cas, on aurait $p = p_0$ qui divise x, ce qui n'est pas le cas, donc p_0 divise y. Mais ceci contredit le fait que $x \wedge y = 1$.

Dès lors, $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux et donc puisque leur produit est $(-x)^p$, il existe bien $a, \alpha \in \mathbb{Z}$ tel que

$$y + z = a^p \quad \text{et} \quad \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p.$$

Par symétrie des rôles, on dipose également de $b, c \in \mathbb{Z}$ tel que $x + z = b^p$ et $y + z = c^p$.

Si $m \in \mathbb{Z}$ n'est pas divisible par q, alors $(m^p)^2 = m^{q-1} = 1 \mod q$. Puisque q est premier, le polynôme $X^2 - 1$ possède exactement deux racines dans $\mathbb{Z}/q\mathbb{Z}$ et donc $m^p = \pm 1 \mod q$. Ainsi, si aucun des entiers x, y, z n'est divisible par q, on a $t^p = \pm 1 \mod q$ pour $t = x, y, z$, ce qui implique que $0 = x^p + y^p + z^p$ vaut $\pm 1, \pm 3$ modulo q. Ceci est impossible puisque $q \geqslant 7$. Exactement l'un des trois entiers x, y, z est donc divisible par q, disons x.

Dès lors, $b^p + c^p - a^p = x + z + x + y - (y + z) = 2x = 0 \mod q$. De plus, $b^p = z \mod q$ et $a^p = y \mod q$. Puisque q ne divise ni y, ni z, on en déduit que $y, z = \pm 1 \mod q$. Si q ne divise pas a, on a de même $a^p = \pm 1 \mod q$ et alors $b^p + c^p - a^p \mod q$ vaut ± 1 ou ± 3 modulo q, ce qui est à nouveau impossible. Donc q divise a. Il en résulte que $y + z = a^p = 0 \mod q$, donc

$$\alpha^p = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = py^{p-1} = (\pm 1)^{p-1}p = p \mod q.$$

Ceci est absurde, puisque α^p devrait être congru à $0, 1$ ou -1 modulo q.

Questions possibles :

- Donner une idée de la résolution de l'équation $x^2 + y^2 = z^2$. Il s'agit de l'équation du théorème de Fermat-Wiles pour $n = 2$ et cette équation décrit les triplets Pythagoriciens. On peut aussi pousser la discussion pour au cas $n = 4$. Voir par exemple *Arithmétique* de Marc Hindry.
- Existe-t-il une infinité de nombre de Sophie Germain ? (on ne sait pas)
- Des exemples simples d'équation diophantienne à réduire modulo un nombre premier.

3.13 Théorème de structure des groupes abéliens finis

Leçons concernées. 102, 104, 120.
Référence. *Mathématiques pour l'agrégation, algèbre et géométrie*, Jean-Étienne Rombaldi.
Remarques. Résultat fondamental qu'il n'est pas inutile de savoir démontrer de toute façon ! Cette démonstration utilise la notion de caractère d'un groupe abélien, très liée au théorème de structure. Sur ce sujet, on peut par exemple consulter *L'algèbre discrète de la transformée de Fourier* de Gabriel Peyré, ou un exercice dans *Exercices de mathématiques pour l'agrégation : Algèbre 1* de Serge Francinou et Hervé Gianella. On peut également trouver une démonstration de la réciprocité quadratique utilisant assez minimalement les caractères dans *Théorie de Galois* d'Ivan Gozart.
Il est bon d'avoir en tête que ce résultat ce généralise aux groupes abéliens de type fini, ce qui peut se démontrer par la forme normale de Smith.
À noter que dans le développement, on ne démontre que l'existence de la décomposition.

Théorème 28 (Théorème de structure des groupes abéliens finis)
Soit G un groupe abélien fini non trivial. Il existe un unique entier $r \geqslant 1$ et d'uniques entiers naturels $n_1, \dots, n_r$ tels que $n_1 \mid \cdots \mid n_r$ et

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

Questions possibles :

- Quels sont les groupes abéliens d'ordre 360 ?
- Donner une idée de la preuve de l'unicité de la décomposition.
- Existe-t-il une généralisation de ce théorème ? (parler des groupes abéliens de *type* fini, mais peut-être aussi de la structure des modules de type fini sur un anneau euclidien/principal si l'on est à l'aise avec ça)
- Que peut-on dire d'un groupe dont tous les éléments sont d'ordre 2 ?

3.14 L'unique entier entre un carré et un cube

Leçons concernées. 122, 126, 142.
Référence. *131 Développements pour l'oral* , D. Lesesvre, P. Montagnon, P. Le Barbenchon & T. Pierron .
Remarques. Un très joli développement qui se fait très naturellement après l'avoir un peu travaillé et qui donne un très bel exemple de résolution d'une équation diophantienne.

Théorème 29 (Une équation diophantienne)
Les solutions de l'équation

$$x^2 + 2 = y^3, \quad x, y \in \mathbb{Z}$$

sont $(-5, 3)$ et $(5, 3)$.

Questions possibles :

- Pourquoi cette équation nous donne-t-elle l'unique entier précédé d'un carré et suivi d'un cube ?
- Sans doute des questions sur les anneaux de la forme $\mathbb{Z}[\sqrt{d}]$ et $\mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$.

3.15 Une version faible du théorème de Bézout

Leçons concernées. 144, 152, 191.
Référence. *Mathématiques pour l'agrégation, Algèbre et Géométrie*, Jean-Étienne Rombaldi.
Remarques. Il faut bien travailler l'étape 2 qui est un peu difficile à bien expliquer et à comprendre du premier coup à mon avis. L'étape 3 ne se trouve que partiellement dans le Rombaldi, mais les calculs ne sont pas très difficiles à mener une fois que l'on a compris l'idée.

On se donne deux polynômes $P, Q \in \mathbb{C}[X][Y]$, notés

$$P(X,Y) = \sum_{k=0}^{n} a_k(X)Y^k \quad \text{et} \quad Q(X,Y) = \sum_{k=0}^{m} b_k(X)Y^k,$$

où les $a_k, b_k \in \mathbb{C}[X]$ et $a_n, b_m \neq 0$. On s'intéresse au nombre de solutions dans $\mathbb{C}^2$ du système

$$\begin{cases} P(x,y) = 0 \\ Q(x,y) = 0. \end{cases} \tag{★}$$

Plus précisément, on va montrer la version faible du théorème de Bézout suivante.

Théorème 30 (Bézout, version faible)
Si P et Q sont premiers entre eux dans $\mathbb{C}(X)[Y]$ et si les polynômes $a_0, \dots, a_n, b_0, \dots, b_m$ n'ont aucune racine commune dans $\mathbb{C}$, alors le système (★) admet au plus $\deg(P)\deg(Q)$ solutions.

Preuve. **Étape 1 :** Montrons tout d'abord que le système (★) n'admet qu'un nombre fini de solutions.

On suppose que le système (★) admet au moins une solution.

Puisque P et Q sont premiers entre eux, leur résultant $R(X) := \mathrm{Res}_Y(P(X,Y), Q(X,Y))$ par rapport à Y est non nul. De plus, si (λ, μ) est une solution du système (★), alors λ est une racine de $R(X)$ et λ peut donc prendre un nombre fini de valeurs dans $\mathbb{C}$.

Les polynômes $a_0, \dots, a_n, b_0, \dots, b_m$ sont premiers entre eux dans $\mathbb{C}[X]$ dans leur ensemble et le théorème de Bézout nous indique qu'il existe $u_0, \dots, u_n, v_0, \dots, v_m \in \mathbb{C}[X]$ tels que

$$u_0a_0 + \cdots + u_na_n + v_0b_0 + \cdots + v_mb_m = 1.$$

Donc si (λ, μ) est une solution de (★), on a l'un des $a_i(\lambda) \neq 0$ ou l'un des $b_j(\lambda) \neq 0$ et donc $P(\lambda, Y) \neq 0$ ou $Q(\lambda, Y) \neq 0$. Puisque μ est racine de ces deux polynômes, il n'y a qu'un nombre fini de valeurs possibles pour $\mu \in \mathbb{C}$ à λ fixé, ce qui achève la preuve.

Étape 2 : On se ramène à un système équivalent à (★), où les degrés de P et Q dans $\mathbb{C}[X,Y]$ sont égaux à leurs degrés dans $\mathbb{C}(X)[Y]$.

Soit $\lambda \in \mathbb{C}$fixé quelconque. On effectue le changement de variable $X = T + \lambda Y, Y = Y$ et on note $\tilde{P}(T,Y) = P(T + \lambda Y, Y)$ et $\tilde{Q}(T,Y) = Q(T + \lambda Y, Y)$. Notons alors

$$P(X,Y) = \sum_{k=0}^{p} P_k(X,Y),$$

où $p = \deg P$ et $P_k \in \mathbb{C}[X,Y]$ est un polynôme homogène de degré k. Notons $P_p := \sum_{i=0}^{n} \alpha_i X^i Y^{n-i}$.

Dans $\mathbb{C}[T,Y]$, le terme en Y^n de $\tilde{P}(T,Y)$ égal au terme de degré n de $\tilde{P}(0,Y) = P(\lambda Y, Y)$, qui est donc $P_p(\lambda Y, Y) = \left(\sum_{i=0}^{n} \alpha_i \lambda^i\right) Y^n$. Au moins l'un des α_i est non nul, donc excepté pour un nombre fini de valeurs de λ, le terme en Y^n de $\tilde{P}(T,Y)$ est non nul, si bien que $\deg_Y \tilde{P} = \deg \tilde{P}$. On a le même

résultat pour Q et donc, excepté pour un nombre fini de valeurs de $\lambda \in \mathbb{C}$, on a $\deg_Y \tilde{P} = \deg \tilde{P}$ et $\deg_Y \tilde{Q} = \deg \tilde{Q}$ simultanément.

Étape 3 : On montre que dans le cadre de l'étape 2, on peut borner efficacement le degré du résultat de P et Q.

Lemme 31 On suppose que les degrés de P et Q dans $\mathbb{C}[X,Y]$ sont égaux à leurs degrés dans $\mathbb{C}(X)[Y]$. Le polynôme $R(X) := \mathrm{Res}_Y(P(X,Y), Q(X,Y)) \in \mathbb{C}[X]$ est de degré au plus $\deg_{X,Y}(P) \cdot \deg_{X,Y}(Q)$.

Preuve. (du lemme 31).
Si P et Q ne sont pas premiers entre eux, alors R est nul. Sinon, $R \neq 0$.

De plus, les écritures $P = \sum_{k=0}^{n} a_k(X)Y^k$ et $Q = \sum_{k=0}^{m} b_k(X)Y^k$ nous indiquent que $\deg(a_k) \leqslant n-k$ et $\deg(b_k) \leqslant m-k$. Par conséquent, si l'on écrit la matrice de Sylvester en Y,

$$S = (S_{ij})_{1\leqslant i,j\leqslant n+m} = \begin{pmatrix} a_0 & & & b_0 & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & a_0 & b_m & & \ddots & \\ a_n & & \vdots & & \ddots & & b_0 \\ & \ddots & \vdots & & & \ddots & \vdots \\ & & a_n & & & & b_m \end{pmatrix},$$

on observe que

$$S_{ij} = \begin{cases} a_{i-j} & \text{si} \quad j \leqslant m \quad \text{et} \quad 0 \leqslant i-j \leqslant n, \\ b_{i-(j-m)} & \text{si} \quad j > m \quad \text{et} \quad 0 \leqslant i-(j-m) \leqslant m, \\ 0 & \text{sinon.} \end{cases}$$

Or,

$$R(X) = \det S = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{m+n} S_{\sigma(j)j}.$$

Et pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\begin{aligned} \deg\left(\prod_{j=1}^{m+n} S_{\sigma(j)j}\right) &\leqslant \sum_{j=1}^{m}(n-(\sigma(j)-j)) + \sum_{j=m+1}^{m+n}(m-(\sigma(j)-j+m)) \\ &= m\cdot n + \sum_{j=1}^{m+n}(\sigma(j)-j) = m\cdot n. \end{aligned}$$

Par conséquént, $R(X) = \det(S(P(X,Y), Q(X,Y)))$ est de degré au plus $n \cdot m$.

✌

Étape 4 :

Nous voilà finalement armés pour démontrer le théorème de Bézout, ou du moins sa version faible. Le système (★) admet un nombre fini de solutions notées $(x_1,y_1),\ldots,(x_r,y_r) \in \mathbb{C}^2$.

En outre, excepté pour un nombre fini de $\lambda \in \mathbb{C}$, les polynômes $P_1(T,Y) := P(T+\lambda Y, Y)$ et $Q_1(T,Y) := Q(T+\lambda Y, Y)$ sont de degré total égal à leur degré en Y. Le nombre d'éléments $\lambda \in \mathbb{C}$ pour lesquels il existe deux indices $i \neq j$ tels que $x_i - \lambda y_i = x_j - \lambda x_j$ étant fini (ceci implique que $\lambda = 0$ ou $x_i \neq x_j$ et $\lambda = \frac{y_j - y_i}{x_j - x_i}$), il existe une infinité de valeurs de λ pour lesquelles les polynômes P_1 et Q_1 sont de degré total égal à leur degré en Y et les $t_i := x_i - \lambda x_i$ sont deux à deux distincts. En outre, on a

$$\tilde{P}(t_i, y_i) = P(t_i - \lambda y_i, y_i) = P(x_i, y_i) = 0 = Q(x_i, y_i) = \tilde{Q}(t_i, y_i).$$

Donc les t_i sont tous racines de $R(T) = \mathrm{Res}_Y(\tilde{P}(T,Y), \tilde{Q}(T,Y))$ et puisque R est de degré au plus $\deg_{X,Y}(P) \cdot \deg_{x,Y}(Q)$, on obtient finalement que $r \leqslant \deg_{X,Y}(P) \cdot \deg_{X,Y}(Q)$.

✌

Questions possibles :

— Pourquoi se place-t-on sur $\mathbb{C}(X)[Y]$ pour le résultant et pas sur $\mathbb{C}[X][Y]$? Dans le Rombaldi, il se place sur un anneau de polynômes à coefficients dans un corps et non dans un anneau, ça permet de ne pas se poser de question sortant du cadre de l'algèbre linéaire usuelle (hors modules) mais ça encombre parfois les preuves pour rien.

— Déterminer les solutions du système

$$\begin{cases} Y^2 - X(X-2)(X+1) = 0 \\ Y^2 + X^2 - 2X = 0 \end{cases}.$$

On trouve $(0,0), (2,0)$ et $(-2, \pm 2i\sqrt{2})$.

— Existe-t-il un cadre dans lequel on a égalité du nombre de solutions et du produit des degrés ? (voir le vrai théorème de Bézout, qui nécessite bien plus de géométrie algébrique)

4 Développements mixtes

4.1 Cartan - Von Neumann

Leçons concernées. 106, 156, 206, 214.
Référence. *Analyse sur les groupes de Lie : une introduction*, Jacques Faraut.
Remarques. Ce développement peut trouver sa place à la fois en algèbre et en analyse. Il faut être au clair sur la notion de sous-variétés. Le théorème d'inversion locale est utilisé explicitement et implicitement (dès que l'on parle de sous-variété).
Le thème sous-jacent de ce développement est celui des groupes de Lie, mais il n'est pas nécessaire d'en parler, même si le jury ne sera sans doute pas dupe. Il est à noter que l'espace $\mathfrak{g}$ est l'espace tangent associé à la variété G en I_n, il est facile à calculer pour des groupes tels que $O_n(\mathbb{R})$ ou $\mathrm{SL}_n(\mathbb{R})$.
Ce développement existe dans plusieurs références, notamment *Analyse pour l'agrégation de mathématiques, 40 développements* de Bernis[2], ainsi que dans *NH2G2, tome 2* de Caldero et Germoni, mais je préfère la version de Faraut.

Lemme 32 (Espace tangent d'un groupe fermé) Soit G un sous-groupe fermé de $\mathrm{GL}_n(R)$. L'ensemble

$$\mathfrak{g} = \{X \in \mathcal{M}_n(\mathbb{R}) \mid \forall t \in \mathbb{R}, \exp(tX) \in G\}$$

est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$.

Preuve. Il est clair que $\mathfrak{g}$ est un sous ensemble de $M_n(\mathbb{R})$ stable par multiplication par un scalaire et contenant la matrice nulle. Reste à montrer qu'il est stable par somme. Soit donc $A, B \in \mathfrak{g}$. Pour tout réel t, on sait que

$$\exp(t(A+B)) = \lim_{p \to +\infty} \exp(\frac{t}{p}A)^p \exp(\frac{t}{p}B)^p.$$

Or, par définition de $\mathfrak{g}$ et puisque G est un groupe, pour tout $n \geqslant 1$, $\exp(\frac{t}{p}A)^p \exp(\frac{t}{p}B)^p \in G$. Donc, G étant fermé, $\exp(t(A+B)) \in G$. Par conséquent, $A + B \in \mathfrak{g}$.

✌

Théorème 33 (Cartan et Von Neumann)
Tout sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$ est une sous-variété de $\mathcal{M}_n(\mathbb{R})$.

Preuve. Soit G un sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$ et $\mathfrak{g}$ l'espace vectoriel introduit au lemme 32. Pour montrer que G est une sous-variété, nous allons montrer que pour tout point $g \in G$, il existe un voisinage U de 0 dans $\mathfrak{g}$, un voisinnage V de g dans $\mathcal{M}_n(\mathbb{R})$ et un $\mathcal{C}^1$-difféomorphisme $\varphi : U \to V$ tel que

$$\varphi(U \cap \mathfrak{g}) = V \cap G.$$

Tâchons tout d'abord de le montrer au point $g = I_n$, avec le difféomorphisme $\varphi = \exp$. Nous allons avoir besoin du lemme suivant.

> **Lemme 34** (Le supplémentaire à la rescousse) Soit $\mathfrak{m}$ un sous-espace vectoriel supplémentaire de $\mathfrak{g}$ dans $\mathcal{M}_n(\mathbb{R})$. Il existe un voisinnage U de 0 dans $\mathfrak{m}$ tel que $\exp U \cap G = \{I_n\}$.

Preuve. (du lemme 34) On raisonne par l'absurde et on suppose qu'il existe une suite $(X_p)_{p\in\mathbb{N}}$ d'éléments de $\mathfrak{m}$ tendant vers 0 telle que si $g_p := \exp X_p$, alors $g_p \neq I_n$ et $g_p \in G$.
La suite $(X_p/\|X_p\|)_{p\in\mathbb{N}}$ est bien définie et est bornée, donc quitte à en extraire une sous-suite, elle converge vers un point $Y \in \mathfrak{m}$. Montrons que $Y \in \mathfrak{g}$. On concluera que $Y \in \mathfrak{m} \cap \mathfrak{g} = 0$, ce qui est impossible puisqu'il est de norme égale à 1.
Soit donc un réel t. Considérons la suite définie par $\lambda_p = \frac{t}{\|X_p\|}$, de sorte que par continuité de l'exponentielle,

$$\exp(tY) = \lim_{p\to+\infty} \exp(\lambda_p X_p).$$

Or, pour tout entier naturel p, on observe que

$$\exp(\lambda_p X_p) = \exp(\lfloor\lambda_p\rfloor X_p + (\lambda_p - \lfloor\lambda_p\rfloor)X_p) = \underbrace{\exp(X_p)^{\lfloor\lambda_p\rfloor}}_{\in G} \cdot \exp((\lambda_p - \lfloor\lambda_p\rfloor)X_p).$$

Puisque $|\lambda_p - \lfloor\lambda_p\rfloor| \leqslant 1$, on sait que $\lim_{p\to+\infty}(\lambda_p - \lfloor\lambda_p\rfloor)X_p = 0$ et donc, à nouveau par fermeture de G, on obtient que $\exp(tY) \in G$. Par suite, $Y \in \mathfrak{g}$, ce qui est contradictoire.

✌

Forts de ce lemme, tâchons de conclure. Considérons l'application

$$\psi : \begin{cases} \mathfrak{g} \times \mathfrak{m} & \longrightarrow \mathrm{GL}_n(\mathbb{R}) \\ (A, B) & \longmapsto \exp A \exp B \end{cases}$$

qui est de classe $\mathcal{C}^1$ et de différentielle en $(0,0)$ inversible. D'après le théorème d'inversion locale, il existe donc un voisinage U de 0 dans $\mathfrak{g}$, un voisinage V de 0 dans $\mathfrak{m}$ et un voisinage W de I_n dans $\mathrm{GL}_n(\mathbb{R})$ tel que ψ réalise un $\mathcal{C}^1$-difféomorphisme de $U \times V$ dans W.
D'après le lemme 34, quitte à réduire V, on peut supposer que $\exp V \cap G = \{I_n\}$. On sait que $\exp U = \psi(U \times 0) \subset W \cap G$, montrons l'égalité. Soit $g \in W \cap G$. Il existe des matrices $(A, B) \in \mathfrak{g} \times \mathfrak{m}$ telles que $g = \exp A \exp B$. Il en résulte que

$$\exp B = \exp(-A)g \in V \cap G = \{I_n\}$$

et donc $g = \exp(A) \in \exp U$. Par conséquent, exp réalise un $\mathcal{C}^1$-difféomorphisme de U dans $W \cap G$.
Si maintenant g est un élément quelconque de G, l'application $L(g) : h \in G \mapsto hg \in G$ est un C^1-difféomorphisme et $L(g) \circ \exp$ réalise donc un $\mathcal{C}^1$-difféomorphisme de U dans $gW \cap G$, ce qui conclue la démonstration.

✌

Questions possibles :

- Que vaut $\mathfrak{g}$ pour $G = \mathrm{SO}_n(\mathbb{R})$, $\mathrm{SL}_n(\mathbb{R})$?
- Montrer "à la main" que $O_n(\mathbb{R})$ est une sous-variété.
- Montrer que $GL_n(\mathbb{C})$ peut être vu comme une sous-variété.
- À quoi servent les groupes de Lie ? (notamment à établir des isomorphismes exceptionnels, à ce sujet voir la fin de la très bonne vidéo de Philippe Caldero où ce qu'il y a dans *NH2G2, tome 2*)

4.2 Convergence des méthodes itératives hermitiennes

Leçons concernées. 158, 162, 226.
Référence. *Analyse numérique matricielle*, Amodei et Dedieu.
Remarques. Les calculs font un peu peur au début, mais après quelques essais on prend le coup et ils font sens. Le seul hic est que le développement ne fait pas de très grandes maths, le coeur de la preuve est en quelque sort caché dans la caractérisation de la convergence par le rayon de convergence (qui résulte en gros du théorème de Gelfand).

Théorème 35
Soit $A \in H_n(\mathbb{C}) \cap \mathrm{GL}_n(\mathbb{C})$ et $M \in \mathrm{GL}_n(\mathbb{C})$ et $N \in \mathcal{M}_n(\mathbb{C})$ telles que $A = M - N$. Soit $b \in \mathbb{C}^n$ et $x_0 \in \mathbb{C}^n$. Alors la suite $(x_k)_{k\in\mathbb{N}}$ définie par

$$\forall k \in \mathbb{N}, \quad x_{k+1} = M^{-1}Nx_k + M^{-1}b$$

converge vers une solution de $Ax = b$ si et seulement si $M^* + N \in H_n^{++}(\mathbb{C})$.

Corollaire 36 Soit $A \in H_n^{++}(\mathbb{C})$. La méthode de relaxation associée à A converge pour $\omega \in]0, 2[$.

Questions possibles :
- Dans quel contexte utilise-t-on les méthodes itératives plutôt que des méthodes exactes pour résoudre des systèmes linéaires ?
- Résoudre à la main un système linéaire.
- Donner l'idée de la preuve de la caractérisation de la convergence des méthodes itératives par le rayon de convergence.

5 Développements d'analyse

5.1 Abel et Tauber faible

Leçons concernées. 230, 241, 243.
Référence. *Analyse pour l'agrégation de mathématiques, 40 développements*, Laurent et Julien Bernis ou *Analyse*, Xavier Gourdon.
Remarques. Il est peut-être un peu alambiqué d'utiliser le premier théorème pour calculer une série du type $\sum \frac{(-1)^n}{n}$ ou $\sum \frac{(-1)^n}{2n+1}$, comme indiqué dans le rapport du jury 2022 de la leçon 243. Bernis[2] donne une autre application qui n'est pas forcément beaucoup plus satisfaisante. Comme indiqué dans le rapport du jury, les théorèmes abéliens permettent de montrer qu'une certaine méthode de sommation coïncide avec une autre. L'exemple le plus simple de théorème "abélien" est le théorème de Césaro. Dans le cadre de ce développement, ce sont la sommation dite d'Abel et la sommation classique qui sont en jeu. Il est à noter que la sommation d'Abel (limite en angulaire en 1 de la série entière associée à la suite) permet notamment de donner un sens à la série $1 - 2 + 3 - 4 + 5 - \cdots$ ce que ne permet pas la sommation classique. Il ne me semble pas forcément pertinent de le mettre dans une leçon, mais ce n'est peut-être pas ridicule de l'avoir dans un coin de sa tête le jour de l'oral.
Tout cela est plus ou moins tiré de l'article wikipédia sur les théorèmes abéliens et taubériens (à prendre avec des pincettes, donc).

Théorème 37 (Abel angulaire)
Soit $\sum_{n=0}^{+\infty} a_n z^n$ une série entière de rayon de convergence $\geqslant 1$, dont on note f la somme. Soit $\theta_0 \in [0, \pi/2[$, on note

$$\mathcal{A} := D(0,1) \cap \{1 - \rho\exp(i\theta) \mid \rho > 0, |\theta| \leqslant \theta_0\}.$$

Si $\sum_{n=0}^{+\infty} a_n$ converge, alors $\lim_{z\to 1, z\in\mathcal{A}} f(z) = \sum_{n=0}^{+\infty} a_n$.

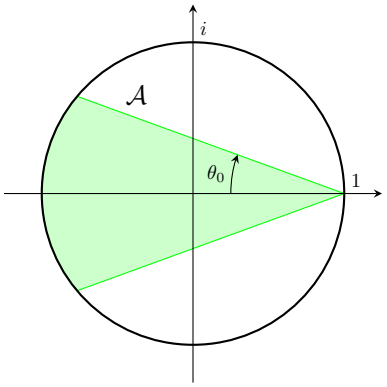


FIGURE 1 – Secteur angulaire $\mathcal{A}$.

Preuve. Notons S la somme de la série $\sum_{n=0}^{+\infty} a_n$, ainsi que S_n ses sommes partielles et R_n ses restes pour $n \in \mathbb{N}$, de sorte que $S_n = S - R_n$.
Soit $n \in \mathbb{N}^*$ et $|z| < 1$.

$$\begin{aligned}
\sum_{k=0}^{n} a_k z^k - S_n &= \sum_{k=1}^{n} a_k (z^k - 1) \\
&= \sum_{k=1}^{n} (R_{k-1} - R_k)(z^k - 1) \\
&= \sum_{k=0}^{n-1} R_k (z^{k+1} - 1) - \sum_{k=0}^{n} R_k (z^k - 1) \\
&= \sum_{k=0}^{n} R_k (z^{k+1} - z^k) - R_n(z^{n+1} - 1) = (z-1)\sum_{k=0}^{n} R_k z^k - \underbrace{R_n(z^{n+1} - 1)}_{\underset{n\to+\infty}{\longrightarrow} 0}
\end{aligned}$$

Ainsi, lorsque n tend vers $+\infty$, on obtient l'identité $f(z) - S = (z-1)\sum_{k=0}^{+\infty} R_k z^k$. Dès lors, pour tout

$n_0 \in \mathbb{N}$,

$$\begin{aligned}|f(z)-S| &\leqslant |z-1|\sum_{k=0}^{n_0}|R_k z^k| + |z-1|\sum_{k=n_0+1}^{+\infty}|R_k z^k| \\ &\leqslant |z-1|\sum_{k=0}^{n_0}|R_k| + \left(\sup_{k>n_0}|R_k|\right)\frac{|z-1|}{1-|z|}\end{aligned}$$

Donc si l'on fixe $\varepsilon > 0$, pour n_0 suffisamment grand, on a $\sup_{k>n_0}|R_k| < \varepsilon$ et donc en posant $M := \sum_{k=0}^{n_0}|R_k|$, on a

$$|f(z)-S| \leqslant |z-1|M + \varepsilon\frac{|z-1|}{1-|z|}.$$

Maintenant, si $z \in \mathcal{A}$, on pose $z = 1-\rho e^{i\theta}$, avec $\rho > 0$ et $|\theta| < \theta_0$. De sorte que

$$\frac{|z-1|}{1-|z|} = \frac{\rho(1+|z|)}{1-|z|^2} = \frac{\rho(1+|z|)}{2\rho\cos(\theta)-\rho^2} \leqslant \frac{2}{2\cos(\theta)-\rho},$$

et donc si $\rho = |1-z| < \cos(\theta_0)$ (ce qui est possible car $0 \leqslant \theta_0 < \pi/2$), par décroissance de cos on obtient

$$\frac{|z-1|}{1-|z|} \leqslant \frac{2}{2\cos(\theta_0)-\cos(\theta_0)} \leqslant \frac{2}{\cos(\theta_0)}.$$

Finalement, il advient donc que

$$\overline{\lim_{z\to 1, z\in\mathcal{A}}}|f(z)-S| \leqslant \frac{2\varepsilon}{\cos(\theta_0)},$$

et puisque $\varepsilon > 0$ était quelconque, on conclue donc bien que $\lim_{z\to 1, z\in\mathcal{A}}|f(z)-S| = 0$.

On démontre ensuite une réciproque partiel du théorème d'Abel angulaire.

Théorème 38 (Tauber faible)
Soit $\sum_{n=0}^{+\infty} a_n z^n$ une série entière de rayon de convergence égal à 1, dont on note f la somme.
On suppose qu'il existe un complexe S tel que $\lim_{x\to 1^-} f(x) = S$.
Si $a_n = o(1/n)$, alors la série de terme général a_n converge et $S = \sum_{n=0}^{+\infty} a_n$.

Preuve. On note S_n les sommes partielles de la série de terme général a_n. Pour tout $0 < x < 1$ et $n \in \mathbb{N}^*$,

$$\begin{aligned}|S_n - f(x)| &\leqslant \sum_{k=0}^{n}|a_k(1-x^k)| + \sum_{k>n}|a_k x^k| \\ &\leqslant \sum_{k=0}^{n}|ka_k(1-x)| + \sum_{k>n}\frac{k}{n}|a_k|x^k \\ &\leqslant (1-x)\sum_{k=0}^{n}k|a_k| + \frac{1}{n}\sup_{k>n}(k|a_k|)\sum_{k>n}x^k \leqslant (1-x)\sum_{k=0}^{n}k|a_k| + \frac{1}{n(1-x)}\sup_{k>n}(k|a_k|).\end{aligned}$$

Ainsi, si $x = 1 - \frac{1}{n}$, on obtient $|S_n - f(1-\frac{1}{n})| \leqslant \frac{1}{n}\sum_{k=0}^{n} k|a_k| + \sup_{k>n}(k|a_k|)$. Le théorème de Césaro nous indique alors que $\frac{1}{n}\sum_{k=0}^{n} k|a_k|$ tend vers 0 lorsque $n \to +\infty$, donc

$$|S_n - S| \leqslant |S_n - f(1-\frac{1}{n})| + |f(1-\frac{1}{n}) - S| \underset{n\to+\infty}{\longrightarrow} 0.$$

✌

Questions possibles :
- Démontrer le théorème de Césaro ? (on ne sait jamais...)
- Que peut-on dire en général du comportement d'une série entière sur le bord de son disque de convergence ? Illustrer par des exemples.

5.2 Banach-Alaoglu

Leçons concernées. 203, 205, 208, 213, 219, 229, 253.
Référence. *Analyse pour l'agrégation de mathématiques*, Julien et Laurent Bernis ou *Éléments d'analyse fonctionnelle*, Francis Hirsch et Gilles Lacombe.
Remarques. Il est bon de savoir s'aventurer un peu en topologie faible et faible-$*$, au moins culturellement. Notamment, le premier théorème reste vérifié sans hypothèse de séparabilité et découle assez vite du théorème de Tychonov (qui est bien sûr très loin de l'agrégation). Le second théorème indique que les fermés bornés pour la topologie faible vérifient la propriété de Bolzano-Weierstrass. Ils sont donc compacts dès lors qu'ils sont métrisables, ce qui est le cas lorsque le dual de H est séparable, c'est-à-dire lorsque H est séparable.
La proposition 41 est noramment utile pour résoudre des équations aux dérivées partielles sur les Sobolev. Mais ce n'est sans doute pas nécessaire de s'aventurer là-dedans pour faire ce développement, juste de l'avoir dans un coin de sa tête.

Théorème 39 (Théorème de Banach-Alaoglu, version evn)
Soit $(E, ||\cdot||)$ un espace vectoriel normé séparable et $(T_n)_{n\in\mathbb{N}}$ une suite bornée de formes linéaires continues sur E. Il existe une extractrice $\varphi : \mathbb{N} \to \mathbb{N}$ et une forme linéaire continue T telle la suite $(T_{\varphi(n)})_{n\in\mathbb{N}}$ converge simplement vers T.

Preuve. L'espace E étant spérable, on dispose d'une suite dense $(x_k)_{k\in\mathbb{N}}$ d'éléments de E. Dans la suite, on notera $M := \sup_{n\in\mathbb{N}} || T_n ||< +\infty$.

La suite $(T_n(x_0))_{n\in\mathbb{N}}$ est une suite réelle bornée (par $M\|x_0\|$), on dispose donc d'une extractrice $\varphi_0 : \mathbb{N} \to \mathbb{N}$ telle que la suite $(T_{\varphi_0(n)}(x_0))_{n\in\mathbb{N}}$ converge vers un réel que l'on notera $T(x_0)$.
De même, la suite $(T_{\varphi_0(n)}(x_1))_{n\in\mathbb{N}}$ est réelle bornée, donc on dispose de $\varphi_1 : \mathbb{N} \to \mathbb{N}$ telle que $(T_{\varphi_0\circ\varphi_1(n)}(x_1))_{n\in\mathbb{N}}$ converge vers un réel noté $T(x_1)$.
Par récurrence, pour tout $k \in \mathbb{N}$, on construit une extractrice $\varphi_k : \mathbb{N} \to \mathbb{N}$ telle que la suite $(T_{\varphi_0\circ\cdots\circ\varphi_k(n)}(x_k))_{n\in\mathbb{N}}$ converge vers un réel noté $T(x_k)$. Notons alors $\varphi : \mathbb{N} \to \mathbb{N}$ l'extractrice définie par $\varphi(n) = \varphi_0 \circ \cdots \circ \varphi_n(n)$.
Pour $k \in \mathbb{N}$ fixé, la suite $T_{\varphi(n)(x_k)}$ est alors une suite extraite de $(T_{\varphi_0\circ\cdots\circ\varphi_k(n)}(x_k))_{n\in\mathbb{N}}$ (à partir d'un certain rang) et converge donc vers $T(x_k)$.

Soit maintenant $x \in E$. Il s'agit de montrer que la suite $(T_{\varphi(n)}(x))_{n\in\mathbb{N}}$ est de Cauchy. Soit $\varepsilon > 0$ fixé quelconque. Il existe un indice k_0 tel que $\|x - x_{k_0}\| < \varepsilon$. Dès lors, si $p, q \in \mathbb{N}$, on a

$$\begin{aligned}|T_{\varphi(q)}(x) - T_{\varphi(p)}(x)| &\leqslant |T_{\varphi(q)}(x - x_{k_0})| + |T_{\varphi(q)}(x_{k_0}) - T_{\varphi(p)}(x_{k_0})| + |T_{\varphi(p)}(x - x_{k_0})| \\ &\leqslant M\|x - x_{k_0}\| + |T_{\varphi(q)}(x_{k_0}) - T_{\varphi(p)}(x_{k_0})| + M\|x - x_{k_0}\| \\ &\leqslant 2M\varepsilon + |T_{\varphi(q)}(x_{k_0}) - T_{\varphi(p)}(x_{k_0})|\end{aligned}$$

La suite $(T_{\varphi(n)}(x_{k_0}))_{n\in\mathbb{N}}$ étant convergeante et donc de Cauchy et ε étant quelconque, il en va de même pour la suite $(T_{\varphi(n)}(x))_{n\in\mathbb{N}}$. Elle converge donc vers un réel que l'on notera $T(x)$.
L'application $T : E \to \mathbb{R}$ ainsi définie est linéaire comme limite simple d'applications linéaires et continue puisque pour tout $n \in \mathbb{N}$ et $x \in E$, $|T_{\varphi(n)}(x)| \leqslant M\|x\|$ et donc par passage à la limite, $|T(x)| \leqslant M\|x\|$.

Théorème 40 (Banach-Alaoglu, version Hilbert)
Soit $(H, \langle\cdot,\cdot\rangle)$ un Hilbert et $(x_n)_{n\in\mathbb{N}}$ une suite bornée dans H. La suite $(x_n)_{n\in\mathbb{N}}$ admet une sous-suite faiblement convergente.

Preuve. Considérons $V = \overline{\text{Vect}\{x_n \mid n \in \mathbb{N}\}} \subset H$ qui est un Hilbert, puisque fermé dans H. Si l'on note $T_n := \langle x_n, \cdot\rangle$, alors d'après le théorème de Banach-Alaoglu version evn, il existe une extractrice $\varphi : \mathbb{N} \to \mathbb{N}$ telle que $(T_{\varphi}(n)_{|V})_{n\in\mathbb{N}}$ converge simplement vers une application linéaire continue T sur V. Or, d'après le théorème de représentation de Riesz, il existe un élément $x \in V$ tel que T coïncide avec $\langle x, \cdot\rangle$ sur V. On a donc montré que $(x_n)_{n\in\mathbb{N}}$ admettait une sous-suite faiblement convergente dans V, il s'agit maintenant d'étendre ce résultat à H.
Soit $y \in H$, que l'on écrit $y =: y_V + z$ selon la décomposition $H = V \oplus V^{\perp}$, de sorte que

$$\langle x_n, y\rangle = \langle x_n, y_V\rangle + \langle x, z\rangle = \langle x, y_V\rangle \underset{n\to\infty}{\longrightarrow} \langle x, y_V\rangle = \langle x, y\rangle.$$

Proposition 41 (Optimisation convexe dans un Hilbert) Soit J une forme linéaire continue sur un Hilbert H, que l'on suppose convexe et coercive (*i.e.* $\lim\limits_{\|x\|\to\infty} J(x) = +\infty$). L'application J admet un minimum global sur H.

Preuve. Puisque J est coercive et continue, elle est minorée. Par conséquent, on peut noter $\alpha := \inf J$ et se donner une suite minimisante $(x_n)_{n\in\mathbb{N}}$ de J. La coercivité de J assure que cette suite est bornée, et donc d'après le théorème de Banach-Alaoglu version Hilbert, on peut supposer (quitte à extraire) que cette suite minimisante converge faiblement vers un élément $x \in H$. Montrons alors que $J(x) = \alpha$. Pour cela, introduisons pour $\beta > \alpha$ le convexe fermé

$$C_\beta := \{y \in H \mid J(y) \leqslant \beta\},$$

dont la convexité est assurée par celle de J et la fermeture par la continuité de J. Par définition, à partir d'un certain rang, la suite $(x_n)_{n\in\mathbb{N}}$ est contenue dans C_β. Notons $p_\beta(x)$ la projection de x sur C_β. D'après la caractérisation de la projection sur un convexe fermé dans un Hilbert, on a pour tout $z \in C_\beta$,

$$\langle x - p_\beta(x), z - p_\beta(x)\rangle \leqslant 0$$

. En particulier, à partir d'un certain rang, on a

$$0 \geqslant \langle x - p_\beta(x), x_n - p_\beta(x)\rangle \underset{n\to\infty}{\longrightarrow} \langle x - p_\beta(x), x - p_\beta(x)\rangle = \|x - p_\beta(x)\|^2,$$

si bien que $x = p_\beta(x) \in C_\beta$. Le réel $\beta > \alpha$ étant quelconque on en déduit bien que $J(x) = \alpha$.

Questions possibles : (ce sont les questions que j'ai eues le jour J)

- En quoi est-ce un résultat de compacité ? C'est un résultat de compacité séquentielle pour la topologie faible-*, qui est la topologie faible dans un Hilbert (car réflexif). La compacité séquentielle coïncide avec la compacité lorsque la topologie est métrisable, ce qui est le cas lorsque l'espace est séparable. Voir *Analyse fonctionnelle* de Haïm Brézis, par exemple.
- Quelles sont les applications de la dernière proposition ? Voir par exemple l'équation $-u'' + |u|^{p-1}u = f$ résolue en minimisant une fonctionelle convexe.

5.3 Cauchy-Peano

Leçons concernées. 203, 206, 219, 220.
Référence. *131 développements pour l'oral*, Pierre le Barbenchon & Cie.
Remarques.

Théorème 42 (Cauchy-Peano)
Soit $(t_0, y_0) \in \mathbb{R} \times \mathbb{R}^n$ et $f : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}$ continue sur un voisinnage ouvert Ω de (t_0, y_0). Le problème de Cauchy

$$\begin{cases} y' = f(t, y) \\ y(t_0) = y_0 \end{cases}$$

admet au moins une solution définie au voisinnage de t_0.

Preuve. Tâchons tout d'abord de travailler sur un domaine agréable. Puisque Ω est ouvert, il existe des réels $a, b > 0$ tels que $[t_0, t_0 + a] \times \overline{B(y_0, b)} \subset \Omega$. La fonction f étant continue sur ce compact, elle y est bornée par par un réel $M > 0$. On fixe $c := \min(a, b/M)$ et $I := [t_0, t_0 + c]$.
Par conséquent, si $\mathcal{A}$ désigne l'ensemble des fonctions M-lipschitziennes de I dans $\mathbb{R}^n$ envoyant t_0 sur y_0, alors toute fonction $z \in \mathcal{A}$ est à valeurs dans $\overline{B(y_0, b)}$, puisque pour tout $t \in I$,

$$\|z(t) - y_0\| = \|z(t) - z(t_0)\| \leqslant M|t - t_0| \leqslant Mc \leqslant b.$$

Pour $z \in \mathcal{A}$, on peut donc définir la fonction g définie sur I par

$$g(t) := \left\| z(t) - y_0 - \int_{t_0}^{t} f(s, z(s))\mathrm{d}s \right\| \leqslant \|z(t) - y_0\| + \int_{t_0}^{t} \|f(s, z(s))\|\mathrm{d}s,$$

qui est continue sur un compact et qui admet donc un maximum noté $F(z)$. On remarque alors que si $F(z) = 0$, on a $z(t) = y_0 + \int_{t_0}^{t} f(s, z(s))\mathrm{d}s$ pour tout $t \in I$, de sorte que z est dérivable et est solution du problème de Cauchy sur I. On va donc montrer qu'on dispose d'un tel z.

Pour cela, montrons que $\mathcal{A}$ est compact (pour la topologie de la norme uniforme).
L'ensemble $\mathcal{A}$ est fermé pour la topologie uniforme et est constitué de fonctions uniformément bornées (par $\|y_0\| + b$).
En outre, toute les fonctions de $\mathcal{A}$ sont uniformément équicontinues. En effet, si $\varepsilon > 0$, si l'on pose $\delta := \varepsilon/M$, alors par M-lipschitziannité,

$$\forall z \in \mathcal{A}, \forall x, y \in I,\ |x - y| < \delta \implies \|z(x) - z(y)\| \leqslant M|x - y| < \varepsilon.$$

Le théorème d'Ascoli nous assure donc que $\mathcal{A}$ est compact pour la topologie uniforme. Montrons maintenant que l'application F est continue sur $\mathcal{A}$.

Soit $(z_n)_{n\in\mathbb{N}}$ une suite de fonctions de $\mathcal{A}$ convergeant uniformément vers $z \in \mathcal{F}$. Par continuité de f, de la norme et de la continuité du maximum sur un segment, on a $F(z_n) \underset{n\to\infty}{\longrightarrow} F(z)$. Par compacité de $\mathcal{A}$, l'application F atteint donc son minimum sur $\mathcal{A}$ en une certaine fonction $\varphi \in \mathcal{F}$. On va donc montrer que F est arbitrairement proche de 0 sur $\mathcal{A}$, ce qui impliquera que $F(\varphi) = 0$.

Soit $k \geqslant 2$ et le problème approché suivant :

$$\begin{cases} y'(t) = f\left(t - \frac{c}{k}, y(t - c/k)\right) & \text{si } t \in \left]t_0 + \frac{c}{k}, t_0 + c\right], \\ y(t) = y_0 & \text{si } t \in \left[t_0, t_0 + \frac{c}{k}\right[. \end{cases}$$

Ce problème admet une unique solution $z_k \in \mathcal{A}$, définie de proche en proche par

$$\begin{cases} z_k(t) = y_0 & \text{si } t \in \left[t_0, t_0 + \frac{c}{k}\right[, \\ z_k(t) = y_0 + \int_{t_0}^{t - \frac{c}{k}} f(s, z_k(s))\mathrm{d}s & \text{si } t \in \left]t_0 + \frac{c}{k}, t_0 + c\right]. \end{cases}$$

Cette fonction z_k est bien dans $\mathcal{A}$ puisque pour tout $u < t \in [t_0, t_0 + c]$,

$$\|z_k(t) - z_k(u)\| \leqslant \int_{\max(t_0, u-\frac{c}{k})}^{\max(t_0, t-\frac{c}{k})} \|f(s, z_k(s))\| \mathrm{d}s \leqslant M|t-u|.$$

Par définition de z_k, si $t \in [t_0, t_0 + \frac{c}{k}]$, on a

$$\left\| z_k(t) - y_0 - \int_{t_0}^{t} f(s, z_k(s) \mathrm{d}s \right\| = \left\| \int_{t_0}^{t} f(s, y_0) \mathrm{d}s \right\| \leqslant \frac{Mc}{k},$$

et si $t \in]t_0 + \frac{c}{k}, t_0 + c]$, on a

$$\left\| z_k(t) - y_0 - \int_{t_0}^{t} f(s, z_k(s) \mathrm{d}s \right\| = \left\| \int_{t-\frac{c}{k}}^{t} f(s, z_k(s)) \mathrm{d}s \right\| \leqslant \frac{Mc}{k}.$$

Par conséquent, pour tout $k \geqslant 2$, $0 \leqslant F(\varphi) \leqslant F(z_k) \leqslant \frac{Mc}{k}$. Donc si l'on fait tendre k vers $+\infty$, on en déduit que $F(\varphi) = 0$. Dès lors, φ est bien une solution du système initial sur $I = [t_0, t_0 + c]$.

On a trouvé une solution à droite de t_0. Pour étendre ce résultat à gauche, considérons le problème

$$\begin{cases} y' = -f(-t, y) =: g(t, y) \\ y(-t_0) = y_0 \end{cases}$$

où la fonction g vérifie les mêmes hypothèses que g. D'après ce que l'on vient de montrer, ce problème admet donc une solution définie sur $[t_0, t_0 + d]$ pour $d > 0$, qui est donc après le changement de variable $t \mapsto -t$ solution du système initial sur $[t_0 - d, t_0]$.

Si maintenant y_g est une solution à gauche et y_d une solution à droite, leur recollement en t_0 noté y est bien continu puisque $y_d(t_0) = y_g(t_0) = t_0$ et dérivable car $y_g'(t_0) = y_d'(t_0) = f(t_0, y_0)$ et est solution du système initial sur un voisinnage de t_0.

✌

Questions possibles :

- Donner un exemple d'équation différentielle qui admet plusieurs solutions maximales distinctes.
- En quoi utilise-t-on la dimension finie ? (on utilise la compacité d'une boule et la formulation intégrale des équations différentielles)

5.4 Développement asymptotique de la série harmonique

Leçons concernées. 224, 230.
Référence. *Oraux X-ENS, Analyse 1*, FGN.
Remarques. Une preuve pas trop dure d'un résultat qui peut servir d'exemple dans un certain nombre de leçons. Ce n'est cependant pas forcément le développement le plus profond qui soit, il faut bien l'avouer.

Théorème 43
On note $H_n = \sum_{k=1}^{n} \frac{1}{k}$ pour $n \in \mathbb{N}^*$. Il existe une constante $\gamma > 0$ tel que

$$H_n \underset{n \to +\infty}{=} \ln(n) + \gamma + \frac{1}{2n} + o\left(\frac{1}{n}\right).$$

De plus, si pour tout $n \in \mathbb{N}^*$ on note $k_n = \min\{k \in \mathbb{N}^* \mid H_k \geqslant n\}$, alors

$$\frac{k_{n+1}}{k_n} \underset{n \to +\infty}{\longrightarrow} e.$$

Questions possibles :
- Démontrer que $H_n \sim \ln(n)$ lorsque $n \to +\infty$.
- Connait-on une formule générale pour le développement asymptotique de H_n ? (Euler-Maclaurin)

5.5 Espace de Bergman

Leçons concernées. 201, 213, 234, 243, 245.
Référence. *Analyse pour l'agrégation de mathématiques*, Julien et Laurent Bernis.
Remarques. Ce développement nécessite de se pencher un peu sur la convergence uniforme sur tout compact qui fait survenir quelques subtilités, notamment lors de la démonstration de la complétude de l'espace de Bergman. Il faut surtout être bien au clair sur le fait que l'espace $\mathcal{C}(\Delta)$ des fonction continues sur le disque unité muni de la topologie de la convergence uniforme est complètement métrisable et que $\mathcal{H}(\Delta)$ est un fermé de $\mathcal{C}(\Delta)$ pour cette même topologie (et est donc lui aussi complètement métrisable). On peut notamment en trouver les détails dans *Analyse complexe* de Amar et Mathéron. Un résultat intéressant à avoir en tête est le théorème de Montel dans le Bernis[2] (qui donne une jolie application d'Ascoli, puis de Riesz).

Définition 44 (Espace de Bergman)
On appelle espace de Bergman du disque unité ouvert Δ de $\mathbb{C}$ l'espace $\mathcal{H}^2(\Delta) := \mathrm{L}^2(\Delta) \cap \mathcal{H}(\Delta)$ des fonction holomorphes et de carré intégrable (pour la mesure de Lebesgue) sur Δ. On le munit du produit scalaire $\langle \cdot, \cdot \rangle$ induit par celui de $\mathrm{L}^2(\Delta)$, dont on note $\| \cdot \|_2$ la norme associée.

Théorème 45
L'espace de Bergman du disque unité est un espace de Hilbert et admet une base hilbertienne $(e_n)_{n\in\mathbb{N}}$, où pour $n \in \mathbb{N}$, on définit

$$e_n : \begin{cases} \Delta & \longrightarrow \mathbb{C} \\ z & \longmapsto \sqrt{\frac{n+1}{\pi}} z^n \end{cases}.$$

Preuve. Nous allons nous servir du lemme suivant, qui permet sur l'espace de Bergman de contrôler la topologie de la convergence uniforme sur tout compact par la topologie de la norme $\| \cdot \|_2$.

Lemme 46 Soit $f \in \mathcal{H}^2(\Delta)$ et K un compact inclus dans Δ. Si Γ désigne le cercle unité, alors

$$\|f\|_\infty \leqslant \frac{1}{\sqrt{\pi}\mathrm{d}(K,\Gamma)} \|f\|_2^2.$$

Preuve. (du lemme 46)
Soit $a \in K$ et $0 \leqslant r < 1 - |a|$, qui est donc tel que $\overline{D(a,r)} \subset \Delta$. On obtient alors, pour tout $0 \leqslant \rho \leqslant r$, d'après le théorème de Cauchy appliqué à $\partial D(a,\rho)$ avec la paramétrisation usuelle,

$$f(a) = \frac{1}{2\pi} \int_0^{2\pi} f(a + \rho e^{i\theta}) \mathrm{d}\theta.$$

Par changement de variable en coordonnées polaires on obtient donc une nouvelle formule de la moyenne,

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

En appliquant l'inégalité de Cauchy-Schwarz, on a alors

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

Si $r \to 1 - |a|$, on conclue que

$$|f(a)| \leqslant \frac{1}{\sqrt{\pi}(1-|a|)}\|f\|_2 \leqslant \frac{1}{\sqrt{\pi}\mathrm{d}(K,\Gamma)}\|f\|_2,$$

puisque $1 - |a| \geqslant \mathrm{d}(a,\Gamma) \geqslant \mathrm{d}(K,\Gamma)$. L'élément $a \in K$ étant initialement quelconque, on conclue à la majoration voulue.

Forts de ce lemme, tâchons de démontrer que $\mathcal{H}^2(\Delta)$ est un espace de Hilbert. Soit donc $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy de $\mathcal{H}^2(\Delta)$.

Si K est un compact inclus dans Δ, pour tout $n, m \in \mathbb{N}$,

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

et donc $(f_n)_{n\in\mathbb{N}}$ est une suite de Cauchy de $\mathcal{H}(\Delta)$ muni de la topologie de la convergence uniforme sur tout compact, qui est un fermé de $\mathcal{C}(\Delta)$ muni de cette même topologie. Ce dernier étant complet, il en va de même pour $\mathcal{H}(\Delta)$ et donc $(f_n)_{n\in\mathbb{N}}$ converge uniformément sur tout compact vers une fonction $f \in \mathcal{H}(\Delta)$. en particulier, la suite $(f_n)_{n\in\mathbb{N}}$ converge simplement vers f sur Δ.
En outre, $(f_n)_{n\in\mathbb{N}}$ est une suite de Cauchy de $\mathrm{L}^2(\Delta)$ et est donc converge vers une fonction $g \in \mathrm{L}^2(\Delta)$. D'après le théorème de Riesz-Fischer, cette suite admet une sous-suite qui converge simplement vers g, d'où l'on déduit que $f = g$ presque partout.
Par conséquent, $(f_n)_{n\in\mathbb{N}}$ converge pour $\|\cdot\|_2$ vers $f \in \mathcal{H}(\Delta) \cap \mathrm{L}^2(\Delta) = \mathcal{H}^2(\Delta)$. Ceci nous permet donc de conclure que $\mathcal{H}^2(\Delta)$ est un espace de Hilbert.

Montrons maintenant que $(e_n)_{n\in\mathbb{N}}$ est une base hilbertienne de l'espace de Bergman du disque unité. C'est une famille orthonormée, puisque par changement de coordonnées polaire,

$$\forall n, m \in \mathbb{N}, \int_\Delta z^p \overline{z}^q \mathrm{d}z = \int_0^1 \int_0^{2\pi} r^n r^m e^{i(n-m)\theta} \mathrm{d}\theta r \mathrm{d}r = 2\pi \int_0^1 r^{m+n+1} \delta_{n,m}\ r = \frac{2\pi}{n+m+2}\delta_{p,q},$$

et donc si $n \neq m$ on a $\langle e_n, e_m\rangle = 0$, tandis que $\|e_n\|_2 = 1$. La famille $(e_n)_{n\in\mathbb{N}}$ est othonormée.

Il s'agit ensuite de montrer que la famille est totale. On se donne $f \in \mathcal{H}^2(\Delta)$ orthogonal à tous les e_n et on va montrer que $f = 0$. L'espace de Bergman étant un Hilbert, cela suffira à montrer que $\mathrm{Vect}(e_n, n \in \mathbb{N})$ est dense par caractérisation de la densité dans un Hilbert.
La fonction f est analytique sur Δ, donc on peut écrire $f(z) =: \sum_{k=0}^{+\infty} a_k z^k$ et l'on par la formule de Cauchy pour tout $0 < r < 1$,

$$\forall k \in \mathbb{N}, a_k = \frac{1}{2\pi r^k}\int_0^{2\pi} f(re^{i\theta})e^{-ik\theta}\ \theta.$$

Ainsi, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} 0 = \langle f, e_n\rangle &= \sqrt{\frac{n+1}{\pi}}\int_0^1 r^n \int_0^{2\pi} f(re^{i\theta})e^{-in\theta}\mathrm{d}\theta r\mathrm{d}r \\ &= \sqrt{\frac{n+1}{\pi}}\int_0^1 r^n \int_0^{2\pi} 2\pi a_n r^{2n+1}\mathrm{d}r = \sqrt{\frac{\pi}{n+1}}a_n. \end{aligned}$$

Et donc finalement, tous les a_n sont nuls et par suite, f est nulle.

Questions possibles :

- Caractériser les fonctions de l'espace de Bergman par leur série entière. Voir par exemple ceci.
- Démontrer le théorème de Weierstrass (sur le caractère fermé de $\mathcal{H}(\Delta)$).
- Que dit le théorème de Riesz-Fischer ?
- À quoi servent les bases hilbertiennes ? (à diagonaliser des opérateurs, par exemple les polynômes de Hermite diagonalisent la transformée de Fourier, la base des série de Fourier diagonalise la dérivation)

5.6 Théorème de Fejér

Leçons concernées. 209, 246.
Référence. *Analyse pour l'agrégation*, Hervé Queffélec et Claude Zuily.
Remarques. Le développement est sans doute un peu court en l'état, on peut calculer les noyaux de Dirichlet et de Féjer au début pour le rallonger.

On rappelle que le noyau de Féjer est défini par $K_N(x) = \dfrac{1}{N}\displaystyle\sum_{n=0}^{N-1} D_n = \dfrac{1}{N}\left(\dfrac{\sin(Nx/2)}{\sin(x/2)}\right)^2$.

Théorème 47 (Fejér)

i. Soit $f \in \mathcal{C}^0(0,2\pi)$. Pour tout $n \geqslant 1$, $\|f * K_n\|_\infty \leqslant \|f\|_\infty$ et $\lim\limits_{n\to+\infty} \|f * K_n - f\|_\infty = 0$.

ii. Soit $1 \leqslant p < +\infty$ et $f \in \mathrm{L}^p$. Pour tout $n \geqslant 1$, $\|f*K_n\|_p \leqslant \|f\|_p$ et $\lim\limits_{n\to+\infty} \|f*K_n - f\|_p = 0$.

Preuve.

i. Tout d'abord, pour tout $n \geqslant 1$, $\|f * K_n\|_\infty \leqslant \|f\|_\infty \|K_n\|_1 = \|f\|_\infty$.
Maintenant, soit $\delta \in]0,\pi]$. Notons $\omega(\delta) := \sup\{|f(u) - f(v)|\ ,\ |u-v| \leqslant \delta\}$ le module de continuité de f. On a alors pour tout $x \in \mathbb{R}$, puisque K_n est positif de norme sur $L^1(0,2\pi)$ égale à 1,

$$\begin{aligned}
|f(x) - f*K_n(x)| &= \left|\frac{1}{2\pi}\int_{-\pi}^{\pi} (f(x) - f(x-t))K_n(t)\,\mathrm{d}t\right| \\
&\leqslant \frac{1}{2\pi}\int_{|t|\leqslant\delta} |f(x) - f(x-t)|K_n(t)\,\mathrm{d}t + \frac{1}{2\pi}\int_{\pi\geqslant|t|>\delta} |f(x) - f(x-t)|K_n(t)\,\mathrm{d}t \\
&\leqslant \frac{\omega(\delta)}{2\pi}\int_{|t|\leqslant\delta} K_n(t)\,\mathrm{d}t + \frac{\|f\|_\infty}{\pi}\int_{\pi\geqslant|t|>\delta} K_n(t)\,\mathrm{d}t \\
&\leqslant \omega(\delta) + \frac{\|f\|_\infty}{N\sin^2(\delta/2)}
\end{aligned}$$

Par conséquent, $\|f * K_n - f\|_\infty \leqslant \omega(\delta) + \frac{\|f\|_\infty}{N\sin^2(\delta/2)}$ et donc en passant à la limite supérieure lorsque $n \to +\infty$,

$$\overline{\lim_{n\to\infty}} \|f * K_n - f\|_\infty \leqslant \omega(\delta).$$

Puisque f est continue et 2π-périodique, elle est uniformément continue et donc $\omega(\delta) \to 0$ lorsque $\delta \to 0$. D'où, enfin, $\lim\limits_{n\to+\infty} \|f * K_n - f\|_p = 0$.

ii. Pour $n \geqslant 1$, appliquons l'inégalité de Hölder par rapport à la mesure de probabilité $K_n(t)\frac{\mathrm{d}t}{2\pi}$:

$$|f*K_n(x)|^p \leqslant \left(\int_{-\pi}^{\pi} 1\cdot|f(x-t)|\cdot K_n(t)\frac{\mathrm{d}t}{2\pi}\right)^p \leqslant 1\cdot\int_{-\pi}^{\pi} |f(x-t)|^p\cdot K_n(t)\frac{\mathrm{d}t}{2\pi} = \frac{1}{2\pi}\int_{-\pi}^{\pi} |f(x-t)|^p K_n(t)\,\mathrm{d}t$$

Dès lors, en appliquant le théorème de Fubini-Tonelli,

$$\begin{aligned}\|f * K_n\|_p^p &\leqslant \frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}|f(x-t)|^p K_n(t)\mathrm{t}\mathrm{x}\\ &= \frac{1}{4\pi^2}\int_{-\pi}^{\pi}K_n(t)\left(\int_{-\pi}^{\pi}|f(x-t)|^p\mathrm{x}\right)\mathrm{t}\\ &= \frac{1}{4\pi^2}\int_{-\pi}^{\pi}K_n(t)\left(\int_{-\pi}^{\pi}|f(x)|^p\mathrm{x}\right)\mathrm{t}\\ &= \|K_n\|_1\cdot\|f\|_p = \|f\|_p^p\end{aligned}$$

De même, on a

$$\begin{aligned}\|f * K_n(x) - f\|_p^p &\leqslant \frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}|f(x-t)-f(x)|^p K_n(t)\mathrm{t}\mathrm{x}\\ &= \frac{1}{4\pi^2}\int_{-\pi}^{\pi}K_n(t)\left(\int_{-\pi}^{\pi}|f(x-t)-f(x)|^p\mathrm{x}\right)\mathrm{t}\\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi}K_n(t)\|f-\tau_t f\|_p^p\mathrm{t}\end{aligned}$$

Or, si l'on note $g : t \mapsto \|f - \tau_{-t}f\|_p^p \in \mathcal{C}^0(0, 2\pi)$, on obtient donc

$$\|f * K_n(x) - f\|_p^p \leqslant g * K_n(0).$$

D'après le point i., on a en particulier $g * K_n(0) \to g(0) = 0$ lorsque $n \to +\infty$ et donc

$$\lim_{n\to+\infty}\|f * K_n - f\|_p = 0.$$

✌

Questions possibles :

- Donner les grandes lignes de la démonstration de la continuité de la translation. (attention, il faut utiliser la densité des fonction lipschitzienne à support compact et non $\mathcal{C}^\infty$ à support compact pour éviter un raisonnement circulaire)
- Démontrer le théorème de Riemann-Lebesgue.
- En quelques mots, que nous dit le théorème de Féjèr ? (que la série de Fourier converge au sens de Césaro)
- Démontrer dans les grandes lignes que les $(e_n)_{n\in\mathbb{Z}}$ constituent une base hilbertienne de $L^2(0, 2\pi)$.

5.7 Formule des compléments

Leçons concernées. 236, 245, 265, 267.
Référence. *Analyse Complexe*, Éric Amar et Étienne Matheron.
Remarques. On ne démontre la formule des compléments que sur $\{0 < \mathrm{Re}(z) < 1\}$, mais elle est valable sur $\mathbb{C}\backslash\mathbb{Z}$, par le principe du prolongement analytique. Cette formule sert notamment à prolonger la fonction ζ au plan complexe.
À l'étape 1 on peut conclure plus rapidement avec le changement de variable $(u, v) := (t, t/s)$, qui évite la machinerie du jacobien. On peut également faire un autre changement de variable pour se ramener à un contour rectangulaire, plus simple (*Complex Analysis*, Stein).

Théorème 48 (Formule des compléments)
Pour tout $z \in \mathbb{C}$ tel que $0 < \mathrm{Re}(z) < 1$,

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

Preuve. **Étape 1 :** (Réduction à un problème de calcul d'intégrale)
Par le principe des zéros isolés, il nous suffit de démontrer la formule des compléments pour $\alpha \in]0,1[$. D'après le théorème de Fubini-Lebesgue, on peut alors écrire

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_{\mathbb{R}_+^*} t^{\alpha-1}e^{-t}\mathrm{d}t \int_{\mathbb{R}_+^*} s^{-\alpha}e^{-s}\mathrm{d}s = \int_{t,s>0} \frac{1}{t}\left(\frac{t}{s}\right)^{\alpha} e^{-(t+s)}\mathrm{d}t\mathrm{d}s.$$

L'application $\varphi : (t,s) \mapsto (t+s, t/s) =: (u,v)$ est un $\mathcal{C}^1$-difféomorphisme de $\mathbb{R}_+^* \times \mathbb{R}_+^*$ dans lui-même d'inverse $(u,v) \mapsto (\frac{uv}{1+v}, \frac{u}{1+v})$. Le jacobien de φ en un point (t,s) vaut :

$$\mathrm{Jac}_{(t,s)}(\varphi) = \begin{vmatrix} 1 & 1 \\ \frac{1}{s} & -\frac{t}{s^2} \end{vmatrix} = -\frac{t+s}{s^2} = -\frac{(1+v)^2}{u}$$

Ainsi, $\mathrm{Jac}_{(u,v)}(\varphi^{-1}) = -\frac{u}{(1+v)^2} = -\frac{t}{v(1+v)}$ et donc, par le changement de variable $(t,s) = (u,v)$, et en utilisant à nouveau Fubini-Lebesgue,

$$\Gamma(\alpha)\Gamma(1-\alpha) = \int_{u,v>0} \frac{v^{\alpha}e^{-u}}{v(1+v)}\mathrm{d}u\mathrm{d}v = \int_{\mathbb{R}_+^*} \frac{1}{v^{1-\alpha}(1+v)}\mathrm{d}v =: I_{1-\alpha}$$

Tâchons donc de calculer $I_\alpha = I_{1-\alpha}$.

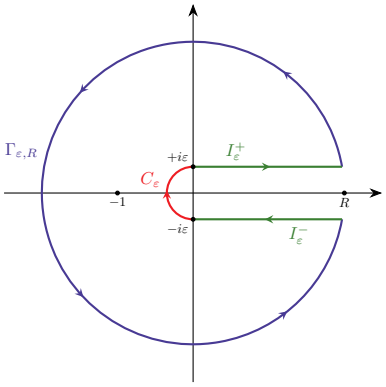
Étape 2 : (Les résidus à la rescousse)
Soit $\Omega := \mathbb{C}\backslash[0,+\infty[$ et soit f définie sur $\Omega\backslash\{-1\}$ par

$$f(z) = \frac{1}{z^{\alpha}(1+z)}$$

où, si $z = re^{i\theta}$ pour $r \in \mathbb{R}_+^*$ et $\theta \in]0,2\pi[$, $z^{\alpha} = r^{\alpha}e^{i\alpha\theta}$. La fonction f est holomorphe sur $\Omega\backslash\{-1\}$ et possède un pôle simple en -1, et on a

$$\mathrm{Res}(f,-1) = \frac{1}{(-1)^{\alpha}} = e^{-i\alpha\pi}.$$

On cherche maintenant à appliquer le théorème des résidus à f. Pour ce faire, fixons-nous deux réels $0 < \varepsilon < 1 < R$, et notons $K_{\varepsilon,R}$ le compact délimité par le demi-cercle $C_\varepsilon := \{z \in \mathbb{C} \mid |z| = \varepsilon,\ \mathrm{Re}(z) \leqslant 0\}$, les deux segments $I_{e,R}^{\pm} := [\pm i\varepsilon, \pm i\varepsilon + \sqrt{R^2-\varepsilon^2}]$ et l'arc de cercle $\Gamma_{\varepsilon,R} := \{Re^{i\theta} \mid \theta \in [-\pi,\pi],\ |\theta| \geqslant \arctan(\varepsilon/\sqrt{R^2-\varepsilon^2})$, avec les orientations fixées sur la figure ci-dessous.



Puisque -1 appartient à l'intérieur de $K_{\varepsilon,R}$, le théorème des résidus nous donne

$$\int_{\partial K_{\varepsilon,R}} f(z)\mathrm{d}z = 2i\pi \mathrm{Ind}(\partial K_{\varepsilon,R}, -1)\mathrm{Res}(f,-1) = 2i\pi e^{-i\alpha\pi}.$$

Étape 3 : (calcul d'une intégrale de contour)
Le terme de gauche se décompose en quatre intégrales :

$$\int_{\partial K_{\varepsilon,R}} f = \int_{C_\varepsilon} f + \int_{I_{e,R}^+} f + \int_{\Gamma_{\varepsilon,R}} f + \int_{I_{e,R}^-} f.$$

Tout d'abord, $\left|\int_{C_\varepsilon} f(z)\mathrm{d}z\right| \leqslant \pi\varepsilon \frac{1}{\varepsilon^\alpha(1-\varepsilon)} \underset{\varepsilon\to 0}{\longrightarrow} 0.$
De plus avec la paramétrisation usuelle d'un arc de cercle,

$$\int_{\Gamma_{\varepsilon,R}} f(z)\mathrm{d}z = \int_{\theta_{\varepsilon,R}}^{2\pi-\theta_{\varepsilon,R}} \frac{iRe^{i\theta}}{R^\alpha e^{i\alpha\theta}(1+Re^{i\theta})}\mathrm{d}\theta = \int_{\theta_{\varepsilon,R}}^{2\pi-\theta_{\varepsilon,R}} iR^{1-\alpha}\frac{e^{i(1-\alpha)\theta}}{1+Re^{i\theta}}\mathrm{d}\theta \underset{\varepsilon\to 0}{\longrightarrow} \int_0^{2\pi} iR^{1-\alpha}\frac{e^{i(1-\alpha)\theta}}{1+Re^{i\theta}}\mathrm{d}\theta,$$

par convergence dominée (où $\theta_{\varepsilon,R} := \arctan(\varepsilon/\sqrt{R^2-\varepsilon^2})$).
Enfin, calculons l'intégrale de f sur $I^-_{e,R}$ et $I^+_{e,R}$.
Si $t>0$, alors $(t+i\varepsilon)$ a pour argument $0 < \arctan\varepsilon/t < 2\pi$ et donc

$$(t+i\varepsilon)^\alpha = |t+i\varepsilon|^\alpha e^{i\alpha\arctan\varepsilon/t} \underset{\varepsilon\to 0}{\longrightarrow} t^\alpha.$$

Cependant, $(t-i\varepsilon)$ a pour argument $-2\pi < -\arctan\varepsilon/t < 0$ et donc

$$(t+i\varepsilon)^\alpha = |t+i\varepsilon|^\alpha e^{i\alpha(2\pi-\arctan\varepsilon/t)} \underset{\varepsilon\to 0}{\longrightarrow} t^\alpha e^{i\alpha 2\pi}.$$

Par convergence dominée, on conclue donc que les intégrales $\int_{I^+_{e,R}} f$ et $\int_{I^-_{e,R}} f$ tendent respectivement vers $\int_0^R \frac{1}{t^\alpha(1+t)}$ et $-\int_0^R \frac{e^{-i\alpha 2\pi}}{t^\alpha(1+t)}$ lorsque ε tend vers 0.
Par conséquent,

$$(1-e^{-2i\alpha\pi})\int_0^R \frac{1}{t^\alpha(1+t)}\mathrm{d}t = 2i\pi e^{-i\pi\alpha} - \int_0^{2\pi} iR^{1-\alpha}\frac{e^{i(1-\alpha)\theta}}{1+Re^{i\theta}}\mathrm{d}\theta.$$

En faisant tendre R vers $+\infty$, on obtient donc que $(1-e^{-2i\alpha\pi})I_\alpha = 2i\pi e^{-i\pi\alpha}$, puisque

$$\left|\int_0^{2\pi} iR^{1-\alpha}\frac{e^{i(1-\alpha)\theta}}{1+Re^{i\theta}}\mathrm{d}\theta\right| \leqslant 2\pi\frac{R^{1-\alpha}}{1-R} \underset{R\to+\infty}{\longrightarrow} 0.$$

(c'est ici que l'on utilise que $0<\alpha<1$). Enfin, on obtient

$$I_\alpha = \frac{2i\pi e^{-i\pi\alpha}}{(1-e^{-2i\alpha\pi})} = \frac{\pi}{\sin(\pi\alpha)}.$$

Questions possibles :
- Justifier les utilisations du théorème de convergence dominée.
- À quoi sert la formule des compléments ? (à prolonger Γ, ζ... voir le Amar et Mathéron)
- Calculer un résidu.
- Avez-vous d'autres exemples d'utilisation du théorème des résidus ?

5.8 Gradient à pas optimal

Leçons concernées. 215, 219, 229, 253.
Référence. *Analyse pour l'agrégation de mathématiques, 40 développements*, Laurent et Julien Bernis.
Remarques. C'est un développement assez long, où il faut choisir judicieusement ce que l'on traite et ce que l'on admet.

Soit $A \in S_n^{++}(\mathbb{R})$ et $b \in \mathbb{R}^n$. On note $\|\cdot\|_A$ la norme associée à A et $\lambda_1 \leqslant \cdots \leqslant \lambda_n$ les valeurs propres de A. Soit $\Phi : x \mapsto \frac{1}{2}\langle Ax, x\rangle - \langle b, x\rangle$.

Théorème 49
L'application φ est différentiable et atteint son unique minimum en $\overline{x} = A^{-1}b$. De plus, $\nabla\Phi(x) = Ax - b = A(x - \overline{x})$.
Soit $x_0 \neq \overline{x}$. On considère la suite $(x_k)_{k\in\mathbb{N}}$ définie par

$$\forall k \in \mathbb{N}, \quad x_{k+1} = x_k - \alpha_k \nabla\Phi(x_k), \quad \text{où} \quad \alpha_k = \frac{\|\nabla\Phi(x_k)\|^2}{\|\nabla\Phi(x_k)\|_A^2}.$$

La suite $(x_k)_{k\in\mathbb{N}}$ converge vers $\overline{x}$ et il existe une constante $C > 0$ telle que

$$\|x_k - \overline{x}\| \leqslant C \left(\frac{\lambda_n - \lambda_1}{\lambda_1 + \lambda_n}\right)^k \|x_0 - \overline{x}\|.$$

Lemme 50 (Inégalité de Kantorovitch) Pour tout $x \in \mathbb{R}^n$ non nul,

$$\frac{\|x\|^4}{\|x\|_A^2 \|x\|_{A^{-1}}^2} \geqslant 4\frac{\lambda_1\lambda_n}{(\lambda_1 + \lambda_n)^2}.$$

Questions possibles :
- Dans la pratique, utilise-t-on le gradient à pas optimal ? Pourquoi ? (parler du gradient à pas constant)
- Présenter la méthode du gradient à pas conjugué.
- Existe-t-il d'autres méthodes pour résoudre un système linéaire ? (méthode LU, méthodes itératives)
- L'inégalité de Kantorovitch est-elle optimale ?

5.9 Hadamard-Lévy

Leçons concernées. 204, 214, 215, 220.
Référence. *Analyse pour l'agrégation de mathématiques, 40 développements*, Laurent et Julien Bernis.
Remarques. Attention, le "vrai" théorème d'Hadamard-Lévy ne fait qu'une hyopthèse $\mathcal{C}^1$ et non $\mathcal{C}^2$, mais la démonstration est bien plus délicate.
Notre preuve utilise un théorème de Cauchy "à paramètre", que l'on peut par exemple trouver dans *Équations différentielles*, Berthelin et qu'il est bon d'admettre, peut-être en disant qu'on le démontre avec un théorème de point fixe à paramètre et le théorème des fonctions implicites.
On peut préférer faire le premier lemme en dernier lieu, une fois que l'on a justifié son utilité.

Lemme 51 Soit $f \in \mathcal{C}^1(\mathbb{R}^d, \mathbb{R}^d)$ telle que pour tout $x \in \mathbb{R}^d$, $\mathrm{d}f(x) \in \mathrm{GL}_d(\mathbb{R})$ et il existe $g \in \mathcal{C}^1(\mathbb{R}^d, \mathbb{R}^d)$ vérifiant $f \circ g = \mathrm{id}_{\mathbb{R}^d}$.
Alors f est un $\mathcal{C}^1$-difféomorphisme de $\mathbb{R}^d$ dans lui-même.

Preuve.
Il suffit de montrer que f est bijective.
La surjectivité de f est assurée par l'existence d'un inverse à droite. Pour conclure à l'injectivité de f, on va montrer que g est surjective par un argument de connexité. Plus précisément, montrons que $g(\mathbb{R}^d)$ est un ouvert-fermé de $\mathbb{R}^d$.
Montrons que c'est fermé. Soit $y \in \mathbb{R}^d$ tel qu'il existe $(x_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{R}^d$ telle que $g(x_n) \underset{n\to+\infty}{\longrightarrow} y \in \mathbb{R}^n$. Par continuité de f, on a ainsi $\lim\limits_{n\to\infty} f \circ g(x_n) = f(y)$, *i.e* $\lim\limits_{n\to\infty} x_n = f(y)$. Par continuité de g, on conclue donc que

$$y = \lim_{n\to\infty} g(x_n) = g(f(y)) \in g(\mathbb{R}^d).$$

Montrons désormais que l'on a affaire à un ouvert. Soit $y = g(x) \in g(\mathbb{R}^d)$. Puisque $\mathrm{d}f(y)$ est inversible, le théorème d'inversion locale nous assure l'existence d'un voisinnage ouvert U de x et d'un voisinnage ouvert V de y tel que f induit un $\mathcal{C}^1$-difféomorphisme de V sur U. En outre, par continuité de g, quitte à réduire U, on peut supposer que $g(U) \subset V$. Ainsi, $g(U) = (f_V)^{-1}(f_V(g(U))) = (f_V)^{-1}(U)$ et est donc un ouvert inclu dans $g(\mathbb{R}^d)$ et contenant y. Il en résulte donc que $g(\mathbb{R}^d)$ est un ouvert. Par connexité de $\mathbb{R}^d$ on a $g(\mathbb{R}^d) = \mathbb{R}^d$.

Utilisons ceci pour montrer que f est injective. Soient $y_1, y_2 \in \mathbb{R}^d$ tels que $f(y_1) = f(y_2)$. Par surjectivité de g, on dispose de $x_i \in \mathbb{R}^d$ tel que $g(x_i) = y_i,\ i = 1, 2$ et alors

$$x_1 = f \circ g(x_1) = f(y_1) = f(y_2) = f \circ g(x_2) = x_2,$$

et finalement, $y_1 = g(x_i) = y_2$, si bien que f est injective et donc bijective.

Théorème 52 (Hadamard-Lévy)
Soit $f \in \mathcal{C}^2(\mathbb{R}^d, \mathbb{R}^d)$. La fonction f est un $\mathcal{C}^1$-difféomorphisme de $\mathbb{R}^d$ dans lui-même si et seulement si pour tout $x \in \mathbb{R}^d$,

$$\mathrm{d}f(x) \in \mathrm{GL}_d(\mathbb{R}) \quad \text{et} \quad \lim_{||x|| \to +\infty} ||f(x)|| = +\infty.$$

Preuve. Tout d'abord, supposons que f est un $\mathcal{C}^1$-difféomorphisme de $\mathbb{R}^d$ dans lui-même. On a $f^{-1} \circ f = \mathrm{id}_{\mathbb{R}^d}$, donc pour tout $x \in \mathbb{R}^d$, $\mathrm{d}f^{-1}(f(x)) \circ \mathrm{d}f(x) = \mathrm{id}_{\mathbb{R}^n}$. Par conséquent, $\mathrm{d}f(x)$ est inversible à gauche et donc inversible.
En outre, si on se donne $R > 0$, alors l'image réciproque de $\overline{B(0,R)}$ par f est un compact et donc en particulier, il existe $A > 0$ tel que $f^{-1}(\overline{B(0,R)}) \subset \overline{B(0,A)}$. Ainsi, pour tout $x \in \mathbb{R}^d$, si $||x|| > A$, alors $||f(x)|| > R$ et donc $\lim\limits_{||x|| \to +\infty} ||f(x)|| = +\infty$.

Tâchons de démontrer la réciproque. On suppose donc que $\mathrm{d}f(x) \in \mathrm{GL}_d(\mathbb{R})$ et $\lim\limits_{||x|| \to +\infty} ||f(x)|| = +\infty$.
Quitte à remplacer f par $f - f(0)$, on suppose que $f(0) = 0$.
On va montrer que f admet un inverse à droite en construisant $s : I \times \mathbb{R}^n \to \mathbb{R}^n$ avec I un intervalle ouvert contenant 0 et 1 tel que $f \circ s(t,x) = tx$ pour tout $(t,x) \in I \times \mathbb{R}^d$. On obtiendra un inverse à droite de f en considérant $s(1, \cdot)$.

Soit donc I un intervalle ouvert contenant 0 et 1 et soit $s : I \times \mathbb{R}^n \to \mathbb{R}^n$ dérivable en la première variable. Alors s est telle qu'on la cherche si et seulement si pour tout $(t,x) \in I \times \mathbb{R}^d$,

$$\mathrm{d}f(s(t,x)) \circ \frac{\partial s}{\partial t}(t,x) = x \quad \text{et} \quad f \circ s(0,x) = 0,$$

ce qui équivaut à dire que pour tout $(t,x) \in I \times \mathbb{R}^d$,

$$\frac{\partial s}{\partial t}(t,x) = (\mathrm{d}f(s(t,x)))^{-1}(x) \quad f \circ s(0,x) = 0.$$

Par conséquent, si pour tout $x \in \mathbb{R}^n$, $s(x, \cdot)$ est solution sur I du problème de Cauchy

$$y' = (\mathrm{d}f(y))^{-1}(x) \quad \text{et} \quad y(0) = 0, \tag{1}$$

alors s conviendra bien. Notons $F : \mathbb{R}^d \times \mathbb{R}^d$ définie par $F(x,y) = (\mathrm{d}f(y))^{-1}(x)$, qui est de classe $\mathcal{C}^1$ puisque f est de classe $\mathcal{C}^2$. Ainsi, pour $x \in \mathbb{R}^d$ fixé, l'application $F(x, \cdot)$ est $\mathcal{C}^1$ et donc globalement lipschitzienne en y. Le théorème de Cauchy-Lipschitz nous permet donc de conclure qu'il existe une unique solution maximale au problème de Cauchy (1) notée $s(\cdot, x)$ et définie sur un intervalle ouvert $]t^-(x), t^+(x)[$ contenant 0.

Supposons par l'absurde qu'il existe $x_0 \in \mathbb{R}^n$ tel que $t^+(x_0) < 1$. D'après le théorème de sortie de tout compact, on a alors $\lim_{t \to t^+(x_0)} ||s(t,x_0)|| = +\infty$ et donc $\lim_{t \to t^+(x_0)} f \circ s(t,x_0)|| = +\infty$. Or,

$$\lim_{t \to t^+(x_0)} ||f \circ s(t,x_0)|| = \lim_{t \to t^+(x_0)} ||tx_0|| = t^+(x_0)||x_0||,$$

ce qui est absurde. On peut donc définir l'application $s(1,\cdot)$ de $\mathbb{R}^d$ dans lui-même, qui est alors telle que $f \circ s(1,\cdot) = \mathrm{id}_{\mathbb{R}^n}$. Cette application est de classe $\mathbb{C}^1$, grâce au théorème de Cauchy à paramètre, applicable puisque F est de classe $\mathcal{C}^1$.

On conclue donc que f est un $\mathcal{C}^1$-difféomorphisme de $\mathbb{R}^d$ dans lui-même par le lemme précédent.

✌

Questions possibles :

- Où a-t-on besoin de l'hypothèse $\mathcal{C}^2$ dans le développement ? Peut-on faire sans ?
- À partir de quoi obtient-on le théorème de Cauchy-Lipschitz à paramètres ? (dire que c'est à partir d'un théorème de point fixe à paramètre obtenu par le théorème des fonctions implicites semble suffire)
- Donner une idée de la preuve du théorème d'inversion locale.
- Donner une application du théorème de Hadamard-Lévy. Voir par exemple ici.

5.10 Intégrale de Dirichlet

Leçons concernées. 235, 236, 239.
Référence. *Analyse pour l'agrégation de mathématiques, 40 développements*, Julien et Laurent Bernis.
Remarques. Le procédé utilisé pour calculer l'intégrale de Dirichlet est d'appliquer une transformée dite de Laplace. La régularité de la transformée de Laplace tombe facilement sur $\mathbb{R}_+^*$, mais il faut travailler pour obtenir la continuité en 0 (cette méthode fonctionne pour de nombreuses intégrales semi-convergentes).

Théorème 53 (Intégrale de Dirichlet)

$$\lim_{x \to +\infty} \int_0^x \frac{\sin t}{t} \mathrm{d}t = \frac{\pi}{2}$$

Preuve. **Étape 1 :** (Bonne définition et transformation de Laplace)
Vérifions tout d'abord que notre limite existe. Par intégration par parties, pour tout $A > 0$,

$$\int_1^A \frac{\sin t}{t} \mathrm{d}t = \left[-\frac{\cos t}{t}\right]_1^A - \int_0^A \frac{\cos t}{t^2} = \underbrace{\frac{\cos A}{A}}_{\longrightarrow 0} - \cos 1 - \int_0^A \frac{\cos t}{t^2}.$$

Puisque $\frac{\cos t}{t^2} \underset{t \to +\infty}{=} O(\frac{1}{t^2})$, la fonction $t \mapsto \frac{\cos t}{t^2}$ est intégrable sur $[1, +\infty[$. Par conséquent,

$$\lim_{x \to +\infty} \int_0^x \frac{\sin t}{t} \mathrm{d}t = \int_0^1 \frac{\sin t}{t} \mathrm{d}t + \lim_{x \to +\infty} \int_1^x \frac{\sin t}{t} \mathrm{d}t$$

existe et on notera donc $\int_0^{+\infty} \frac{\sin t}{t} \mathrm{d}t := \lim_{x \to +\infty} \int_0^x \frac{\sin t}{t} \mathrm{d}t$.

Soit $x > 0$. On a : $\lim_{t \to +\infty} t^2 \cdot e^{-xt} \frac{\sin t}{t} = 0$, donc $e^{-xt} \frac{\sin t}{t} \underset{t \to +\infty}{=} o(\frac{1}{t^2})$. Donc puisque $t \mapsto e^{-xt} \frac{\sin t}{t}$ est continue sur $\mathbb{R}_+$, elle est intégrable sur $\mathbb{R}_+$. On peut donc définir

$$F : \begin{cases} \mathbb{R}_+ & \longrightarrow \mathbb{R} \\ x & \longmapsto \int_{\mathbb{R}_+} e^{-xt} \frac{\sin t}{t} \mathrm{d}t \end{cases}$$

en posant $F(0) = \int_0^{+\infty} \frac{\sin t}{t} \mathrm{d}t$.

Étape 2 : (Continue dérivabilité de F sur $]0, +\infty[$)

Considérons $a > 0$ et montrons que F est de classe $\mathcal{C}^1$ sur $[a, +\infty]$.

— À $x \in [a, +\infty]$ fixé, l'application $t \mapsto e^{-xt}\frac{\sin t}{t}$ intégrable sur $\mathbb{R}_+$.

— Pour tout $t \in \mathbb{R}_+$, l'application $x \mapsto e^{-xt}\frac{\sin t}{t}$ est de classe $\mathcal{C}^1$ et admet pour dérivée $x \mapsto -e^{-xt}\sin t$.

— Enfin, pour tout $(x,t) \in [a, +\infty] \times \mathbb{R}_+$, $|-e^{-xt}\sin t| \leqslant e^{-at} \in \mathrm{L}^1$.

Par théorème de dérivation sous le signe intégral, F est de classe $\mathcal{C}^1$ sur $[a, +\infty]$ et

$$\forall x > a,\ F'(x) = -\int_{\mathbb{R}} e^{-xt}\sin t \mathrm{d}t.$$

Puisque $a > 0$ était quelconque, on en déduit donc que F est de classe $\mathcal{C}^1$ sur $]0, +\infty[$.

Étape 3 : (Détermination de F sur $]0, +\infty[$)

L'expression de la dérivée de F nous donne

$$\begin{aligned}\forall x > 0,\ F'(x) &= -\int_{\mathbb{R}_+} e^{-xt}\sin t \mathrm{d}t = -\int_{\mathbb{R}} \mathrm{Im}\left(e^{(i-x)t}\right)\mathrm{d}t = -\mathrm{Im}\left(\int_{\mathbb{R}} e^{(i-x)t}\mathrm{d}t\right)\\ &= -\mathrm{Im}\left(\left[\frac{e^{(i-x)t}}{i-x}\right]_0^{+\infty}\right) = \mathrm{Im}\left(\frac{1}{i-x}\right) = -\frac{1}{1+x^2}.\end{aligned}$$

Il existe donc une constante $C > 0$ telle que $\forall x > 0,\ F(x) = C - \arctan(x)$. Or, pour tout $t \in \mathbb{R}_+$, $e^{-xt}\frac{\sin t}{t} \underset{x\to+\infty}{\to} 0$ et pour tout $(x,t) \in [1, +\infty[\times\mathbb{R}_+$,

$$|e^{-xt}\frac{\sin t}{t}| \leqslant e^{-xt} \leqslant e^{-t} \in \mathrm{L}^1,$$

donc par théorème de convergence dominée, $\lim\limits_{x\to+\infty} F(x) = 0 = C - \frac{\pi}{2}$. Donc pour tout $x > 0$,

$$F(x) = \frac{\pi}{2} - \arctan(x).$$

Étape 4 : (Continuité de F en 0)

On a, pour tout $t \in \mathbb{R}_+$, $\sup\limits_{x\geqslant 0} |e^{-xt}\frac{\sin t}{t}| = |\frac{\sin t}{t}|$. Or, la fonction $t \mapsto \frac{\sin t}{t}$ n'est pas intégrable sur $\mathbb{R}$. En effet, $|\frac{\sin t}{t}| \geqslant \frac{\sin^2 t}{t}$ et par intégration par partie et avec un peu de trigonométrie,

$$\begin{aligned}\int_{\mathbb{R}_+} \frac{|\sin t|}{t}\mathrm{d}t \geqslant \int_{[1,+\infty[} \frac{\sin^2 t}{t}\mathrm{d}t &= \int_{[1,+\infty[} \frac{1-\cos(2t)}{2t}\mathrm{d}t\\ &= \underbrace{\left[\frac{2t-\sin(2t)}{4t}\right]_1^{+\infty}}_{\geqslant\ 0} + \underbrace{\int_{[1,+\infty[} \frac{2t-\sin(2t)}{4t^2}\mathrm{d}t}_{=\ +\infty} = +\infty\end{aligned}$$

On ne peut donc pas appliquer le théorème de continuité sous le signe intégrale en 0. Il nous faut ruser. Pour tout $x > 0$, on observe que par intégration par partie,

$$F(x) = \big[-e^{-xt}\underbrace{\int_t^{+\infty}\frac{\sin u}{u}\mathrm{d}u}_{=:\ g(t)}\big]_0^{+\infty} - \int_{\mathbb{R}_+} xe^{-xt}g(t)\mathrm{d}t = \int_0^{+\infty}\frac{\sin t}{t}\mathrm{d}t - x\int_{\mathbb{R}_+} e^{-xt}g(t)\mathrm{d}t$$

Soit maintenant $\varepsilon > 0$. Puisque $\lim\limits_{t\to+\infty} g(t) = 0$, il existe un réel $T > 0$ tel que pour tout $t > T$, $|g(t)| < \varepsilon$. Par conséquent, pour tout $x > 0$,

$$\begin{aligned}|F(x) - F(0)| = \left|x\int_{\mathbb{R}_+} e^{-xt}g(t)\mathrm{d}t\right| &\leqslant x\int_0^T e^{-xt}|g(t)|\mathrm{d}t + x\int_T^{+\infty} e^{-xt}|g(t)|\mathrm{d}t\\ &\leqslant xT\|g\|_{+\infty,[0,T]}\mathrm{d}t + \varepsilon\int_{\mathbb{R}_+} xe^{-xt} \leqslant xT\|g\|_{+\infty,[0,T]} + \varepsilon\end{aligned}$$

En passant à la limite inférieure lorsque $x \to 0$, on obtient donc $\overline{\lim_{x\to 0}}|F(x) - F(0)| \leqslant \varepsilon$ et donc

$$F(x) \underset{x\to 0}{\longrightarrow} F(0).$$

En d'autres termes, $F(0) = \lim_{x\to 0}(\frac{\pi}{2} - \arctan(x)) = \frac{\pi}{2}$.

Questions possibles :

- Pourquoi n'a-t-on pas directement appliqué le théorème de continuité sous l'intégrale en 0 ? (si l'on n'a pas eu le temps de l'expliquer pendant le développement)
- A-t-on d'autres démonstration du calcul de l'intégrale de Dirichlet ? (à la pelle, par les résidus, par Fourier-Plancherel...)
- Calculer $\displaystyle\int_0^{+\infty} \frac{\sin^2 t}{t^2}\mathrm{d}t$.
- Calculer un équivalent de $\displaystyle\int_0^x \left|\frac{\sin t}{t}\right| \mathrm{d}t$ lorsque $x \to +\infty$.

5.11 Inversion de Fourier L^1

Leçons concernées. 235, 239, 250.
Référence. *Cours d'analyse. Théorie des distributions et analyse de Fourier*, Jean-Michel Bony.
Remarques. On utilise dans ce développement la densité de $\mathcal{C}_c^0$ dans L^1, il faut avoir une idée de la démonstration (pas besoin de suites régularisante, ni de convolution).
La démonstration du lemme 54 n'est pas donnée dans le livre de Jean-Michel Bony (il indique seulement d'utiliser la densité des fonction continues à support compact), et celle du lemme 56 n'y est qu'esquissée, mais c'est un grand classique en transformée de Fourier. Il est de toute façon difficile de tout faire en 15 minutes, on peut par exemple admettre le lemme 56.

Lemme 54 (Suite régularisante) Soit $\chi \in \mathrm{L}^1(\mathbb{R})$ telle que $\int \chi = 1$. Pour tout $\varepsilon > 0$, on pose $\chi_\varepsilon := \frac{1}{\varepsilon}\chi(\frac{\cdot}{\varepsilon})$ et, pour $f \in \mathrm{L}^1(\mathbb{R})$, on note $f_\varepsilon := f * \chi_\varepsilon$. Dans L^1, $f_\varepsilon \underset{\varepsilon\to 0}{\longrightarrow} f$.

Preuve. Montrons d'abord le résultat pour $f \in \mathcal{C}_c^0$ (l'ensemble des fonctions continues à support compact). On concluera ensuite sur L^1 tout entier par un argument de densité.
Fixons $\eta > 0$. La fonction f est à support compact et est donc uniformément continue. Dès lors, il existe un réel $\delta > 0$ tel que pour tout $x, y \in \mathbb{R}$, $|x - y| < \delta \implies |f(x) - f(y)| < \eta$. Choisissons $\delta < 1$.
En effectuant le changement de variable $\varepsilon s = t$, on remarque que

$$f * \chi_\varepsilon\,(x) = \int_{\mathbb{R}} f(x-t)\chi(t/\varepsilon)\frac{\mathrm{d}t}{\varepsilon} = \int_{\mathbb{R}} f(x-\varepsilon s)\chi(s)\mathrm{d}s.$$

En se donnant $R > 0$ tel que $\mathrm{supp}(f) \subset [-R, R]$, on obtient alors pour tout $\varepsilon > 0$,

$$\begin{aligned}
\|f_\varepsilon - f\|_{\mathrm{L}^1} = \int_{\mathbb{R}} |f * \chi_\varepsilon\,(x) - f(x)|\,\mathrm{d}x &\leqslant \int_{\mathbb{R}^2} |f(x-\varepsilon s) - f(x)| \cdot |\chi(s)|\mathrm{d}s\mathrm{d}x \\
&\leqslant \int_{\mathbb{R}} |\chi(s)| \left(\int_{\mathbb{R}} |f(x-\varepsilon s) - f(x)|\mathrm{d}x\right)\mathrm{d}s \\
&= \int_{|s|<\frac{\delta}{\varepsilon}} |\chi(s)| \left(\int_{[-R-1,R+1]} |f(x-\varepsilon s) - f(x)|\mathrm{d}x\right)\mathrm{d}s \\
&+ \int_{|s|\geqslant\frac{\delta}{\varepsilon}} |\chi(s)| \left(\int_{\mathbb{R}} |f(x-\varepsilon s) - f(x)|\mathrm{d}x\right)\mathrm{d}s \\
&\leqslant (2R+2)\eta \int_{|s|<\frac{\delta}{\varepsilon}} |\chi(s)|\mathrm{d}s + 2\|f\|_{\mathrm{L}^1} \int_{|s|\geqslant\frac{\delta}{\varepsilon}} |\chi(s)|\mathrm{d}s \\
&\leqslant (2R+2)\eta\|\chi\|_{\mathrm{L}^1} + 2\|f\|_{\mathrm{L}^1} \int_{|s|\geqslant\frac{\delta}{\varepsilon}} |\chi(s)|\mathrm{d}s
\end{aligned}$$

En passant à la limite supérieure lorsque $\varepsilon \to 0$, on obtient

$$\overline{\lim_{\varepsilon\to 0}} \|f_\varepsilon - f\|_{\mathrm{L}^1} \leqslant (2R+2)\eta\|\chi\|_{\mathrm{L}^1},$$

et puisque η était quelconque, on en déduit que $f_\varepsilon \underset{\varepsilon\to 0}{\longrightarrow} f$ dans L^1.

Soit maintenant $f \in \mathrm{L}^1$ quelconque et $\eta > 0$. Par densité de $\mathcal{C}_c^0$ dans L^1, il existe g continue à support compact telle que $\|f-g\|_{\mathrm{L}^1} < \eta$. Dès lors, on obtient par inégalité triangulaire :

$$\begin{aligned}\overline{\lim_{\varepsilon\to 0}} \|f_\varepsilon - f\|_{\mathrm{L}^1} &\leqslant \overline{\lim_{\varepsilon\to 0}} \left(\|f_\varepsilon - g_\varepsilon\|_{\mathrm{L}^1} + \|g_\varepsilon - g\|_{\mathrm{L}^1} + \|g-f\|_{\mathrm{L}^1}\right)\\ &\leqslant \overline{\lim_{\varepsilon\to 0}} \|(f-g)*\chi_\varepsilon\|_{\mathrm{L}^1} + 0 + \eta\\ &\leqslant \overline{\lim_{\varepsilon\to 0}} \left(\|f-g\|_{\mathrm{L}^1}\cdot\|\chi_\varepsilon\|_{\mathrm{L}^1}\right) + \eta \leqslant 2\eta\end{aligned}$$

Puisque η était quelconque, on conclue donc bien au résultat annoncé.

Définition 55 (Transformée de Fourier)
Soit $f \in \mathrm{L}^1$. On appelle transformée de Fourier de f l'application $\hat{f} := \mathcal{F}(f)$ définie par

$$\hat{f}(t) = \int_{\mathbb{R}} f(x)e^{-ixt}\mathrm{d}x.$$

De manière analogue, on définit $\overline{\mathcal{F}}(f)(t) = \int_{\mathbb{R}} f(x)e^{ixt}\mathrm{d}x$.

Lemme 56 (Transformée de Fourier d'une gaussienne) Soit $a > 0$ fixé quelconque. On a

$$\mathcal{F}(e^{-ax^2})(t) = \sqrt{\frac{\pi}{a}}e^{-t^2/4a}.$$

Preuve. Commençons par le démontrer dans le cas où $a = 1$. On a $\mathcal{F}\left(e^{-x^2}\right)(t) = \int_{\mathbb{R}} e^{-x^2}e^{-ixt}\mathrm{d}t$, donc par théorème de dérivation sous l'intégrale, $\mathcal{F}\left(e^{-x^2}\right)$ est de classe $\mathcal{C}^1$ et

$$\mathcal{F}\left(e^{-x^2}\right)'(t) = \int_{\mathbb{R}} -ixe^{-x^2}e^{-ixt}\mathrm{d}t = \underbrace{\left[\frac{i}{2}e^{-x^2}e^{-ixt}\right]_{-\infty}^{+\infty}}_{=0} - \frac{t}{2}\int_{\mathbb{R}} e^{-x^2}e^{-ixt}\mathrm{d}x = -\frac{t}{2}\mathcal{F}(e^{-x^2})(t)$$

Dès lors, $\mathcal{F}\left(e^{-x^2}\right)$ est solution de l'équation différentielle $y' + 2ty = 0$ et donc, puisque $\mathcal{F}\left(e^{-x^2}\right)(0) = \sqrt{\pi}$, on a $\mathcal{F}\left(e^{-ax^2}\right)(t) = \sqrt{\pi}e^{-t^2/4}$.
Si maintenant $a > 0$ est quelconque, on a (par changement de variable linéaire dans la transformée de Fourier)

$$\mathcal{F}\left(e^{-ax^2}\right)(t) = \mathcal{F}\left(e^{-(\sqrt{a}x)^2}\right)(t) = \sqrt{\frac{1}{a}}\mathcal{F}\left(e^{-x^2}\right)(t/\sqrt{a}) = \sqrt{\frac{\pi}{a}}e^{-t^2/4a}.$$

Théorème 57 (Inversion de Fourier dans L^1)
Soit $f \in \mathrm{L}^1$ telle que $\hat{f} \in \mathrm{L}^1$. On a

$$f = \frac{1}{2\pi}\overline{\mathcal{F}}(\hat{f}).$$

Preuve. On peut écrire

$$\overline{\mathcal{F}}(\hat{f})(t) = \int_{\mathbb{R}} e^{itx}\hat{f}(x)\mathrm{d}x = \int_{\mathbb{R}}\int_{\mathbb{R}} e^{i(t-s)x}f(s)\mathrm{d}s\mathrm{d}x.$$

Il semble tout naturel d'appliquer les théorèmes de Fubini pour continuer le calcul, mais cela n'est pas possible puisque la fonction $\big((s,x)\mapsto e^{i(t-s)x}f(s)\big)$ n'est pas intégrable sur $\mathbb{R}^2$. On pose donc, pour tout $\varepsilon > 0$,

$$I_\varepsilon(t) := \frac{1}{2\pi}\int_{R^2} e^{i(t-s)x}e^{-\varepsilon^2x^2/4}f(s)\mathrm{d}s\mathrm{d}x.$$

D'après le théorème de Fubini-Tonelli, la fonction $\Big((s,x)\mapsto e^{i(t-s)x}e^{-\varepsilon^2x^2/4}f(s)\Big)$ est intégrable, par conséquent on peut appliquer le théorème de Fubini-Lebesgue. D'où

$$I_\varepsilon(t) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}e^{-\varepsilon^2x^2/4}\int_{\mathbb{R}} e^{-sx}f(s)\mathrm{d}s\mathrm{d}x = \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}e^{-\varepsilon^2x^2/4}\hat{f}(x)\mathrm{d}x.$$

À ε fixé, on a $|e^{itx}e^{-\varepsilon^2x^2/4}\hat{f}(x)| \leqslant |\hat{f}(x)|$, donc puisque la fonction $\hat{f}$ est supposée intégrable, en appliquant le théorème de convergence dominée, on obtient

$$\lim_{\varepsilon\to 0} I_\varepsilon(t) = \frac{1}{2\pi}\overline{\mathcal{F}}(\hat{f})(t).$$

D'autre part, toujours d'après le théorème de Fubini-Lebesgue,

$$I_\varepsilon(t) = \frac{1}{2\pi}\int_{\mathbb{R}} f(s)\int_{\mathbb{R}} e^{i(t-s)x}e^{-\varepsilon^2x^2/4}\mathrm{d}x\mathrm{d}s = \int_{\mathbb{R}} f(s)G(s-t)\mathrm{d}s = f * G_\varepsilon(t),$$

où l'on pose $G_\varepsilon(s) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{-itx}e^{-\varepsilon^2x^2/4}\mathrm{d}x = \frac{1}{2\pi}\mathcal{F}\left(e^{-\varepsilon^2x^2/4}\right) = \frac{1}{\sqrt{\pi}\varepsilon}e^{-(t/\varepsilon)^2}$.
De sorte que l'on a $\int_{\mathbb{R}} G_1 = 1$ et $G_\varepsilon = \frac{1}{\varepsilon}G_1(\frac{\cdot}{\varepsilon})$. En appliquant le lemme 54, on obtient donc $I_\varepsilon \underset{\varepsilon\to 0}{\to} f$ dans L^1.
D'après le théorème de Riesz-Fischer, on peut extraire une sous-suite de $(I_\varepsilon)_{\varepsilon>0}$ qui converge presque partout vers f lorsque $\varepsilon \to 0$. Or, on a déjà montré que I_ε convergeait simplement vers $\frac{1}{2\pi}\overline{\mathcal{F}}(\hat{f})$. Finalement, par unicité de la limite simple,

$$f = \frac{1}{2\pi}\overline{\mathcal{F}}(\hat{f}).$$

✌

Questions possibles :

- Démontrer le lemme 56.
- Existe-t-il une fonction $e \in \mathrm{L}^1$ qui soit neutre pour le produit de convolution sur L^1 ?
- La transformée de Fourier est-elle injective ?
- Démontrer le lemme de Riemann-Lebesgue.
- Calculer la transformée de Fourier de $x \mapsto \dfrac{1}{1+x^2}$.

5.12 Lemme de Grothendieck

Leçons concernées. 201, 205, 206, 208, 234.
Référence. *Analyse pour l'agrégation de mathématiques, 40 développements*, Julien et Laurent Bernis.
Remarques. Dans la plupart des démonstrations de ce résultat, on utilise le théorème du théorème du graphe fermé plutôt que le théorème d'isomorphisme de Banach (qui sont équivalents), mais ce dernier est ici plus naturel à mon avis. Il faut faire bien attention aux histoires de "μ-presque pour tout x" qui surviennent à l'étape 3 et savoir se justifier face à d'éventuelles questions à ce sujet.
Le rapport du jury cite explicitement ce résultat pour la leçon 206, mais pour bien se convaincre que l'on *utilise* bien la dimension finie (et non pas seulement qu'on l'illustre), on peut souligner le recours à $\mathbb{C}^N$ à l'étape 3 et mettre en avant l'équivalence de deux normes que l'on montre à l'étape 1, qui n'aurait intuitivement pas lieu d'être en dimension infinie.

Théorème 58 (Grothendieck)
Soit $(X, \mathcal{A}, \mu)$ un espace probabilisé et $1 \leqslant p < +\infty$. Tout sous-espace vectoriel V fermé dans $\mathrm{L}^p(\mu)$ et contenu dans $\mathrm{L}^\infty(\mu)$ est de dimension finie.

Preuve.

Étape 1 : Les normes $\|\cdot\|_p$ et $\|\cdot\|_\infty$ sont équivalentes sur V.
Puisque μ est une mesure de probabilité, on dispose de l'injection canonique continue

$$i : (^\infty, \|\cdot\|_\infty) \hookrightarrow (^p, \|\cdot\|_p).$$

En particulier, on sait que $\|\cdot\|_p \leqslant \|\cdot\|_\infty$ sur V.
De plus, V étant fermé dans ^{p}, par continuité de i, $V = i^{-1}(V)$ est fermé dans $^\infty$. Les espaces ^{p} et $^\infty$ étant des espaces de Banach, l'espace V qui est fermé dans ces deux espaces est un Banach pour les normes $\|\cdot\|_p$ et $\|\cdot\|_\infty$.
Par conséquent, d'après le théorème d'isomorphisme de Banach, la bijection linéaire et continue

$$i_V : (V, \|\cdot\|_\infty) \hookrightarrow (V, \|\cdot\|_p)$$

est bicontinue et donc il existe une constante $\alpha > 0$ telle que $\|\cdot\|_\infty \leqslant \alpha\|\cdot\|_p$ sur V.

Étape 2 : La norme $\|\cdot\|_2$ est plus fine que la norme $\|\cdot\|_\infty$ sur V *i.e.* il existe une constante $\beta > 0$ telle que $\|\cdot\|_\infty \leqslant \beta\|\cdot\|_2$ sur V.
Si $p < 2$, d'après l'inégalité de Hölder et puisque μ est une mesure de probabilité, on obtient pour $f \in V$,

$$\|f\|_p = \left(\int_X |f|^p \cdot 1 \mathrm{d}\mu\right)^{\frac{1}{p}} \leqslant \left(\int_X (|f|^p)^{2/p} \mathrm{d}\mu\right)^2 \cdot \left(\int_X 1^{\frac{2p}{2-p}} \mathrm{d}\mu\right)^{\frac{2-p}{2}} = \|f\|_2$$

Dès lors, d'après la première étape, $\|f\|_\infty \leqslant \alpha\|f\|_2$.
Maintenant, si $p \geqslant 2$, pour tout $f \in V$, on peut écrire $|f|^p = |f|^{p-2}|f|^2$. On obtient donc

$$\|f\|_p = \left(\int_X |f|^{p-2} \cdot |f|^2 \mathrm{d}\mu\right)^{\frac{1}{p}} \leqslant \left(\int_X \|f\|_\infty^{p-2} |f|^2 \mathrm{d}\mu\right)^{\frac{1}{p}} = \|f\|_\infty^{\frac{p-2}{p}} \|f\|_2^{\frac{2}{p}}$$

Par conséquent, $\|f\|_\infty \leqslant \alpha\|f\|_\infty^{\frac{p-2}{p}} \|f\|_2^{\frac{2}{p}}$ et donc $\|f\|_\infty \leqslant \alpha^{\frac{p}{2}}\|f\|_2$.
On pose donc $\beta := \max(\alpha, \alpha^{\frac{p}{2}})$.

Étape 3 : Le cardinal d'une famille libre de V est borné par β^2.
Soit $(f_i)_{1 \leqslant i \leqslant N}$ une famille libre de V, avec $N \in \mathbb{N}$. Quitte à lui appliquer le procédé d'orthonormalisation de Gram-Schmidt dans $\mathrm{L}^2(\mu) \supset L^\infty(\mu) \supset V$, on peut supposer que cette famille est ortonormée. Considérons alors l'application

$$T : \begin{cases} \overline{\mathrm{B}_{\mathbb{C}^N}(0,1)} & \longrightarrow V \\ (b_1, \ldots, b_N) & \longmapsto \displaystyle\sum_{i=1}^N b_i f_i \end{cases}$$

Si $\|\cdot\|$ désigne la norme hermitienne canonique sur $\mathbb{C}^N$, l'espace $(\overline{\mathrm{B}_{\mathbb{C}^N}(0,1)}, \|\cdot\|)$ est séparable, et on peut donc s'en donner une suite dense $(b^{(k)})_{k\in\mathbb{N}}$, de sorte que pour tout $k \in \mathbb{N}$,

$$\|T(b^{(k)})\|_\infty \leqslant \beta\|T(b^{(k)})\|_2 = \beta\sqrt{\sum_{i=1}^N (b_i^{(k)})^2} \leqslant \beta.$$

Par conséquent, μ-presque pour tout $x \in X$, pour tout $k \in \mathbb{N}$, $|T(b^{(k)})(x)| \leqslant \beta$. Pour $x \in X$ fixé, l'application $b \mapsto T(b)(x)$ définie sur $\overline{\mathrm{B}_{\mathbb{C}^N}(0,1)}$ étant continue (car linéaire en dimension finie), on peut étendre notre inégalité : μ-presque pour tout $x \in X$,

$$\forall b \in \overline{\mathrm{B}_{\mathbb{C}^N}(0,1)},\ |T(b)(x)| \leqslant \beta.$$

Dans $\overline{\mathrm{B}_{\mathbb{C}^N}(0,1)}$, on définit alors $c_x := 0$ si $(f_1(x),\dots,f_N(x)) = 0$ et $c_x := \dfrac{(\overline{f_1(x)},\dots,\overline{f_N(x)})}{\|(f_1(x),\dots,f_N(x))\|}$ sinon. De sorte que μ-presque pour tout x, si $c_x \neq 0$,

$$\beta \geqslant |T(c_x)(x)| = \frac{1}{\|(f_1(x),\dots,f_N(x))\|}\left|\sum_{i=1}^{N}\overline{f_i(x)}f_i(x)\right| = \sqrt{\sum_{i=1}^{N}|f_i(x)|^2}.$$

Cette même inégalité est trivialement vérifiée si $c_x = 0$. Par conséquent,

$$N = \sum_{i=1}^{N}\int_X |f_i(x)|^2 \mathrm{d}\mu(x) \leqslant \beta^2.$$

Le cardinal de toute famille libre de V est ainsi majoré par β^2, ce qui implique que V est de dimension finie.

Questions possibles :
- En quoi utilise-t-on la dimension finie ?
- Montrer que tout sous-espace vectoriel fermé de $\mathcal{C}^0([0,1])$ inclu dans $\mathcal{C}^1([0,1])$ est de dimension finie. On peut en trouver la preuve à la fin du Bernis[2].
- Clarifier les utilisations des "presque pour tout" à l'étape 3.

5.13 Logarithme et Brouwer

Leçons concernées. 204, 267.
Référence. *131 Développements pour l'oral*, Pierre Le Barbenchon & Co.
Remarques. Dans le développement initial, il est proposé de démontrer également la proposition 60 et le lemme 61, ce qui me semble être un programme un peu trop chargé. La démonstration de la proposition 60 est un classique de la théorie des groupes topologiques (voir par exemple *Nouvelles histoires hédonistes de groupes et de géométries, tome 2*) et s'insère à mon avis bien dans le plan, et le lemme 61 ne présente pas un très grand intérêt.
Ce développement ne se recase pas énormément, mais il a l'avantage de couvrir deux leçons difficiles en terme de développements (surtout la 267) et me paraît intéressant et original.
Il est à noter que la proposition 62 est une joli application du théorème de Heine, que l'on ne doit pas croiser si souvent.
Enfin, il vaut mieux avoir quelques idées sur ce que sont la simple connexité et les retracts, cela permet d'aborder la démonstration du théorème de Brouwer bien plus sereinement.

On a tout d'abord besoin d'un peu de théorie des groupes topolgiques.

Définition 59 (Groupe topologique)
Un groupe topologique est un groupe muni d'une topologie pour laquelle le produit et l'inversion sont continues.

Proposition 60 Soit G un groupe topologique, supposé connexe. Tout sous-groupe H de G tel que l'élément neutre e est intérieur à H ($e \in \overset{\circ}{H}$) est égal à G.

Dans la suite, K désigne un compact étoilé de $\mathbb{R}^d$ par rapport à 0.

Lemme 61 L'ensemble $\mathcal{C}(K,\mathbb{C}^*)$ muni du produit de fonctions et de la topologie de la convergence uniforme sur K est un groupe topologique.

Démarrons maintenant le développement à proprement parler.

Proposition 62 Le groupe $G := \mathcal{C}(K, \mathbb{C}^*)$ est connexe par arcs.

Preuve. Tout d'abord, par connexité par arcs de $\mathbb{C}^*$, toutes les applications constantes peuvent être reliées à la fonction constante égale à 1 (notée 1_G).
Soit maintenant $g \in G$, montrons que g peut être reliée à l'application constante égale à $g(0)$ (et donc à 1_G). Pour cela, on introduit le chemin

$$\gamma : \begin{cases} [0,1] & \longrightarrow G \\ t & \longmapsto (x \mapsto g(tx)) \end{cases},$$

qui est bien défini, puisque K étant étoilé et contenant 0, pour $t \in [0,1]$ et $x \in K$, on a $tx \in K$. On a $\gamma(0) \equiv g(0)$ et $\gamma(1) = g$, donc il nous reste seulement à montrer que γ est continue.
D'après le théorème de Heine, g est uniformément continue sur K. Par conséquent, si on se donne $\varepsilon > 0$, alors il existe $\delta > 0$ tel que pour tous $x, y \in K$, $||x - y|| < \delta \implies |g(x) - g(y)| < \varepsilon$.
Soit donc $t_0 \in [0,1]$ fixé. Fixons $M := \max_{x \in K} ||x||$. Si $t \in [0,1]$ est tel que $|t_0 - t| < \delta / M$, alors pour tout $x \in K$,

$$|\gamma(t_0)(x) - \gamma(t)(x)| = |g(t_0 x) - g(tx)| \leqslant \varepsilon,$$

et donc $||\gamma(t_0) - \gamma(t)||_\infty < \varepsilon$.

✌

Théorème 63 (Existence d'un logarithme)
Pour toute fonction $f \in \mathcal{C}(K, \mathbb{C}^*)$, il existe une fonction $g \in \mathcal{C}(K, \mathbb{C})$ telle que $f = \exp(g)$.

Preuve. Considérons H l'ensemble des éléments de G admettant un logarithme continu (*i.e.* vérifiant les conclusions du théorème). On va montrer que H est un sous-groupe de G et que son intérieur contient 1_G, ce qui conluera la démonstration, par connexité de G.

L'élément neutre appartient à H, car $\exp(0) = 1$.
Si $h_1, h_2 \in H$, alors il existe $g_1, g_2 \in \mathcal{C}(K, \mathbb{C})$ telles que $h_i = \exp(g_i)$ et donc $h_1 \cdot h_2^{-1} = \exp(g_1 - g_2) \in H$, puisque $g_1 - g_2 \in \mathcal{C}(K, \mathbb{C})$.
(Alternative : H est l'image par le morphisme de groupes exp du groupe $(\mathcal{C}(K, \mathbb{C}), +)$.)

Montrons maintenant que $1_G \in \overset{\circ}{H}$. Soit $g \in B_G(1_G, 1/2)$ (la boule ouverte dans G). Soit alors $f := g - 1_G$, de sorte que $f \in \mathcal{C}(K, \mathbb{C})$ et $||f||_\infty < 1/2$. On peut alors définir

$$h : \begin{cases} K & \longrightarrow \mathbb{C} \\ x & \longmapsto \ln(1 + f(x)) \end{cases},$$

où ln désigne la détermination principale du logarithme sur $\mathbb{C} \backslash \mathbb{R}_-$. Ainsi, h est continue et l'on a $g = 1 + f = \exp(h) \in H$. Par conséquent, $B_G(1_G, 1/2) \subset H$ et donc $H = G$.

✌

On démontre l'application suivante, le théorème de Brouwer en dimension 2.

Théorème 64 (Brouwer)
Toute fonction continue de D dans lui-même admet un point fixe, où D désigne le disque unité fermé de $\mathbb{R}^2$.

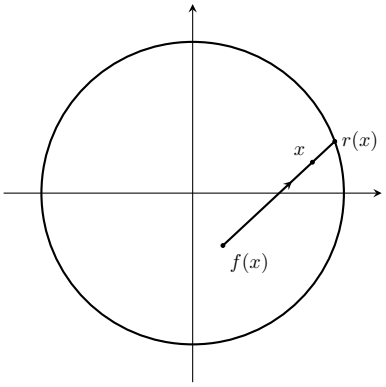


FIGURE 2 – Construction géométrique de $r(x)$.

Preuve. Supposons par l'absurde qu'il existe une application f continue de D dans lui-même sans point fixe. On va utiliser f pour construire une application continue r de D dans lui-même, égale à l'identité sur ∂D.

Pour tout $x \in D$, on a $x - f(x) \neq 0$, donc on peut définir l'application r comme l'unique intersection de ∂D avec la demi-droite ouverte d'origine $f(x)$ et de direction $x - f(x)$. On dispose donc de $t(x) > 0$ tel que $r(x) = f(x) + t(x)(x - f(x))$ et $|r(x)| = 1$. (voir Figure 1)

Notons que par définition, r est égale à l'identité sur ∂D. Montrons donc que l'application $x \mapsto t(x)$ est continue, ce qui assurera la continuité de r. Pour $x \in D$, on cherche donc $t > 0$ tel que :

$$|r(x)| = 1 \ i.e. \ 0 = |x - f(x)|^2 t^2 + 2t\langle f(x), x - f(x)\rangle + |f(x)|^2 - 1 =: P_x(t).$$

Le polynôme P_x est un polynôme de degré 2 en t, de coefficient dominant strictement positif et tel que $P_x(0) = |f(x)|^2 - 1 \leqslant 0$ et $P_x(1) = |x|^2 - 1$. Donc par le théorème des valeurs intermédiaires, P_x admet une racine réelle strictement négative et une racine réelle strictement supérieure à 1. Cette dernière est donc donnée par

$$t(x) = \frac{2\langle f(x), x - f(x)\rangle + \sqrt{\Delta_x}}{2|f(x) - x|^2},$$

où Δ_x désigne le discriminant de P_x, qui est une fonction continue de x. Ainsi, t et donc r est une fonction continue sur D.

En assimilant $\mathbb{R}^2$ à $\mathbb{C}$, la fonction r est donc un élément de $\mathcal{C}(D, \mathbb{C}^*)$ et puisque D est un compact étoilé en 0, il existe $f \in \mathcal{C}(D, \mathbb{C})$ telle que $r = \exp(f)$. Or, comme $|r| = 1$, on a $\mathrm{Re}(f) = 0$ et on peut donc se donner la fonction continue $\varphi := \mathrm{Im}(f) \in \mathcal{C}(D, \mathbb{R})$, de sorte que $r = \exp(i\varphi)$.
La restriction de φ à ∂D est injective, puisque celle de r l'est. Puisque ∂D est un compact, $\varphi_{|\partial D}$ est donc un homéomorphisme de ∂D dans $I := \varphi(\partial D)$. Par ailleurs, ∂D est un compact connexe, donc I est un segment. On dispose donc d'un homéomorphisme entre le cercle unité et un segment, ce qui est absurde (pour le voir, on peut remarque qu'en enlevant un point quelconque du cercle, il reste connexe, ce qui n'est pas le cas pour un segment). Le théorème est donc démontré.

✌

Questions possibles :
- Donner d'autres exemples de groupes topologiques.
- Le théorème de Brouwer est-il vrai en dimension quelconque ? Démontrer-le en dimension 1.

5.14 Marche aléatoire sur le N-gone

Leçons concernées. 155, 261, 262, 264.
Référence. Aucune.
Remarques. Développement tiré de la page de Benjamin Fleuriault. Le seul cas impair est peut-être

un peu court, à moins de bien prendre son temps. Le cas pair peut-être ajouté pour le compléter, même si le résultat obtenu est plus difficile à interpréter. Il vaut mieux l'avoir en tête de toute façon, c'est une question qui peut venir naturellement.

Théorème 65 (Marche aléatoire sur $\mathbb{Z}/N\mathbb{Z}$)
Soit $N \geqslant 3$ un entier impair et $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires à valeurs dans $\mathbb{Z}/N\mathbb{Z}$ telles que

$$X_0 = 0 \text{ p.s.} \quad \text{et} \quad \forall n \in \mathbb{N}, \forall k \in \mathbb{Z}/N\mathbb{Z}, \forall \varepsilon \in \{\pm 1\},\ \mathbb{P}(X_n = k + \varepsilon \mid X_n = k) = \frac{1}{2}.$$

La suite $(X_n)_{n\in\mathbb{N}}$ converge en loi vers la loi uniforme sur $\mathbb{Z}/N\mathbb{Z}$.

Preuve. Considérons pour tout $n \in \mathbb{N}$ le vecteur p_n défini par

$$p_n = \begin{pmatrix} \mathbb{P}(X_n = 0) \\ \vdots \\ \mathbb{P}(X_n = N-1) \end{pmatrix}.$$

D'après la formule des probabilités totales, pour tout $k \in \mathbb{Z}/n\mathbb{Z}$,

$$\mathbb{P}(X_{n+1} = k) = \sum_{j=0}^{N-1} \mathbb{P}(X_{n+1} = k \mid X_n = j)\mathbb{P}(X_n = j) = \frac{1}{2}(\mathbb{P}(X_n = k-1) + \mathbb{P}(X_n = k+1)),$$

donc si l'on note

$$A = \begin{pmatrix} 0 & \frac{1}{2} & 0 & \cdots & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \cdots & 0 & \frac{1}{2} & 0 \end{pmatrix},$$

alors $p_0 = {}^t(1\ 0 \cdots 0)$ et $p_{n+1} = Ap_n$, donc $p_n = A^n p_0$. Autrement dit, la matrice A est la matrice comportant des $\frac{1}{2}$ sur sa sous-diagonale et sa sur-diagonale, ainsi que dans les coins inférieur gauche et supérieur droit et des zéros ailleurs. On peut alors écrire $A = \frac{1}{2}(J + J^{-1})$, avec

$$J = \begin{pmatrix} 0 & 1 & & & (0) \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 1 & & (0) & & 0 \end{pmatrix}.$$

La matrice J est la transposée de la matrice compagnon du polynôme $X^N - 1$, donc $X^N - 1$ est son polynôme minimal. Ainsi, J admet N valeurs propres distinctes, à savoir les ω^k, $k = 0, \ldots, N-1$, avec $\omega = e^{\frac{2i\pi}{N}}$. Cette matrice est donc diagonalisable et donc si Q_k est la matrice de la projection spectrale associée à ω^k, on peut écrire

$$J = \sum_{k=0}^{N-1} \omega^k Q_k.$$

Par conséquent, on obtient que

$$A = \frac{1}{2}(J + J^{-1}) = \frac{1}{2}\sum_{k=0}^{N-1}(\omega^k + \omega^{-k})Q_k = \sum_{k=0}^{N-1} \cos\left(\frac{2k\pi}{N}\right) Q_k.$$

Dès lors, il advient que

$$\forall n \in \mathbb{N}, \quad A^n = \sum_{k=0}^{N-1} \cos\left(\frac{2k\pi}{N}\right)^n Q_k.$$

Puisque N est impair, pour $k \in \{1, \dots, N-1\}$, on a $\frac{2k}{N} \not\equiv 0 \mod \pi$ et donc $|\cos\left(\frac{2k\pi}{N}\right)| < 1$. Par conséquent, on obtient que $\cos\left(\frac{2k\pi}{N}\right)^n \underset{n\to\infty}{\longrightarrow} 0$ et donc

$$A^n \underset{n\to\infty}{\longrightarrow} Q_0,$$

et ainsi,

$$p_n = A^n p_0 \underset{n\to\infty}{\longrightarrow} Q_0 p_0.$$

La matrice A est symétrique réelle, donc d'après le théorème spectral, ses projecteurs spectraux sont orthogonaux. On remarque en outre qu'un vecteur propre de J associé à 1 est le vecteur $\mu = {}^t(1 \cdots 1)$, puisque J est stochastique. Donc l'image de Q_0 est la droite engendrée par μ (les espaces propres de J sont tous des droites) et donc

$$Q_0 p_0 = \frac{\langle \mu, p_0 \rangle}{\langle \mu, \mu \rangle} \mu = \frac{1}{N} \mu$$

Autrement dit,

$$\begin{pmatrix} \mathbb{P}(X_n = 0) \\ \vdots \\ \mathbb{P}(X_n = N-1) \end{pmatrix} \underset{n\to\infty}{\longrightarrow} \begin{pmatrix} \frac{1}{N} \\ \vdots \\ \frac{1}{N} \end{pmatrix},$$

et les variables aléatoires considérées étant discrètes, on a donc bien la convergence en loi de la suite $(X_n)_{n\in\mathbb{N}}$ vers la loi uniforme sur $\mathbb{Z}/N\mathbb{Z}$.

✌

Remarque. On peut se poser la question de ce qu'il advient lorsque N est pair. La démarche est la même, la parité n'est advenue que lors de l'étude de la convergence des $\cos\left(\frac{2k\pi}{N}\right)^n$ en fonction de k. Si l'on écrit $N = 2M$, on a donc toujours que pour $k \in \{0, \dots, N-1\} \backslash \{0, M\}$, $\frac{2k}{N} \not\equiv 0 \mod \pi$ et donc

$$\cos\left(\frac{2k\pi}{N}\right)^n \underset{n\to\infty}{\longrightarrow} 0.$$

Cependant, si $k = M$, on a $\cos\left(\frac{2M\pi}{N}\right) = -1$ et donc

$$p_{2n} = A^{2n} p_0 \underset{n\to\infty}{\longrightarrow} (Q_0 + Q_M) p_0 \quad \text{et} \quad p_{2n+1} = A^{2n+1} p_0 \underset{n\to\infty}{\longrightarrow} (Q_0 - Q_M) p_0.$$

Or, un vecteur propre associé à $\omega^M = -1$ est $\nu = {}^t(1 \ -1 \ \cdots \ 1 \ -1)$, et donc

$$Q_M p_0 = \frac{\langle \nu, p_0 \rangle}{\langle \nu, \nu \rangle} \nu.$$

Donc finalement,

$$p_{2n} \underset{n\to\infty}{\longrightarrow} \frac{1}{N}(\mu + \nu) = \begin{pmatrix} \frac{2}{N} \\ 0 \\ \vdots \\ \frac{2}{N} \\ 0 \end{pmatrix} \quad \text{et} \quad p_{2n+1} \underset{n\to\infty}{\longrightarrow} \frac{1}{N}(\mu - \nu) = \begin{pmatrix} 0 \\ \frac{2}{N} \\ \vdots \\ 0 \\ \frac{2}{N} \end{pmatrix}.$$

Questions possibles :

- Pourquoi peut-on caractériser la convergence en loi ainsi ?
- Calculer les puissances de la matrice J.
- Peut-être des questions sur un téhorème ergodique, mais ça va loin et je n'y connais pas grand chose.

5.15 Marche aléatoire sur $[0,1]$

Leçons concernées. 209, 261, 262, 265, 266.
Référence. *131 développements pour l'oral*, Pierre Le Barbenchon & Cie.
Remarques. Il est à noter que la proposition est une application bien utile du théorème d'approximation de Weierstrass.
Le lemme 68 admet deux preuves différentes, la deuxième est sans doute plus rapide et plus naturelle si on est à l'aise avec.

Considérons une suite $(\xi_n)_{n\in\mathbb{N}}$ de variables aléatoires de même loi de Bernoulli de paramètre $p \in]0,1[$ ainsi qu'une suite $(U_n)_{n\in\mathbb{N}}$ de variables aléatoire de même loi uniforme sur $[0,1]$. On suppose que ces variables sont indépendantes. Soit alors $X_0 \equiv x$ pour un certain $x \in [0,1]$ et

$$\forall n \in \mathbb{N},\ X_{n+1} = U_n X_n + \xi_n(1-U_n).$$

On va chercher à déterminer la loi limite des X_n. Pour cela, nous aurons tout d'abord besoin du lemme suivant.

Proposition 66 Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléaoires à valeurs dans $[0,1]$. Puisque les X_n sont à valeurs dans $[0,1$, ils admettent des moments à tout ordre. On suppose que les moments des X_n convergent vers les moments d'une mesure de probabilité μ sur $[0,1]$. Alors $(X_n)_{n\in\mathbb{N}}$ converge en loi vers μ.

Preuve. On a que pour tout $k \in \mathbb{N}$, $\mathbb{E}[X_n^k] \underset{n\to\infty}{\longrightarrow} \int_0^1 t^k \mathrm{d}\mu(t)$. Par linéarité de l'espérance, on a donc que pour toute fonction polynomiale $g : [0,1] \to \mathbb{R}$,

$$\mathbb{E}[g(X_n)] \underset{n\to\infty}{\longrightarrow} \int_0^1 g(t)\mathrm{d}\mu(t).$$

Soit à présent $f : [0,1] \to \mathbb{R}$ une fonction continue et $\varepsilon > 0$. D'après le théorème d'approximation de Weierstrass, il existe une fonction polynomiale $g_\varepsilon : [0,1] \to \mathbb{R}$ telle que $||g_\varepsilon - \varphi||_\infty \leqslant \varepsilon$. Par conséquent, pour tout $n \in \mathbb{N}$, on a $\mathbb{E}[||g_\varepsilon(X_n) - \varphi(X_n)||_\infty] \leqslant \varepsilon$ et donc par inégalité triangulaire,

$$\left|\mathbb{E}[\varphi(X_n)] - \int_0^1 \varphi(t)\mathrm{d}\mu(t)\right| \leqslant \varepsilon + \left|\mathbb{E}[g_\varepsilon(X_n)] - \int_0^1 \varphi(t)\mathrm{d}\mu(t)\right|.$$

En passant à la limite supérieure, on en déduit donc que $\overline{\lim_{n\to+\infty}} \left|\mathbb{E}[\varphi(X_n)] - \int_0^1 \varphi(t)\mathrm{d}\mu(t)\right| \leqslant \varepsilon$, d'où, puisque ε était quelconque, $\lim_{n\to+\infty} \left|\mathbb{E}[\varphi(X_n)] - \int_0^1 \varphi(t)\mathrm{d}\mu(t)\right| = 0$. On a donc bien la convergence en loi attendue.

✌

On va utiliser cette condition nécessaire de convergence en loi pour démontrer le résultat suivant.

Théorème 67
La suite (X_n) converge en loi vers une loi bêta de paramètres p et $1-p$. Pour rappel, la densité d'une loi bêta de paramètres α et β est donnée par

$$\forall x \in [0,1], f_{\alpha,\beta}(x) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1} = \frac{1}{B(\alpha,\beta)} x^{\alpha-1}(1-x)^{\beta-1},$$

où Γ désigne la fonction gamma et B la fonction bêta.

Preuve. Puisque les X_n sont à valeurs dans $[0,1]$, ils admettent des moments à tout ordre. On note alors pour $n,k\in\mathbb{N}$, $m_{k,n}:=\mathbb{E}[X_n^k]$. En utilisant l'indépendance de U_n et de X_n et en conditionnant par ξ_n, on obtient

$$\begin{aligned} m_{n+1,k}=\mathbb{E}[X_{n+1}^k] &= (1-p)\mathbb{E}[X_{n+1}^k \mid \xi_n=0]+p\mathbb{E}[X_n^k\mid \xi=1]\\ &=(1-p)\mathbb{E}[(U_nX_n)^k]+p\mathbb{E}[(U_nX_n+(1-U_n))^k]\\ &=(1-p)\mathbb{E}[U_n^k]m_{n,k}+p\mathbb{E}[(U_n(X_n-1)+1)^k]\\ &=\frac{1-p}{k+1}m_{n,k}+p\int_0^1\mathbb{E}[(u(X_n-1)+1)^k]\mathrm{d}u \end{aligned}$$

Où la dernière égalité provient du théorème de transfert. En utilisant le théorème de Fubini-Lebesgue, on a

$$\begin{aligned} m_{n+1,k} &= \frac{1-p}{k+1}m_{n,k}+p\mathbb{E}\left[\int_0^1(u(X_n-1)+1)^k\mathrm{d}u\right]\\ &=\frac{1-p}{k+1}m_{n,k}+p\mathbb{E}\left[\mathbb{1}_{X_n<1}\frac{X_n^{k+1}-1}{(k+1)(X_n-1)}+\mathbb{1}_{X_n=1}\right]\\ &=\frac{1-p}{k+1}m_{n,k}+\frac{p}{k+1}\sum_{j=0}^k\mathbb{E}[X_n^j]\\ &=\frac{1-p}{k+1}m_{n,k}+\frac{p}{k+1}\sum_{j=0}^k m_{n,j}=\frac{1}{k+1}m_{n,k}+\frac{p}{k+1}\sum_{j=0}^{k-1}m_{n,j}, \end{aligned}$$

où les dernières égalités proviennent de la linéarité de l'espérance. On va maintenant montrer par récurrence forte sur k que $(m_{n,k})_{n\in\mathbb{N}}$ converge pour tout $k\in\mathbb{N}$. Pour cela, nous aurons besoin du lemme suivant.

> **Lemme 68** Soit $(b_n)_{n\in\mathbb{N}}$ une suite réelle convergente vers $b\in\mathbb{R}$, soit $a\in[0,1]$ et $(u_n)_{n\in\mathbb{N}}$ une suite vérifiant la relation de récurrence $u_{n+1}=au_n+b_n$ pour tout $n\in\mathbb{N}$. La suite (u_n) est convergente de limite $\frac{b}{1-a}$.

Preuve. (du lemme 68) Considérons $\varepsilon>0$. À partir d'un certain rang N, on a $|b_n-b|\leqslant\varepsilon$, donc

$$\forall n\geqslant N,\ au_n+b-\varepsilon\leqslant u_{n+1}\leqslant au_n+b+\varepsilon.$$

Ainsi, si l'on définit les suites arithmético-géométriques $(v_n)_{n\geqslant N}$ et $(w_n)_{n\geqslant N}$ par $v_N=w_N=u_N$ et

$$v_{n+1}=av_n+b-\varepsilon\quad\text{et}\quad w_{n+1}=aw_n+b+\varepsilon,$$

de sorte que pour tout $n\geqslant N$, $v_n\leqslant u_n\leqslant w_n$. Or, $\lim\limits_{n\to+\infty}v_n=\frac{b-\varepsilon}{1-a}$ et $\lim\limits_{n\to+\infty}w_n=\frac{b+\varepsilon}{1-a}$. On en déduit donc que $\frac{b-\varepsilon}{1-a}\leqslant\underline{\lim}\limits_{n\to+\infty}u_n\leqslant\overline{\lim}\limits_{n\to+\infty}u_n\leqslant\frac{b+\varepsilon}{1-a}$. Puisque ε était quelconque, on conclue que $(u_n)_{n\in\mathbb{N}}$ est convergente de limite $\frac{b}{1-a}$.

✌

Preuve. (altrenative du lemme 46) Soit $\ell:=\frac{b}{1-a}$. On a alors $\ell=a\ell+b$ et donc pour tout $k\in\mathbb{N}$,

$$u_{k+1}-\ell=a(u_k-\ell)+b_k-b\underset{k\to+\infty}{=}a(u_k-\ell)+o(1).$$

Dès lors, $a^{-(k+1)}(u_{k+1}-\ell)-a^{-k}(u_k-\ell) \underset{k\to+\infty}{=} o(a^{-k})$. Puisque $a^{-1}>1$, la série de terme général positif a^{-n} diverge et donc par sommation,

$$a^{-n}(u_n-\ell)-(u_0-\ell)=\sum_{k=0}^{n-1}\left(a^{-(k+1)}(u_{k+1}-\ell)-a^{-k}(u_k-\ell)\right) \underset{k\to+\infty}{=} o(\sum_{k=0}^{n-1}a^{-k}) \underset{k\to+\infty}{=} o(a^{-n}).$$

On en déduit donc que $u_n-\ell \underset{k\to+\infty}{=} o(1)$, c'est le résultat voulu.

Nous voilà maintenant armés pour attaquer la récurrence. La propriété est évidente pour $k=0$, puisque $m_{n,0}=1$.
Soit donc $k\geqslant 1$. On suppose que pour tout $0\leqslant j<k$, la suite $(m_{n,j})_{n\in\mathbb{N}}$ converge. Pour tout $n\in\mathbb{N}$, on pose alors $a:=\frac{1}{k+1}$ et $b_n:=\dfrac{p}{k+1}\displaystyle\sum_{j=0}^{k-1}m_{n,j}$, de sorte que

$$\forall n\in\mathbb{N},\ m_{n+1,k}=am_{n,k}+b_n$$

Ainsi, d'après le lemme que l'on vient de montrer, la suite $(m_{n,k})_{n\in\mathbb{N}}$ converge vers une limite m_k, ce qui conclut la récurrence.
De par la relation entre les $m_{n,k}$, on déduit que pour tout $k\in\mathbb{N}$, on a

$$m_k=\frac{1}{k+1}m_k+\frac{p}{k+1}\sum_{j=0}^{k-1}m_j \quad i.e. \quad m_k=\frac{p}{k}\sum_{j=0}^{k-1}m_j=\frac{p}{k}m_{k-1}+\frac{k-1}{k}m_{k-1}=\frac{p+k-1}{k}m_{k-1}.$$

On en déduit donc par récurrence que $m_k=\frac{1}{k!}\prod_{j=0}^{k-1}(p+j)$, puisque $m_0=1$. Comparons-maintenant cela aux moments de la loi bêta pour conclure. Pour tout $k\in\mathbb{N}$, le moment d'ordre k de la loi bêta de paramètres p et $1-p$ est

$$\begin{aligned}\frac{1}{B(p,1-p)}\int_0^1 t^k t^{p-1}(1-t)^{-p} &= \frac{B(k+p,1-p)}{B(p,1-p)}\\ &= \frac{\Gamma(k+p)\Gamma(1-p)}{\Gamma(k+1)}\frac{\Gamma(1)}{\Gamma(p)\Gamma(1-p)}\\ &= \frac{\Gamma(k+p)}{k!\Gamma(p)}=\frac{1}{k!}\prod_{j=0}^{k-1}(p+j)=m_k,\end{aligned}$$

En utilisant la relation fonctionnelle $\Gamma(z+1)=z\Gamma(z)$ et le fait que $\Gamma(n+1)=n!$ pour $n\in\mathbb{N}$. En utilisant la proposition 1, on en conclue donc bien que la suite $(X_n)_{n\in\mathbb{N}}$ converge en loi vers une loi bêta de paramètres p et $1-p$.

Questions possibles :
- Pourquoi la suite $(X_n)_{n\in\mathbb{N}}$ modélise-t-elle une marche aléatoire sur $[0,1]$?
- Pourquoi a-t-on $\mathbb{P}(X_n=1)=0$?
- Quelle est l'allure de la densité limite ? À quoi sert la loi bêta en probabilités ?

5.16 Méthode de Newton

Leçons concernées. 223, 224, 226, 228.
Référence. *Petit guide de calcul différentiel*, François Rouvière.
Remarques. Un développement qui ne vole pas très haut, mais qui bouche bien les trous du couplage.

Théorème 69 (Méthode de Newton)
Soit $f \in \mathcal{C}^2([c,d],\mathbb{R})$ telle que $f(c) < 0 f(d)$ et $f'(x) > 0$ pour tout $x \in [c,d]$. On considère la suite récurrente définie par $x_{n+1} = F(x_n),\ \forall n \in \mathbb{N}$, avec

$$\forall x \in [c,d],\ F(x) = x - \frac{f(x)}{f'(x)}.$$

Alors f admet un zéro unique $a \in]c,d[$ et

i. Il existe $\varepsilon > 0$ tel que our tout $x_0 \in [a-\varepsilon, a+\varepsilon]$, la suite $(x_n)_{n\in\mathbb{N}}$ a une convergence d'ordre deux vers a.

ii. Si de plus on suppose f strictement convexe (*i.e.* $f'' > 0$), pour tout $x_0 \in [a,d]$, $(x_n)_{n\in\mathbb{N}}$ est strictement décroissante ou constante avec

$$(x_{n+1} - a) \underset{n\to+\infty}{\sim} \frac{1}{2}\frac{f''(a)}{f'(a)}(x_n - a)^2.$$

Preuve. La fonction f est continue strictement croissante sur $[c,d]$, et $f(c) < 0 < f(d)$ donc elle s'annule en un unique point $a \in]c,d[$. Puisque $f(a) = 0$, pour tout $x \in [c,d]$ fixé,

$$\begin{aligned} F(x) - a &= x - a - \frac{f(x) - f(a)}{f'(x)} \\ &= \frac{f(a) - f(x) - f'(x)(a-x)}{f'(x)}. \end{aligned}$$

En appliquant la formule de Taylor à l'ordre 2 à f entre a et x, on obtient donc z compris strictement entre a et x tel que

$$F(x) - a = \frac{1}{2}\frac{f''(z)}{f'(x)}(x-a)^2.$$

Donc si l'on pose $C := \frac{\max|f''|}{2\min|f'|}$ (qui est bien définit par compacité de $[c,d]$ et par caractère $\mathcal{C}^2$ de f), on obtient l'inégalité

$$\forall x \in [c,d],\ |F(x) - a| \leqslant C|x-a|^2.$$

Par conséquent, si l'on se donne $\varepsilon > 0$ tel que $C\varepsilon < 1$ et tel que $I := [a-\varepsilon, a+\varepsilon] \subset [c,d]$, on a pour tout $x \in I$, $|F(x) - a| \leqslant C\varepsilon^2 < \varepsilon$ et donc F stabilise l'intervalle I.
Soit maintenant $x_0 \in I$. La suite $(x_n)_{n\in\mathbb{N}}$ est à valeurs dans I et

$$C|x_{n+1} - a| = C|F(x_n) - a| \leqslant (C|x_n - a|)^2 \leqslant \cdots \leqslant (C|x_0 - a|)^{2^{n+1}} \leqslant (C\varepsilon)^{2^{n+1}}.$$

Ceci nous permet de conclure, puisque $C\varepsilon < 1$.

Supposons maintenant que f soit strictement convexe sur $[c,d]$. Montrons que $]a,d]$ est stable par F. Pour $x \geqslant a$, on a $F(x) = x - \frac{f(x)}{f'(x)} \leqslant x$ et $F(x) - a = \frac{1}{2}\frac{f''(z)}{f'(x)}(x-a)^2 \geqslant 0$. Ceci montre bien que $[a,d]$ est stable par F, mais aussi que pour $x_0 \in]a,d]$, on a $a < x_{n+1} = F(x_n) < x_n$ pour tout $n \in \mathbb{N}$.
La suite $(x_n)_{n\in\mathbb{N}}$ est donc strictement décroissante (si $x_0 > a$) ou constante (si $x_0 = a$). Elle admet donc une limite ℓ qui vérifie $F(\ell) = \ell$ *i.e.* $f(\ell) = 0$ et donc $\ell = a$. Par conséquent,

$$\forall n \in \mathbb{N},\ 0 \leqslant x_{n+1} - a \leqslant C(x_n - a)^2.$$

Enfin, si $x_0 > a$, alors $x_n > a$ pour tout $n \in \mathbb{N}$ et pour un certain $a < z_n < x_n$, on a

$$\frac{x_{n+1} - a}{(x_n - a)^2} = \frac{1}{2}\frac{f''(z_n)}{f'(x_n)} \underset{n\to+\infty}{\longrightarrow} \frac{1}{2}\frac{f''(a)}{f'(x_n)}.$$

✌

Proposition 70 (Un exemple) On fixe $y > 0$ et on considère $f : x \mapsto x^2 - y$. La suite $(x_n)_{n\in\mathbb{N}}$ associée à la suite de Newton pour $x_0 > a := \sqrt{y}$ vérifie

$$0 < x_n - a \leqslant 2a\left(\frac{x_0 - a}{2a}\right)^{2^n}.$$

Preuve. Toutes les hypothèses du point ii. du théorème précédent sont vérifiées pour les intervalles $[c, d]$ avec $c^2 < y < d^2$ et $c > 0$. Il s'agit donc d'itérer la fonction $F : x \mapsto x - \frac{x^2-y}{2x} = \frac{1}{2}(x + \frac{y}{x})$. On a

$$F(x) - a = \frac{(x-a)^2}{2x} \quad \text{et} \quad F(x) + a = \frac{(x+a)^2}{2x},$$

d'où $\dfrac{F(x)-a}{F(x)+a} = \left(\dfrac{x-a}{x+a}\right)^2$. Ainsi, en notant $\varphi : x \mapsto \frac{x-a}{x+a}$ et $G : x \mapsto x^2$, on peut écrire $F = \varphi^{-1} \circ G \circ \varphi$. Par conséquent, pour tout $n \in \mathbb{N}$,

$$x_n = (\varphi^{-1} \circ G \circ \varphi)^n(x_0) = \varphi^{-1} \circ G^n \circ \varphi(x_0) \quad i.e. \quad \frac{x_n - a}{x_n + a} = \left(\frac{x_0 - a}{x_0 + a}\right)^{2^n}.$$

Ceci peut se ré-écrire

$$1 + \frac{2a}{x_n - a} = \left(1 + \frac{2a}{x_0 - a}\right)^{2^n} \geqslant 1 + \left(\frac{2a}{x_0 - a}\right)^{2^n} \quad i.e. \quad 0 < x_n - a \leqslant 2a\left(\frac{x_0 - a}{2a}\right)^{2^n}.$$

✌

Questions possibles :
- Connaissez-vous d'autres méthodes de résolution numérique d'équations ? (la méthode de la sécante, par exemple)
- Pourquoi x_{n+1} est l'intersection de la tangente en x_n avec l'axe des abscisses ? Pourquoi a-t-on choisi cette fonction F ? (pour converger vers un point fixe super-attractif)

5.17 Méthode des petits pas

Leçons concernées. 223, 224, 226.
Référence. *Éléments d'analyse réelle*, Jean-Étienne Rombaldi.
Remarques. Ce n'est pas forcément le développement le plus profond qui soit, il faut bien l'avouer.

Théorème 71
Soit f une fonction continue sur $[0, b] \subset \mathbb{R}_+$. On suppose qu'il existe $\alpha, \beta, p > 0$ tel que

$$f(x) \underset{x\to 0}{=} x - \alpha x^{p+1} + \beta x^{2p+1} + o(x^{2p+1}).$$

Alors il existe $\eta > 0$ tel que si $x_0 \in]0, \eta[$, alors la suite $(x_n)_{n\in\mathbb{N}}$ définie par récurrence par

$$\forall n \in \mathbb{N}, \quad x_{n+1} = f(x_n)$$

est bien définie et vérifie

$$x_n \underset{n\to\infty}{=} \frac{1}{(np\alpha)^{\frac{1}{p}}} - \frac{\delta}{\alpha p}\frac{\ln(n)}{(np\alpha)^{1+\frac{1}{p}}} + o\left(\frac{\ln(n)}{(np\alpha)^{1+\frac{1}{p}}}\right),$$

où $\delta = \beta - \frac{(1+p)\alpha}{2}$.

Questions possibles :
- Avez-vous des exemples d'application de ce résultat ? (sin ou $\ln(1+x)$)
- Donner un équivalent à l'infini d'une suite définie par récurrence implicitiement ou explicitement.

5.18 Séries lacunaires sans dérivées

Leçons concernées. 228, 241, 246, 250.
Référence. *Analyse pour l'agrégation*, Hervé Queffélec et Claude Zuily.
Remarques. La définition des suites lacunaires n'est ici que pour rendre le développement compréhensible. Elle est bien entendu à inclure dans le plan, augmentée d'exemples (comme la fonction de Weierstrass).
Dans la suite, on utilise la transformation de Fourier sur l'espace de Schwartz $\mathcal{S}(\mathbb{R})$, dont on ne peut pas parler dans tous les plans concernés par ce développement.

Définition 72 (Suite lacunaire)
Une suite $\Lambda = (\lambda_n)_{n\in\mathbb{N}}$ de réels distincts est dite séparée si pour tout entier n, la distance de λ_n au reste de la suite est non nulle, *i.e* $\mu_n := d(\lambda_n, \Lambda\backslash\{\lambda_n\}) > 0$.
La suite Λ est dite lacunaire si elle est séparée et si $\lim\limits_{n\to+\infty} \mu_n = +\infty$.

Théorème 73 (Une classe de fonctions continues sans dérivées)
Soit $\Lambda = (\lambda_n)_{n\in\mathbb{N}}$ une suite lacunaire de réels, $\sum \varepsilon_n$ une série absolument convergente de complexes et $f : \mathbb{R} \to \mathbb{C}$ la fonction définie par la série normalement convergente

$$\forall t \in \mathbb{R},\ f(t) = \sum_{n=0}^{+\infty} \varepsilon_n e^{i\lambda_n t}$$

Si f est dérivable en au moins un point, alors $\varepsilon_n \underset{n\to+\infty}{=} o(\frac{1}{\mu_n})$.
Par contraposé, si $\sum \frac{1}{\mu_n} < +\infty$ et s'il existe une constante $|\varepsilon_n| > \frac{\delta}{\mu_n}$ pour tout n, alors la fonction f est partout non dérivable.

Preuve. Nous allons utiliser la structure lacunaire de f pour en caractériser les coefficients ε_n grâce au lemme suivant.

Lemme 74 Soit φ une fonction de $\mathcal{S}(\mathbb{R})$ l'espace de Schwartz, de transformée de Fourier $\hat{\varphi} : x \mapsto \int_{\mathbb{R}} \varphi(t)e^{-itx}$x telle que

$$\hat{\varphi}(0) = 1 \quad \text{et} \quad \forall |x| \geqslant 1, \hat{\varphi}(x) = 0.$$

Pour tout entier n, on note $\varphi_n(t) = \mu_n \varphi(\mu_n t)$. On a alors, pour tout entier $n \in \mathbb{N}$,

$$\varepsilon_n = \int_{\mathbb{R}} f(t)e^{-i\lambda_n t}\varphi(t)\text{t} \quad \text{et} \quad |\varepsilon_n| \leqslant \int_{\mathbb{R}} |f(\frac{t}{\mu_n})||\varphi(t)|\text{t}.$$

Preuve. (du lemme 74) Tout d'abord, l'existence d'une telle fonction test φ est assurée, car si ψ est une fonction plateau paire à support dans $[-1, 1]$, avec $\psi(0) = \frac{1}{2\pi}$, on peut considérer $\varphi = \hat{\psi}$. La formule d'inversion de Fourier dans l'espace de Schwartz nous donne, par parité de ψ, $\hat{\varphi} = 2\pi\psi \in \mathcal{S}(\mathbb{R})$.

On remarque alors que pour tout entier n, $\hat{\varphi}_n(x) = \hat{\varphi}(\frac{x}{\mu_n})$. De sorte que

$$\begin{aligned}\int_{\mathbb{R}} \sum_{k=0}^{+\infty} \varepsilon_k e^{i(\lambda_k-\lambda_n)t}\varphi_n(t)\mathrm{t} &= \sum_{k=0}^{+\infty} \int_{\mathbb{R}} \varepsilon_k e^{i(\lambda_k-\lambda_n)t}\varphi_n(t)\mathrm{t} = \sum_{k=0}^{+\infty} \varepsilon_k \hat{\varphi}_n(\lambda_n-\lambda_k) \\ &= \sum_{k=0}^{+\infty} \varepsilon_k \hat{\varphi}(\frac{\lambda_n-\lambda_k}{\mu_n}) = \varepsilon_n \hat{\varphi}(0) = \varepsilon_n.\end{aligned}$$

On conclue au second point du lemme en appliquant l'inégalité triangulaire et un changement de variables.

✌

On commence par traiter le cas où f est dérivable en 0 et on suppose en outre que $f(0) = f'(0) = 0$. Le lemme 74 nous indique que pour tout $n \in \mathbb{N}$,

$$|\mu_n \varepsilon_n| \leqslant \int_{\mathbb{R}} \underbrace{\mu_n |f(\frac{t}{\mu_n})||\varphi(t)|}_{=:g_n(t)} \mathrm{t}$$

La suite de fonctions mesurables $(g_n)_{n\in\mathbb{N}}$ converge simplement vers la fonction $f'(0)\varphi \equiv 0$. On va donc chercher à appliquer le théorème de convergence dominée pour conclure. Par hypothèse sur f et f', au voisinnage de 0, $f(t) = o(t)$. Par conséquent, il existe un réel $\delta > 0$ tel que pour tout $|t| \leqslant \delta, |f(t)| \leqslant |t|$. En outre, si $|t| > \delta$, alors

$$|f(t)| \leqslant \sum_{n=0}^{+\infty} |\varepsilon_n| \leqslant \frac{\sum_{n=0}^{+\infty} |\varepsilon_n|}{\delta} |t|$$

Il existe donc une constante $C > 0$ telle que $|f(t)| \leqslant C|t|$ sur $\mathbb{R}$. Par conséquent, pour tout $n \in \mathbb{N}$ et $t \in \mathbb{R}$,

$$g_n(t) \leqslant C\mu_n |\frac{t}{\mu_n}\varphi(t)| = C|t\varphi(t)| =: h(t)$$

où $h \in L^1(\mathbb{R})$, puisque $\varphi \in \mathcal{S}(\mathbb{R})$. Le théorème de convergence dominée nous donne donc que $\lim\limits_{n\to+\infty} \mu_n \varepsilon_n = 0$.

Dans le cas général, on suppose f dérivable au point t_0. Cherchons des constantes $a, b \in \mathbb{C}$ telles que la fonction g définie par

$$\forall t \in \mathbb{R},\ g(t) = f(t+t_0) - ae^{i\lambda_0 t} - be^{i\lambda_1 t} = \sum_{n=0}^{+\infty} \varepsilon'_n e^{i\lambda_n t},$$

avec $\varepsilon'_n = \varepsilon_n e^{i\lambda_n t_0}$ si $n \geqslant 2$, est nulle et de dérivée nulle au point 0. En évaluant en 0 et en dérivant, on déduit que l'on a

$$\begin{cases} a + b = f(t_0) \\ \lambda_0 a + \lambda_1 b = -if'(t_0) \end{cases}$$

Le déterminant associé à ce système est $\lambda_1 - \lambda_0 \neq 0$ et donc de telles constantes a et b existent. En appliquant le premier cas à une telle fonction g, on conclue donc que $\varepsilon'_n \underset{n\to+\infty}{=} o(\frac{1}{\mu_n})$, et ainsi $\varepsilon_n \underset{n\to+\infty}{=} o(\frac{1}{\mu_n})$.

✌

Questions possibles : (questions que j'ai eues le jour J)

— Comment peut-on construire la fonction ψ ?

— Donner un exemple de fonction continue sans dérivée. Par exemple la fonction de Weierstrass.

5.19 Théorème de Polya par le dénombrement

Leçons concernées. 190, 230, 264, 266.
Référence. *131 Développements pour l'oral* , D. Lesesvre, P. Montagnon, P. Le Barbenchon & T. Pierron.
Remarques. Attention, la première étape de la preuve est assez mal rédigée dans *131 développements*. Il faut sans doute bien réviser les chaînes de Markov pour présenter ce résultat.

Théorème 75 (Théorème de Polya)
Soit $(X_n)_{n\in\mathbb{N}}$ une suite de variables aléatoires modélisant une marche aléatoire sur $\mathbb{Z}^d$ et vérifiant

$$X_0 = 0 \quad \text{et} \quad \forall n \in \mathbb{N}^*,\ X_n = \sum_{k=1}^{n} \xi_k,$$

où les ξ_k sont des variables aléatoires i.i.d de loi uniforme sur $\{\pm e_1, \dots, \pm e_d\}$, où $e_1, \dots, e_d$ désignent les vecteurs de la base canonique de $\mathbb{R}^d$. La suite $(X_n)_{n\in\mathbb{N}}$ est récurrente (i.e. revient en 0 en un temps fini presque sûrement) ssi $d \leqslant 2$.

Questions possibles :
- Pourquoi la transcience/récurrence est-elle caractérisée par la nature de la série des $\mathbb{P}(X_n = 0)$? (il faut bien être au point sur Markov fort, voir par exemple *Chaînes de Markov*, de Carl Graham)
- Démontrer la formule de Stirling ou de Wallis.
- Démontrer la minoration

$$\min\{i!j!k! \mid i, j, k \in \{0, \dots, 3n\}, i + j + k = 3n\} = n!^3.$$

6 Développements abandonnés

6.1 Méthode de relaxation

Leçons concernées. 158, 162, 226.
Référence. *Analyse pour l'agrégation de mathématiques, 40 développements*, Julien et Laurent Bernis.
Remarques.

Définition 76 (Méthode de relaxation)
Soit $A = D - T^+ - T^- \in \mathrm{GL}_d(\mathbb{C})$, où D est une matrice diagonale, et T^+ (resp. T^-) est une matrice strictement triangulaire supérieure (resp. inférieure). Pour $\omega > 0$, on note $M_\omega = \frac{1}{\omega}D - T^-$ et $N_\omega = \frac{1-\omega}{\omega}D + T^+$, de sorte que $A = M_\omega - N_\omega$ et $M_\omega \in \mathrm{GL}_d(\mathbb{C})$.
Soit $b \in \mathbb{C}^d$. Soit $x_0 \in \mathbb{C}^d$ et $(x_n)_{n\in\mathbb{N}}$ la suite définie par la relation $x_{n+1} = M_\omega^{-1}N_\omega x_n + M_\omega^{-1}b$ (on suppose D inversible). On dit que la méthode de relaxation converge si pour toute donnée initiale x_0, la suite $(x_n)_{n\in\mathbb{N}}$ correspondante converge.

Remarque. Dans la définition précédente, si $(x_n)_{n\in\mathbb{N}}$ a pour limite x, alors le vecteur x est la seule solution du système $Ax = b$.

Théorème 77
Soit $A \in \mathcal{M}_d(\mathbb{C})$ une matrice hermitienne définie positive, $\omega > 0$ et $b \in \mathbb{C}^d$. La méthode de relaxation associée converge si et seulement $\omega \in]0, 2[$.

Preuve. Notons tout d'abord que puisque A est hermitienne définie positive, si $e_1, \dots, e_d$ est la base canonique de $\mathbb{C}^d$ comme $\mathbb{C}$-espace vectoriel, on a $a_{ii} = {}^t e_i A e_i = e_i^* A e_i > 0$ et donc D est à coefficients diagonaux stritement positifs (et donc M_ω est bien inversible.) Supposons que $\omega \in]0, 2[$.

La matrice A étant hermitienne définie positive, on peut lui associer une norme hermitienne $\|\cdot\|$ définie par $\|z\| = (z^* A z)^{\frac{1}{2}}$ pour tout $z \in \mathbb{C}^d$. Par abus de notation, notons également $\|\cdot\|$ la norme subordonnée sur $\mathcal{M}_d(\mathbb{C})$ associée. On a

$$\|M_\omega^{-1} N_\omega\| = \|I_n - M_\omega^{-1} A\|.$$

Soit $y \in \mathbb{C}^d$ de norme 1 et $z := M_\omega^{-1} A y$, de sorte que $Ay = M_\omega z$ et $y* = z * M_\omega^* A^{-1}$, d'où

$$\begin{aligned} \|y - z\|^2 &= (y-z)^* A (y-z) \\ &= y^* A y - y^* A z - z^* A y + z^* A z \\ &= 1 - z^* M_\omega^* z - z^* M_\omega z + z^* A z = 1 - z^* (M_\omega^* - N_\omega) z. \end{aligned}$$

Puisque A est hermitienne, on a $(T^-)^* = T^+$ et $D^* = D$, donc

$$M_\omega^* + N_\omega = (\frac{1}{\omega} D - T^-)^* + (\frac{1-\omega}{\omega} D + T^+) = \frac{2-\omega}{\omega} D.$$

Puisque $\frac{2-\omega}{\omega} > 0$ et $y \neq 0$, on a $z \neq 0$, donc

$$\|y - z\|^2 = 1 - \underbrace{\frac{2-\omega}{\omega} z^* D z}_{>0} < 1.$$

Par compacité de la phère unité pour la norme $\|\cdot\|$, on a

$$\|M_\omega^{-1} N_\omega\| = \|I_n - M_\omega^{-1} A\| = \sup_{\|y\|=1} \|y - M_\omega^{-1} A y\| < 1.$$

Or, si x est la solution du système $Ax = b$, on a $x = M_\omega^{-1} M_\omega x = M_\omega^{-1} N_\omega x + M_\omega^{-1} b$. Ainsi, pour tout entier $k \in \mathbb{N}$, $x_{k+1} - x = M_\omega^{-1} N_\omega (x_k - x)$. Par conséquent,

$$\forall k \in \mathbb{N},\ x_{k+1} - x = (M_\omega^{-1} N_\omega)^{k+1} (x_0 - x).$$

On en déduit donc que $\|x_{k+1} - x\| \leqslant \|M_\omega^{-1} N_\omega\|^{k+1} \|x_0 - x\|$, ce qui implique bien la convergence de la méthode de relaxation vers x.

Supposons maintenant que $\omega \geqslant 2$ et trouvons un vecteur initial x_0 faisant diverger la méthode de relaxation.

On a tout d'abord $\det(M_\omega^{-1} N_\omega) = \det(M_\omega^{-1}) \det(N_\omega) = \det(\frac{1}{\omega} D)^{-1} \det(\frac{1-\omega}{\omega} D) = (1-\omega)^n$. Par conséquent, le rayon spectral ρ de $M_\omega^{-1} N_\omega$ est tel que $1 < |1-\omega| = |\det(M_\omega^{-1} N_\omega)|^{\frac{1}{n}} \leqslant \rho$.
Considérons maintenant une valeur propre λ de $M_\omega^{-1} N_\omega$ telle que $|\lambda| = \rho$ et v un vecteur propre associé à λ. Posons $x_0 = x + v_0$, de sorte que

$$\forall n \in \mathbb{N}^\times,\ x_n - x = (M_\omega^{-1} N_\omega)^n \underbrace{(x_0 - x)}_{=\ v} = \lambda^n v.$$

Par conséquent, $\|x_n - x\| = \rho^n \|v\| \underset{n \to +\infty}{\longrightarrow} +\infty$.

6.2 Un anneau principal non-euclidien

Leçons concernées. 122.
Référence. *Cours d'algèbre*, Daniel Perrin.
Remarques. Ce développement ne recase quasiment pas, mais le résultat est très joli et pourrait peut-être ouvrir la discussion sur les anneaux d'entiers et les corps de nombres.

Proposition 78 (Condition nécessaire pour être euclidien) Soit A un anneau euclidien muni du stathme v. Il existe $x \in A$ non inversible tel que la restriction de la projection canonique $A \twoheadrightarrow A/(x)$ à $A^\times \cup \{0\}$ soit surjective. En particulier, $A/(x)$ est un corps.

Preuve. Si A est un corps, $x = 0$ convient. Sinon, on se donne $x \in A$ non-nul et non-inversible tel que $v(x)$ soit minimal. Si $a \in A$, on dispose de $q, r \in A$ tel que $v(r) < v(x)$ et $a = xq + r$. Par conséquent, $a = r \mod x$.
Si $r = 0$, alors $a = 0 \mod x$. Sinon, on a $v(r) < v(x)$ et donc r est inversible.

✌

Proposition 79 L'anneau $A = \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ n'est pas eucldien.

Preuve. On pose $\alpha := \frac{1+i\sqrt{19}}{2}$, qui vérifie $\alpha^2 - \alpha + 5 = 0$. Ainsi,

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

Cet anneau est intègre comme sous-anneau de $\mathbb{C}$ et est stable par conjugaison, puisque $\overline{\alpha} = 1 - \alpha$. Pour $z = a + b\alpha \in A$, on pose donc $N(z) = z\overline{z} = a^2 + ab + 5b^2 \in \mathbb{N}$. De plus, $N(zz') = N(z)N(z')$ et $N(z) > 0$ ssi $z \neq 0$.

Calculons $A^\times$. Si $z = a + b\alpha \in A^\times$, alors $N(zz^{-1}) = 1 = N(z)N(z^{-1})$, si bien que $N(z) = 1$. Par conséquent, $a^2 + ab + 5b^2 = 1$. Or,

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

Ainsi, $1 = N(z) \geqslant 4b^2$. On en déduit que $b = 0$ et donc $a = \pm 1$. D'où $A^\times = \{\pm 1\}$ (il est clair que 1 et -1 sont inversibles).

Supposons par l'absurde que A est euclidien. Il existe $x \in A$ tel que $A/(x)$ est un corps à 2 ou 3 éléments d'après la proposition 79. On a donc un morphisme d'anneaux surjectif $\varphi : A \to k$, avec $k = \mathbb{F}_2$ ou $\mathbb{F}_3$. La restriction de φ à $\mathbb{Z}$ est la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$ et on dispose donc de $\beta := \varphi(\alpha) \in k$ qui vérifie $\beta^2 - \beta + 5 = 0$. Les polynômes $X^2 + X + 1$ et $X^2 - X - 1$ n'ont cependant pas de racines respectivement dans $\mathbb{F}_2$ et $\mathbb{F}_3$.

✌

Proposition 80 L'anneau A est principal.

Preuve. Montrons tout d'abord qu'on dispose d'une pseudo-division euclidienne sur A.

Lemme 81 (pseudo-division euclidienne) Soit $a, b \in A$ non nuls. Il existe $q, r \in A$ vérifiant

$$r = 0 \text{ ou } N(r) < N(b) \quad \text{et} \quad a = bq + r \text{ ou } 2a = bq + r.$$

Preuve. à faire

✌

Tâchons maintenant de montrer que A est principal. Démontrons tout d'abord que l'idéal (2) est maximal dans A, *i.e.* $A/(2)$ est un corps. On remarque que

$$A/(2) \simeq (\mathbb{Z}[X]/(X^2 - X + 5))/(2) \simeq \mathbb{Z}[X]/(2, X^2 - X + 5) \simeq \mathbb{F}_2[X]/(X^2 + X + 1).$$

Le polynôme X^2+X+1 étant irréductible sur $\mathbb{F}_2$, $A/(2)$ est bien un corps.

Soit I un idéal non-nul de A et $a \in I$ non-nul tel que $N(a)$ soit minimale. Supposons par l'absurde que $I \neq (a)$. Dans ce cas, on dispose de $x \in I \backslash (a)$ dont on effectue la pseudo-division euclidienne par a. Si $x = aq + r$, avec $N(r) < N(a)$ ou $r = 0$, alors puisque $r \in I$, on a $r = 0$ et donc $x \in (a)$, impossible. Donc $2a = aq + r$, avec $N(r) < N(a)$ ou $r = 0$. Pour les mêmes raisons, on a $r = 0$ et donc $2x = aq$. L'idéal (2) est maximal et donc premier, ce qui implique que a ou q appartient à (2). Si $q = 2q'$, alors par intégrité, $x = aq'$, impossible. Donc $q \notin (2)$ et $a = 2a'$. D'où $x = a'q \in (a')$. Puisque (2) est maximal et ne contient pas q, on a $(2, q) = A$. Par conséquent, il existe $\lambda, \mu \in A$ tels que

$$2\lambda + q\mu = 1.$$

Dès lors, $a' = a\lambda + x\mu \in I$. Or, $N(a') < N(a)$, puisque $2a' = a$, ce qui est notre contradiction.

✌

6.3 Une suite d'extensions algébriques

Leçons concernées. 151, 125.
Référence. *Algèbre linéaire*, Michel Cognet.
Remarques.

Théorème 82
Soient $a_1, \dots, a_n$ des entiers naturels supérieurs ou égaux à 2 et sans facteur carré. L'extension $K_n := \mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_n}]$ est de degré 2^n. Soit alors

$$G_n := \{X_J \mid J \subset \{1, \dots, n\}$$

Preuve. **Étape 1 :** (une ré-écriture des K_n)

Pour $j \in \{1, \dots, n\}$, notons $x_j := \sqrt{a_j}$ et pour $J \subset \{1, \dots, n\}$, on notera $X_J = \prod_{j \in J} x_j$. On pose alors

$$G_n := \{X_J \mid J \subset \{1, \dots, n\}\}.$$

Montrons que $K_n = \mathrm{Vect}(G_n)$. Il est clair que $\mathrm{Vect}(G_n) \subset K_n$. En outre, pour deux parties I, J de $\{1, \dots, n\}$, on a

$$X_I X_J = \prod_{j \in I \cap J} X_{I \Delta J} \in \mathrm{Vect}(G_n),$$

où $I \Delta J = I \cup J - I \cap J$ désigne la différence symétrique de I et J. Ainsi, $\mathrm{Vect}(G_n)$ est un espace vectoriel stable par produit. C'est donc une algèbre stable par produit contenant $\mathbb{Q}$ et les $x_1, \dots, x_n$, d'où $K_n \subset \mathrm{Vect}(G_n)$.

Étape 2 : (K_1 est de degré 2)

On a $K_1 = \mathbb{Q}[x_1]$ et puisque x_1 est sans facteur carré, son polynôme minimal sur $\mathbb{Q}$ est $X^2 - a_1$, si bien que $[K_1 : \mathbb{Q}] = 2$.

Étape 3 : (K_n est de degré 2^n)

Travaillons par récurrence sur n pour montrer

(H_n) : Pour tout entiers $a_1, \dots, a_n \geqslant 2$ premiers entre eux sans facteurs carrés, $[K_n : \mathbb{Q}] = 2^n$.

L'initialisation a été démontrée à l'étape 1. On se donne donc un entier $n \geqslant 2$ et on suppose que pour tout entier $m \geqslant n$, (H_m) est vérifié. Tâchons de démontrer que (H_{n+1}) l'est aussi.

Tout d'abord, par hypothèse de récurrence, on a

$$[K_{n+1} : \mathbb{Q}] = [K_{n+1} : K_n] \cdot [K_n : \mathbb{Q}] = 2^n [K_{n+1} : K_n].$$

Puisque G_{n+1} possède 2^{n+1} éléments et engendre K_{n+1} sur $\mathbb{Q}$, on sait que $[K_{n+1} : \mathbb{Q}] \leqslant 2^{n+1}$ et par conséquent, $[K_{n+1} : K_n] \in 1, 2$. Supposons par l'absurde que $[K_{n+1} : K_n] = 1$ et donc $K_n = K_{n-1}$.

Par les mêmes arguments et l'hypothèse de récurrence, on sait en revanche que pour tout $m < n$, $[K_{m+1} : K_m] = 2$. En particulier, $[K_n : K_{n-1}] = 2$ et donc $(1, x_n)$ est une base de K_n en tant que K_{n-1}-espace vectoriel.
Or, $x_{n+1} \in K_{n+1} = K_n$, donc il existe des éléments $\alpha, \beta \in K_{n-1}$ tels que $x_{n+1} = \alpha + \beta x_n$. En passant la relation au carré, on obtient

$$\alpha^2 + a_n\beta^2 + 2\alpha\beta x_n = x_{n+1}^2 = a_{n+1} \in \mathbb{Q} \subset K_{n-1}$$

et puisque $(1, x_n)$ forme une base de K_n sur K_{n-1}, on en déduit que $\alpha\beta = 0$.

Supposons que $\alpha = 0$. On a alors $x_{n+1} = \beta x_n$ et donc $x_n x_{n+1} = a_n\beta \in K_{n-1}$. Soit H l'extension $\mathbb{Q}[x_1, \ldots, x_{n-1}, x_n x_{n+1}]$ sur $\mathbb{Q}$. Par hypothèse de récurrence, H est une extension de degré 2^n. Or, $H \subset K_{n-1}$, qui est de degré 2^{n-1}, ce qui est impossible.

Par conséquent, β est nul et donc $x_{n+1} = \alpha \in K_{n-1}$. Soit maintenant H' l'extension $\mathbb{Q}[x_1, \ldots, x_{n-1}, x_{n+1}]$ contenue dans K_{n-1}. Par hypothèse de récurrence, elle est de degré 2^n, ce qui est absurde, puisque K_{n-1} est elle de degré 2^{n-1}.

L'extension K_{n+1} est donc bel et bien de degré 2^{n+1}.

✌

Corollaire 83 Soit $s \geqslant 2$. Le réel $q := \sqrt{1} + \sqrt{2} + \cdots + \sqrt{s}$ est irrationnel.

Preuve. Considérons n le nombre d'entiers naturels premiers compris entre 1 et s et notons $a_1, \ldots, a_n$ ces n entiers premiers.
Le théorème que l'on vient de démontrer nous permet d'affirmer que sous les mêmes notations, K_n est une extension de $\mathbb{Q}$ de degré 2^n. Soit alors G_n la partie génératrice de K_n exhibée à l'étape 1 de la preuve du théorème. Elle est de cardinal 2^n, et c'est donc une $\mathbb{Q}$-base de K_n.
Soit $i \geqslant 2$ qui n'est pas un carré. Soit $J_i \subset \{1, \ldots, n\}$ tel que $\alpha_i := \sqrt{i}/X_{J_i}$ est un entier (il suffit de considérer l'ensemble non vide J_i des indices des facteurs premiers de valuation impaire dans i). Dès lors, si I est le sous-ensemble de $\{1, \ldots, s$ consitué des entiers qui ne sont pas des carrés, il existe un entier α_0 tel que

$$q = \alpha_0 \cdot 1 + \sum_{i \in I} \alpha_i X_{J_i}.$$

Quitte à regrouper les J_i égaux, on obtient donc un ensemble H de parties de $\{1, \ldots, n$ et une famille d'entiers naturels non nuls $(\beta_J)_{J \in H}$ tel que

$$q = \alpha_0 X_\varnothing + \underbrace{\sum_{J \in H} \beta_J X_J}_{\neq\, 0}.$$

Puisque $X_\varnothing \cup H$ est une famille $\mathbb{Q}$-libre, on en déduit donc $q \notin X_\varnothing \mathbb{Q} = \mathbb{Q}$.

✌